Guida Esplicativa al Codice Amministrazione Digitale

Rev 1.0 - 27 novembre 2015

Rosario Cirrito

Segreteria Generale

Regione Siciliana

venerdì 27 novembre 2015

Scenario

Il primo riferimento organico per l'informatica nella P.A. è stato il D.Lgs. N. 39/1993 il cui obiettivo era disciplinare la progettazione, lo sviluppo e la gestione dei sistemi informativi automatizzati delle amministrazioni statali.

Il suddetto decreto chiarisce le finalità d'uso dei sistemi informativi:

- Miglioramento dei servizi
- Trasparenza Amministrativa
- Potenziamento dei supporti per le decisioni pubbliche
- Contenimento dei costi dell'azione amministrativa

nonché I criteri per lo sviluppo dei suddetti sistemi:

- Integrazione e interconnessione
- Rispetto degli standard
- Collegamento con il sistema statistico nazionale

Lo stesso decreto focalizza sull'amministrazione stessa la responsabilità dei progetti di informatizzazione evitando il più possibile il ricorso a fornitori esterni i quali negli anni precedenti, approfittando delle scarse conoscenze informatiche dei dirigenti della P.A.,erano usi a proporre soluzioni non sempre pienamente in linea con le esigenze della stessa offrendo spesso le stesse a prezzi non proprio allineati ai valori di mercato.

Il suddetto Decreto prescrive (art.2) "… *le amministrazioni provvedono di norma con proprio personale alla progettazione, allo sviluppo e alla gestione dei propri sistemi informativi automatizzati*", introduce la **figura del responsabile per i sistemi informativi automatizzati** (art.10) e riserva ai **dirigenti informatici** (art.11) una quota dei dirigenti della dotazione organica.

Gli articoli soprarichiamati sono tuttora vigenti ma non sempre compiutamente applicati.

Il Ruolo Unico della dirigenza ha di fatto cancellato la distinzione tra Dirigente Tecnico e Amministrativo e stroncato sul nascere il riconoscimento di qualsivoglia figura dirigenziale specifica nel settore informatico. Questo è probabilmente uno dei motivi della scarsa qualità generale raggiunta dalla informatizzazione della Amministrazione Regionale.

Con la successiva **legge n.59/97** il legislatore si è prefisso di sburocratizzare I rapporti tra PA e cittadino sostituendo il documento di carta con il **documento elettronico** (art.15 tuttora vigente). Gli aspetti relativi alla **firma** sono affrontati dal **D.P.R. 513/97 che introduce la firma digitale** mentre il successivo **D.P.R n. 428/98 definisce I flussi documentali ed il protocollo informatico**.

Finalmente il **D.P.R. n.445/2000**, procede al "riordino" del settore raccogliendo come **testo unico** tutte le disposizioni legislative e regolamentari in materia di documentazione amministrativa, sia Informatica che cartacea tradizionale, introducendo la importantissima de-certificazione dei medesimi con il **divieto a tutte le amm.zi pubbliche di richiedere la presentazioni di certificati ogni qualvolta sia possibile l'acquisizione d'ufficio** delle relative informazioni. Il D.P.R., tuttora largamente vigente, è la norma di riferimento della **gestione documentale**.

A distanza di 15 anni quanta strada sia tuttora da percorrere è sotto gli occhi di tutti noi.

Il Codice dell'Amministrazione Digitale

Introdotto nel quadro normativo nella formulazione originaria del D.lgs. 82/2005, il **CAD ha segnato un'importante svolta nella vita delle amministrazioni pubbliche e nei rapporti di queste con i cittadini e le imprese**.

Per la prima volta veniva infatti sancito da una legge sia il **diritto dei cittadini di relazionarsi con le amministrazioni pubbliche attraverso le tecnologie telematiche** (ossia attraverso Internet e il computer), sia l'**obbligo per le amministrazioni di attrezzarsi in conseguenza** in modo da rendere effettivamente esigibili i nuovi diritti.

Negli anni successivi divenne evidente che parte delle previsioni allora formulate rimaneva disattesa. La necessità di attribuire maggiore incisività alle prescrizioni normative richiedeva dunque un aggiornamento del quadro regolatorio anche per tenere conto del rapido mutamento tecnologico produttivo dell'ultimo quinquennio, .

Con il D.lgs n. 235/2010, pubblicato sulla Gazzetta Ufficiale del 10 gennaio 2011, n. 6 entra in vigore il nuovo Codice dell'Amministrazione Digitale che, nelle intenzioni del legislatore, deve rappresentare il secondo pilastro su cui si basa il processo di rinnovamento della pubblica amministrazione avviato con l'approvazione del Decreto legislativo n. 150/2009 (la cosiddetta "riforma Brunetta") che ha inteso introdurre nella PA principi di meritocrazia, premialità, trasparenza e responsabilizzazione dei dirigenti.

Il nuovo Codice dell'Amministrazione Digitale costituisce un insieme organico di norme che si pone l'**obiettivo di creare le condizioni giuridiche e organizzative** perché si possa finalmente completare **il passaggio da un'amministrazione basata su carta e sul riconoscimento de visu dei cittadini ad una "amministrazione digitale",** ispirata a modelli operativi e strumenti di comunicazione in grado di sfruttare appieno i vantaggi e le potenzialità offerte dalle nuove tecnologie.

In questo quadro, disporre di **indicazioni chiare sulla validità e sull'efficacia probatoria del documento elettronico** - nonché far riferimento a **specifiche regole tecniche per la formazione, tenuta e conservazione del documento stesso** - rappresentano le condizioni essenziali per rendere effettivo il passaggio dalla carta al digitale.

Il nuovo CAD risponde a queste esigenze di effettività imponendo alle strutture pubbliche alcune regole chiave su come ottemperare alla nuova domanda senza

incertezze e dubbi interpretativi. I capisaldi del nuovo codice sono:

1) esigibilità dei diritti per cittadini e imprese: i cittadini e le imprese hanno diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione pubblica. Quindi per un'amministrazione non è più possibile obbligare i cittadini a recarsi agli sportelli per presentare documenti cartacei, per firmare domande o istanze, per fornire chiarimenti: per tutto questo **deve essere sempre e dovunque disponibile un canale digitale sicuro, certificato e con piena validità giuridica** che permetta di dialogare con la PA dal proprio computer. Il nuovo Codice amplia questo diritto anche verso i gestori di servizi pubblici. Il complesso della riforma della PA permette poi di esigere questo diritto anche mediante l'uso dell'azione collettiva (class action) e introduce l'effettiva disponibilità degli strumenti necessari nella valutazione dei dirigenti e delle organizzazioni.

2) chiarezza, validità giuridica e sicurezza: il CAD dissipa molte incertezze, **chiarisce dubbi di validità e di effettiva valenza probatoria dei documenti informatici**, rassicura gli operatori, indica strumenti concreti e disponibili. Ancora, attraverso una maggiore apertura al mercato, crea le condizioni per un'innovazione diffusa, spinta dalla domanda e sostenuta da un'offerta qualificata e consapevole. Il Codice, inoltre, fa chiarezza sulle molte opportunità che il nuovo assetto regolatorio offre alle PA.

3) valutazione e premialità: i risultati delle PA dovranno essere effettivamente misurati e andranno in parte ad incentivare il personale interessato (secondo le norme del Decreto legislativo n.150/2009), in parte a finanziare nuova innovazione.

Focus su Capo I - PRINCIPI GENERALI

Carlo Mochi Sismondi - Presidente FORUM PA

Alla sua nascita, nel marzo del 2005, il Codice dell'Amministrazione digitale fu salutato da alcuni come una svolta storica nella nostra amministrazione, da altri come un libro di sogni e di principi vaghi che nulla aveva a che fare con la realtà. L'allora Ministro Lucio Stanca annunciava risparmi di 10 miliardi l'anno, Franco Bassanini lamentava che si trattasse di un insieme di utopie e promesse prive di concretezza. In realtà avevano torto e ragione entrambi: i dieci miliardi l'anno purtroppo non si sono visti, ma il Codice è stato uno strumento essenziale per sancire diritti e per dare base giuridica ad una

digitalizzazione ancora troppo vulnerabile.

Sono passati nove anni e sei Governi da allora; un nuovo decreto legislativo, il 235 del 2010, che, sotto l'egida di Renato Brunetta, ha rinnovellato il CAD; successivi e molteplici interventi legislativi, a volte scoordinati tra loro e tesi più a far immediata cassa che a ripensare organicamente la materia. Molto si è fatto, ma ancora molto, troppo resta da fare per una PA che di diventare digitale, interconnessa e interoperabile non vuol proprio saperne, aiutata da una politica di continui stop & go, di priorità incerte ed effimere, di debole governance.

Sono da allora cambiate anche le sensibilità e sempre più lo strumento della digitalizzazione è percepito anche, e a volte soprattutto, come strumento di apertura, di trasparenza, di partecipazione dei cittadini alla vita delle amministrazioni e al loro controllo. Il tema dell'open government si affianca quindi come macro obiettivo a quello dell'efficienza, esaltato dalle necessità di revisione della spesa, e a quello della qualità dei servizi che i cittadini pretendono, sempre più, semplici e veloci.

Dopo un decennio dall'inizio dei lavori per redigere il CAD e dopo vent'anni di riforme a getto continuo, la PA avrebbe ora bisogno di una moratoria normativa e di passare dal tempo delle leggi al tempo dei manuali. Dall'enfasi sulle riforme all'attenzione continua ai comportamenti; dall'illusione che una legge cambi il mondo, alla serena consapevolezza della necessità di cura, di assistenza, di tenacia, di costanza senza arretramenti o scorciatoie, senza deroghe o ritardi.

È questo il tempo esaltato come tempo del cambiamento, ma la PA senza la digitalizzazione non potrà cambiare, rendere questo processo roba da Azzeccagarbugli è deprecabile, ma sperare che si possa compiere senza la certezza del diritto è colpevolmente ingenuo.

CAPO I - PRINCIPI GENERALI

SEZIONE I - DEFINIZIONI, FINALITÀ E AMBITO DI APPLICAZIONE

ART. 1. DEFINIZIONI

1. Ai fini del presente codice si intende per:

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

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

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

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

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

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

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

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

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

*i-bis. **copia informatica di documento analogico**: il documento informatico avente*

contenuto identico a quello del documento analogico da cui è tratto;

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

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

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

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

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

n. ***dato pubblico****: il dato conoscibile da chiunque;*

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

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

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

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

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

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

successivamente modificati;

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

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

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

u. ***gestione informatica dei documenti****: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;*

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

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

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

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

z. ***pubbliche amministrazioni centrali****: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed*

amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

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

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

L'art.1, qui riportato nella versione attualmente in vigore, ha subito parecchie modifiche ed inserimenti rispetto alla versione originale per tener conto delle sopravvenute esigenze tecnologiche dell'ultimo decennio. Le singole definizioni saranno riprese e commentate nel prosieguo delle trattazioni specifiche.

ART. 2. FINALITÀ E AMBITO DI APPLICAZIONE

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

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

[2-bis. Tutte le disposizioni previste dal presente codice per le pubbliche amministrazioni si applicano, ove possibile tecnicamente e a condizione che non si producano nuovi o maggiori oneri per la finanza pubblica ovvero, direttamente o indirettamente, aumenti di costi a carico degli utenti, anche ai soggetti privati preposti all'esercizio di attività

amministrative.]

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

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

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

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

L'ambito di applicazione è quindi **universalmente ampio** e così deve necessariamente essere se si vuole garantire la interoperabilità tra le varie P.A.

ART. 3. DIRITTO ALL'USO DELLE TECNOLOGIE

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

[1-bis. Il principio di cui al comma 1 si applica alle amministrazioni regionali e locali nei limiti delle risorse tecnologiche ed organizzative disponibili e nel rispetto della loro autonomia normativa)]

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

NORME CORRELATE

- D.M. 3 aprile 2013, n. 55, "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244".

FOCUS: ACCESSIBILITÀ E USABILITÀ

a cura di Simonetta Zingarelli

Per le PP.AA. rispettare le norme su accessibilità e usabilità dei siti vuol dire garantire ai propri utenti siti istituzionali a norma in base ai criteri di elevata usabilità e reperibilità, in modo da fornire ai destinatari informazioni complete, chiare e comprensibili. I requisiti devono consentire anche ai disabili di accedere alle informazioni e ai servizi delle PA. Il sito dovrebbe, quindi, essere concepito come accessibile a tutti i cittadini fin dalla sua progettazione.

I principi generali in tema di accessibilità e usabilità sono dettati nel Codice dell'amministrazione digitale (D.Lgs. 82/2005). Altra disposizione primaria di fondamentale importanza è la **L. n. 4/2004**, cosiddetta "Legge Stanca", in cui sono contente regole più specifiche per **consentire l'utilizzo dei servizi telematici delle PA anche da parte delle persone con disabilità**. La definizione di accessibilità contenuta nella suddetta legge stabilisce che i sistemi informatici devono consentire, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire

informazioni fruibili, senza discriminazioni, anche da coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

Il concetto di accessibilità riguarda, quindi, tutti gli aspetti che permettono l'utilizzo di un sito web, tra cui anche software e hardware, architettura di rete, locazione geografica e qualità delle informazioni pubblicate.

Le norme generali sull'accessibilità sono state oggetto di modifica da parte del D.L. 179/2012, convertito in L. 221/2012; nel provvedimento viene posto l'accento sulla necessità di garantire il rispetto dei principi di uguaglianza e di non discriminazione nell'ambito dell'utilizzo delle tecnologie telematiche.

L'intento delle norme in esame è, infatti, quello di ribadire in maniera puntuale l'importanza di questi principi e rendere più chiari gli obblighi delle PPAA in tema di accessibilità anche nel rispetto degli utenti con disabilità.

È quanto emerge, ad esempio, dalla modifica dell'articolo 12 del CAD, il quale prevede che le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzino le tecnologie dell'informazione e della comunicazione per realizzare gli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, anche nel rispetto dei principi di uguaglianza e di non discriminazione, così da garantire a cittadini e imprese il diritto all'uso delle tecnologie.

Tra le novità introdotte dal D.L. 179/2012 di particolare rilevanza è la disposizione che prevede che tutte le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n.165, **pubblichino nel proprio sito web gli obiettivi di accessibilità per l'anno corrente**.

Il suddetto decreto prevede, inoltre, in caso di inadempimento delle regole previste sull'accessibilità dei servizi erogati, la possibilità di effettuare una segnalazione anche in via telematica all'Agenzia per l'Italia digitale. L'Agenzia, nel caso in cui ritenga la segnalazione fondata, richiede l'adeguamento dei servizi assegnati in un termine non superiore a 90 giorni.

Il mancato rispetto delle nuove norme è rilevante ai sensi della valutazione della performance individuale dei dirigenti responsabili e comporta, inoltre, responsabilità dirigenziale e disciplinare ai sensi del D.Lgs. 165/2001.

ART. 3-BIS. DOMICILIO DIGITALE DEL CITTADINO

1. Al fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, ***è facoltà di ogni cittadino*** indicare alla pubblica amministrazione*, secondo le modalità stabilite al comma 3,* ***un proprio indirizzo di posta elettronica certificata****, rilasciato ai sensi dell'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, quale suo domicilio digitale.*

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

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

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

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

all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.

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

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

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

NORME CORRELATE

- D.L. 21 giugno 2013, n. 69, "Disposizioni urgenti per il rilancio dell'economia", convertito con modificazioni dalla L. 9 agosto 2013, n. 98.

FOCUS: DOMICILIO DIGITALE

a cura di Alessandra Cortese

Il domicilio digitale del cittadino, introdotto con l'art. 4 del Decreto Crescita 2.0 (convertito in Legge n.221 del 17 Dicembre 2012), trova già in precedenza un esplicito riconoscimento all'interno del C.A.D.

Col nuovo art. 3-bis, nell'esercizio del diritto all'uso delle nuove tecnologie, viene data facoltà ai cittadini di individuare un proprio indirizzo di posta elettronica certificata cosicché, trasmettendolo alla pubblica amministrazione, assurga a domicilio dal quale inviare e ricevere documenti informatici per via telematica e dialogare in maniera più veloce con le PA. L'indirizzo di PEC deve essere rilasciato ai sensi dell'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 ovvero secondo le modalità previste e specificate dal D.P.C.M. 6 maggio 20094, decreto - quest'ultimo - grazie al quale è stata avviata la

procedura di affido del servizio di comunicazione elettronica certificata tra pubblica amministrazione e cittadino.

Per ragioni di opportunità e chiarezza è utile puntualizzare che la normativa di riferimento ha una portata tutt'altro che innovativa, in quanto si intende riesumare la CEC-PAC che il governo ha "regalato" ai cittadini che ne facessero richiesta.

Al comma 2 art. 3-bis si specifica che l'indirizzo indicato dal cittadino come suo domicilio digitale verrà inserito nell'ANPR (Anagrafe Nazionale della Popolazione Residente) e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi. L'ANPR rappresenta un centro unico di gestione dati che subentra all'Indice Nazionale delle Anagrafi(INA) e all'Anagrafe della popolazione italiana residente all'estero (AIRE)5 ed entro il 31 dicembre 2014 subentrerà anche alle anagraficomunali.

Misure per favorire la diffusione del domicilio digitale e per incentivare l'utilizzo degli strumenti elettronici sono state in ultimo adottate con il decreto legge 69/20136, che modifica l'art.10 del d.l. 70/20117.

La previsione, nel decreto legge 69/2013, della facoltà di richiedere la casella di posta elettronica certificata al rilascio del documento unificato (in cui confluiscono carta di identità elettronica e la tessera sanitaria elettronica), si trasforma - in sede di conversione in legge - in un'assegnazione de iure che obbliga il cittadino a eleggere un domicilio digitale; quest'ultimo - prevede la norma - verrà assegnato secondo le modalità e i criteri previsti dal decreto del Ministero dell'Interno.

Attualmente i primi commi dell'art. 3-bis risultano non particolarmente semplici da applicare, in quanto sarebbe necessario coordinare in modo organico le varie disposizioni con le rispettive modifiche, resta però chiaro l'intento dei commi 4 e ss che precisano che dal 1° gennaio 2013 le PPAA e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato, ciò significa che qualora le comunicazioni, nonostante l'indicazione del domicilio digitale, avvengano anche attraverso i mezzi ordinari, saranno da ritenersi come mai effettuate.

Qualora, diversamente, non venga indicato un domicilio digitale, le PPAA - per comunicare col cittadino - effettueranno una copia analogica sottoscritta con firma autografa del documento informatico sottoscritto con firma digitale o avanzata, inviata

attraverso posta ordinaria o posta raccomandata con avviso di ricevimento.
Per quanto attiene ai profili di conservazione dei documenti è bene fare un rimando diretto alle regole tecniche ex art. 71 CAD disposte dal D.P.C.M. 3 dicembre 2013.

ART. 4. PARTECIPAZIONE AL PROCEDIMENTO AMMINISTRATIVO INFORMATICO

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

ART. 5. EFFETTUAZIONE DEI PAGAMENTI CON MODALITÀ INFORMATICHE

1. I soggetti di cui all'articolo 2, comma 2, e i gestori di pubblici servizi nei rapporti con l'utenza ***sono tenuti a far data dal 1° giugno 2013 ad accettare i pagamenti ad essi spettanti****, a qualsiasi titolo dovuti, anche con l'uso delle tecnologie dell'informazione e della comunicazione. A tal fine:*
a) ***sono tenuti a pubblicare nei propri siti istituzionali e a specificare nelle richieste di pagamento****:*
1) ***i codici IBAN*** *identificativi del conto di pagamento, ovvero dell'imputazione del versamento in Tesoreria, di cui all'articolo 3 del decreto del Ministro dell'economia e delle finanze 9 ottobre 2006, n. 293,* ***tramite i quali i soggetti versanti possono effettuare i pagamenti mediante bonifico bancario o postale, ovvero gli identificativi del conto corrente postale sul quale i soggetti versanti possono effettuare i pagamenti mediante bollettino postale****;*
2) ***i codici identificativi del pagamento da indicare obbligatoriamente per il versamento****;*
b) si avvalgono di prestatori di servizi di pagamento, individuati mediante ricorso agli strumenti di acquisto e negoziazione messi a disposizione da Consip o dalle centrali di committenza regionali di riferimento costituite ai sensi dell'articolo 1, comma 455, della

legge 27 dicembre 2006, n. 296, per ***consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito, prepagate ovvero di altri strumenti di pagamento elettronico disponibili, che consentano anche l'addebito in conto corrente, indicando sempre le condizioni, anche economiche, per il loro utilizzo****. Il prestatore dei servizi di pagamento, che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito, i codici identificativi del pagamento medesimo, nonché i codici IBAN identificativi dell'utenza bancaria ovvero dell'imputazione del versamento in Tesoreria. Le modalità di movimentazione tra le sezioni di Tesoreria e Poste Italiane S.p.A. dei fondi connessi alle operazioni effettuate sui conti correnti postali intestati a pubbliche amministrazioni sono regolate dalla convenzione tra il Ministero dell'economia e delle finanze e Poste Italiane S.p.A. stipulata ai sensi dell'articolo 2, comma 2, del decreto-legge 1° dicembre 1993, n. 487, convertito, con modificazioni, dalla legge 29 gennaio 1994, n. 71.*

2. Per le finalità di cui al comma 1, lettera b), le amministrazioni e i soggetti di cui al comma 1 possono altresì avvalersi dei servizi erogati dalla piattaforma di cui all'articolo 81 comma 2-bis e dei prestatori di servizi di pagamento abilitati.

3. Dalle previsioni di cui alla lettera a) del comma 1 possono essere escluse le operazioni di pagamento per le quali la verifica del buon fine dello stesso debba essere contestuale all'erogazione del servizio; in questi casi devono comunque essere rese disponibili modalità di pagamento di cui alla lettera b) del medesimo comma 1.

3-bis. I micro-pagamenti dovuti a titolo di corrispettivo dalle pubbliche amministrazioni di cui all'articolo 1, comma 450, della legge 27 dicembre 2006, n. 296, come modificato dall'articolo 7, comma 2, del decreto-legge 7 maggio 2012, n. 52, convertito, con modificazioni, dalla legge 6 luglio 2012, n. 94, per I contratti di acquisto di beni e servizi conclusi tramite gli strumenti elettronici di cui al medesimo articolo 1, comma 450, stipulati nelle forme di cui all'articolo 11, comma 13, del codice di cui al decreto legislativo 12 aprile 2006, n. 163, e successive modificazioni, sono effettuati mediante strumenti elettronici di pagamento se richiesto dalle imprese fornitrici.

3-ter. Con decreto del Ministero dell'economia e delle finanze da pubblicare entro il 1°

marzo 2013 sono definiti i micro-pagamenti in relazione al volume complessivo del contratto e sono adeguate alle finalità di cui al comma 3-bis le norme relative alle procedure di pagamento delle pubbliche amministrazioni di cui al citato articolo 1, comma 450, della legge n. 296 del 2006. Le medesime pubbliche amministrazioni provvedono ad adeguare le proprie norme al fine di consentire il pagamento elettronico per gli acquisti di cui al comma 3-bis entro il 1° gennaio 2013.

4. L'Agenzia per l'Italia digitale, sentita la Banca d'Italia, definisce linee guida per la specifica dei codici identificativi del pagamento di cui al comma 1, lettere a) e b) e le modalità attraverso le quali il prestatore dei servizi di pagamento mette a disposizione dell'ente le informazioni relative al pagamento medesimo.

5. Le attività previste dal presente articolo si svolgono con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

NORME CORRELATE

- Determinazione 22 gennaio 2014, n. 8/2014 dell'Agenzia per l'Italia digitale, "Linee Guida per l'effettuazione dei pagamenti in favore della PA e dei gestori di pubblici servizi".

FOCUS: PAGAMENTI IN MODALITÀ ELETTRONICA

a cura di Sarah Ungaro

Con l'obiettivo di promuovere l'utilizzo di sistemi integrati di pagamento telematico e di fatturazione elettronica nelle transazioni - come previsto dall'Agenda digitale europea - che favoriscono una maggiore semplificazione e razionalizzazione, nonché la trasparenza, il monitoraggio e la rendicontazione della spesa pubblica, anche le pubbliche amministrazioni italiane sono in procinto di digitalizzare completamente questi processi, aderendo all'articolato sistema di incassi e pagamenti predisposto per il settore pubblico.

In tale prospettiva, la scelta del legislatore di definire un quadro normativo all'interno del quale si inseriscono le regole, gli standard e le infrastrutture per la gestione dei pagamenti alle PA e per la fatturazione elettronica, coinvolge non solo, ovviamente, le amministrazioni centrali e locali, ma anche I cittadini, le imprese e i prestatori di servizi

di pagamento.

Con particolare riferimento agli strumenti individuati dal legislatore, l'**adozione obbligatoria della fattura elettronica per la fornitura di beni e servizi alle pubbliche amministrazioni è stata introdotta con la Legge numero 244 del 24 dicembre 2007** (all'articolo 1, commi 209-214). Precisamente - a decorrere dal 6 giugno 2014 per per Ministeri, Agenzie fiscali ed enti nazionali di previdenza e dal 31 marzo 2015 per le restanti PPAA (comprese quelle locali, come stabilito dal D.L. 24 aprile 2014, n. 66, ad oggi non ancora convertito in legge) - **le fatture in forma cartacea non potranno più essere accettate da parte della pubblica amministrazione, né in mancanza sarà possibile procedere al relativo pagamento**.

In attuazione di queste disposizioni è stato emanato il Decreto Ministeriale n. 55 del 3 aprile 2013 (cui ha fatto seguito la Circolare interpretativa n. 1 del 31 marzo 2014 del Dipartimento delle Finanze e della Funzione pubblica), che ha reso operativo quanto stabilito dalla Legge 244/2007 in merito all'obbligo di emissione, trasmissione e conservazione in forma elettronica delle fatture nei rapporti con la PA.

In particolare, la trasmissione delle fatture dovrà avvenire attraverso il **Sistema di Interscambio** (SdI), che rappresenterà il punto di incontro tra gli attori interessati dal processo di fatturazione elettronica.

In questo processo di digitalizzazione si inserisce poi un ulteriore tassello, rappresentato dal progetto dei pagamenti elettronici a favore della PA.

A tale scopo, sono state pubblicate in G. U. le Linee guida per l'effettuazione dei pagamenti elettronici a favore delle pubbliche amministrazioni e dei gestori di pubblici servizi.

Il documento è stato predisposto dall'Agenzia per l'Italia Digitale, ai sensi dell'articolo 5, comma 4, del CAD (D.Lgs. 7 marzo 2005, n. 82) e si inserisce in quel trend volto a conseguire una sempre maggiore semplificazione e razionalizzazione del settore pubblico.

Il primo passo verso la completa digitalizzazione dei pagamenti era stato fatto, per quanto riguarda le pubbliche amministrazioni centrali, con la predisposizione del Sistema informatizzato dei pagamenti della PA (SIPA) e, per i pagamenti di scuole ed

enti locali, con l'introduzione dell'Ordinativo Informatico Locale (OIL).

A tal riguardo, con il D.L. n. 179/2012 (convertito in L. 221/12) era stato introdotto l'obbligo per le pubbliche amministrazioni di accettare i pagamenti - a qualsiasi titolo dovuti - anche con l'uso delle tecnologie dell'informazione e della comunicazione, avvalendosi per le attività di incasso e pagamento della piattaforma tecnologica di cui all'articolo 81 del CAD, denominata Nodo dei Pagamenti-SPC, peraltro già attiva dal giugno 2012.

Nello specifico, già l'art. 5 del CAD aveva previsto che le PA e i gestori di pubblici servizi nei rapporti con cittadini e imprese dovessero accettare i pagamenti a essi spettanti anche utilizzando le tecnologie dell'informazione e della comunicazione e dunque attraverso gli idonei strumenti telematici.

Con particolare riferimento agli strumenti per effettuare i pagamenti in modalità elettronica, le Linee guida prevedono:

a) il bonifico bancario o postale ovvero il bollettino postale, ai sensi dell'art. 5, comma 1, lett. A) del CAD (tali pagamenti potranno essere effettuati presso ATM o POS - fisici o virtuali - messi a disposizione dai prestatori di servizi di pagamento, ovvero essere eseguiti autorizzando addebiti diretti da parte dell'utilizzatore finale);

b) i versamenti effettuati con "carte di debito, di credito, prepagate ovvero di altri strumenti di pagamento elettronico disponibili, che consentano anche l'addebito in conto corrente", avvalendosi anche dei prestatori di servizi di pagamento individuati secondo la procedura di cui al comma 1, lettera b) dell'art. 5 del CAD.

ART. 5-bis. COMUNICAZIONI TRA IMPRESE E AMMINISTRAZIONI PUBBLICHE

1. ***La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione****. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese****.*

2. DigitPA, anche avvalendosi degli uffici di cui all'articolo 17, provvede alla verifica dell'attuazione del comma 1 secondo le modalità e i termini indicati nel decreto di cui al comma 2.

3. Il Governo promuove l'intesa con regioni ed enti locali in sede di Conferenza unificata per l'adozione degli indirizzi utili alla realizzazione delle finalità di cui al comma 1.

NORME CORRELATE

- D.P.C.M. 22 luglio 2011, "Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni".

FOCUS: COMUNICAZIONI DIGITALI NELLA PA, TRA PA E TRA PA E CITTADINO

a cura di Andrea Lisi

L'art. 45 del Codice dell'amministrazione digitale costituisce la principale chiave di lettura interpretativa per comprendere come si comunica nella Società dell'Informazione. Secondo tale fondamentale articolo "i documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale". Quindi, per comprendere se una comunicazione possa essere ritenuta rilevante occorre definire e regolamentare gli strumenti idonei a garantire la verifica della provenienza di quell'oggetto informatico inviato. Ovviamente ciò non mette in discussione il fatto che il documento che si invia telematicamente possa essere informatico "nativo" (e quindi debba, dal punto di vista probatorio, seguire le regole contenute negli articoli 20 e 21 del CAD) oppure una copia informatica di documento cartaceo (e segua le regole dell'art. 22 del CAD) o anche una copia informatica (o duplicato informatico) di documento informatico (e quindi segua le regole dell'art. 23bis del CAD).

Per quanto riguarda le comunicazioni amministrative nella fase endoprocedimentale, il legislatore precisa nell'art. 34, comma 2 che "per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71". Tale articolo deve leggersi in combinato disposto con il comma 2 dell'art. 23ter, nel quale il legislatore afferma,

invece, che "i documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile", costringendo l'interprete a misurarsi con una difficile differenziazione dottrinale tra "documenti aventi rilevanza esclusivamente interna" e "documenti costituenti atti amministrativi con rilevanza interna al procedimento".

Per quanto riguarda le comunicazioni tra PA, l'art. 47 del CAD rende obbligatorio l'utilizzo della posta elettronica o della cooperazione applicativa per tutte le comunicazioni di documenti tra pubbliche amministrazioni, precisando però che ai fini dell'avvio del procedimento amministrativo tali 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, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. Viene in ogni caso esclusa per tali finalità la trasmissione di documenti a mezzo telefax.

Per quanto riguarda le **istanze e le dichiarazioni da presentare per via telematica alle pubbliche amministrazioni**, interviene l'art. 65 del CAD, il quale specifica che **esse sono valide, ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, solo se**:

vengono sottoscritte con firma digitale o firma elettronica qualificata, oppure l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi (o con qualsiasi diverso strumento di identificazione valido ai sensi dell'art. 64 del CAD coma 2) **oppure, ancora, se trasmesse dall'autore con PEC identificativa**. **In tutti questi casi, le istanze e le dichiarazioni inviate o compilate su sito sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento**. Ovviamente l'art. 65 fa anche riferimento all'invio telematico di documenti informatici. Per l'invio telematico di documenti originariamente analogici (e quindi di copia per immagine degli stessi) gli strumenti dell'art. 65 del CAD vanno

misurati e coordinati con quanto comunque stabilito dal già richiamato art. 38 del T.U.D.A. (DPR 445/2000), il quale in particolare prevede che "tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica". In particolare, "le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo. Le istanze e la copia fotostatica del documento di identità possono essere inviate per via telematica".
È indispensabile che il delicato coordinamento tra questi articoli sia specificamente regolamentato nel Manuale di gestione documentale dell'ente e nel Regolamento PEC.

ART. 6. UTILIZZO DELLA POSTA ELETTRONICA CERTIFICATA

*1. **Per le comunicazioni** di cui all'articolo 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, **le pubbliche amministrazioni utilizzano la posta elettronica certificata**. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano.*

1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali.

[2. Le disposizioni di cui al comma 1 si applicano anche alle pubbliche amministrazioni regionali e locali salvo che non sia diversamente stabilito.]

[2-bis. Le pubbliche amministrazioni regionali e locali hanno facoltà di assegnare ai cittadini residenti caselle di posta elettronica certificata atte alla trasmissione di documentazione ufficiale.]

NORME CORRELATE

- DPCM 6 maggio 2009, "Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini", (c.d. CEC-PAC).

ART. 6-bis INDICE NAZIONALE DEGLI INDIRIZZI PEC DELLE IMPRESE E DEI PROFESSIONISTI

*1. **Al fine di favorire la presentazione di istanze, dichiarazioni e dati**, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, **è istituito**, entro sei mesi dalla data di entrata in vigore della presente disposizione e con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, **il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti**, presso il Ministero per lo sviluppo economico.*

*2. **L'accesso all'INI-PEC è consentito** alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini **tramite sito web e senza necessità di autenticazione**. L'indice è realizzato in formato aperto, secondo la definizione di cui all'articolo 68, comma 3.*

3. Il Ministero per lo sviluppo economico, al fine del contenimento dei costi e dell'utilizzo razionale delle risorse, sentita l'Agenzia per l'Italia digitale, si avvale per la realizzazione e gestione operativa dell'Indice nazionale di cui al comma 1 delle strutture informatiche delle Camere di commercio deputate alla gestione del registro imprese e ne definisce con proprio decreto, da emanare entro 60 giorni dalla data di entrata in vigore della presente disposizione, le modalità di accesso e di aggiornamento.

4. Nel decreto di cui al comma 4 sono anche definite le modalità e le forme con cui gli ordini e i collegi professionali comunicano all'Indice nazionale di cui al comma 1 tutti gli indirizzi PEC relativi ai professionisti di propria competenza e sono previsti gli strumenti telematici resi disponibili dalle Camere di commercio per il tramite delle proprie strutture informatiche al fine di ottimizzare la raccolta e aggiornamento dei medesimi indirizzi.

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

NORME CORRELATE

- D.L. 29 novembre 2008, n.185, "Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale", convertito con modificazioni dalla legge 28 gennaio 2009, n.2. - D.L. 18 ottobre 2012, n. 179, "Ulteriori misure urgenti per la crescita del Paese", convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 - D.M. 19 marzo 2013, "Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti (INI-PEC)".

ART. 7. QUALITÀ DEI SERVIZI RESI E SODDISFAZIONE DELL'UTENZA

1. Le pubbliche amministrazioni provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti.

2. ***Entro il 31 maggio di ciascun anno le pubbliche amministrazioni centrali trasmettono*** *al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie* ***una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza.***

ART. 8. ALFABETIZZAZIONE INFORMATICA DEI CITTADINI

1. Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni.

ART. 9. PARTECIPAZIONE DEMOCRATICA ELETTRONICA

1. Le pubbliche amministrazioni favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi.

FOCUS: PARTECIPAZIONE DEMOCRATICA ELETTRONICA

a cura di Nina Preite

La Pubblica Amministrazione inizia ad aprire le sue porte a una comunicazione interattiva, prevedendo molti spazi di ricezione. È proprio qui che si incontra il beneficio del canale web nella comunicazione istituzionale, ovvero la possibilità di avvalersi di un canale interattivo "a due vie" e quindi particolarmente adatto a un'amministrazione attenta ai bisogni degli utenti e in costante dialogo con i cittadini. Il rapporto con i cittadini deve essere gestito, nella comunicazione, non solo seguendo i principi di trasparenza, usabilità e accessibilità, ma è importante anche creare nel messaggio una certa identità riconoscibile.

Anche il diffondersi del concetto di e-Government ha sviluppato un nuovo modo di pensare al front-office, che porta all'esplorazione di modalità di collegamento tra PA e cittadini basate sulle nuove tecnologie. La manifestazione più tangibile di questo fenomeno è nella rapida diffusione di siti web, la cui utilità non è percettibile se essi non sono collegati a una reingegnerizzazione dell'intera attività di back office.

Nell'ultimo ventennio si sono succedute una serie di norme che hanno dettato numerose disposizioni in materia di obblighi di pubblicazione sui siti web istituzionali, portando le PPAA a un adeguamento costante delle informazioni pubblicate. Dalla L. 241/90 fino al D.lgs 165/01, si distinguono i principi di efficienza (rapporto tra risultati ottenuti e risorse utilizzate), efficacia (rapporto tra risultati e obiettivi), controllo di gestione e analisi costi-benefici. La presenza della PA in Rete attraverso il sito istituzionale presuppone la progettazione di un sito Internet che deve seguire criteri che garantiscano l'accessibilità per tutte le tipologie di utenti, anche per quelli con disabilità. Il mancato rispetto delle regole di usabilità, crea una vera e propria barriera alla possibilità di usufruire delle informazioni o dei servizi on-line.

La presenza in Rete delle PA è necessaria al completamento del concetto di e-Government. Le possibilità offerte dalla rete sono infinite: dal più banale e inizialmente più gettonato sito vetrina, agli sportelli virtuali che possono essere, al pari degli sportelli fisici, fonte di erogazione di servizi al cittadino, dal sito web al portale istituzionale, da punti di erogazione informatizzati a punti di erogazione appoggiati a reti telematiche di terze parti. Nel progetto di definizione e di realizzazione di un sito web o di un portale, la

Pubblica amministrazione prima di pensare ai contenuti, più o meno ovvi, deve trovare modalità adeguate di contatto con il cittadino. Il prodotto dovrà essere usabile e accessibile.Il controllo diffuso da parte dei cittadini sulla legittimità dell'azione amministrativa è il carattere essenziale della trasparenza pubblica e si auspica possa essere un modo per rafforzare la democrazia. Infatti se una PA è costretta a comportamenti legittimi, attiva un circolo virtuoso utile non solo ai cittadini. Questo dovrebbe favorire la responsabilità delle istituzioni e dei loro decisori poiché il cittadino può farsi un giudizio sul loro operato e dunque essi sono chiamati a rispondere delle proprie scelte. La trasparenza pubblica assurge a strumento indispensabile per assicurare i diritti di partecipazione spettanti al cittadino in quanto titolare della sovranità, anche nei confronti delle istituzioni pubbliche che esercitano i poteri loro attribuiti dalla legge ai fini del perseguimento di finalità di interesse generale.Il principio di trasparenza dell'attività amministrativa entra nel nostro ordinamento con la legge n. 241 del 1990 che contribuisce a costruire la trasparenza sia come valore culturale e patrimonio condiviso dall'amministrazione sia come modalità organizzativa da preferire nello svolgimento della funzione pubblica.

Oggi, invece, alla luce del D.Lgs. 33/2013 (c.d. Decreto Trasparenza), la trasparenza è intesa come "accessibilità totale" e tutti i cittadini hanno il diritto di avere dati chiari, leggibili e in formato aperto su come viene gestita la "cosa pubblica".

In particolare, la pubblicazione dei dati sui siti istituzionali deve avvenire ai sensi dell'art. 68 del Codice dell'amministrazione digitale.

Il cittadino diventa, quindi, attore principale e, attraverso il sito web istituzionale, esercita forme di controllo diffuso sull'agire amministrativo, verificando che i servizi erogati siano di qualità, efficaci ed efficienti, nel rispetto di quanto previsto dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005).

ART. 10. SPORTELLO UNICO PER LE ATTIVITÀ PRODUTTIVE

1. Lo sportello unico per le attività produttive di cui all'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, eroga i propri servizi verso l'utenza in via telematica.

[2. Gli sportelli unici consentono l'invio di istanze, dichiarazioni, documenti e ogni altro

atto trasmesso dall'utente in via telematica e sono integrati con i servizi erogati in rete dalle pubbliche amministrazioni.]

[3. Al fine di promuovere la massima efficacia ed efficienza dello sportello unico, anche attraverso l'adozione di modalità omogenee di relazione con gli utenti nell'intero territorio nazionale, lo Stato, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, individua uno o più modelli tecnico-organizzativi di riferimento, tenendo presenti le migliori esperienze realizzate che garantiscano l'interoperabilità delle soluzioni individuate.]

4. Lo Stato realizza, nell'ambito di quanto previsto dal sistema pubblico di connettività di cui al presente decreto, un sistema informatizzato per le imprese relativo ai procedimenti di competenza delle amministrazioni centrali anche ai fini di quanto previsto all'articolo 11.

NORME CORRELATE

- D.P.R. n. 160/2010, "Modalità telematiche di comunicazione e trasferimento dei dati tra il SUAP e I soggetti coinvolti nel procedimento".

ART. 11. REGISTRO INFORMATICO DEGLI ADEMPIMENTI AMMINISTRATIVI PER LE IMPRESE

1. Presso il Ministero delle attività produttive, che si avvale a questo scopo del sistema informativo delle camere di commercio, industria, artigianato e agricoltura, è istituito il Registro informatico degli adempimenti amministrativi per le imprese, di seguito denominato «Registro», il quale contiene l'elenco completo degli adempimenti amministrativi previsti dalle pubbliche amministrazioni per l'avvio e l'esercizio delle attività di impresa, nonché i dati raccolti dalle amministrazioni comunali negli archivi informatici di cui all'articolo 24, comma 2, del decreto legislativo 31 marzo 1998, n. 112. Il Registro, che si articola su base regionale con apposite sezioni del sito informatico, fornisce, ove possibile, il supporto necessario a compilare in via elettronica la relativa modulistica

2. É fatto obbligo alle amministrazioni pubbliche, nonché ai concessionari di lavori e ai concessionari e gestori di servizi pubblici, di trasmettere in via informatica al Ministero

delle attività produttive l'elenco degli adempimenti amministrativi necessari per l'avvio e l'esercizio dell'attività di impresa.

3. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro delle attività produttive e del Ministro delegato per l'innovazione e le tecnologie, sono stabilite le modalità di coordinamento, di attuazione e di accesso al Registro, nonché di connessione informatica tra le diverse sezioni del sito.

4. Il Registro è pubblicato su uno o più siti telematici, individuati con decreto del Ministro delle attività produttive.

5. Del Registro possono avvalersi le autonomie locali, qualora non provvedano in proprio, per i servizi pubblici da loro gestiti.

6. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 2, della legge 29 luglio 2003, n. 229.

NORME CORRELATE

- D.P.C.M. 3 aprile 2006, n. 200, "Regolamento recante modalità di coordinamento, attuazione ed
accesso al Registro informatico degli adempimenti amministrativi".

Sezione III - Organizzazione delle pubbliche amministrazioni Rapporti fra Stato,Regioni e autonomie locali

Art. 12. Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa

1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività ***utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per la garanzia dei diritti dei cittadini e delle imprese*** *di cui al capo I, sezione II, del presente decreto.*

1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n. 150, dettano disposizioni per l'attuazione delle disposizioni del presente decreto.

1-ter. ***I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto*** *ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilita' penali, civili e contabili previste dalle norme vigenti.* ***L'attuazione delle disposizioni del presente decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.***

2. Le pubbliche amministrazioni ***adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati****, con misure informatiche, tecnologiche, e procedurali di sicurezza,* ***secondo le regole tecniche di cui all'articolo 71.***

3. Le pubbliche amministrazioni ***operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici****, ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni, da esse erogati,*

qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.

4. ***Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati****.*

5. ***Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonche*****'** ***l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71****.*

5-bis. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione attraverso le tecnologie dell'informazione e della comunicazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

Art. 13. Formazione informatica dei dipendenti pubblici

1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'ambito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive, ai sensi dell'articolo 8 della legge 9 gennaio 2004, n. 4.

Art. 14. Rapporti tra Stato, Regioni e autonomie locali

1. In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilita' dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.

2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e

adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all'articolo 71.

2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali.

2-ter. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese.

3. Lo Stato, ai fini di quanto previsto ai commi 1 e 2, istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.

3-bis. Ai fini di quanto previsto ai commi 1, 2 e 3, è istituita senza nuovi o maggiori oneri per la finanza pubblica, presso la Conferenza unificata, previa delibera della medesima che ne definisce la composizione e le specifiche competenze, una Commissione permanente

per l'innovazione tecnologica nelle regioni e negli enti locali con funzioni istruttorie e consultive.

Art. 15. Digitalizzazione e riorganizzazione

1. La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12, comma 1, avviene anche attraverso il migliore e piu' esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.

2. In attuazione del comma 1, ***le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attivita' gestionali, I documenti, la modulistica, le modalita' di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese,*** *assicurando che*

l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformita' alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71.

2-bis. Le pubbliche amministrazioni nella valutazione dei progetti di investimento in materia di innovazione tecnologica tengono conto degli effettivi risparmi derivanti dalla razionalizzazione di cui al comma 2, nonche' dei costi e delle economie che ne derivano.

2-ter. Le pubbliche amministrazioni, quantificano annualmente, ai sensi dell'articolo 27, del decreto legislativo 27 ottobre 2009, n.150, i risparmi effettivamente conseguiti in attuazione delle disposizioni di cui ai commi 1 e 2. Tali risparmi sono utilizzati, per due terzi secondo quanto previsto dall'articolo 27, comma 1, del citato decreto legislativo n.150 del 2009 e in misura pari ad un terzo per il finanziamento di ulteriori progetti di innovazione.

3. ***La digitalizzazione dell'azione amministrativa e' attuata dalle pubbliche amministrazioni con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea****.*

3-bis. Le funzioni legate alle tecnologie dell'informazione e della comunicazione, di seguito denominate «funzioni ICT», nei comuni sono obbligatoriamente ed esclusivamente esercitate in forma associata, secondo le forme previste dal testo unico di cui al decreto legislativo 18 agosto 2000, n. 267, da parte dei comuni con popolazione fino a 5.000 abitanti, esclusi i comuni il cui territorio coincide integralmente con quello di una o più isole e il comune di Campione d'Italia.

3-ter. Le funzioni ICT di cui al comma 3-bis comprendono la realizzazione e la gestione di infrastrutture tecnologiche, rete dati, fonia, apparati, di banche dati, di applicativi software, l'approvvigionamento di licenze per il software, la formazione informatica e la consulenza nel settore dell'informatica.

3-quater. La medesima funzione ICT non può essere svolta da più di una forma associativa.

3-quinquies. Il limite demografico minimo che l'insieme dei comuni, che sono tenuti ad esercitare le funzioni ICT in forma associata, deve raggiungere è fissato in 30.000 abitanti, salvo quanto disposto dal comma 3-sexies.

3-sexies. Entro due mesi dalla data di entrata in vigore della presente disposizione, nelle materie di cui all'articolo 117, commi terzo e quarto, della Costituzione, la regione individua con propria legge, previa concertazione con i comuni interessati nell'ambito del Consiglio delle autonomie locali, la dimensione territoriale ottimale e omogenea per area geografica per lo svolgimento, in forma obbligatoriamente associata da parte dei comuni con dimensione territoriale inferiore ai 5.000 abitanti, delle funzioni di cui al comma 3-ter, secondo i principi di economicità, di efficienza e di riduzione delle spese, fermo restando quanto stabilito dal comma 3-bis del presente articolo.

3-septies. A partire dalla data fissata dal decreto di cui al comma 3-octies, I comuni non possono singolarmente assumere obbligazioni inerenti alle funzioni e ai servizi di cui ai commi 3-bis e 3-ter. Per tale scopo, all'interno della gestione associata, i comuni individuano un'unica stazione appaltante.

3-octies. Le funzioni di cui al comma 3-bis e i relativi tempi di attuazione sono definiti con decreto del Ministro per la pubblica amministrazione e la semplificazione, previa intesa in sede di Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e successive modificazioni, da emanare entro sei mesi dalla data di entrata in vigore della presente disposizione." sono stati aggiunti dall'art. 47 ter, D.L. 9 febbraio 2012, n. 5, convertito con L. 4 aprile 2012, n. 35 e successivamente abrogati dall'art. 19, D.L. 6 luglio 2012, n. 95, convertito con L. 7 agosto 2012, n. 135.

Art. 16. Competenze del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie

1. Per il perseguimento dei fini di cui al presente codice, il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie, nell'attivita' di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle pubbliche amministrazioni centrali per lo sviluppo dei sistemi informativi:

a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni centrali, e ne verifica l'attuazione;

b) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto

utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni centrali;

c) sostiene progetti di grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale, con particolare attenzione per i progetti di carattere intersettoriale;

d) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie;

e) detta norme tecniche ai sensi dell'articolo, 71 e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle pubbliche amministrazioni centrali e delle loro interconnessioni, nonche' della loro qualita' e relativi aspetti organizzativi e della loro sicurezza.

2. Il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie riferisce annualmente al Parlamento sullo stato di attuazione del presente codice.

Art. 17. Strutture per l'organizzazione, l'innovazione e le tecnologie

1. Le pubbliche amministrazioni centrali garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo. A tale fine, le predette amministrazioni individuano un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, responsabile del coordinamento funzionale. Al predetto ufficio afferiscono i compiti relativi a:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia (2), in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi, di telecomunicazioni e fonia, dell'amministrazione;

c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettivita', nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilita' anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

e) analisi della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle

tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualita' dei servizi nonche' di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una piu' efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico, e delle norme in materia di accessibilita' e fruibilita'.

1-bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facolta' di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi.

1-ter. DigitPA assicura il coordinamento delle iniziative di cui al comma 1, lettera c), con le modalita' di cui all'articolo 51.

Art. 18. Conferenza permanente per l'innovazione tecnologica

1. E' istituita la Conferenza permanente per l'innovazione tecnologica con funzioni di consulenza al Presidente del Consiglio dei Ministri, o al Ministro delegato per l'innovazione e le tecnologie, in materia di sviluppo ed attuazione dell'innovazione tecnologica nelle amministrazioni dello Stato.

2. La Conferenza permanente per l'innovazione tecnologica è presieduta da un rappresentante della Presidenza del Consiglio dei Ministri designato dal Presidente del

Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; ne fanno parte il Presidente del DigitPA, i componenti di DigitPA, il Capo del Dipartimento per l'innovazione e le tecnologie, nonché i responsabili delle funzioni di cui all'articolo 17.

3. La Conferenza permanente per l'innovazione tecnologica si riunisce con cadenza almeno semestrale per la verifica dello stato di attuazione dei programmi in materia di innovazione tecnologica e del piano triennale di cui all'articolo 9 del decreto legislativo 12 febbraio 1993, n. 39.

4. Il Presidente del Consiglio dei Ministri, o il Ministro delegato per l'innovazione e le tecnologie, provvede, con proprio decreto, a disciplinare il funzionamento della Conferenza permanente per l'innovazione tecnologica.

5. La Conferenza permanente per l'innovazione tecnologica può sentire le organizzazioni produttive e di categoria.

6. La Conferenza permanente per l'innovazione tecnologica opera senza rimborsi spese o compensi per i partecipanti a qualsiasi titolo dovuti, compreso il trattamento economico di missione; dal presente articolo non devono derivare nuovi o maggiori oneri per il bilancio dello Stato.

Art. 19. Banca dati per la legislazione in materia di pubblico impiego

1. E' istituita presso la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, una banca dati contenente la normativa generale e speciale in materia di rapporto di lavoro alle dipendenze delle pubbliche amministrazioni.

2. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, cura l'aggiornamento periodico della banca dati di cui al comma 1, tenendo conto delle innovazioni normative e della contrattazione collettiva successivamente intervenuta, e assicurando agli utenti la consultazione gratuita.

3. All'onere derivante dall'attuazione dei presente articolo si provvede ai sensi dell'articolo 21, comma 3, della legge 29 luglio 2003, n. 229.

CAPO II - DOCUMENTO INFORMATICO E FIRME ELETTRONICHE; TRASFERIMENTI, LIBRI E SCRITTURE

SEZIONE I - Documento informatico

ART. 20. DOCUMENTO INFORMATICO

1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

[2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.]

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

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.
5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.
5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71.

NORME CORRELATE
- D.P.C.M. 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

FOCUS: DOCUMENTO INFORMATICO
a cura di Sarah Ungaro
L'art. 1, comma 1, lett. p) del Codice dell'amministrazione digitale (di cui al D.Lgs. n. 82/2005) definisce il documento informatico come la "rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti".
Ma che valore ha un documento informatico?
In merito a tale profilo, ai sensi dell'art. 20, comma 1 bis, del CAD, **il documento informatico soddisfa i requisiti della forma scritta quando garantisce in modo oggettivo qualità, integrità, sicurezza e immodificabilità**: in base alle medesime caratteristiche, il documento informatico fornito di firma elettronica "semplice" è liberamente valutabile in giudizio, secondo l'art. 21, comma 1, del citato Codice. Già da una prima analisi delle norme, viene dunque in rilievo l'importanza assunta dalle tecnologie scelte per garantire la validità del documento informatico e, tra queste, rientra sicuramente la firma elettronica.
Infatti, se nel mondo analogico utilizziamo il documento scritto e sottoscritto per avere una documentazione certa che mantenga traccia delle nostre azioni e possa essere

esibita in caso di contestazione, per ottenere le medesime garanzie nel mondo digitale **dobbiamo utilizzare dei processi informatici che possano parimenti garantire la paternità di un documento e preservarne l'integrità e l'autenticità nel tempo**.

In questo quadro normativo, e soprattutto in relazione alle firme elettroniche semplici e avanzate (ovvero quelle firme la cui realizzazione è libera), 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", in base agli artt. 43 e ss. del CAD, insieme ai documenti e a tutte le altre informazioni relative al processo di firma elettronica. **Un idoneo sistema di conservazione, infatti, è in grado di garantire l'integrità dei dati oggetto di archiviazione e consente l'esibizione e la valida produzione in giudizio a fini probatori dei documenti e delle relative informazioni a essi associate**.

In tale contesto, anche il concetto di "formazione" del documento informatico si è di riflesso modificato, assumendo una connotazione "dinamica": in effetti, in base a quanto espresso dall'art. 3 comma 1 della Bozza di Regole tecniche del documento informatico e gestione documentale (nella versione attualmente disponibile sul sito dell'AgID), tale nozione di documento ricomprende le seguenti azioni principali:

a) **redazione tramite l'utilizzo di appositi strumenti software**;

b) **acquisizione della copia per immagine** su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico, acquisizione per via telematica o su supporto informatico;

c) **registrazione informatica delle informazioni risultanti da transazioni informatiche** o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) **generazione o raggruppamento anche in via automatica di un insieme di dati**, provenienti da una o più basi dati anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

In particolare, i commi 6 e 7 dell'art. 3 della menzionata bozza di Regole tecniche sulla formazione del documento informatico stabiliscono che "nel caso di documento informatico formato ai sensi del comma 1, lettere c) e d), **le caratteristiche di**

immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione. Laddove non sia presente, al documento informatico immodificabile è associato un riferimento temporale".

Occorre evidenziare che la stessa nozione "dinamica" di documento informatico è stata accolta dal recente Decreto del Ministero dell'Economia e delle Finanze 11 dicembre 2013, n. 141, con cui è stato emanato il "Regolamento recante norme per la dematerializzazione delle quietanze di versamento alla Tesoreria statale", col quale si intende completare la dematerializzazione delle quietanze emesse dalle tesorerie statali a fronte dei versamenti effettuati presso le stesse tesorerie. In particolare, l'art. 6 del citato Decreto stabilisce che "nel rispetto degli accordi stabiliti nell'ambito del Sistema Informatizzato dei Pagamenti della Pubblica Amministrazione, nel Protocollo d'intesa sono definite le modalità di firma dei flussi telematici". In tal senso, dunque, facendo espresso riferimento alle modalità di firma dei "flussi telematici", le norme del DMEF n. 141/2013 già contemplano una nozione "dinamica" di documento informatico, maggiormente in linea con l'art. 3 della bozza delle nuove Regole tecniche, la quale, come già specificato, ricomprende anche i flussi informativi che, ovviamente, andranno inseriti in un sistema di conservazione a norma.

ART. 21. DOCUMENTO INFORMATICO SOTTOSCRITTO CON FIRMA ELETTRONICA

*1. **Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio**, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.*

*2. **Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale**, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che **garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento**, **ha l'efficacia prevista dall'articolo 2702 del codice civile**. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si*

presume riconducibile al titolare, salvo che questi dia prova contraria.

2-bis. Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

ART. 22. COPIE INFORMATICHE DI DOCUMENTI ANALOGICI

*1. **I documenti informatici contenenti copia** di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in*

origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, ***hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.***

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

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

4. ***Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico****, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.*

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

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

NORME CORRELATE

- D.P.C.M. 21 marzo 2013, "Individuazione di 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, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni".

E' certamente il caso di riflettere profondamente sulla **assurdità** di certe procedure di pubblicazione tuttora purtroppo fin troppo frequenti.

Ci si riferisce in particolare alla **pubblicazione sul portale istituzionale della Regione Siciliana di documenti "scannerizzati".**

Un primo aspetto da tenere in considerazione è **che la maggior parte di documenti scannerizzati non sono altro che documenti che nascono originariamente in forma digitale**. Documenti originati nei seguenti formati:

- TXT (testo semplice)
- ODT (documenti office per testo)
- ODS (documenti office per fogli di calcolo)
- ODP (documenti office per presentazioni)
- TeX o LaTeX (un linguaggio di impaginazione molto usato in campo scientifico/matematico)
- DVI (formato di descrizione testo usato in molti sistemi unix-like)
- PS o PDF (descrizione di documenti, standard ISO 32000)
- XML (un linguaggio di markup)
- HTML e XHTML (linguaggio di markup, gestito dalla W3C)
- JPEG (immagini)
- PNG (immagini)
- SVG (immagini vettoriali, gestito dalla W3C)
- OpenEXR (immagini)

risultano **documenti digitali in formato aperto, l'unico tipo di formato ammesso dalle norme per la pubblicazione sui siti delle PA.**

Questo tipo di documenti ha dimensioni fisiche tipiche abbastanza ridotte pari a circa qualche centinaio di KByte o al massimo di qualche MByte.

Se si pubblicano questi documenti sui siti istituzionali lo spazio fisico di memorizzazione sui server si mantiene ridotto e il trasferimento dai server delle P.A. al PC dell'utente avviene in modo abbastanza veloce. In più si rispettano pienamente le regole relative al formato aperto.

Quando invece si procede alla stampa del documento originale lo si trasforma in documento analogico; la successiva **scannerizzazione** lo riconduce in forma digitale ma con l'**aggravio delle dimensioni fisiche con ingombro di memoria come minimo decuplicato** e con la **distruzione delle caratteristiche di formato aperto** giacché il documento scannerizzato acquisice come immagine ogni carattere di testo.

La motivazione alla base delle procedure di pubblicazione di documenti scannerizzati nasce dalla **errata convinzione che pubblicando un documento scannerizzato dopo la firma autografa apposta sulla copia stampata possa conferire un maggior grado di autorevolezza al documento stesso**. Ciò non è vero poiché la firma "scannerizzata" non è una firma elettronica La riproduzione digitale di un segno grafico quale è la firma scannerizzata può essere presa da un documento e (appunto) incollata su un altro da chiunque, quindi non può validare né i dati né l'identità.

La procedura corretta da adottare è invece quella adottata ad esempio dalla Gazzetta Ufficiale Italiana.

Riportiamo per esteso in corsivo quanto pubblicato nel sito della GURI.

"Nell'ottica di fornire una Gazzetta Ufficiale autentica nella sua forma digitalizzata, l'Istituto Poligrafico e Zecca dello Stato, in accordo con il Ministero della Giustizia, ha ideato un processo integrato che consente di garantire l'autenticità delle informazioni legislative fornite attraverso i canali telematici.

Il Decreto Legislativo 7 marzo 2005 n. 82 "Codice dell'Amministrazione digitale", definisce le pubblicazioni contenute su supporti informatici valide e rilevanti a tutti gli effetti di legge in quanto la riproduzione è effettuata in modo tale da garantire la

conformità dei documenti agli atti originali. Cio' al fine di rendere possibile l'esonero della produzione ed esibizione del formato originale su supporto cartaceo quando richiesto ad ogni effetto di legge.

La Gazzetta Ufficiale telematica, distribuita in formato elettronico attraverso il sito www.gazzettaufficiale.it, a partire dal 2 gennaio 2009 ottempera alla disposizione legislativa indicata attraverso un complesso processo informatico che, avvalendosi anche di strumenti concettualmente avanzati quali "timbro" e "firma digitale", ne attesta l'autenticità.

Il "timbro digitale" apposto su ogni pagina della pubblicazione consente di garantire il processo produttivo della Gazzetta Ufficiale da parte dell'Istituto Poligrafico e Zecca dello Stato.

La "firma digitale", apposta dal responsabile del relativo processo di pubblicazione, assicura la conformità del contenuto della Gazzetta Ufficiale in versione digitale ovvero che l'oggetto della sottoscrizione non ha subito alcuna alterazione rispetto alla versione cartacea.

Il citato processo informatico adottato dall'Istituto Poligrafico e Zecca dello Stato ha consentito di rendere manifesta l'autenticità della G.U. nella sua integrità.

Al fine di consentire la verifica di autenticità, oltre che della versione digitale anche della corrispondente versione cartacea, l'Istituto Poligrafico e Zecca dello Stato mette a disposizione un applicativo che permette di evidenziare eventuali manomissioni su ogni singola pagina della Gazzetta Ufficiale.

L'applicativo predisposto per la lettura del "timbro digitale", rappresentato da un codice grafico bidimensionale apposto su ciascuna pagina della Gazzetta Ufficiale, consente di verificare l'autenticità del documento attraverso:

- *la visualizzazione del certificato che attesta la produzione della Gazzetta Ufficiale con il processo controllato adottato dall'Istituto Poligrafico e Zecca dello Stato.*
- *la coerenza della tipolologia e degli estremi di pubblicazione della Gazzetta Ufficiale a cui si riferisce la pagina in esame: serie, numero, data di pubblicazione e numero di pagina.*
- *la verifica dell'integrità del documento ovvero che il contenuto di ciascuna*

pagina della Gazzetta Ufficiale riprodotta in "locale" non sia stato modificato in riferimento a quello effettivamente pubblicato e memorizzato sui server dell'Istituto Poligrafico e Zecca dello Stato.

Eventuali manomissioni del documento sono evidenziate dal software attraverso segnalazioni grafiche.

Verifica di Autenticità

Per attivare la procedura di verifica sopra descritta è necessario scaricare ed installare sul proprio Personal Computer l'applicativo citato che consente di effettuare:

- *un primo livello di verifica per accertare, senza necessità di collegamento internet, il certificato di provenienza, gli estremi ed il tipo di G.U. comprensivo di numero di pagina.*
- *un secondo livello di verifica per evidenziare, attraverso la rete telematica, eventuali differenze tra il testo originale (archiviato sui server del Poligrafico) e quello riprodotto in "locale" rilevando, dal confronto, eventuali alterazioni di contenuto.*

L'applicativo consente di controllare una pagina di G.U. sia in formato PDF che in formato cartaceo: in quest'ultimo caso deve essere preventivamente scannerizzata e trasformata in formato PDF.

Nel caso si desideri "verificare" una pagina cartacea e' necessario utilizzare scanner compatibili con lo standard Twain; per ogni informazione sull'utilizzazione dell'applicativo si rimanda alle indicazioni riportate sullo stesso."

Nel caso della pubblicazione di decreti dirigenziali/presidenziali e di delibere basterebbe invece la **apposizione firma digitale del responsabile del procedimento sul documento informatico originale contenente la segnatura del protocollo informatico**, ammesso tutto ciò sia realmente necessaria per una pubblicazione sul web la cui finalità è più quella di dare trasparenza alla azione amministrativa che quella di rendere disponibili documenti opponibili a terzi in caso di giudizio.

ART. 23. COPIE ANALOGICHE DI DOCUMENTI INFORMATICI

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con

firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

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

ART. 23-bis. DUPLICATI E COPIE INFORMATICHE DI DOCUMENTI INFORMATICI

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71.

2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

ART. 23-ter. DOCUMENTI AMMINISTRATIVI INFORMATICI

1. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

2. I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.

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

altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.

4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e sentiti DigitPA e il Garante per la protezione dei dati personali.

5. Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.

5-bis. I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4.

6. Per quanto non previsto dal presente articolo si applicano gli articoli 21, 22, 23 e 23-bis.

NORME CORRELATE

- Circolare dell'Agenzia per l'Italia digitale n. 62/2013, recante le "Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD".

ART. 23-quater. RIPRODUZIONI INFORMATICHE

1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente:

«, informatiche».

FOCUS: COPIE E DUPLICATI

a cura di Andrea Lisi e Gianni Penzo Doria

1. La copia della copia della copia digitale: da "archetipo non originale" a "esemplare"

Tanto in ambiente digitale quanto nel mondo tradizionale, i documenti sono rappresentativi di contenuti e, contestualmente, di forme atte a stabilirne l'affidabilità. Forma e contenuto, inoltre, necessitano di alcuni interventi peculiari, idonei a garantire la forza probatoria e l'opponibilità nei confronti di terzi.

Non si tratta di una novità. Anzi, come ci ha insegnato il progetto Interpares (www.interpares.org), il mondo digitale è fatto esclusivamente di copie, dal momento che **con l'introduzione dell'informatica è scomparsa** una delle caratteristiche peculiari del documento, che lo ha caratterizzato dalle origini della scrittura ai nostri giorni: **l'originalità**. Infatti, un file copiato è sempre uguale a se stesso, con l'eccezione dei sistemi descrittivi che possono accompagnarlo lungo il ciclo di vita (ad es., un set di metadati).

Non solo. **Con l'ambiente digitale svanisce anche la caratteristica di originarietà**. In poche parole, per poter conservare un documento, risulta necessario modificarlo continuamente, trasferirlo da un supporto a un altro, modificarne la sequenza di bit in fase di migrazione o di conversione, in considerazione del fatto che esso soffre dell'altra faccia del progresso: l'obsolescenza.

In buona sostanza, **il mondo digitale vive ontologicamente di copie**, derivate dalla copia primigenia, una sorta di "archetipo non originale", cioè un ossimoro, un oggetto originato per la prima volta e affisso in un supporto. Negli anni, nei decenni e nei secoli, per potersi conservare lungo la traditio digitale, il documento ha la necessità di subire – a parità di contenuto intellettuale – una serie di trasformazioni, che lo evolveranno nella copia della copia della copia della ennesima copia del primo archetipo digitale.

In definitiva, viviamo in un mondo di copie o, preferibilmente, di "esemplari". Avremo, pertanto, non più originali e copie, ma un esemplare in copia autentica, un esemplare in copia conforme e così via.

2. La normativa in materia di copie digitali

Le nuove definizioni di copie e di duplicato, che tra poco esamineremo, sono state introdotte con la seconda modifica ufficiale del CAD, in virtù del D.Lgs. 235/2010. Esse recuperano in larga misura – pur tra qualche disattenzione – le procedure del notariato medioevale utilizzate in caso di estrazione di copie da un originale prodotto o posseduto, attraverso:

1) la riscrittura del solo contenuto, a mano o via OCR ("copia informatica di documento analogico");

2) una sua riproduzione grafica, per quanto sia possibile ammettere in linea metodologica che la forma per immagine abbia la stessa configurazione di una sequenza binaria ("copia per immagine su supporto informatico di documento analogico");

3) una diversa sequenza di bit a parità di contenuto, ma non di forma, com'è la conversione, ad esempio, di un file testuale in un pdf ("copia informatica di documento informatico");

4) la più classica delle copie, qui impropriamente definita "duplicato", ma che in realtà rappresenta il "riversamento diretto di un file" (duplicato informatico).

Esaminiamo, allora, le definizioni tratte dall'art. 1, comma 1, del CAD:

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

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

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

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

Tenendo presente che l'informatica non può capovolgere le regole del diritto, ben si possono comprendere i contenuti degli articoli 22, 23, 23 bis, 23-ter del CAD, dedicati

rispettivamente alle copie informatiche di documenti analogici, alle copie analogiche di documenti informatici, ai duplicati e copie di documenti informatici e, quindi, alle specifiche problematiche di copia e riproduzione dei documenti amministrativi informatici. Questi articoli non possono non leggersi, infatti, secondo i principi generali presenti nel codice civile agli articoli 2712, 2714, 2715 e 2719, ai quali peraltro rimandano. Secondo tali principi generali, il "sigillo" apposto da un pubblico ufficiale è l'unica forma di attestazione formale che nel nostro ordinamento possa garantire a una copia informatica (o cartacea) di documento analogico (o digitale) le garanzie di autenticità o di conformità.

Ovvio anche che, per i principi generali del diritto, una copia per immagine tratta da un documento analogico o una copia cartacea di documento informatico o, ancora, una copia informatica o un estratto di un documento informatico, in mancanza di un'attestazione di conformità da parte di un pubblico ufficiale a ciò autorizzato, hanno comunque un valore giuridico, ma sono disconoscibili.

Da un punto di vista giuridico processuale, in caso di eventuale disconoscimento, un giudice può decidere - in base alla loro affidabilità, alla loro qualità e al contesto di acquisizione, nonché in base a eventuali altre evidenze probatorie - di attribuire uno specifico valore probatorio alle copie. Inutile sottolineare ancora come il legislatore del CAD, preso atto della particolare natura del documento digitale, abbia confermato l'equipollenza nel valore formale e probatorio tra originale informatico e il suo duplicato.

In base a questi principi generali, si può comprendere come il legislatore abbia sottolineato che, ai sensi dell'art. 22, comma 4, del CAD **una copia per immagine di documento cartaceo** - pur se originale analogico unico non ricompreso nell'elenco (peraltro riduttivo) fornito dal DPCM 21 marzo 2013 - sia idonea ad assolvere gli obblighi di conservazione (purché ovviamente la conservazione digitale sia effettuata in linea con le regole tecniche e quindi sia considerabile "a norma di legge"), **ma possa sostituire, dal punto di vista strettamente probatorio, l'originale formato in origine su supporto analogico solo nei limiti dei principi generali del diritto e, cioè, in base al ruolo/funzione di chi abbia effettuato l'acquisizione**.

SEZIONE II - Firme elettroniche e certificatori

ART. 24. FIRMA DIGITALE

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

NORME CORRELATE

- D.P.C.M. 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

ART. 25. FIRMA AUTENTICATA

1. ***Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato****.*

2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui

all'articolo 24, comma 2. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

FOCUS: FIRME ELETTRONICHE

a cura di Luigi Foglia

A seguito della riforma del Codice dell'Amministrazione digitale intervenuta con il D.Lgs 235/2010, il quadro delle firme elettroniche contempla, oggi, 4 tipologie di firma: firma elettronica "semplice", firma elettronica avanzata, firma elettronica qualificata, firma digitale.

La firma elettronica semplice, strumento concepito a livello comunitario soprattutto per regolamentare le transazioni commerciali tipiche dell'e-commerce (dal più "classico" pagamento on line con carta di credito fino a quello effettuabile con lo smartphone), ha un valore giuridico mutevole in base ai livelli di sicurezza/certezza giuridica del processo che la forma e spetta al giudice di volta in volta valutarne l'effettivo valore.

Alle altre tre tipologie di firma, invece, viene riconosciuta la medesima validità della "forma scritta e sottoscritta" anche se con notevoli limitazioni per la FEA. Infatti, se la firma digitale (insieme alle firme elettroniche qualificate) è affidabile in re ipsa e garantisce con certezza al documento informatico su cui è apposta imputabilità giuridica e forma scritta - grazie alla presenza di rigorosi standard internazionali che ne regolamentano tecnologie e processi di realizzazione -, la firma elettronica semplice e la FEA non hanno, al contrario, dei riferimenti tecnologici univoci e chiaramente delineati, per questo motivo la loro affidabilità è direttamente conseguente al contesto in cui vengono utilizzate e alle soluzioni tecnologiche a cui si ricorre.

Lo stesso CAD prevede poi che le firme elettroniche siano ulteriormente e specificamente regolate da successive regole tecniche che, attualmente, sono contenute nel DPCM 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

In materia di firme qualificate e digitali, le principali novità riguardano la regolamentazione della firma remota come particolare procedura di firma elettronica qualificata o digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte del titolare delle stesse. La firma remota, quindi, potrà essere realizzata, ma solo mediante l'uso di HSM (insieme di hardware e software che realizza un dispositivo sicuro di generazione della firma in grado di gestire uno o più coppie di chiavi crittografiche) custoditi e gestiti sotto la responsabilità del certificatore accreditato. In alternativa gli HSM potranno essere custoditi e gestiti dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi.

In ogni caso tutte le misure organizzative e tecniche per realizzare la firma remota dovranno essere esplicitamente approvate, per le rispettive competenze, da AgID e da OCSI.

Le principali novità contenute nelle nuove regole tecniche sono però relative alla FEA che, seppur già prevista a livello comunitario fin dalla direttiva 1999/93/CE, non era mai stata compiutamente regolata nel nostro ordinamento.

In tema di FEA, le nuove regole tecniche stabiliscono che la realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva (art. 55 del d.p.c.m. del 22 febbraio 2013). La FEA, inoltre, non è vincolata a un certificato qualificato o a un dispositivo sicuro, come invece richiesto per le firme elettroniche qualificate e per quelle digitali (species entrambe del genere firma elettronica avanzata).

La libertà tecnologica della FEA è quindi garantita, ma allo stesso tempo deve essere assicurata la qualità, la sicurezza, l'integrità e l'immodificabilità del documento sottoscritto con FEA. È da considerare, però, che a fronte di questa libertà il legislatore ha limitato l'efficacia giuridica della FEA ai soli rapporti intercorrenti tra il soggetto che dispone della FEA e il sottoscrittore che ne ha preventivamente accettato le condizioni di utilizzo: vincolo, questo, che non vale per le pubbliche amministrazioni, le quali potranno utilizzare la FEA nell'ambito delle attività endoprocedimentali e nei rapporti con i cittadini.

Le soluzioni di FEA dovranno rispondere ai requisiti organizzativi e tecnologici previsti dagli articoli 56 e 57 delle Regole tecniche e potranno essere sia certificate da una terza parte indipendente autorizzata allo scopo, sia in relazione al loro grado di conformità alla norma ISO/IEC 27001 o alla norma ISO/IEC 15408 (livello EAL 1 o superiore), al fine di mettere in risalto il livello di corrispondenza della soluzione di firma a quanto previsto dalle stesse regole tecniche.

La firma elettronica semplice, ma soprattutto la FEA, costituiscono, quindi, dei processi tecnologici "neutri" che diventano, se correttamente tracciati e conservati, prove informatiche producibili in giudizio e acquistano garanzia di "forma scritta" quando rispondono ai requisiti previsti dal nostro ordinamento e sono utilizzati in modo da garantire la paternità e l'integrità della documentazione digitale. In particolare la FEA non deve essere riconducibile a un determinato software o a una determinata tecnologia, ma essa si riferisce genericamente a un qualsiasi sistema sicuro e affidabile che garantisca l'appartenenza a un determinato soggetto di un documento informatico reso immodificabile.

ART. 26. CERTIFICATORI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 27. CERTIFICATORI QUALIFICATI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 28. CERTIFICATI QUALIFICATI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 29. ACCREDITAMENTO

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 30. RESPONSABILITÀ DEL CERTIFICATORE

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 31. VIGILANZA SULL'ATTIVITÀ DEI CERTIFICATORI E DEI GESTORI DI POSTA ELETTRONICA CERTIFICATA

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 32. OBBLIGHI DEL TITOLARE E DEL CERTIFICATORE

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 32-bis. SANZIONI PER I CERTIFICATORI QUALIFICATI E PER I GESTORI DI POSTA ELETTRONICA CERTIFICATA

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 33. USO DI PSEUDONIMI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 34. NORME PARTICOLARI PER LE PUBBLICHE AMMINISTRAZIONI E PER ALTRI SOGGETTI QUALIFICATI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 35. DISPOSITIVI SICURI E PROCEDURE PER LA GENERAZIONE DELLA FIRMA

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 36. REVOCA E SOSPENSIONE DEI CERTIFICATI QUALIFICATI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare

interesse ai fini della presente guida)

ART. 37. CESSAZIONE DELL'ATTIVITÀ

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

SEZIONE III - Trasferimenti di fondi, libri e scritture

ART. 38. TRASFERIMENTI DI FONDI

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

ART. 39. LIBRI E SCRITTURE

(il contenuto dell'articolo è omesso per brevità non essendo ritenuto di particolare interesse ai fini della presente guida)

CAPO III - Formazione, gestione e conservazione dei documenti informatici

ART. 40. FORMAZIONE DI DOCUMENTI INFORMATICI

1. ***Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.***

[2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.]

3. Con apposito regolamento, da emanarsi entro 180 giorni dalla data di entrata in vigore del presente codice, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che possono essere redatti in originale anche su supporto cartaceo in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.

4. Il Presidente del Consiglio dei Ministri, con propri decreti, fissa la data dalla quale viene riconosciuto il valore legale degli albi, elenchi, pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti già realizzati dalle amministrazioni, su supporto informatico, in luogo dei registri cartacei.

Per secoli l'uomo ha prodotto documenti sui supporti più vari, pietre, steli, papiro, pergamena, fino alla moderna carta; e sempre da secoli apporre, nero su bianco, la propria firma su un documento è stato l'unico modo per vincolarci in modo serio. Con il documento informatico siamo di fronte ad una svolta epocale perché per la prima volta il contenuto (costituito adessso da una sequenza più o meno lunga di bit) non ha un proprio supporto fisico tanto da poter essere trasmesso, quasi instantaneamente,

all'altro capo del mondo. Se prima si era sicuri che appondo la propria firma su un documento si stava firmando proprio quello adesso firmando digitalmente un documento non avremo mai la certezza che firmiamo proprio quello che stiamo leggendo.

Il documento informatico, secondo l'art.1 comma 1°, lett. P) del Codice dell'amministrazione digitale, di cui al D.lgs. N82/2005, come modificato dal D.Lgs 235/2010, è la "*rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti*". I documenti informatici essendo null'altro che una sequenza di bit sono per propria natura facilmente modificabili; al contrario di un qualsiasi documento scritto su supporto cartaceo; in merito a tale profilo il documento informatico, ai sensi dell'art.20 comma 1 bis del CAD n.82/2005, soddisfa I requisiti della forma scritta quando garantisce in modo oggettivo qualità, integrità, sicurezza e immodificabilità: in base alle medesime caratteristiche, il documento informatico fornito di firma elettronica "semplice" è *liberamente valutabile in giudizio*, secondo l'art.21 comma 1 del citato Codice.

ART. 40-BIS. PROTOCOLLO INFORMATICO

1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 47, commi 1 e 3, 54, comma 2-ter e 57-bis, comma 1, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71.

NORME CORRELATE

- D.P.C.M. 3 DICEMBRE 2013, "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

FOCUS: PROTOCOLLO INFORMATICO

a cura di G. Penzo Doria e S. Zingarelli

1. La normativa vigente

L'introduzione del protocollo informatico nelle amministrazioni pubbliche ha

costituito il punto di partenza necessario per la gestione dei documenti in ambiente digitale. Sulla base di quanto previsto inizialmente dal DPR 428/1998, poi abrogato e confluito nel DPR 445/2000, gli uffici devono essere individuati per aree organizzative omogenee (AOO). Prescindendo dalla **definizione del legislatore, piuttosto incongrua, per AOO** si intende un insieme di risorse umane e strumentali dotato di propri organi di governo e di gestione con autonomia organizzativa. **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.

Tale innovazione non è avvenuta in maniera omogenea in tutte le amministrazioni, tanto che –nonostante l'obbligo di realizzare un sistema di gestione documentale dal 1° gennaio 2004 – molti enti si sono adeguati con estremo ritardo e, in alcuni casi, ciò non ha prodotto un sistema efficiente com'era nelle finalità della legge.

Le norme principali sul protocollo informatico sono oggi contenute nel DPR 445/2000 e nel D.Lgs. 82/2005. A completamento della normativa, è da poco stato emanato il DPCM 3 dicembre 2013 (che sostituisce il DCPM 31 ottobre 2000) in cui sono previste le "**regole tecniche** per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005". Le regole forniscono i dettami che ogni sistema di protocollo informatico deve rispettare nell'ambito della "formazione, rilascio, tenuta, conservazione, gestione, trasmissione di atti e documenti da parte di organi della pubblica amministrazione".

Se il DPR 445/2000 e il D.Lgs. 82/2005 disciplinano, quindi, la regolamentazione primaria per il corretto sviluppo dei sistemi di gestione documentale della PA, le regole tecniche definiscono i criteri e le specifiche informazioni previste nelle operazioni di gestione del fl usso dei documenti.

Il DPCM 3 dicembre 2013 ha apportato, in verità, limitate novità sostanziali rispetto alla precedente regolamentazione. Le disposizioni in esso contenute riprendono, infatti, quanto già previsto dal DPCM sostituito. Sono però da sottolineare alcuni aspetti

rilevanti.

Innanzitutto, il provvedimento in oggetto ha allineato le regole tecniche alle norme primarie emanate successivamente al 2000: il D.Lgs. 82/2005 e il DPR 68/2005 in materia di posta elettronica certificata. Al comma 3 dell'art. 5 delle nuove regole tecniche sul protocollo si dispone, inoltre, che **il manuale di gestione sia reso pubblico mediante la pubblicazione sui rispettivi siti istituzionali**; mentre, in riferimento alle modalità di registrazione dei documenti informatici, l'art. 18 del decreto prescrive che **alla registrazione di protocollo siano associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna del messaggio oggetto di registrazione rilasciato dal sistema di posta certificata**. Rilevante appare anche la disposizione relativa al **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.**

Infine, notevole importanza riveste la clausola in riferimento ai requisiti minimi di sicurezza dei sistemi di protocollo informatico, che impongono di rispettare le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al D.Lgs. 30 giugno 2003, n. 196.

2. La natura del registro di protocollo

Il registro di protocollo è uno strumento dell'archivio corrente grazie al quale i documenti sono trattati sotto un profilo giuridico e sotto un profilo gestionale. Attraverso di esso, infatti, le amministrazioni pubbliche esercitano principalmente due funzioni:

a. **funzione notarile**, di tipo attestativo, certificatorio, inerente all'efficacia dell'azione amministrativa;

b. **funzione gestionale**, di carattere organizzativo, per lo più legato alla gestione dei documenti.

Sotto il primo profilo, infatti, il protocollo ha natura di atto pubblico di fede privilegiata ed è il principale strumento di trasparenza dell'attività amministrativa. Riguardo al secondo profilo, più strettamente manageriale, si ricorda che esso è il più importante mezzo di

corredo coevo alla formazione dei documenti.

Per ottemperare a queste sue due principali funzioni, gli elementi costitutivi del registro di protocollo possono essere distinti in tre principali categorie:

a. elementi di rilevanza giuridico-probatoria

b. elementi gestionali del documento e dell'archivio

c. elementi inerenti a dati di persone, affari, attività e procedimenti.

Gli elementi di rilevanza giuridico-probatoria, sono sei:

i. numero di protocollo;

ii. data di registrazione;

iii. corrispondente (mittente, per i documenti in arrivo e destinatario per i documenti in partenza);

iv. oggetto;

v. numero degli allegati;

vi. descrizione degli allegati.

I primi quattro sono previsti dalla normativa vigente (DPR 445/2000, art. 53), gli ultimi due, invece, dall'esame di copiosa dottrina e giurisprudenza. A essi, infine, se ne aggiungono altri tre obbligatori ma dipendenti dal contesto: data e numero di protocollo del documento ricevuto, se disponibili, nonché l'impronta del documento informatico, se trasmesso per via telematica.

ART. 41. PROCEDIMENTO E FASCICOLO INFORMATICO

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.

1-bis. La gestione dei procedimenti amministrativi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all'articolo 54, commi 2-ter e 2-quater.

2. La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, I documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via

telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990,n. 241.

2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque

rispettano i criteri dell'interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell'articolo 71, di concerto con il Ministro della funzione pubblica.

2-ter. Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo

medesimo;

b) delle altre amministrazioni partecipanti;

c) del responsabile del procedimento;

d) dell'oggetto del procedimento;

e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;

e-bis) dell'identificativo del fascicolo medesimo (5). (6)

2-quater. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare

e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la

facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è

inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n.

241 del 1990. (7)

3. Ai sensi degli articoli da 14 a 14-quinquies della legge 7 agosto 1990, n. 241, previo accordo tra le

amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti
informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime.

NORME CORRELATE
- D.P.C.M. 3 dicembre 2013, "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".
- D.P.C.M. 3 dicembre 2013, "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

ART. 42. DEMATERIALIZZAZIONE DEI DOCUMENTI DELLE PUBBLICHE AMMINISTRAZIONI

1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

Art 43. RIPRODUZIONE E CONSERVAZIONE DEI DOCUMENTI

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.
2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei

documenti agli originali.

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.

FOCUS: CONSERVAZIONE DIGITALE

a cura di Andrea Lisi

Il Capo III del Codice dell'amministrazione digitale è dedicato alla "formazione, gestione e conservazione dei documenti informatici" e - secondo quanto previsto dall'art. 2 comma 3 - nei suoi articoli 40, 43 e 44 è applicabile anche ai privati. Da ciò si evince senza alcuna ombra di dubbio che non ci può essere una corretta conservazione di documenti informatici se essi non sono stati correttamente formati e gestiti.

La conservazione digitale è, infatti, solo la parte finale e fondamentale di un unico processo digitale che mira a garantire nel tempo l'autenticità, l'integrità e la leggibilità dei documenti informatici (e quindi anche dei metadati a corredo degli stessi) correttamente prodotti.

In particolare, secondo le attuali regole tecniche sulla conservazione dei documenti informatici, contenute nel DPCM del 3 dicembre 2013 (pubblicato in GU n. 59 del 12-3-2014 - Suppl. Ordinario n. 20), e in attuazione di quanto previsto dall'articolo 44, comma 1 del Codice, il sistema di conservazione - dalla presa in carico fino all'eventuale scarto - consiste nell'adozione di regole, procedure e tecnologie finalizzate a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità dei seguenti oggetti informatici:

a) i documenti informatici e i documenti amministrativi informatici con i metadati a essi associati;

b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati

a essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale. I requisiti di autenticità, integrità, affidabilità, leggibilità, reperibilità devono essere assicurati mediante la predisposizione di un processo di conservazione attraverso il quale si provveda, in estrema sintesi, all'acquisizione e alla verifica del pacchetto di versamento, alla generazione del rapporto di versamento, alla preparazione del pacchetto di archiviazione sottoscritto con firma digitale o firma elettronica qualificata del responsabile della conservazione e, infine, alla preparazione del pacchetto di distribuzione, sempre sottoscritto con firma digitale o firma elettronica qualificata dello stesso responsabile.

È importante evidenziare che con l'entrata in vigore delle nuove Regole tecniche è obbligatoria l'adozione del Manuale della conservazione, un «documento informatico» che deve illustrare dettagliatamente I ruoli, le responsabilità, gli obblighi e le eventuali deleghe dei soggetti coinvolti, le tipologie degli oggetti informatici conservati, il modello di funzionamento e il processo di conservazione e di trattamento dei pacchetti di archiviazione (con particolare riferimento alle modalità di presa in carico dei pacchetti di versamento e alla predisposizione del rapporto di versamento, che ora viene reso obbligatorio e per il quale è prevista la necessaria apposizione di un riferimento temporale), le procedure per la produzione di duplicati o copie, le normative in vigore nei luoghi dove sono conservati i documenti (e ciò è sintomatico dell'attenzione che occorre nella scelta dell'eventuale fornitore esterno del servizio di conservazione), nonché le infrastrutture utilizzate e le misure di sicurezza adottate.

La conservazione digitale può essere realizzata dal Responsabile della conservazione all'interno della struttura organizzativa del produttore dei documenti oppure affidata a un soggetto esterno mediante contratto o convenzione di servizio, che preveda l'obbligo del rispetto del manuale della conservazione predisposto dallo stesso Responsabile. Nello specifico, si dispone che le pubbliche amministrazioni realizzino i processi di conservazione all'interno della propria struttura organizzativa oppure li affidino a conservatori accreditati, pubblici o privati, di cui all'articolo 44-bis, comma 1, del CAD. In particolare, è prescritto che i sistemi di conservazione delle pubbliche amministrazioni e dei conservatori accreditati dall'AgID prevedano la materiale conservazione dei dati e

delle copie di sicurezza sul territorio nazionale e garantiscano un accesso ai dati presso la sede del produttore (dunque delle stesse PPAA e degli stessi conservatori accreditati) e misure di sicurezza conformi a quelle stabilite nel decreto. Relativamente alla tecnologia con la quale assicurare la conservazione, le nuove Regole tecniche restano neutre, lasciando sostanzialmente la possibilità al Responsabile della conservazione di scegliere liberamente con quali tecniche raggiungere gli obiettivi della conservazione (garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti informatici conservati). L'unica eccezione è rappresentata dalla necessità di sottoscrivere digitalmente il pacchetto di archiviazione, mentre per gli altri due pacchetti la firma digitale è solo una possibilità (pur essendo molto opportuno utilizzarla, soprattutto quando si affida il servizio di conservazione in outsourcing).

ART. 44. REQUISITI PER LA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

1. Il sistema di conservazione dei documenti informatici assicura:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei fl ussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza. (2)

1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti

informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

NORME CORRELATE

- D.P.C.M. 3 dicembre 2013, "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

FOCUS: RESPONSABILE DELLA CONSERVAZIONE E ALTRE FIGURE PROFESSIONALI OBBLIGATORIE PER PA E IMPRESE

a cura Andrea Lisi

Il **Responsabile della conservazione** è la **figura centrale del sistema di conservazione dei documenti informatici**.

Egli è la persona fisica, interna all'ente, che per legge ha l'obbligo di conservazione di un determinato documento e definisce e attua le politiche del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia.

Nello svolgere queste attività egli può, sotto la propria responsabilità, delegare lo svolgimento del processo di conservazione - o parte di esso - a uno o più soggetti di specifica competenza ed esperienza in relazione alle attività a essi delegate. Inoltre, **il Responsabile della conservazione può decidere di affidare il processo di conservazione a un conservatore esterno oppure chiedere la certificazione della conformità del processo di conservazione a soggetti pubblici o privati che offrano idonee garanzie organizzative e tecnologiche**, ovvero a soggetti a cui sia stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, comma 1 del Codice dell'Amministrazione Digitale, "distinti dai conservatori o dai conservatori accreditati".

Inoltre, secondo le attuali regole tecniche, **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 (Codice per la protezione dei dati personali) e dal disciplinare tecnico di cui all'allegato B dello stesso Codice**, nonché coerentemente a quanto previsto dagli artt. 50-bis e 51 del Codice dell'Amministrazione Digitale.

In particolare, il Codice dell'Amministrazione Digitale e le nuove Regole tecniche per la corretta gestione e la tutela di un archivio elettronico **prevedono obbligatoriamente la presenza di un team composto dal Responsabile della conservazione, dal Responsabile della sicurezza, dal Responsabile del trattamento dei dati e dal Responsabile del protocollo informatico e degli archivi (ove previsto) che devono operare d'intesa tra loro**. Con specifico riferimento alle pubbliche amministrazioni, le figure obbligatorie che devono operare d'intesa fra di loro sono, dunque:

- **il Responsabile della conservazione** (tendenzialmente configurabile nella professionalità di un informatico e/o digital preservation officer con conoscenze anche di informatica giuridica, diritto dell'informatica e basi di archivistica), il quale deve coordinare e presidiare i sistemi informatici informativi e documentali garantendone una durata nel tempo;
- **il Responsabile per il trattamento dei dati personali** (tendenzialmente riconducibile alla figura professionale o di un consulente giuridico/organizzativo che abbia anche cognizioni di informatica e sicurezza informatica oppure di un esperto di sicurezza informatica con cognizioni di diritto) che deve occuparsi della protezione del dato nei database e negli archivi digitali;
- **il Responsabile del protocollo, dei flussi documentali e degli archivi** (un archivista che abbia anche conoscenze base di informatica, informatica giuridica e diritto dell'informatica), il quale deve presidiare la componente archivistica di qualsiasi sistema di conservazione dei documenti informatici.

A conferma di ciò, secondo la recente Circolare AgID n. 65 del 10 aprile 2014, che definisce le modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici, il conservatore che intenda conseguire l'accreditamento presso AgID deve necessariamente garantire all'interno

della sua struttura la presenza di una serie di figure professionali, tra le quali sono espressamente previsti proprio il Responsabile della conservazione, il Responsabile del trattamento dei dati personali e il Responsabile del protocollo, dei flussi documentali e degli archivi.

In tale contesto normativo, dunque, **è ormai imprescindibile per qualsiasi soggetto pubblico o privato valorizzare le figure professionali del Responsabile della conservazione e del Responsabile privacy, titolari di compiti, poteri e funzioni fondamentali,** che ricoprono ruoli chiave nella gestione dei processi digitali e ai quali è necessario garantire, dunque, un'adeguata preparazione, un costante aggiornamento e il riconoscimento di specifiche competenze.

Proprio per dare regolamentazione e il giusto riconoscimento a queste due figure che operano in maniera complementare, è da poco nata l'associazione **ANORC Professioni**, prima associazione italiana che ha aperto per i Responsabili della conservazione e i Responsabili del trattamento due registri nazionali, istituendo un percorso virtuoso di formazione e aggiornamento a loro dedicato.

ART. 44-bis. CONSERVATORI ACCREDITATI

1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.

2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31. 3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.

NORME CORRELATE

- D.P.C.M. 3 dicembre 2013, "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".
- Circolare dell'Agenzia per l'Italia digitale del 10 aprile 2014, n. 65, "Modalità per

l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82".

CAPO IV - TRASMISSIONE INFORMATICA DEI DOCUMENTI

ART. 45. VALORE GIURIDICO DELLA TRASMISSIONE

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

ART. 46. DATI PARTICOLARI CONTENUTI NEI DOCUMENTI TRASMESSI

1. Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

ART. 47. TRASMISSIONE DEI DOCUMENTI ATTRAVERSO LA POSTA ELETTRONICA TRA LE PUBBLICHE AMMINISTRAZIONI

1. ***Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica*** *o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.*

1-bis. ***L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare****.*

2. Ai fini della ***verifica della provenienza*** *le comunicazioni sono valide se:*

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. ***È in ogni caso esclusa la trasmissione di documenti a mezzo fax****;*

d) ovvero ***trasmesse attraverso sistemi di posta elettronica certificata*** *di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.*

3. ***Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo.*** *La pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.*

ART. 48. POSTA ELETTRONICA CERTIFICATA

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.

2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.

NORME CORRELATE

- D.P.R. 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3".
- D.M. 2 novembre 2005, "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della PEC"; "Regole Tecniche PEC" (Allegato al DM 2 novembre 2005).
- Circolare CNIPA n. 56 del 21 maggio 2009, "Modalità per la presentazione della domanda di iscrizione nell'elenco pubblico dei gestori PEC".
- Circolare CNIPA 7 dicembre 2006, n. 51, "Espletamento della vigilanza e del controllo sulle attività esercitate dai Gestori di PEC".
- Nota integrativa alle Regole tecniche PEC, 5 maggio 2008.
- D.L. 29 dicembre 2009, n. 193, "Interventi urgenti in materia di funzionalità del sistema giudiziario", convertito con modificazioni dalla L. 22 febbraio 2010, n. 24.
- D.L. 18 ottobre 2012, n. 179, "Ulteriori misure urgenti per la crescita del Paese", convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221.

FOCUS: POSTA ELETTRONICA CERTIFICATA

a cura di Gianni Penzo Doria

1. Il contesto normativo

Secondo la definizione giuridicamente rilevante più recente, contenuta nell'art. 1, comma 1, lett. V-bis, del D.Lgs. 82/2005, per **posta elettronica certificata** (PEC) si intende un "**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**".

In poche parole, **la PEC rappresenta in ambiente digitale l'equivalente della raccomandata a/r in ambiente tradizionale**. La sua introduzione nel nostro ordinamento giuridico risale al DPR 11 febbraio 2005, n.68, Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3. Dunque, un mese prima della pubblicazione del CAD, il legislatore volle intervenire sul fronte dello scambio affidabile di messaggi e di

documenti informatici. Pochi mesi più tardi, inoltre, furono pubblicate anche le Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata, contenute nel DM 2 novembre 2005, uscite assieme a un allegato di specifiche inerenti alle Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata.

Negli anni successivi, il legislatore italiano è intervenuto più volte in materia, nel tentativo – a volte con mezzi e soluzioni discutibili – di rafforzarne l'utilizzo. A queste intenzioni, risale l'art. 4 del DPCM 6 maggio 2009, in virtù del quale il messaggio veicolato tramite PEC si intende "firmato" con "sottoscrizione elettronica". Qui nasce il primo equivoco di fondo: **la PEC non nasce per "sottoscrivere" i documenti digitali, ma per assicurarne l'avvenuta trasmissione e ricezione, indipendentemente dal loro valore e dalla loro efficacia**. Confondere l'autore con il vettore è un errore che non giova all'amministrazione digitale italiana, come vedremo nel paragrafo seguente. Il cerchio, tuttavia, si è chiuso con un aggravio esemplificativo, laddove all'art. 61, comma 1, del DPCM 22 febbraio 2013, si è stabilito che l'invio di un messaggio di PEC si intende sottoscritto con firma elettronica avanzata, peraltro limitato alle comunicazioni nei confronti delle amministrazioni pubbliche.

2. L'applicazione della PEC e i problemi di uno strumento non europeo

La PEC non esiste in Europa, ma soltanto in Italia (e in pochi altri Stati nel mondo). Nelle corrette intenzioni del legislatore, la PEC avrebbe dovuto essere uno degli elementi indispensabili per la PA digitale, destinato ad affiancarsi al documento informatico e alle firme elettroniche, però senza sostituirsi a essi.

La PEC, infatti, è un vettore qualificato di documenti digitali, tanto che potrebbe non contenere un testo, ma "trasportare" semplicemente uno o più oggetti informatici. Così come la spedizione di una raccomandata con avviso di ricevimento non serve a sottoscrivere il documento contenuto nella busta, la PEC è in grado di garantire al mittente "dichiarato" esclusivamente una consegna affidabile, con la garanzia dell'accettazione e dell'avvenuta consegna.

Da un punto di vista tecnologico, è ben chiaro che il messaggio PEC può essere "chiuso" in una busta digitale comprendente anche gli allegati trasmessi e quindi potrebbe dare al ricevente evidenze informatiche sulla provenienza del testo della mail

e dei file spediti, ma, Codice e Normativa europea alla mano, ciò non equivale a sottoscrizione. C'è di più. Recentemente è stato osservato che l'invio di PEC è solamente equiparabile alla sottoscrizione elettronica, con la conseguenza che l'eventuale richiesta di autenticazione di un messaggio di PEC è irricevibile da parte di un notaio o di un pubblico ufficiale.

In definitiva, tutto ciò che è possibile da un punto di vista informatico, non necessariamente lo diventa anche dal punto di vista del diritto. Inoltre, fatto non secondario, la natura di "sottoscrizione elettronica" viene novellata in una normativa secondaria, qual è il DPCM, nonché in un contesto di merito legato non alla PEC, bensì alla CEC-PAC o comunque Postacertificat@. Le conseguenze, in merito a un ipotetico contenzioso, sono facilmente immaginabili. Prescindiamo pure dalla facile disconoscibilità, ma non dal fatto che l'azione giuridica dell'invio di un messaggio non implica la sottoscrizione del documento o dei documenti allegati, soprattutto quando il mittente è diverso dall'autore del documento. Infatti, con la PEC di Caio è possibile trasmettere un documento di Tizio.

Tornando al parallelismo con il sistema tradizionale, è come se venisse spedito un documento non firmato inserito in una busta inviata tramite raccomandata con avviso di ricevimento. In questo caso, il mittente Caio avrà la prova qualificata della consegna al destinatario Sempronio, ma il documento non risulterà sottoscritto da Tizio.

La PEC, pertanto, deve continuare a essere considerata un vettore qualificato indispensabile per l'amministrazione digitale, ma che nulla ha a che spartire con il carattere di "valida" istanza per un'amministrazione pubblica. Anzi, la PEC potrebbe essere spedita anche vuota, cioè non trasmettere alcun testo nel body message, "veicolando" invece un documento informatico sottoscritto con firma avanzata, qualificata o digitale e recuperando in questo modo il senso della definizione di posta elettronica contenuta nel DPR 68/2005 come «sistema elettronico di trasmissione di documenti informatici».

In definitiva, la PEC non può essere considerata uno strumento "chiuso" e idoneo di per sé a determinare l'affidabilità di un documento o un insieme di documenti digitali. Essa, quindi, deve essere utilizzata assieme alla firma digitale (o alle firme elettroniche), al protocollo informatico, al documento digitale per poter essere efficacemente uno dei

tasselli dell'amministrazione digitale italiana.

ART. 49. SEGRETEZZA DELLA CORRISPONDENZA TRASMESSA PER VIA TELEMATICA

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

CAPO V - DATI DELLE PUBBLICHE AMMINISTRAZIONI E SERVIZI IN RETE

SEZIONE I - DATI DELLE PUBBLICHE AMMINISTRAZIONI

ART. 50. DISPONIBILITÀ DEI DATI DELLE PUBBLICHE AMMINISTRAZIONI

1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.

2. Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive; è fatto comunque salvo il disposto dell'articolo 43, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

3. Al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni l'amministrazione titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari, secondo le regole tecniche del sistema pubblico di connettività di cui al presente decreto.

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.*

NORME CORRELATE

- "Linee guida per il disaster recovery delle pubbliche amministrazioni ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale", 2013 (AgID)

FOCUS: CONTINUITÀ OPERATIVA E DISASTER RECOVERY

a cura di Graziano Garrisi

L'articolo 50-bis del Codice dell'Amministrazione Digitale obbliga le pubbliche amministrazioni a proteggere il prezioso patrimonio informativo pubblico detenuto garantendo la continuità operativa e il disaster recovery, a salvaguardia dell'integrità, disponibilità e continuità nella fruibilità delle informazioni. Questo adempimento trae origine dall'articolo 34, comma 2, del d.lgs. 30 dicembre 2010, n. 235 che ha introdotto il summenzionato art. 50-bis nel D. Lgs. n. 82/2005, rubricato "Continuità operativa", volto a fornire alle PPAA gli strumenti per adottare piani di emergenza utili a fronteggiare eventi disastrosi (come terremoti, inondazioni, allagamenti, incendi, black-out etc.) e ad assicurare la continuità delle
operazioni indispensabili per il servizio e il ritorno al normale funzionamento.

L'art. 50-bis, in particolare, impone alle pubbliche amministrazioni di definire il piano di Continuità Operativa (per brevità "CO"), la cui funzionalità deve essere verificata con cadenza almeno biennale e che deve contenere la descrizione delle relative procedure da seguire, tenendo conto delle risorse umane, strutturali e tecnologiche di ciascuna realtà amministrativa e delle idonee misure preventive. L'articolo sancisce, poi, l'obbligo per le pubbliche amministrazioni di delineare altresì un piano di disaster recovery (o "DR") che costituisce parte integrante del piano di CO e che fissa quali misure tecniche e organizzative le pubbliche amministrazioni debbano adottare per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

Si prevede, inoltre, che DigitPA (ora AgID) provveda, oltre alla verifica annuale dell'aggiornamento dei piani di disaster recovery delle amministrazioni, anche alla stesura delle "Linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche".

A tal proposito, AgID ha pubblicato nel 2013 la nuova versione delle "Linee Guida per il Disaster Recovery delle PA", introducendo precisazioni su vari aspetti, tra i quali:

- il ruolo della continuità operativa e l'importanza delle soluzioni di DR;
- i livelli di soluzioni tecnologiche (Tier) adottati convenzionalmente per ciascuna classe di criticità della PA e le caratteristiche dei Data Center;

- i ruoli e le responsabilità necessari alla gestione delle soluzioni di DR, con particolare riferimento al ruolo del Responsabile della continuità operativa;
- i servizi minimi essenziali;
- nuovi format di "Studio di fattibilità" e di "Piani di Continuità Operativa e di Disaster Recovery"
- le principali criticità emerse nelle attività di supporto agli studi di fattibilità tecnica.

I contenuti delle citate Linee Guida non si limitano a dare attuazione all'art. 50-bis del CAD, ma contengono anche indicazioni sui contenuti del piano di continuità operativa e dello studio di fattibilità tecnica (per brevità "SFT").

Per lo svolgimento delle attività previste e per la predisposizione e l'attuazione dei piani di CO e di Disaster Recovery sono stati individuati nuovi ruoli all'interno delle pubbliche amministrazioni: la corretta gestione delle responsabilità all'interno dell'Ente assume, infatti, un'importanza fondamentale per la realizzazione dei Piani di Continuità, dal momento che deve essere individuato del personale idoneo e qualificato alla realizzazione delle attività previste, che sia in grado di prendere decisioni rapide ed efficaci per risolvere le criticità, anche quelle non preventivabili dai Piani.

Tra le nuove figure che, seppur non espressamente disciplinate dal nuovo CAD, sono comunque a esso riconducibili, c'è quella del **Responsabile della Continuità Operativa**, specificamente indicata nelle citate Linee Guida, a cui vengono affidati l'implementazione, il coordinamento e la responsabilità della buona riuscita di un piano di CO, e che dovrà saper gestire tutte le attività finalizzate alle realizzazione e mantenimento del progetto di CO e di DR, lavorando a stretto contatto con il "Comitato di gestione della crisi", organismo di vertice a cui spetta la direzione strategica dell'intera struttura in occasione dell'apertura della crisi e, inoltre, la responsabilità di garantire e controllare l'intero progetto.

Si ricorda, infine, che nelle citate Linee guida viene sempre richiamato il rispetto degli artt. 31 e 34 del d.lgs. 196/2003 (c.d. Codice in materia di protezione dei dati personali); questo nuovo obbligo per le pubbliche amministrazioni, infatti, deve essere coordinato con quanto previsto dalla normativa privacy. A tal fine si riporta un'importante indicazione da parte dell'Autorità Garante per la protezione dei dati personali (cfr. parere sullo schema di "Linee-guida per il Disaster Recovery delle pubbliche amministrazioni"

del 4 luglio 2013) per quanto riguarda il periodo di conservazione dei dati di backup:

- i salvataggi devono avere un "periodo di ritenzione", passato il quale vengono eliminati;
- tale periodo deve essere commisurato alle finalità della conservazione dell'informazione (dei dati, delle applicazioni e dei processi) e deve essere precisamente indicato in tutti i documenti interessati, quali Piano di Continuità Operativa (PCO), Piano di DR (PDR) e DPS.

Nella precedente versione delle citate Linee Guida, infatti, si prevedevano periodi di conservazione anche illimitati (o particolarmente lunghi) e il Garante aveva ritenuto tale previsione non conforme al principio di finalità nel trattamento di dati personali.

Concludendo, è possibile affermare che il CAD, con l'introduzione dell'art. 50-bis, rafforza ulteriormente il quadro giuridico in ambito privacy e obbliga le PPAA ad assicurare oltreché la corretta formazione,

raccolta e conservazione di dati, anche la costante operatività dei sistemi informativi quale presupposto

fondamentale per la qualità e costante fruibilità delle informazioni e dei servizi resi ai cittadini e alle

imprese.

ART. 51. SICUREZZA DEI DATI, DEI SISTEMI E DELLE INFRASTRUTTURE DELLE PUBBLICHE AMMINISTRAZIONI

1. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

1-bis. DigitPA, ai fini dell'attuazione del comma 1:

a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso

non autorizzato o non consentito o non conforme alle finalità della raccolta.

2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.

ART. 52. ACCESSO TELEMATICO E RIUTILIZZO DEI DATI DELLE PUBBLICHE AMMINISTRAZIONI

1. L'accesso telematico a dati, documenti e procedimenti e il riutilizzo dei dati e documenti è disciplinato dai soggetti di cui all'articolo 2, comma 2, secondo le disposizioni del presente codice e nel rispetto della normativa vigente. Le pubbliche amministrazioni pubblicano nel proprio sito web, all'interno della sezione «Trasparenza, valutazione e merito», il catalogo dei dati, dei metadati e delle relative banche dati in loro possesso ed i regolamenti che ne disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo, fatti salvi i dati presenti in Anagrafe tributaria.

2. I dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza di cui all'articolo 2, comma 1, lettera h), del decreto legislativo 24 gennaio 2006, n. 36, si intendono rilasciati come dati di tipo aperto ai sensi all'articolo 68, comma 3, del presente Codice. L'eventuale adozione di una licenza di cui al citato articolo 2, comma 1, lettera h), è motivata ai sensi delle linee guida nazionali di cui al comma 7.

3. Nella definizione dei capitolati o degli schemi dei contratti di appalto relativi a prodotti e servizi che comportino la raccolta e la gestione di dati pubblici, le pubbliche amministrazioni di cui all'articolo 2, comma 2, prevedono clausole idonee a consentire l'accesso telematico e il riutilizzo, da parte di persone fisiche e giuridiche, di tali dati, dei metadati, degli schemi delle strutture di dati e delle relative banche dati.

4. Le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle pubbliche amministrazioni rientrano tra i parametri di valutazione della performance dirigenziale ai sensi dell'articolo 11, comma 9, del decreto legislativo 27 ottobre 2009, n. 150.

5. L'Agenzia per l'Italia digitale promuove le politiche di valorizzazione del patrimonio informativo pubblico nazionale e attua le disposizioni di cui al capo V del presente Codice.

6. Entro il mese di febbraio di ogni anno l'Agenzia trasmette al Presidente del Consiglio

dei Ministri o al Ministro delegato per l'innovazione tecnologica, che li approva entro il mese successivo, un'Agenda nazionale in cui definisce contenuti e gli obiettivi delle politiche di valorizzazione del patrimonio informativo pubblico e un rapporto annuale sullo stato del processo di valorizzazione in Italia; tale rapporto è pubblicato in formato aperto sul sito istituzionale della Presidenza del Consiglio dei Ministri.

7. L'Agenzia definisce e aggiorna annualmente le linee guida nazionali che individuano gli standard tecnici, compresa la determinazione delle ontologie dei servizi e dei dati, le procedure e le modalità di attuazione delle disposizioni del Capo V del presente Codice con l'obiettivo di rendere il processo omogeneo a livello nazionale, efficiente ed efficace. Le pubbliche amministrazioni di cui all'articolo 2, comma 2, del presente Codice si uniformano alle suddette linee guida.

8. Il Presidente del Consiglio o il Ministro delegato per l'innovazione tecnologica riferisce annualmente al Parlamento sullo stato di attuazione delle disposizioni del presente articolo.

9. L'Agenzia svolge le attività indicate dal presente articolo con le risorse umane, strumentali, e finanziarie previste a legislazione vigente.

NORME CORRELATE

- D.L. 18 ottobre 2012, n. 179, "Ulteriori misure urgenti per la crescita del Paese", convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221. - "Agenda nazionale per la valorizzazione del patrimonio informativo pubblico", pubblicata dall'Agenzia per l'Italia digitale il 9 maggio 2014.

ART. 53. CARATTERISTICHE DEI SITI

1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano I principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54.

2. DigitPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali.

3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.

NORME CORRELATE

- "Protocollo eGLU 1.0 per l'analisi esplorativa dei siti web delle PA", 2013 (AgID)

ART. 54. CONTENUTO DEI SITI DELLE PUBBLICHE AMMINISTRAZIONI

1. I siti delle pubbliche amministrazioni contengono i dati di cui al decreto legislativo recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, adottato ai sensi dell'articolo 1, comma 35, della legge 6 novembre 2012, n. 190.

NORME CORRELATE

- D.lgs. 14 marzo 2013,n. 33, "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni".
- "Linee Guida per i siti web delle PA", 2011(DigitPA)
- "Vademecum Open Data", ver. Beta, 2011(DigitPA)
- "Vademecum PA e social media", 2011(DigitPA)
- "Vademecum Indicazioni gestione web PA" (DigitPA)
- "Vademecum Nomi a dominio nel SDL "gov.it", 2011 (DigitPA)
- "Vademecum Pubblicare nell'albo on line", 2011 (DigitPA)

FOCUS: TRASPARENZA

a cura di Graziano Garrisi

Negli ultimi tempi si è assistito al proliferare di provvedimenti in tema di pubblicità e digitalizzazione dei procedimenti amministrativi, fino al più recente D.Lgs. n. 33 del 14 marzo 2013 (c.d. Decreto Trasparenza), recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, emanato a seguito della delega conferita al Governo con la legge c.d. "Anticorruzione" n. 190/2012, in particolare attraverso il comma 35 dell'art.

1. Il Decreto Trasparenza se, da un lato, ha contribuito a fornire un quadro organico e ben delineato degli adempimenti in materia di pubblicità e conoscibilità degli atti e dei documenti delle PPAA, dall'altro si aggiunge - e in alcuni casi si sovrappone - ai principi già contenuti nel Codice dell'Amministrazione digitale (D.Lgs. n. 82/2005). Appare subito lodevole, dunque, l'intento del Legislatore di contrastare le dinamiche ancora opache dell'agire amministrativo dietro cui possono celarsi pratiche corruttive o illecite; tuttavia tale proposito risulta fortemente compromesso da una disattenta valutazione delle conseguenze che comporta la pubblicazione di alcune categorie di dati nei siti istituzionali degli enti (posto che per "pubblicazione" si intende quella effettuata dalle PPAA nella sezione "Amministrazione trasparente" della home page dei siti istituzionali).
Infatti l'Autorità Garante per la protezione dei dati personali, con il provvedimento n. 49 del 7 febbraio 2013, ha espresso un parere sul Decreto Trasparenza, formulando alcune osservazioni sui confini dell'Amministrazione aperta, osservazioni che sono poi state recepite (in parte) nel testo definitivo del Decreto, rendendo il concetto di "accessibilità totale" più rispondente alla tutela accordata con il Codice Privacy.
Sono stati infatti opportunamente posti alcuni limiti al principio dell'accessibilità totale come nel trattamento riguardante i dati sensibili e giudiziari di cui all'art. 4, comma 1, lett. d) ad e) del decreto legislativo 30 giugno 2003, n. 196 o le erogazioni pubbliche destinate a determinate categorie di beneficiari, in ragione di delicate condizioni personali - economiche, familiari, sanitarie - la cui pubblicazione costituirebbe una grave, palese e ingiustificata violazione dei dati personali o addirittura sensibili, in ossequio, quindi, ai principi di necessità, pertinenza e proporzionalità nel trattamento dei dati.
Nello specifico, dunque, non dovrebbero essere oggetto di pubblicazione i dati relativi a: i titoli dell'erogazione dei benefici (come ad esempio l'attribuzione di borse di studio a soggetti portatori di handicap, o il riconoscimento di un buono sociale a favore di anziani non autosufficienti o con l'indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario); i criteri di attribuzione (come l punteggi attribuiti con l'indicazione degli "indici di autosufficienza nelle attività della vita quotidiana"); nonché, la destinazione dei contributi erogati (come, ad esempio, il contributo per donne che hanno subito violenze).

Come ha ricordato l'Autorità Garante per la protezione dei dati personali, l'ente pubblico deve intraprendere un'attività che comporta la diffusione di dati personali solo quando è strettamente necessario e soprattutto rispetto a dati personali idonei a rivelare lo stato di salute deve valutare con estrema attenzione le tecniche di redazione dei provvedimenti e dei loro allegati, privilegiando modalità che consentano di menzionare tali dati solo negli atti a disposizione negli uffici e consultabili dagli interessati e controinteressati, oppure utilizzando espressioni di carattere più generale o, se necessario, codici numerici.

Per garantire la conoscibilità dei dati senza che essi vengano estrapolati dal contesto nei quali sono inseriti, l'Autorità Garante, inoltre, raccomanda l'utilizzo di motori di ricerca interni ai siti delle pubbliche amministrazioni, non consentendo l'indicizzazione e la facile reperibilità degli stessi attraverso i comuni motori di ricerca generalisti (es. Google). Un'attenzione particolare, inoltre, deve essere riservata alla durata della pubblicazione dei documenti, poiché devono essere stabiliti periodi di permanenza on line differenziati a seconda della natura dei documenti, garantendone altresì un'accessibilità selettiva in base alla scadenza del termine di pubblicazione. Tutte le accortezze brevemente richiamate sono state attuate dall'Autorità Garante con l'emanazione del regolamento n. 1/2013 concernente gli obblighi di pubblicità e trasparenza relativi all'organizzazione e all'attività del Garante per la protezione dei dati personali.

Nel Decreto Trasparenza si segnala inoltre l'introduzione del nuovo istituto dell'Accesso Civico, (art. 5 del d. lgs. n. 33/2013) che contempla il diritto di chiunque di richiedere gratuitamente al Responsabile della trasparenza dell'amministrazione interessata l'accesso ai documenti, dati o informazioni nei casi in cui sia stata omessa la loro pubblicazione obbligatoria.

Il D.Lgs. n. 33/2013, inoltre, prevede specifiche sanzioni per la violazione degli obblighi di trasparenza, contemplando addirittura l'inversione dell'onere della prova a carico del Responsabile della trasparenza, il quale risponderà dell'inadempimento degli obblighi di pubblicazione imposti dalla normativa vigente, salvo che non provi che lo stesso è dipeso da causa a lui non imputabile.

Concludendo, la realizzazione della "trasparenza pubblica" - e non la semplice

pubblicazione sui siti web istituzionali – integra una "finalità di rilevante interesse pubblico" e, pertanto, sul piano applicativo, se veramente le singole amministrazioni vorranno procedere correttamente al trattamento dei dati personali nello svolgimento della propria attività istituzionale, dovranno autoregolamentarsi predisponendo tutte le misure organizzative e di sicurezza preventive e idonee a evitare la lesione del diritto alla protezione dei dati personali degli interessati e, conseguentemente, l'irrogazione di pesanti sanzioni.

ART. 55. CONSULTAZIONE DELLE INIZIATIVE NORMATIVE DEL GOVERNO

1. La Presidenza del Consiglio dei Ministri può pubblicare su sito telematico le notizie relative ad iniziative normative del Governo, nonché i disegni di legge di particolare rilevanza, assicurando forme di partecipazione del cittadino in conformità con le disposizioni vigenti in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali. La Presidenza del Consiglio dei Ministri può inoltre pubblicare atti legislativi e regolamentari in vigore, nonché i massimari elaborati da organi di giurisdizione.

2. Con decreto del Presidente del Consiglio dei Ministri sono individuate le modalità di partecipazione del cittadino alla consultazione gratuita in via telematica.

ART. 56. DATI IDENTIFICATIVI DELLE QUESTIONI PENDENTI DINANZI ALL'AUTORITÀ GIUDIZIARIA DI OGNI ORDINE E GRADO

1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti.

2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.

2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003.

ART. 57. MODULI E FORMULARI

*[1. **Le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica**, nel rispetto dei requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, **l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge**, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.*

*2. 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 altresì rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili**.]*

ART. 57-bis. INDICE DEGLI INDIRIZZI DELLE PUBBLICHE AMMINISTRAZIONI

1. Al fine di assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi è istituito l'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi, nel quale sono indicati gli indirizzi di posta elettronica certificata da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi ed i privati.

2. La realizzazione e la gestione dell'indice sono affidate a DigitPA, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche.

3. Le amministrazioni aggiornano gli indirizzi e i contenuti dell'indice tempestivamente e comunque con cadenza almeno semestrale secondo le indicazioni di DigitPA. La mancata comunicazione degli elementi necessari al completamento dell'indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

SEZIONE II - FRUIBILITÀ DEI DATI

ART. 58. MODALITÀ DELLA FRUIBILITÀ DEL DATO

1. Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato.

2. Ai sensi dell'articolo 50, comma 2, nonché al fine di agevolare l'acquisizione d'ufficio ed il controllo sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, ***le Amministrazioni titolari di banche dati accessibili per via telematica predispongono****, sulla base delle linee guida redatte da DigitPA, sentito il Garante per la protezione dei dati personali,* ***apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico****. Le convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000.*

3. DigitPA provvede al monitoraggio dell'attuazione del presente articolo, riferendo annualmente con apposita relazione al Ministro per la pubblica amministrazione e l'innovazione e alla Commissione per la valutazione, la trasparenza e l'integrità delle amministrazione pubbliche di cui all'articolo 13 del decreto legislativo 27 ottobre 2009, n. 150.

3-bis. In caso di mancata predisposizione delle convenzioni di cui al comma 2, il Presidente del Consiglio dei Ministri stabilisce un termine entro il quale le amministrazioni interessate devono provvedere. Decorso inutilmente il termine, il Presidente del Consiglio dei Ministri può nominare un commissario ad acta incaricato di predisporre le predette convenzioni. Al Commissario non spettano compensi, indennità o rimborsi.

3-ter. Resta ferma la speciale disciplina dettata in materia di dati territoriali.

NORME CORRELATE

- Determinazione Commissariale dell'Agenzia per l'Italia digitale n. 132/2013 DIG,

"Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico".
- Determinazione Commissariale dell'Agenzia per l'Italia digitale n. 126 /2013 DIG, "Linee guida per la stesura di convenzioni volte a disciplinare le modalità di accesso ai dati delle pubbliche amministrazioni, in attuazione delle disposizioni di cui all'articolo 58 del Codice dell'Amministrazione Digitale riguardante "Modalità della fruibilità del dato".
- "Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico", Agenzia per l'Italia digitale, 2013.

ART. 59. DATI TERRITORIALI

1. Per dato territoriale si intende qualunque informazione geograficamente localizzata.
2. É istituito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, con il compito di definire le regole tecniche per la realizzazione delle basi dei dati territoriali, la documentazione, la fruibilità e lo scambio dei dati stessi tra le pubbliche amministrazioni centrali e locali in coerenza con le disposizioni del presente decreto che disciplinano il sistema pubblico di connettività.
3. Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso DigitPA è istituito il ***Repertorio nazionale dei dati territoriali****.*
4. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, previa intesa con la Conferenza unificata di cui all'articolo 8 decreto legislativo 28 agosto 1997, n. 281, sono definite la composizione e le modalità per il funzionamento del Comitato di cui al comma 2.
5. Con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare, per i profili relativi ai dati ambientali, sentito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 luglio 1998, n. 281, sono definite le regole tecniche per la definizione del contenuto del repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di successivo aggiornamento dello stesso, per la formazione, la documentazione e lo scambio dei dati

territoriali detenuti dalle singole amministrazioni competenti, nonché le regole ed i costi per l'utilizzo dei dati stessi tra le pubbliche amministrazioni centrali e locali e da parte dei privati.

6. La partecipazione al Comitato non comporta oneri né alcun tipo di spese ivi compresi compensi o gettoni di presenza. Gli eventuali rimborsi per spese di viaggio sono a carico delle amministrazioni direttamente interessate che vi provvedono nell'ambito degli ordinari stanziamenti di bilancio.

7. Agli oneri finanziari di cui al comma 3 si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3.

7-bis. Nell'ambito dei dati territoriali di interesse nazionale rientra la base dei dati catastali gestita dall'Agenzia del territorio. Per garantire la circolazione e la fruizione dei dati catastali conformemente alle finalità ed alle condizioni stabilite dall'articolo 50, il direttore dell'Agenzia del territorio, di concerto con il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni e previa intesa con la Conferenza unificata, definisce con proprio decreto entro la data del 30 giugno 2006, in coerenza con le disposizioni che disciplinano il sistema pubblico di connettività, le regole tecnico-economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni.

NORME CORRELATE

- D.Lgs. 27 gennaio 2010 , n. 32, "Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)".
- D.M. 10 novembre 2011, "Regole tecniche per la definizione del contenuto del Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di aggiornamento dello stesso".

ART. 60. BASE DI DATI DI INTERESSE NAZIONALE

1. Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni, anche per

fini statistici, per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti.

2. Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. La realizzazione di tali sistemi informativi e le modalità di aggiornamento sono attuate secondo le regole tecniche sul sistema pubblico di connettività di cui all'articolo 73 e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni.

3. Le basi di dati di interesse nazionale sono individuate con decreto del Presidente del Consiglio dei Ministri, su proposta del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri di volta in volta interessati, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nelle materie di competenza e sentiti il Garante per la protezione dei dati personali e l'Istituto nazionale di statistica. Con il medesimo decreto sono altresì individuate le strutture responsabili della gestione operativa di ciascuna base di dati e le caratteristiche tecniche del sistema informativo di cui al comma 2.

3-bis. In sede di prima applicazione e fino all'adozione del decreto di cui al comma 3, sono individuate le seguenti basi di dati di interesse nazionale:

*a) **repertorio nazionale dei dati territoriali**;*

*b) **anagrafe nazionale della popolazione residente**;*

c) banca dati nazionale dei contratti pubblici di cui all'articolo 62-bis;

*d) **casellario giudiziale**;*

*e) **registro delle imprese**;*

f) gli archivi automatizzati in materia di immigrazione e di asilo di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 27 luglio 2004, n. 242, f-bis) Anagrafe nazionale degli assistiti (ANA)

4. Agli oneri finanziari di cui al presente articolo si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma

2, della legge 16 gennaio 2003, n. 3.

NORME CORRELATE

- D.P.R. 27 luglio 2004, n. 242, "Regolamento per la razionalizzazione e la interconnessione delle comunicazioni tra Amministrazioni pubbliche in materia di immigrazione".
- D.L. 18 ottobre 2012, n. 179, "Ulteriori misure urgenti per la crescita del Paese", convertito con modificazioni dalla L. 17 dicembre 2012, n. 221.
- L. 27 dicembre 2013, n. 147, "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato".

ART. 61. DELOCALIZZAZIONE DEI REGISTRI INFORMATICI

1. Fermo restando il termine di cui all'articolo 40, comma 4, i pubblici registri immobiliari possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice, secondo le regole tecniche stabilite dall'articolo 71, nel rispetto delle normativa speciale e dei principi stabiliti dal codice civile. In tal caso i predetti registri possono essere conservati anche in luogo diverso dall'Ufficio territoriale competente.

ART. 62. ANAGRAFE NAZIONALE DELLA POPOLAZIONE RESIDENTE - ANPR

1. È istituita presso il Ministero dell'interno l'Anagrafe nazionale della popolazione residente (ANPR), quale base di dati di interesse nazionale, ai sensi dell'articolo 60, che subentra all'Indice nazionale delle anagrafi(INA), istituito ai sensi del quinto comma dell'articolo 1 della legge 24 dicembre 1954, n. 1228, recante «Ordinamento delle anagrafidella popolazione residente» e all'Anagrafe della popolazione italiana residente all'estero (AIRE), istituita ai sensi della legge 27 ottobre 1988, n. 470, recante «Anagrafe e censimento degli italiani all'estero». Tale base di dati è sottoposta ad un audit di sicurezza con cadenza annuale in conformità alle regole tecniche di cui all'articolo 51. I risultati dell'audit sono inseriti nella relazione annuale del Garante per la protezione dei dati personali.

2. Ferme restando le attribuzioni del sindaco di cui all'articolo 54, comma 3, del testo

unico delle leggi sull'ordinamento degli enti locali, approvato con il decreto legislativo 18 agosto 2000, n. 267, l'ANPR subentra altresì alle anagrafidella popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni. Con il decreto di cui al comma 6 è definito un piano per il graduale subentro dell'ANPR alle citate anagrafi, da completare entro il 31 dicembre 2014. Fino alla completa attuazione di detto piano, l'ANPR acquisisce automaticamente in via telematica i dati contenuti nelle anagrafi tenute dai comuni per i quali non è ancora avvenuto il subentro. L'ANPR è organizzata secondo modalità funzionali e operative che garantiscono la univocità dei dati stessi.

3. L'ANPR assicura al singolo comune la disponibilità dei dati anagrafici della popolazione residente e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, nonché la disponibilità dei dati anagrafici e dei servizi per l'interoperabilità con le banche dati tenute dai comuni per lo svolgimento delle funzioni di competenza. L'ANPR consente esclusivamente ai comuni la certificazione dei dati anagrafici nel rispetto di quanto previsto dall'articolo 33 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, anche in modalità telematica. I comuni inoltre possono consentire, anche mediante apposite convenzioni, la fruizione dei dati anagrafici da parte dei soggetti aventi diritto. L'ANPR assicura alle pubbliche amministrazioni e agli organismi che erogano pubblici servizi l'accesso ai dati contenuti nell'ANPR.

4. Con il decreto di cui al comma 6 sono disciplinate le modalità di integrazione nell'ANPR dei dati dei cittadini attualmente registrati in anagrafiistituite presso altre amministrazioni nonché dei dati relativi al numero e alla data di emissione e di scadenza della carta di identità della popolazione residente.

5. Ai fini della gestione e della raccolta informatizzata di dati dei cittadini, le pubbliche amministrazioni di cui all'articolo 2, comma 2, del presente Codice si avvalgono esclusivamente dell'ANPR, che viene integrata con gli ulteriori dati a tal fine necessari.

6. Con uno o più decreti del Presidente del Consiglio dei Ministri, su proposta del Ministro dell'interno, del Ministro per la pubblica amministrazione e la semplificazione e del Ministro delegato all'innovazione tecnologica, di concerto con il Ministro dell'economia e delle finanze, d'intesa con l'Agenzia per l'Italia digitale, la Conferenza

permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano nonché con la Conferenza Stato - città, di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, per gli aspetti d'interesse dei comuni, sentita l'ISTAT e acquisito il parere del Garante per la protezione dei dati personali, sono stabiliti i tempi e le modalità di attuazione delle disposizioni del presente articolo, anche con riferimento:

a) alle garanzie e alle misure di sicurezza da adottare nel trattamento dei dati personali, alle modalità e ai tempi di conservazione dei dati e all'accesso ai dati da parte delle pubbliche amministrazioni per le proprie finalità istituzionali secondo le modalità di cui all'articolo 58;

b) ai criteri per l'interoperabilità dell'ANPR con le altre banche dati di rilevanza nazionale e regionale, secondo le regole tecniche del sistema pubblico di connettività di cui al capo VIII del presente decreto, in modo che le informazioni di anagrafe, una volta rese dai cittadini, si intendano acquisite dalle pubbliche amministrazioni senza necessità di ulteriori adempimenti o duplicazioni da parte degli stessi;

c) all'erogazione di altri servizi resi disponibili dall'ANPR, tra i quali il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati di cui all'articolo 74 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, compatibile con il sistema di trasmissione di cui al decreto del Ministro della salute in data 26 febbraio 2010, pubblicato nella Gazzetta Ufficiale n. 65 del 19 marzo 2010.

NORME CORRELATE

- D.L. 18 ottobre 2012, n. 179, "Ulteriori misure urgenti per la crescita del Paese", convertito con modificazioni dalla L. 17 dicembre 2012, n. 221.
- D.P.C.M. 23 agosto 2013, n. 109, "Regolamento recante disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'articolo 2, comma 1, del decretolegge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe Nazionale della Popolazione Residente (ANPR)".
- Circolare del Ministero dell'Interno n. 19/2013, "Anagrafe Nazionale della Popolazione Residente".

- Circolare del Ministero dell'Interno n. 23/2013, "Installazione del nuovo sistema di sicurezza dell'Anagrafe Nazionale della Popolazione Residente".

FOCUS: ANAGRAFE NAZIONALE DELLA POPOLAZIONE RESIDENTE

a cura di Rita Conte

Con l'istituzione dell'Anagrafe Nazionale della Popolazione Residente (ANPR) ogni cittadino ha la possibilità di indicare alla Pubblica Amministrazione un proprio indirizzo PEC quale suo domicilio digitale, il quale sarà reso disponibile a tutte le PA e ai gestori o esercenti di pubblici servizi, che potranno così comunicare con il cittadino esclusivamente tramite posta elettronica certificata.

L'Anagrafe Nazionale della Popolazione Residente (ANPR) è stata istituita ai sensi dell'art. 2 del Decreto Crescita 2.0 (DL n. 179/2012 convertito in L. 221/2012), il quale ha sostituito l'art. 62 del CAD e ha previsto che l'ANPR subentrasse all'Indice nazionale delle anagrafi(INA) e all'Anagrafe della popolazione italiana residente all'estero (AIRE), nonché alle anagrafidella popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni. Al fine di dare attuazione al piano (che deve completarsi entro il 31 dicembre 2014), è stato pubblicato in G. U. n. 230 del 01/10/2013 il D.P.C.M n. 109 del 23 agosto 2013, recante il Regolamento per l'attuazione dell'Anagrafe Nazionale della Popolazione Residente (ANPR) (D.P.C.M. del 23 agosto 2013, n. 109 - Regolamento recante disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe Nazionale della Popolazione Residente (ANPR).

In base alle nuove disposizioni contenute nel DPCM n. 109/2013 viene data attuazione all'ANPR che costituirà una base di dati di interesse nazionale volta a migliorare la prassi della pubblica amministrazione italiana e l'erogazione dei servizi resi al cittadino.

Nello specifico il regolamento stabilisce che le modalità di accesso delle pubbliche amministrazioni e degli organismi che erogano pubblici servizi ai dati e ai servizi dell'ANPR saranno disciplinate da apposite convenzioni, aperte all'adesione di tutte le amministrazioni interessate, ai sensi dell'articolo 58, comma 2, del CAD.

I vari step di attuazione dell'ANPR, nonché i sistemi di sicurezza che riguardano la fase di prima attuazione, sono descritti nel documento allegato al DPCM n. 109/2013, all'interno del quale sono stabilite le fasi progettuali con cui sarà istituita l'Anagrafe Nazionale della Popolazione Residente e, in particolare, vengono illustrate le modalità di scambio dei dati tra le anagraficomunali e l'Anagrafe Nazionale della Popolazione Residente e tra quest'ultima e gli enti centrali della Pubblica Amministrazione interessati alla notifica delle informazioni anagrafiche.

Difatti, tutte le funzioni inerenti alla gestione, all'aggiornamento e alla consultazione dell'ANPR sono affidate al CNSD (Centro Nazionale Servizi Demografici), costituito con decreto del Ministro dell'Interno del 23 aprile 2002 presso la Direzione Centrale per i Servizi Demografici.

Inoltre, nel DPCM si precisa che in futuro, con l'emanazione di altri decreti del Presidente del Consiglio dei ministri, saranno disciplinate le ulteriori modalità di attuazione delle disposizioni dell'art. 62 del CAD, anche con riferimento al subentro dell'ANPR alle anagraficomunali, alle relative misure di sicurezza, e alle specifiche tecniche concernenti l'organizzazione e il flusso dei dati.

L'istituzione dell'ANPR consente alla PA di poter disporre dei dati anagrafici della popolazione residente e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite; di erogare altri servizi tra i quali il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati; di operare secondo un nuovo sistema di sicurezza.

Con Circolare n. 19, del 3 ottobre 2013, si è sottolineato come nella prima fase di realizzazione del progetto, l'aspetto innovativo attenga al fondamentale passaggio a un nuovo sistema di sicurezza, disciplinato dalla successiva Circolare del Ministero dell'Interno n. 23/2013.

ART. 62-bis. Banca dati nazionale dei contratti pubblici

1. Per favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi ed assicurare l'efficacia, la trasparenza e il controllo in tempo reale dell'azione amministrativa per l'allocazione della spesa pubblica in lavori, servizi e forniture, anche al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e

prevenire fenomeni di corruzione, si utilizza la «Banca dati nazionale dei contratti pubblici» (BDNCP) istituita, presso l'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, della quale fanno parte i dati previsti dall'articolo 7 del decreto legislativo 12 aprile 2006, n. 163, e disciplinata, ai sensi del medesimo decreto legislativo, dal relativo regolamento attuativo.

NORME CORRELATE

- Deliberazione dell'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture n. 111 del 20 dicembre 2012 (così come modificata nelle adunanze dell'8 maggio e del 5 giugno 2013).

ART. 62-ter. ANAGRAFE NAZIONALE DEGLI ASSISTITI

1. Per rafforzare gli interventi in tema di monitoraggio della spesa del settore sanitario, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pubbliche amministrazioni, è istituita, nell'ambito del sistema informativo realizzato dal Ministero dell'economia e delle finanze in attuazione di quanto disposto dall'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, l'Anagrafe nazionale degli assistiti (ANA).

2. L'ANA, realizzata dal Ministero dell'economia e delle finanze, in accordo con il Ministero della salute in relazione alle specifiche esigenze di monitoraggio dei livelli essenziali di assistenza (LEA), nel rispetto delle previsioni di cui al comma 5 dell'articolo 62 del presente decreto, subentra, per tutte le finalità previste dalla normativa vigente, alle anagrafie agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, ai sensi dell'articolo 7 della legge 7 agosto 1982, n. 526, che mantengono la titolarità dei dati di propria competenza e ne assicurano l'aggiornamento.

3. L'ANA assicura alla singola azienda sanitaria locale la disponibilità dei dati e degli strumenti per lo svolgimento delle funzioni di propria competenza e garantisce l'accesso ai dati in essa contenuti da parte delle pubbliche amministrazioni per le relative finalità istituzionali, secondo le modalità di cui all'articolo 58, comma 2, del presente decreto.

4. Con il subentro dell'ANA, l'azienda sanitaria locale cessa di fornire ai cittadini il libretto sanitario personale previsto dall'articolo 27 della legge 23 dicembre 1978, n.

833. È facoltà dei cittadini di accedere in rete ai propri dati contenuti nell'ANA, secondo le modalità di cui al comma 1 dell'articolo 6 del presente decreto, ovvero di richiedere presso l'azienda sanitaria locale competente copia cartacea degli stessi.

5. In caso di trasferimento di residenza del cittadino, l'ANA ne dà immediata comunicazione in modalità telematica alle aziende sanitarie locali interessate dal trasferimento. L'azienda sanitaria locale nel cui territorio è compresa la nuova residenza provvede alla presa in carico del cittadino, nonché all'aggiornamento dell'ANA per i dati di propria competenza. Nessun'altra comunicazione in merito al trasferimento di residenza è dovuta dal cittadino alle aziende sanitarie locali interessate.

6. L'ANA assicura al nuovo sistema informativo sanitario nazionale realizzato dal Ministero della salute in attuazione di quanto disposto dall'articolo 87 della legge 23 dicembre 2000, n. 388, con le modalità definite dal decreto del Presidente del Consiglio dei ministri di cui al comma 7, l'accesso ai dati e la disponibilità degli strumenti funzionali a garantire l'appropriatezza e l'efficacia delle prestazioni di cura erogate al cittadino, nonché per le finalità di cui all'articolo 15, comma 25-bis, del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135.

7. Entro il 30 giugno 2014, con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della salute e del Ministro dell'economia e delle finanze, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono stabiliti:

a) i contenuti dell'ANA, tra i quali devono essere inclusi il medico di medicina generale, il codice esenzione e il domicilio;

b) il piano per il graduale subentro dell'ANA alle anagrafie agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, da completare entro il 30 giugno 2015;

c) le garanzie e le misure di sicurezza da adottare, i criteri per l'interoperabilità dell'ANA con le altre banche dati di rilevanza nazionale e regionale, nonché le modalità di cooperazione dell'ANA con banche dati già istituite a livello regionale per le medesime finalità, nel rispetto della normativa sulla protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e delle regole tecniche del sistema pubblico di connettività, ai sensi del presente decreto.

SEZIONE III - Servizi in rete

ART. 63. ORGANIZZAZIONE E FINALITÀ DEI SERVIZI IN RETE

1. Le pubbliche amministrazioni centrali individuano le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei principi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.

2. Le pubbliche amministrazioni e i gestori di servizi pubblici progettano e realizzano i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente. A tal fine, sono tenuti ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti, in conformità alle regole tecniche da emanare ai sensi dell'articolo 71. Per le amministrazioni e i gestori di servizi pubblici regionali e locali le regole tecniche sono adottate previo parere della Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali di cui all'articolo 14, comma 3-bis.

3. Le pubbliche amministrazioni collaborano per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione.

3-bis. ***A partire dal 1° gennaio 2014****, allo scopo di incentivare e favorire il processo di informatizzazione e di potenziare ed estendere i servizi telematici, i soggetti di cui all'articolo 2, comma 2, utilizzano* ***esclusivamente i canali e i servizi telematici, ivi inclusa la posta elettronica certificata, per l'utilizzo dei propri servizi, anche a mezzo di intermediari abilitati, per la presentazione da parte degli interessati di denunce, istanze e atti e garanzie fideiussorie, per l'esecuzione di versamenti fiscali, contributivi, previdenziali, assistenziali e assicurativi, nonché per la richiesta di attestazioni e certificazioni.***

3-ter. A partire dal 1° gennaio 2014 i soggetti indicati al comma 3-bis utilizzano esclusivamente servizi telematici o la posta elettronica certificata anche per gli atti, le

comunicazioni o i servizi dagli stessi resi.

3-quater. I soggetti indicati al comma 3-bis, almeno sessanta giorni prima della data della loro entrata in vigore, pubblicano nel sito web istituzionale l'elenco dei provvedimenti adottati ai sensi dei commi 3-bis e 3-ter, nonché termini e modalità di utilizzo dei servizi e dei canali telematici e della posta elettronica certificata.

3-quinquies. Con decreto del Presidente del Consiglio dei Ministri, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e successive modificazioni, da emanare entro sei mesi dalla data di entrata in vigore della presente disposizione, sono stabilite le deroghe e le eventuali limitazioni al principio di esclusività indicato dal comma 3-bis, anche al fine di escludere l'insorgenza di nuovi o maggiori oneri per la finanza pubblica.

FOCUS: SERVIZI IN RETE

a cura di Sarah Ungaro

Il Codice dell'Amministrazione digitale disciplina i servizi in rete delle pubbliche amministrazioni, prevedendo le modalità di accesso agli stessi all'art. 64. In particolare, si individuano la Carta d'identità elettronica (CIE) e la Carta nazionale dei servizi (CNS) quali strumenti attraverso cui deve essere garantito l'accesso "indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni". Tuttavia, in concreto, occorre considerare le criticità connesse alla diffusione e all'effettivo utilizzo di tali documenti elettronici tra i cittadini. Pertanto, come stabilito dal comma 2 dell'art. 64 del CAD, l'accesso ai servizi in rete delle pubbliche amministrazioni può essere consentito anche attraverso altri strumenti che permettano "l'individuazione del soggetto che richiede il servizio".

In attuazione di tale previsione, con il Decreto Legge 21 giugno 2013, n. 69, recante "Disposizioni urgenti per l'economia" (c.d. "Decreto del Fare"), convertito con modificazioni dalla Legge 9 agosto 2013, n. 98, **il Legislatore ha introdotto il Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)**.

In particolare, al comma 2-bis dell'art. 64 del CAD è stabilito che "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema

pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)".

Nello specifico, si stabilisce che con l'istituzione del sistema SPID, le pubbliche amministrazioni potranno consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1 dello stesso art. 64 del CAD (ossia la carta d'identità elettronica e la carta nazionale dei servizi, le quali dovrebbero peraltro essere sostituite dal documento digitale unificato), ovvero mediante servizi offerti dal medesimo sistema SPID. In particolare, quest'ultimo **è costituito come insieme aperto di soggetti pubblici e privati che,** previo accreditamento da parte dell'Agenzia per l'Italia digitale, **gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.**

In tale contesto, particolare attenzione meritano le disposizioni di cui all'art. 65 del CAD, dedicate alle istanze e alle dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

Tale norma individua le modalità di invio e di trasmissione di istanze e dichiarazioni a una pubblica amministrazione ritenute idonee ope legis ad "accertarne la fonte di provenienza" che "soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale", ai sensi dell'art. 45 CAD. Nello specifico, le modalità individuate dall'art. 65 sono:

a) **la sottoscrizione mediante la firma digitale o la firma elettronica qualificata**, il cui certificato è rilasciato da un certificatore accreditato;

b) **l'identificazione dell'autore effettuata dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi**, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

c) **l'identificazione dell'autore effettuata dal sistema informatico con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio** (come previsto dall'art. 64, comma 2), nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente, nonché quando le istanze e le

dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

c-bis) **la trasmissione mediante la casella di posta elettronica certificata dell'autore, purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare,** anche per via telematica secondo modalità definite con il Decreto del Presidente del Consiglio dei Ministri 27 settembre 2012, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato.

Peraltro, le modalità elencate dall'art. 65 del CAD sono richiamate anche dall'art. 38 del TUDA (Testo unico sulla documentazione amministrativa, di cui al DPR 445/2000).

ART. 64. MODALITÀ DI ACCESSO AI SERVIZI EROGATI IN RETE DALLE PUBBLICHE AMMINISTRAZIONI

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

2-ter Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, gestiscono i servizi di registrazione e di

messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.

2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

2-sexies. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

a) al modello architetturale e organizzativo del sistema;

b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;

d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

[3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal

Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007 (8) a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi.]

FOCUS: L'IDENTITÀ DIGITALE DEL CITTADINO E DELL'IMPRESA

a cura di Giovanni Manca

Scenario storico dell'identità digitale

Da oltre quindici anni lo sviluppo della rete nella pubblica amministrazione e la conseguente offerta di servizi in rete ha creato il paradosso di "un servizio" – "una identità".

A partire dal 2001 e poi nel 2004 si è provato a risolvere il problema con la Carta d'Identità Elettronica (CIE) e la Carta Nazionale dei Servizi (CNS). I risultati si rispecchiano in una CIE ancora in fase sperimentale da oltre dieci anni e una CNS che può vantare storie di successo in sanità elettronica ma che, al di là dell'aritmetica che la vede nelle mani di oltre metà della popolazione italiana, non è percepita a livello nazionale come lo strumento per l'identificazione informatica del cittadino ai servizi in rete della

pubblica amministrazione.

È importante sottolineare che numerosi servizi sono disponibili tramite PIN (si pensi ai servizi telematici fiscali e al portale INPS) ma anche tramite OTP in analogia con i servizi di internet banking.

Naturalmente anche la firma digitale può costituire identità digitale quando viene utilizzata per la sottoscrizione del documento informatico.

Il Legislatore è recentemente intervenuto con il Sistema Pubblico di Identità Digitale (SPID) introdotto con l'articolo 17-ter della Legge 9 agosto 2013, n. 98 che ha modificato l'articolo 64 del CAD.

Lo SPID apre la gestione dell'identità anche ai privati e aggrega precedenti meccanismi di utilizzo dell'identità digitale applicando un modello generale, al momento dichiarato come tecnologicamente neutro. In tale neutralità, comunque, si intravedono i modelli di identità di base con username e password, I meccanismi di One Time Password (OTP) e i certificati digitali. Risulta possibile anche l'utilizzo di tecnologia basata sulla biometria.

Nello SPID ritroviamo anche i modelli di identità federata già sviluppati per il Sistema Pubblico di Connettività. Infine ricordiamo che nello SPID è possibile gestire gli attributi e i ruoli dei titolari (per esempio l'iscrizione a un albo professionale o l'appartenenza a un particolare profilo di utenza).

Lo strumento più diffuso (ma il più utilizzato è il PIN) per l'identità digitale è la CNS. Quest'ultima è nata nel 2004 per garantire una gestione unificata dell'identità digitale a fronte di un incerto sviluppo della CIE e della contemporanea volontà politica di erogazione di significativi finanziamenti per lo sviluppo di servizi in rete nella pubblica amministrazione.

Non era infatti accettabile che il cittadino potesse usufruire di questa serie di servizi senza un'identità digitale strutturata e soprattutto non frammentata per singolo servizio. Nasce in questo periodo anche lo slogan "Dalle code al click" per rappresentare il momento storico nel quale il cittadino non si deve recare più allo sportello della PA ma può operare in modo perfettamente alternativo anche da casa o comunque in modalità telematica.

Contemporaneamente allo SPID è in corso di definizione anche il Documento Digitale Unificato - DDU. Questo è basato su una tessera dimensione carta di credito e contiene sia le funzioni di identità a vista, gestite tramite la sicurezza fisica del supporto plastico, che una serie di funzionalità elettroniche. In particolare il DDU aggrega le funzionalità a radiofrequenza dell'identità in analogia con il passaporto elettronico e quelle della CNS standard: per supportare queste funzionalità ha due chip a bordo. Il DDU dovrebbe accogliere anche le funzionalità di tessera sanitaria quindi sul suo dorso è stampato anche il codice fiscale in analogia con la TS-CNS.

Conclusioni

In una situazione significativamente disomogenea per l'identità digitale lo SPID

costituisce un modello utile per aggregare nella stessa architettura le varie tipologie di identità digitale sviluppatesi nel tempo. In questa architettura è importante anche la possibilità di fare impresa per operatori privati come le banche e i certificatori accreditati di firma digitale.

Le prime descrizioni del modello funzionale dello SPID fanno trasparire una elevata complessità che dovrà essere gestita con in mente alcuni importanti capisaldi sintetizzati di seguito:

1) evitare la proliferazione di gestori di identità soprattutto all'interno delle PPAA;

2) introdurre un modello efficace per la gestione degli attributi e dei ruoli degli utenti;

3) curare in termini di diffusione e semplicità gli strumenti di accesso per cittadini e imprese;

4) garantire un adeguato supporto agli utenti evitando la proliferazione di contact center;

5) verificare che il modello funzionale sia applicato da tutte le PPAA con meccanismi già utilizzati

per il Sistema di Interscambio nella fatturazione elettronica per la PA.

ART. 65. ISTANZE E DICHIARAZIONI PRESENTATE ALLE PUBBLICHE AMMINISTRAZIONI PER VIA TELEMATICA

1. Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

a) se sottoscritte mediante la firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato;

b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente nonché quando le istanze e le dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

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

1-bis. Con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia, possono essere individuati I casi in cui è richiesta la sottoscrizione mediante firma digitale.

1-ter. Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate ai sensi e con le modalità di cui al comma 1, lettere a), c) e c-bis), comporta responsabilità dirigenziale e responsabilità disciplinare dello stesso.

2. Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.

[3. Dalla data di cui all'articolo 64, comma 3, non è più consentito l'invio di istanze e dichiarazioni con le modalità di cui al comma 1, lettera c). (8)]

4. Il comma 2 dell'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:

«2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82».

NORME CORRELATE

- D.P.R. 28 dicembre 2000, n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".
- D.P.C.M. 27 settembre 2012, "Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata, ai sensi dell'articolo

65, comma 1, lettera c-bis), del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni".

SEZIONE IV - Carte elettroniche

ART. 66. CARTA D'IDENTITÀ ELETTRONICA E CARTA NAZIONALE DEI SERVIZI

1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica, e dell'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281. (1)

2. Le caratteristiche e le modalità per il rilascio, per la diffusione e l'uso della carta nazionale dei servizi sono definite con uno o più regolamenti, ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, adottati su proposta congiunta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nel rispetto dei seguenti principi:

a) all'emissione della carta nazionale dei servizi provvedono, su richiesta del soggetto interessato, le pubbliche amministrazioni che intendono rilasciarla;

b) l'onere economico di produzione e rilascio della carta nazionale dei servizi è a carico delle singole amministrazioni che la emettono;

c) eventuali indicazioni di carattere individuale connesse all'erogazione dei servizi al cittadino, sono possibili nei limiti di cui al decreto legislativo 30 giugno 2003, n. 196;

d) le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio;

e) la carta nazionale dei servizi può essere utilizzata anche per i pagamenti informatici tra soggetti privati e pubbliche amministrazioni, secondo quanto previsto dalla normativa vigente.

3. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della

denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, devono contenere:

a) i dati identificativi della persona;

b) il codice fiscale.

4. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, possono contenere, a richiesta dell'interessato ove si tratti di dati sensibili:

a) l'indicazione del gruppo sanguigno;

b) le opzioni di carattere sanitario previste dalla legge;

c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;

d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;

e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.

5. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con le regole tecniche di cui all'articolo 71, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.

6. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi, nonché le modalità di impiego.

7. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e

delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'ambito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.

8. Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni.

8-bis. Fino al 31 dicembre 2011, la carta nazionale dei servizi e le altre carte elettroniche ad essa conformi possono essere rilasciate anche ai titolari di carta di identità elettronica.

NORME CORRELATE

- L. 18 giugno 2009, n. 69, "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile".
- D.L. 13 maggio 2011, n. 70, "Semestre Europeo - Prime disposizioni urgenti per l'economia", convertito, con modificazioni, dalla L. 12 luglio 2011, n. 106.
- D.L. 18 ottobre 2012, n. 179, "Ulteriori misure urgenti per la crescita del Paese", convertito con modificazioni, dalla L. 17 dicembre 2012, n. 221.

FOCUS: CARTE ELETTRONICHE

a cura di Nina Preite

L'articolo 66 del Codice dell'Amministrazione digitale introduce come strumenti di autentificazione personale, nonché di autenticazione per l'accesso ai servizi in rete offerti dalla pubbliche amministrazioni, la Carta d'identità elettronica e la Carta Nazionale dei Servizi.

Successivamente a quanto stabilito dal CAD, la legge 106/2011 (articolo 10) ha introdotto il comma 2 bis all'articolo 7-vicies ter del decreto-legge 31 gennaio 2005, n.7 (Convertito con modificazioni dalla legge 31 marzo 2005, n. 43), disponendo che l'emissione della Carta d'identità elettronica (CIE) sia ora un'attività riservata al

Ministero dell'Interno e prevedendo, inoltre, la progressiva "unificazione sul medesimo supporto della carta d'identità elettronica con la tessera sanitaria, nonché il rilascio gratuito del documento unificato". Tutto ciò con l'intento dichiarato di incoraggiare la diffusione degli strumenti elettronici, di aumentare l'efficienza nell'erogazione dei servizi ai cittadini e di semplificare il procedimento di rilascio dei documenti obbligatori di identificazione.

Il decreto ministeriale del 20 giugno 2011, invece, è esclusivamente dedicato a disciplinare le "Modalità di assorbimento della Tessera Sanitaria nella Carta nazionale dei servizi". Dalla lettura dell'art. 3, si evince che la richiesta di emissione unificata di Tessera sanitaria e Carta nazionale dei servizi, da rivolgere al Ministero dell'economia e delle finanze, sia una mera facoltà riservata alle Regioni e alle Province autonome per i propri assistiti. Gli enti territoriali - definiti dalla norma come "enti emettitori" - che intendano avvalersi di tale facoltà, dovranno stipulare un'apposita convenzione con l'Agenzia delle Entrate, dotarsi di un sistema di gestione della componente CNS nel documento unificato TS-CNS, nonché garantire il rispetto degli standard tecnologici previsti dalla normativa vigente.

Di particolare interesse è l'allegato n. 2 al citato decreto, riguardante le "Specifiche tecniche del sistema di gestione della componente CNS delle TS-CNS", con cui si impone alle Regioni che intendano fare richiesta per l'emissione delle carte l'adozione di un sistema regionale per la gestione dell'intero ciclo di vita delle stesse, comprendente la definizione di un modello organizzativo e operativo e i relativi servizi software, ai fini del funzionamento del Card Management System (CSM) regionale.

Le norme in oggetto sembrerebbero, dunque, riservare alle Regioni la facoltà di assorbire la TS nella CNS, e dunque non si tratterebbe di un provvedimento generale come, invece, previsto dalla norma di cui all'art. 10 della legge 106/2011.

Considerando, inoltre, quanto previsto dagli articoli 64 e 66 del CAD - che disciplinano, rispettivamente, le modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni, la Carta d'identità elettronica e la Carta nazionale dei servizi - non si può non rilevare come la contemplata possibilità di utilizzare la CIE e la CNS quali strumenti di autenticazione telematica anche per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni sia rimasta, purtroppo, inattuata.

Il passaggio successivo alla prima unificazione tra TS e CNS arriva con la partenza del progetto di documento digitale unificato (DDU), introdotto dal D.L. 18 ottobre 2012, n. 179, convertito con modificazioni, dalla L. 17 dicembre 2012, n. 221.

La realizzazione del DDU, che sostituisce la carta di identità e la tessera sanitaria, consente di dotare tutti i cittadini di un valido strumento per l'accesso ai servizi in rete.

Tuttavia, ad oggi si è ancora in attesa del Decreto del Ministero dell'Interno che, ai sensi di quanto previsto dall'art. 1 del D.L. 179/2012 (che ha modificato il comma 3 dell'art. 10 del D.L. 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106), avrebbe dovuto stabilire entro 6 mesi le modalità tecniche di produzione, distribuzione gestione e supporto all'utilizzo del documento unificato.

CAPO VI - SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI

ART. 67. MODALITÀ DI SVILUPPO ED ACQUISIZIONE

1. Le pubbliche amministrazioni centrali, per i progetti finalizzati ad appalti di lavori e servizi ad alto contenuto di innovazione tecnologica, possono selezionare una o più proposte utilizzando il concorso di idee di cui all'articolo 57 del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554.

2. Le amministrazioni appaltanti possono porre a base delle gare aventi ad oggetto la progettazione, o l'esecuzione, o entrambe, degli appalti di cui al comma 1, le proposte ideative acquisite ai sensi del comma 1, previo parere tecnico di congruità di DigitPA; alla relativa procedura è ammesso a partecipare, ai sensi dell'articolo 57, comma 6, del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554, anche il soggetto selezionato ai sensi del comma 1, qualora sia in possesso dei relativi requisiti soggettivi.

FOCUS: OPEN DATA E RIUSO

a cura di Morena Ragone

Quando si parla di dati aperti, pensare a una sintesi di poche righe è compito improbo; è invece possibile focalizzare l'attenzione su alcuni concetti base, in un percorso attraverso quelle che, a mio avviso, sono le tre parole chiave dell'ecosistema dei dati aperti: riutilizzo, titolare e "chiunque".

Il trait d'union ci viene idealmente fornito dall'evoluzione normativa italiana - che, in questo specifico ambito, in alcuni casi ha fatto più e meglio di altri Paesi, che pure conoscono teoria e pratica dei dati aperti da tempo risalente.

Se volessimo fissare una data, potremmo partire dall'ottobre 2012, con l'adozione del **decreto legge n. 179/2012** che, introducendo l'Agenda Digitale italiana, rubrica un articolo 9 "Documenti informatici, dati di tipo aperto e inclusione digitale" che riscrive

l'articolo 52 del Codice dell'Amministrazione digitale - il decreto legislativo n. 82/2005 - e inserisce nel suo articolato, all'articolo 68, comma 3 la definizione di "**dati di tipo aperto**".

L'articolo 52 abbraccia dati, documenti e procedimenti precisando che **le pubbliche amministrazioni ne disciplinano l'accesso a fini di riutilizzo**: si evidenzia, così, il primo concetto chiave, il riutilizzo, già previsto dall'art. 2, comma 1 lett. e) del d. lgs. n. 36/2006 – il testo con cui si è recepita in Italia la direttiva **Public Sector Information 2003/98/CE** - e consentito per i dati ed i documenti del patrimonio informativo pubblico.

Il comma 2 dello stesso articolo 52 introduce nel nostro ordinamento un principio di "open by default": "i dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza di cui all'articolo 2, comma 1, lettera h), del decreto legislativo 24 gennaio 2006, n. 36, si intendono rilasciati come dati di tipo aperto ai sensi all'articolo 68, comma 3, del presente Codice".

I dati privi di licenza, quindi, si considerano accompagnati da una licenza aperta; l'eventuale adozione di una licenza tra quelle previste dal decreto-legislativo 24 gennaio 2006, n. 36, all'articolo 2, comma 1 lett. h) va, invece, motivata.

Le indicazioni su quale licenza utilizzare le ha fornite AgID - l'Agenzia per l'Italia Digitale - organo deputato a promuove le politiche di valorizzazione del patrimonio informativo pubblico nazionale - con la prima versione delle Linee Guida previste dal comma 7 dello stesso art. 52, pubblicate lo scorso 1 agosto.

La portata della disposizione è superiore a quanto di primo acchito possa sembrare, e consente, forse, finanche di rendere più compiuto il dettato normativo del precedente articolo 5014, con quel riferimento al "resi disponibili" finora sostanzialmente inapplicato: il Tribunale Amministrativo, da tanto argomentando, ha stabilito che "la disposizione legislativa impone un obbligo generalizzato di pubblicazione esteso a tutte le banche dati, con la sola eccezione dell'Anagrafe tributaria detenuta dall'Amministrazione finanziaria".

Il nuovo obbligo di pubblicazione, quindi, relativo al catalogo di dati, metadati e banche dati in possesso dell'Amministrazione, rende la stessa inadempiente e, di conseguenza, passibile di accesso civico.

Dalla lettura del capoverso, emerge con chiarezza anche l'importanza del concetto di

titolarità del dato: solo le amministrazioni titolari, infatti, potranno disporne per il riutilizzo, come previsto dall'art. 5, comma 415 del d. lgs. 36/2006.

Altra fondamentale modifica, quella introdotta sempre dall'articolo 9 del decreto-legge n. 179/2012 già citato, la cui lettera b) sostituisce integralmente il previgente comma 3 dell'articolo 68, inserendo, tra l'altro, la nozione di "dati di tipo aperto", riprendendone i tre aspetti fondamentali - rispettivamente, elemento giuridico, tecnico ed economico - della definizione internazionalmente accettata.

Il senso di tale attività resta, ovviamente, il riutilizzo; se, quindi, la formazione o la raccolta dei dati comporta per la PA l'avvio di un processo di reingegnerizzazione dell'intera attività, la PA stessa non potrà esimersi dall'affrontare alcune specifiche questioni, tecniche e giuridiche, ancora aperte sul tema, già affrontate, queste ultime, in un articolo pubblicato su ForumPA - e solo all'esito di tale complesso procedimento, pertanto, il soggetto sotteso dalla norma, quel "chiunque" così indeterminato ma, proprio per questo, così importante potrà fruire della totalità dell'informazione pubblica.

Dipende anche da noi, in qualità di interpreti ma anche di possibili fruitori, non rendere tutto questo lettera morta.

ART. 68. ANALISI COMPARATIVA DELLE SOLUZIONI

1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei princìpi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:

a) software sviluppato per conto della pubblica amministrazione;

b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;

c) software libero o a codice sorgente aperto;

d) software fruibile in modalità cloud computing;

e) software di tipo proprietario mediante ricorso a licenza d'uso;

f) software combinazione delle precedenti soluzioni.

1-bis. A tal fine, le pubbliche amministrazioni prima di procedere all'acquisto, secondo le procedure di cui al codice di cui al decreto legislativo 12 aprile 2006 n. 163, effettuano

una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri:

a) costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;

b) livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;

c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito.

1-ter. Ove dalla valutazione comparativa di tipo tecnico ed economico, secondo i criteri di cui al comma 1-bis, risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a software liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso. La valutazione di cui al presente comma è effettuata secondo le modalità e i criteri definiti dall'Agenzia per l'Italia digitale, che, a richiesta di soggetti interessati, esprime altresì parere circa il loro rispetto.

2. Le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottano soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70, che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze.

2-bis. Le amministrazioni pubbliche comunicano tempestivamente a DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche, e organizzative, adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche.

3. Agli effetti del presente decreto legislativo si intende per:

a) formato dei dati di tipo aperto, un formato di dati reso pubblico, documentato

esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;

b) dati di tipo aperto, i dati che presentano le seguenti caratteristiche:

1) sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;

2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera a), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;

3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione. L'Agenzia per l'Italia digitale deve stabilire, con propria deliberazione, i casi eccezionali, individuati secondo criteri oggettivi, trasparenti e verificabili, in cui essi sono resi disponibili a tariffe superiori ai costi marginali. In ogni caso, l'Agenzia, nel trattamento dei casi eccezionali individuati, si attiene alle indicazioni fornite dalla direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, sul riutilizzo dell'informazione del settore pubblico, recepita con il decreto legislativo 24 gennaio 2006, n. 36.

4. DigitPA istruisce ed aggiorna, con periodicità almeno annuale, un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati.

NORME CORRELATE

- Circolare 6 dicembre 2013 n.63 dell'Agenzia per l'Italia digitale, Allegato alla determinazione commissariale n. 193/2013DIG del 6 dicembre 2013, recante "Linee guida per la valutazione comparativa prevista dall'art. 68 del D.Lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione digitale"

ART. 69. RIUSO DEI PROGRAMMI INFORMATICI

1. ***Le pubbliche amministrazioni che siano titolari di programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno obbligo di***

darli in formato sorgente, completi della documentazione disponibile, in uso gratuito ad altre pubbliche amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni.

2. Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto ove possibile, che ***i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme*** *e conformi alla definizione e regolamentazione effettuata da DigitPA, ai sensi dell'articolo 68, comma 2.*

3. ***Le pubbliche amministrazioni inseriscono, nei contratti per l'acquisizione di programmi informatici o di singoli moduli, di cui al comma 1, clausole che garantiscano il diritto di disporre dei programmi ai fini del riuso da parte della medesima o di altre amministrazioni.***

4. Nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, le stesse possono includere clausole, concordate con il fornitore, che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso dei programmi o dei singoli moduli. Le clausole suddette definiscono le condizioni da osservare per la prestazione dei servizi indicati.

NORME CORRELATE

- "Linee guida per l'inserimento ed il riuso di programmi informatici o parti di essi pubblicati nella banca dati dei programmi informatici riutilizzabili" (DigitPA).

ART. 70. BANCA DATI DEI PROGRAMMI INFORMATICI RIUTILIZZABILI

1. DigitPA, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, valuta e rende note applicazioni tecnologiche realizzate dalle pubbliche amministrazioni, idonee al riuso da parte di altre pubbliche amministrazioni anche con riferimento a singoli moduli, segnalando quelle che, in base alla propria valutazione, si configurano quali migliori pratiche organizzative e tecnologiche.

2. Le pubbliche amministrazioni centrali che intendono acquisire programmi applicativi valutano preventivamente la possibilità di riuso delle applicazioni analoghe rese note da DigitPA ai sensi del comma 1, motivandone l'eventuale mancata adozione.

ART. 71. REGOLE TECNICHE

1. Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con I Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, ed il Garante per la protezione dei dati personali nelle materie di competenza, previa acquisizione obbligatoria del parere tecnico di DigitPA.

[1-bis. Entro nove mesi dalla data di entrata in vigore del presente decreto, con uno o più decreti del Presidente del Consiglio dei Ministri emanati su proposta del Ministro delegato per l'innovazione e le tecnologie, sentito il Ministro per la funzione pubblica, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono adottate le regole tecniche e di sicurezza per il funzionamento del sistema pubblico di connettività.]

1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.

2. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo.

NORME CORRELATE

- D.P.C.M. 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".
- D.P.C.M. 3 dicembre 2013, "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis,41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".
- D.P.C.M. 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82

del 2005".

- D.P.C.M. 1 aprile 2008, "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività".

- D.M. 10 novembre 2011, "Regole tecniche per la definizione del contenuto del Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di aggiornamento dello stesso".

- D.P.C.M. 27 settembre 2012, "Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata".

CAPO VIII - SISTEMA PUBBLICO DI CONNETTIVITÀ E RETE INTERNAZIONALE DELLA PUBBLICA AMMINISTRAZIONE

SEZIONE I - DEFINIZIONI RELATIVE AL SISTEMA PUBBLICO DI CONNETTIVITÀ

ART. 72. DEFINIZIONI RELATIVE AL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. Ai fini del presente decreto si intende per:

a) "trasporto di dati": i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;

b) "interoperabilità di base": i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini;

c) "connettività": l'insieme dei servizi di trasporto di dati e di interoperabilità di base;

d) "interoperabilità evoluta": i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;

e) "cooperazione applicativa": la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

ART. 73. SISTEMA PUBBLICO DI CONNETTIVITÀ (SPC)

1. Nel rispetto dell'articolo 117, secondo comma, lettera r), della Costituzione, e nel rispetto dell'autonomia dell'organizzazione interna delle funzioni informative delle regioni e delle autonomie locali il presente Capo definisce e disciplina il Sistema pubblico di connettività (SPC), al fine di assicurare il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e promuovere l'omogeneità nella elaborazione e trasmissione dei dati stessi, finalizzata allo scambio e diffusione delle informazioni tra le pubbliche amministrazioni e alla realizzazione di servizi integrati.

2. Il SPC è l'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, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei fl ussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

3. La realizzazione del SPC avviene nel rispetto dei seguenti principi:

a) sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica del sistema;

b) economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa;

c) sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.

3-bis. Le regole tecniche del Sistema pubblico di connettività sono dettate ai sensi dell'articolo 71.

NORME CORRELATE

- D. Lgs. 28 febbraio 2005 n. 42

ART. 74. RETE INTERNAZIONALE DELLE PUBBLICHE AMMINISTRAZIONI

1. Il presente decreto definisce e disciplina la Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC. La Rete costituisce l'infrastruttura di connettività che collega, nel rispetto della normativa vigente, le pubbliche amministrazioni con gli uffici italiani all'estero, garantendo adeguati livelli di sicurezza e qualità.

Sezione II - Sistema pubblico di connettività (SPC)

ART. 75. PARTECIPAZIONE AL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. Al SPC partecipano tutte le amministrazioni di cui all'articolo 2, comma 2.

2. Il comma 1 non si applica alle amministrazioni di cui al decreto legislativo 30 marzo 2001, n. 165, limitatamente all'esercizio delle sole funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali.

3. Ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 11 novembre 1994, n. 680, nonché dell'articolo 25 del decreto legislativo 30 giugno 2003, n. 196, è comunque garantita la connessione con il SPC dei sistemi informativi degli organismi competenti per l'esercizio delle funzioni di sicurezza e difesa nazionale, nel loro esclusivo interesse e secondo regole tecniche che assicurino riservatezza e sicurezza. É altresì garantita la possibilità di connessione al SPC delle autorità amministrative indipendenti.

3-bis. Il gestore di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse possono usufruire della connessione al SPC e dei relativi servizi, adeguandosi alle vigenti regole tecniche, previa delibera della Commissione di cui all'articolo 79.

FOCUS: SISTEMA PUBBLICO DI CONNETTIVITÀ

a cura di Luigi Rufo

Il Sistema pubblico di connettività (SPC) rappresenta il risultato di un lungo processo, iniziato negli anni '90 e stimolato dall'esigenza sempre più sentita dalla Pubblica Amministrazione d'informatizzarsi e di interconnettere fra loro le singole amministrazioni - statali, regionali e locali - così da valorizzare il patrimonio informativo pubblico e razionalizzare economicamente i contratti non omogenei legati al servizio di fornitura di telecomunicazione, stipulati con i vari prestatori di connettività.

Tutte queste esigenze hanno trovato pieno riscontro con il D. Lgs. 28 febbraio 2005 n. 42, che istituì il Sistema pubblico di connettività, i cui princìpi cardine sono elencati all'art. 2 comma 317:

"a) **sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica** del sistema;

b) **economicità nell'utilizzo dei servizi di rete, di interoperabilità' e di supporto alla cooperazione applicativa** ;

c) **sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione**".

Una prima, dettagliata, definizione del SPC arriva con il D. Lgs. 7 marzo 2005 n. 82 (Codice dell'amministrazione Digitale, d'ora in avanti CAD), che all'art. 73 comma 2 definisce il Sistema Pubblico di Connettività come: "l'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, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei fl ussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione".

Alla luce di ciò, guardando nell'insieme le regole tecniche del SPC - emanate con il D.P.C.M. del 1° aprile 2008 - e i princìpi ispiratori, si va oltre la funzione della Rete Unitaria della pubblica amministrazione(Rupa), già in uso, orientata prevalentemente ai servizi di connettività di tutte le amministrazioni centrali, e a costituire invece un vero e proprio framework nazionale di interoperabilità.

Tuttavia, si deve sottolineare che al SPC non partecipano le amministrazioni che svolgono funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali (art. 75 comma 2, CAD).

Il Sistema pubblico di connettività, operativamente, ha molte potenzialità, oltre ai servizi di connettività (servizio di trasporto dati) e i servizi d'interoperabilità (servizi di posta elettronica certificata, di identificazione, di autenticazione ecc.), è in grado di fornire, sfruttando la rete Internet, anche servizi di cooperazione applicativa (Spcoop) - attivi 24 ore su 24 -: detto in altri termini è in grado di consentire "l'interazione fra i sistemi informativi delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi" (Art. 72, comma 1, lettera e, CAD), ai fini dell'erogazione di servizi finali integrati.

Ebbene, è interessante rilevare proprio come secondo l'art. 76 del CAD, si prevede che "gli scambi di documenti informatici fra le pubbliche amministrazioni nell'ambito del

SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido a ogni effetto di legge". Si arriva così, attraverso il SPC, a una "abilitazione giuridica" degli scambi documentali - in modalità di cooperazione applicativa – che, se sono svolti nel rispetto delle regole tecniche19, danno ai documenti piena validità a ogni effetto di legge.

Nel suo insieme il SPC è coordinato da una Commissione (art. 79, CAD) preposta ad attuare e supervisionare gli indirizzi strategici. Ma per soddisfare esigenze legate, in senso stretto, alla sua realizzazione, ricoprono un ruolo importante anche l'AgID (Agenzia per l'Italia Digitale) a livello nazionale e le Regioni nell'ambito del proprio territorio: l'art. 83 del CAD prevede, infatti, che "per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, […],stipulano, espletando specifiche procedure ad evidenza pubblica per la selezione dei contraenti, nel rispetto delle vigenti norme in materia, uno o più contratti-quadro con più fornitori per i servizi di cui all'articolo 77, con cui i fornitori si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite".

In conclusione possiamo provare a riassumere dicendo che il Sistema pubblico di connettività definisce e gestisce nel suo insieme, sia azioni di coordinamento (regolate da accordi di servizio) sia azioni di governance sul patrimonio informativo. E l'AgID, già Digitpa, nel pieno rispetto dei "compiti e oneri" che le sono stati conferiti (art. 86 comma 4, CAD), ha previsto d'investire come budget previsionale 2014-2020, per la progettazione, realizzazione, gestione e evoluzione del SPC circa 1,95 miliardi di euro.

ART. 76. SCAMBIO DI DOCUMENTI INFORMATICI NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. Gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido ad ogni effetto di legge.

NORME CORRELATE

- D.P.C.M. 1 aprile 2008, "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività".

ART. 77. FINALITÀ DEL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. Al SPC sono attribuite le seguenti finalità:

a) fornire un insieme di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse, definiti negli aspetti di funzionalità, qualità e sicurezza, ampiamente graduabili in modo da poter soddisfare le differenti esigenze delle pubbliche amministrazioni aderenti al SPC;

b) garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualità e la miglior fruibilità degli stessi da parte dei cittadini e delle imprese;

c) fornire un'infrastruttura condivisa di interscambio che consenta l'interoperabilità tra tutte le reti delle pubbliche amministrazioni esistenti, favorendone lo sviluppo omogeneo su tutto il territorio nella salvaguardia degli investimenti effettuati;

d) fornire servizi di connettività e cooperazione alle pubbliche amministrazioni che ne facciano richiesta, per permettere l'interconnessione delle proprie sedi e realizzare così anche l'infrastruttura interna di comunicazione;

e) realizzare un modello di fornitura dei servizi multifornitore coerente con l'attuale situazione di mercato e le dimensioni del progetto stesso;

f) garantire lo sviluppo dei sistemi informatici nell'ambito del SPC salvaguardando la sicurezza dei dati, la riservatezza delle informazioni, nel rispetto dell'autonomia del patrimonio informativo delle singole amministrazioni e delle vigenti disposizioni in materia di protezione dei dati personali.

ART. 78. COMPITI DELLE PUBBLICHE AMMINISTRAZIONI NEL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. Le pubbliche amministrazioni nell'ambito della loro autonomia funzionale e gestionale adottano nella ***progettazione e gestione dei propri sistemi informativi, ivi inclusi gli aspetti organizzativi, soluzioni tecniche compatibili con la cooperazione***

applicativa con le altre pubbliche amministrazioni, *secondo le regole tecniche di cui all'articolo 73, comma 3-bis. Le stesse pubbliche amministrazioni, ove venga loro attribuito, per norma, il compito di gestire soluzioni infrastrutturali per l'erogazione di servizi comuni a più amministrazioni, adottano le medesime regole per garantire la compatibilità con la cooperazione applicativa potendosi avvalere di modalità atte a mantenere distinti gli ambiti di competenza.*

2. Per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, le responsabilità di cui al comma 1 sono attribuite al dirigente responsabile dei sistemi informativi automatizzati, di cui all'articolo 10, comma 1, dello stesso decreto legislativo.

2-bis. Le pubbliche amministrazioni centrali e periferiche di cui all' articolo 1, comma 1, lettera z), del presente codice, inclusi gli istituti e le scuole di ogni ordine e grado, le istituzioni educative e le istituzioni universitarie, nei limiti di cui all' articolo 1, comma 449, secondo periodo, della legge 27 dicembre 2006, n. 296, sono tenute, a decorrere dal 1° gennaio 2008 e comunque a partire dalla scadenza dei contratti relativi ai servizi di fonia in corso alla data predetta ad utilizzare i servizi ***"Voce tramite protocollo Internet" (VoIP) previsti dal sistema pubblico di connettività o da analoghe convenzioni stipulate da CONSIP.***

2-ter. DigitPA effettua azioni di monitoraggio e verifica del rispetto delle disposizioni di cui al comma 2-bis.

2-quater. Il mancato adeguamento alle disposizioni di cui al comma 2-bis comporta la riduzione, nell'esercizio finanziario successivo, del 30 per cento delle risorse stanziate nell'anno in corso per spese di telefonia.

ART. 79. COMMISSIONE DI COORDINAMENTO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. É istituita la Commissione di coordinamento del SPC, di seguito denominata: «Commissione», preposta agli indirizzi strategici del SPC.

2. La Commissione:

a) assicura il raccordo tra le amministrazioni pubbliche, nel rispetto delle funzioni e dei compiti spettanti a ciascuna di esse;

b) approva le linee guida, le modalità operative e di funzionamento dei servizi e delle procedure per realizzare la cooperazione applicativa fra i servizi erogati dalle amministrazioni;

c) promuove l'evoluzione del modello organizzativo e dell'architettura tecnologica del SPC in funzione del mutamento delle esigenze delle pubbliche amministrazioni e delle opportunità derivanti dalla evoluzione delle tecnologie;

d) promuove la cooperazione applicativa fra le pubbliche amministrazioni, nel rispetto delle regole tecniche di cui all'articolo 71;

e) definisce i criteri e ne verifica l'applicazione in merito alla iscrizione, sospensione e cancellazione dagli elenchi dei fornitori qualificati SPC di cui all'articolo 82;

f) dispone la sospensione e cancellazione dagli elenchi dei fornitori qualificati di cui all'articolo 82;

g) verifica la qualità e la sicurezza dei servizi erogati dai fornitori qualificati del SPC;

h) promuove il recepimento degli standard necessari a garantire la connettività, l'interoperabilità di base e avanzata, la cooperazione applicativa e la sicurezza del Sistema.

3. Le decisioni della Commissione sono assunte a maggioranza semplice o qualificata dei componenti in relazione all'argomento in esame. La Commissione a tale fine elabora, entro tre mesi dal suo insediamento, un regolamento interno da approvare con maggioranza qualificata dei suoi componenti.

ART. 80. COMPOSIZIONE DELLA COMMISSIONE DI COORDINAMENTO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. La Commissione è formata da diciassette componenti incluso il Presidente di cui al comma 2, scelti tra persone di comprovata professionalità ed esperienza nel settore, nominati con decreto del Presidente del Consiglio dei Ministri: otto componenti sono nominati in rappresentanza delle amministrazioni statali previa deliberazione del Consiglio dei Ministri, sette dei quali su proposta del Ministro per l'innovazione e le tecnologie ed uno su proposta del Ministro per la funzione pubblica; i restanti otto sono nominati su designazione della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997,n. 281. Uno dei sette componenti proposti dal Ministro per

l'innovazione e le tecnologie è nominato in rappresentanza della Presidenza del Consiglio dei Ministri. Quando esamina questioni di interesse della rete internazionale della pubblica amministrazione la Commissione è integrata da un rappresentante del Ministero degli affari esteri, qualora non ne faccia già parte.

2. Il Presidente della Commissione è il Commissario del Governo per l'attuazione dell'agenda digitale o, su sua delega, il Direttore dell'Agenzia digitale. Il Presidente e gli altri componenti della Commissione restano in carica per un triennio e l'incarico è rinnovabile.

3. La Commissione è convocata dal Presidente e si riunisce almeno quattro volte l'anno.

4. L'incarico di Presidente o di componente della Commissione e la partecipazione alle riunioni della Commissione non danno luogo alla corresponsione di alcuna indennità, emolumento, compenso e rimborso spese e le amministrazioni interessate provvedono agli oneri di missione nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

5. Per i necessari compiti istruttori la Commissione si avvale di DigitPA e sulla base di specifiche convenzioni, di organismi interregionali e territoriali. (3)

6. La Commissione può avvalersi, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica, della consulenza di uno o più organismi di consultazione e cooperazione istituiti con appositi accordi ai sensi dell'articolo 9, comma 2, lettera c), del decreto legislativo 28 agosto 1997, n. 281.

7. Ai fini della definizione degli sviluppi strategici del SPC, in relazione all'evoluzione delle tecnologie dell'informatica e della comunicazione, la Commissione può avvalersi, nell'ambito delle risorse finanziarie assegnate a DigitPA a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica, di consulenti di chiara fama ed esperienza in numero non superiore a cinque secondo le modalità definite nei regolamenti di cui all'articolo 87.

ART. 81. RUOLO DEL CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE

1. DigitPA, nel rispetto delle decisioni e degli indirizzi forniti dalla Commissione, anche

avvalendosi di soggetti terzi, gestisce le risorse condivise del SPC e le strutture operative preposte al controllo e supervisione delle stesse, per tutte le pubbliche amministrazioni di cui all'articolo 2, comma 2.

2. DigitPA, anche avvalendosi di soggetti terzi, cura la progettazione, la realizzazione, la gestione e l'evoluzione del SPC per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39.

2-bis. Al fine di dare attuazione a quanto disposto dall'articolo 5, DigitPA, mette a disposizione, attraverso il Sistema pubblico di connettività, una piattaforma tecnologica per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, al fine di assicurare, attraverso strumenti condivisi di riconoscimento unificati, l'autenticazione certa dei soggetti interessati all'operazione in tutta la gestione del processo di pagamento.

ART. 82. FORNITORI DEL SISTEMA PUBBLICO DI CONNETTIVITÀ

1. Sono istituiti uno o più elenchi di fornitori a livello nazionale e regionale in attuazione delle finalità di cui all'articolo 77.

2. I fornitori che ottengono la qualificazione SPC ai sensi dei regolamenti previsti dall'articolo 87, sono inseriti negli elenchi di competenza nazionale o regionale, consultabili in via telematica, esclusivamente ai fini dell'applicazione della disciplina di cui al presente decreto, e tenuti rispettivamente da DigitPA a livello nazionale e dalla regione di competenza a livello regionale. I fornitori in possesso dei suddetti requisiti sono denominati fornitori qualificati SPC.

3. I servizi per i quali è istituito un elenco, ai sensi del comma 1, sono erogati, nell'ambito del SPC, esclusivamente dai soggetti che abbiano ottenuto l'iscrizione nell'elenco di competenza nazionale o regionale.

4. Per l'iscrizione negli elenchi dei fornitori qualificati SPC è necessario che il fornitore soddisfi almeno I seguenti requisiti:

a) disponibilità di adeguate infrastrutture e servizi di comunicazioni elettroniche;

b) esperienza comprovata nell'ambito della realizzazione gestione ed evoluzione delle soluzioni di sicurezza informatica;

c) possesso di adeguata rete commerciale e di assistenza tecnica;

d) possesso di adeguati requisiti finanziari e patrimoniali, anche dimostrabili per il tramite di garanzie rilasciate da terzi qualificati.

5. Limitatamente ai fornitori dei servizi di connettività dovranno inoltre essere soddisfatti anche i seguenti requisiti:

a) possesso dei necessari titoli abilitativi di cui al decreto legislativo 1° agosto 2003, n. 259, per l'ambito territoriale di esercizio dell'attività;

b) possesso di comprovate conoscenze ed esperienze tecniche nella gestione delle reti e servizi di comunicazioni elettroniche, anche sotto il profilo della sicurezza e della protezione dei dati.

ART. 83. CONTRATTI QUADRO

1. Al fine della realizzazione del SPC, DigitPA a livello nazionale e le regioni nell'ambito del proprio territorio, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, nonché per garantire la fruizione, da parte delle pubbliche amministrazioni, di elevati livelli di disponibilità dei servizi e delle stesse condizioni contrattuali proposte dal miglior offerente, nonché una maggiore affidabilità complessiva del sistema, promuovendo, altresì, lo sviluppo della concorrenza e assicurando la presenza di più fornitori qualificati, stipulano, espletando specifiche procedure ad evidenza pubblica per la selezione dei contraenti, nel rispetto delle vigenti norme in materia, uno o più contratti-quadro con più fornitori per i servizi di cui all'articolo 77, con cui i fornitori si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite. (2)

2. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, sono tenute a stipulare gli atti esecutivi dei contratti-quadro con uno o più fornitori di cui al comma 1, individuati da DigitPA. Gli atti esecutivi non sono soggetti al parere di DigitPA e, ove previsto, del Consiglio di Stato. Le amministrazioni non ricomprese tra quelle di cui al citato art. 1, comma 1, del decreto legislativo n. 39 del 1993, hanno facoltà di stipulare gli atti esecutivi di cui al presente articolo.

ART. 84. MIGRAZIONE DELLA RETE UNITARIA DELLA PUBBLICA AMMINISTRAZIONE

1. Le Amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio

1993, n. 39, aderenti alla Rete unitaria della pubblica amministrazione, presentano a DigitPA, secondo le indicazioni da esso fornite, i piani di migrazione verso il SPC, da attuarsi entro diciotto mesi dalla data di approvazione del primo contratto quadro di cui all'articolo 83, comma 1, termine di cessazione dell'operatività della Rete unitaria della pubblica amministrazione.

2. Dalla data di entrata in vigore del presente articolo ogni riferimento normativo alla Rete unitaria della pubblica amministrazione si intende effettuato al SPC.

SEZIONE III - RETE INTERNAZIONALE DELLA PUBBLICA AMMINISTRAZIONE E COMPITI DEL CNIPA

ART. 85. COLLEGAMENTI OPERANTI PER IL TRAMITE DELLA RETE INTERNAZIONALE DELLE PUBBLICHE AMMINISTRAZIONI

1. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che abbiano l'esigenza di connettività verso l'estero, sono tenute ad avvalersi dei servizi offerti dalla Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC.

2. Le pubbliche amministrazioni di cui al comma 1, che dispongono di reti in ambito internazionale sono tenute a migrare nella Rete internazionale delle pubbliche amministrazioni entro il 15 marzo 2007, fatto salvo quanto previsto dall'articolo 75, commi 2 e 3.

3. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, ivi incluse le autorità amministrative indipendenti, possono aderire alla Rete internazionale delle pubbliche amministrazioni.

ART. 86. COMPITI E ONERI DEL DIGITPA

1. DigitPA cura la progettazione, la realizzazione, la gestione ed evoluzione della Rete internazionale delle pubbliche amministrazioni, previo espletamento di procedure concorsuali ad evidenza pubblica per la selezione dei fornitori e mediante la stipula di appositi contratti-quadro secondo modalità analoghe a quelle di cui all'articolo 83.

2. DigitPA, al fine di favorire una rapida realizzazione del SPC, per un periodo almeno pari a due anni a decorrere dalla data di approvazione dei contratti-quadro di cui all'articolo 83, comma 1, sostiene i costi delle infrastrutture condivise, a valere sulle risorse già previste nel bilancio dello Stato.

3. Al termine del periodo di cui al comma 2, i costi relativi alle infrastrutture condivise sono a carico dei fornitori proporzionalmente agli importi dei contratti di fornitura, e una quota di tali costi è a carico delle pubbliche amministrazioni relativamente ai servizi da esse utilizzati. I costi, i criteri e la relativa ripartizione tra le amministrazioni sono determinati annualmente con decreto del Presidente del Consiglio dei Ministri, su proposta della Commissione, previa intesa con la Conferenza unificata cui all'articolo 8

del decreto legislativo 28 agosto 1997, n. 281, salvaguardando eventuali intese locali finalizzate a favorire il pieno ingresso nel SPC dei piccoli Comuni nel rispetto di quanto previsto dal comma 5.

4. DigitPA sostiene tutti gli oneri derivanti dai collegamenti in ambito internazionale delle amministrazioni di cui all'articolo 85, comma 1, per i primi due anni di vigenza contrattuale, decorrenti dalla data di approvazione del contratto quadro di cui all'articolo 83; per gli anni successivi ogni onere è a carico della singola amministrazione contraente proporzionalmente ai servizi acquisiti.

5. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che aderiscono alla Rete internazionale delle pubbliche amministrazioni, ai sensi dell'articolo 85, comma 3, ne sostengono gli oneri relativi ai servizi che utilizzano.

NORME CORRELATE

- Decreto legge 22 giugno 2012, n. 83, "Misure urgenti per la crescita del Paese" (convertito con modificazioni dalla Legge 4 aprile 2012, n. 134).

ART. 87. REGOLAMENTI

1. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono adottati regolamenti per l'organizzazione del SPC, per l'avvalimento dei consulenti di cui all'articolo 80, comma 7, e per la determinazione dei livelli minimi dei requisiti richiesti per l'iscrizione agli elenchi dei fornitori qualificati del SPC di cui all'articolo 82.

CAPO IX - DISPOSIZIONI TRANSITORIE FINALI E ABROGAZIONI

ART. 88. NORME TRANSITORIE PER LA FIRMA DIGITALE

1. I documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori iscritti nell'elenco pubblico già tenuto dall'Autorità per l'informatica nella pubblica amministrazione sono equivalenti ai documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori accreditati.

ART. 89. AGGIORNAMENTI

1. La Presidenza del Consiglio dei Ministri adotta gli opportuni atti di indirizzo e di coordinamento per assicurare che i successivi interventi normativi, incidenti sulle materie oggetto di riordino siano attuati esclusivamente mediante la modifica o l'integrazione delle disposizioni contenute nel presente codice.

ART. 90. ONERI FINANZIARI

1. All'attuazione del presente decreto si provvede nell'ambito delle risorse previste a legislazione vigente.

ART. 91. ABROGAZIONI

1. Dalla data di entrata in vigore del presente testo unico sono abrogati:

a) il decreto legislativo 23 gennaio 2002, n. 10;

b) gli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 2, comma 1, ultimo periodo, 6; 8; 9; 10; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 36, commi 1, 2, 3, 4, 5 e 6; 51; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A);

c) l'articolo 26, comma 2, lettere a), e), h), della legge 27 dicembre 2002, n. 289;

d) l'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3;

e) gli articoli 16, 17, 18 e 19 della legge 29 luglio 2003, n. 229.

2. Le abrogazioni degli articoli 2, comma 1, ultimo periodo; 6, commi 1 e 2; 10; 36, commi 1, 2, 3, 4, 5 e 6; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto legislativo 28 dicembre 2000, n. 443 (Testo B).

3. Le abrogazioni degli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 6, commi 3 e 4; 8; 9; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 51; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C).

3-bis. L'articolo 15, comma 1, della legge 15 marzo 1997, n. 59, è abrogato.

3-ter. Il decreto legislativo 28 febbraio 2005, n. 42, è abrogato.

ART. 92. ENTRATA IN VIGORE DEL CODICE

1. Le disposizioni del presente codice entrano in vigore a decorrere dal 1° gennaio 2006. Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. É fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Conclusioni

La redazione della presente guida ha avuto lo scopo di offrire ai colleghi della Amministrazione una panoramica il più possibile completa sulle prescrizioni del CAD e sulle problematiche interpretative sollevate.

Se si sia o meno riusciti nel compito che ci si era prefisso lasciamo che sia il lettore a giudicarlo; eventuali suggerimenti di revisione/approfondimento dei contenuti potranno comunque essere inviati all'indirizzo di posta elettronica: rcirrito@regione.sicilia.it.

APPENDICE - Profilo degli Autori citati

Andrea Lisi

Avvocato esperto in diritto delle nuove tecnologie, Presidente ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti), Vice-Presidente ANORC Professioni, Segretario Generale AIFAG (Associazione Italiana Firma elettronica avanzata biometrica e Grafometrica) e Coordinatore del Digital & Law Department dello Studio Legale Lisi. È Docente presso la Document Management Academy e la MIS Academy della SDA Bocconi. Direttore editoriale della rivista professionale "Il Documento Digitale" pubblicata da Lex et Ars.

Rita Maria Conte

Laureata in Scienze filosofiche all'Università del Salento ha conseguito un Master di II livello in Management Pubblico e e-Government. Ha collaborato a vari progetti svolti da aziende e pubbliche amministrazioni nel settore dell'eGovernment.

Alessandra Cortese

Laureata in Giurisprudenza presso l'Università degli Studi di Messina dal 2013 è iscritta al Registro Praticanti del Foro di Messina. Attualmente frequenta il Master di II Livello in "Diritto dell'informatica e Teoria e Tecnica della Normazione" organizzato dall'Università La Sapienza di Roma.

Luigi Foglia

Luigi Foglia è avvocato dal 2009. Consulente senior del Digital & Law Department dello Studio Legale Lisi occupandosi principalmente di diritto dell'innovazione digitale, contratti di outsourcing informatico, formazione e conservazione digitale del documento informatico, firme elettroniche, fatturazione elettronica, innovazione nella PA, privacy, licenze d'uso software e disaster recovery. È delegato territoriale per la sede di Lecce e Responsabile della conservazione digitale di ANORC.

Graziano Garrisi

Avvocato del Foro di Lecce. Componente del Consiglio Direttivo di ANORC e Vice Coordinatore di ABIRT. Consulente senior del Digital & Law Department dello Studio Legale Lisi, occupandosi principalmente di consulenza legale in materia di privacy e diritto delle nuove tecnologie, nonché nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e D.Lgs. 196/2003. Relatore in numerosi convegni è autore di

pubblicazioni in materia di diritto delle nuove tecnologie sulle principali riviste di settore.

Giovanni Manca

Laureato in Ingegneria Elettronica, con 30 anni circa di esperienza attualmente svolge attività di consulenza sulle tematiche di dematerializzazione e sicurezza ICT per numerose aziende specializzate. Ha partecipato, tra l'altro, ai progetti per la prima firma elettronica nella pubblica amministrazione, alla messa in opera dei servizi telematici fiscali, alla progettazione dei documenti elettronici (CIE, CNS) e alla stesura delle principali norme per la cosiddetta dematerializzazione. Ha partecipato alla stesura delle più importanti normative tecniche sui temi del governo elettronico. È componente dell'Advisory Board di ANORC, del comitato scientifico di AIFAG ed è Presidente della Commissione di valutazione di ANORC Professioni. Of counsel del Digital & Law Department.

Carlo Mochi Sismondi

Ha una laurea in economia e commercio e una in filosofia. È l'ideatore di FORUM PA, la più grande ed importante manifestazione italiana, espositiva e congressuale, dedicata all'innovazione nella pubblica amministrazione e nei sistemi territoriali, che guida dal 1989 in qualità di direttore generale, prima, e di presidente e partner attualmente. Ha collaborato con 15 Governi (dal penultimo Governo Andreotti al Governo Monti) e con 13 diversi Ministri della Funzione Pubblica, mantenendo una sostanziale terzietà pur contribuendo a sostenerne tutte le azioni innovative. Si è occupato di marketing, di progetti di privato-sociale - tra cui la realizzazione del primo progetto integrato di lotta alla povertà a Tor Bella Monaca (Roma) - e di ricerca. Insegna e scrive sui temi della riforma della pubblica amministrazione, della comunicazione pubblica, dell'e-Government.

Gianni Penzo Doria

Direttore Generale dell'Università degli Studi dell'Insubria (Varese e Como) e Presidente di ANORC Professioni. Dirigente pubblico di ruolo, ha sviluppato gli interessi sul fronte dell'informatica giuridica, della diplomatica del documento digitale e della conservazione affidabile dei documenti per enti pubblici e per aziende private. Svolge attività di formazione e di consulenza per la semplificazione/reingegnerizzazione dei sistemi informativi documentali (per il 2014 collabora con l'Università Bocconi, con la Banca

d'Italia, con il Consorzio interuniversitario sulla formazione, con OmniaDOC e con Cineca/Kion). È autore di numerose pubblicazioni e di interventi sul web in materia. Of counsel del Digital & Law Department.

Nina Preite

Laureata in Sociologia e Ricerca sociale presso l'Università del Salento. Ha conseguito un Master di II livello in Management pubblico ed e-Government. Si occupa del settore formazione della Digital & Law Department, di progetti ed eventi formativi, di rapporti istituzionali e della segreteria organizzativa di ANORC e ANORC Professioni.

Morena Ragone

Giurista, studiosa di diritto di internet e delle nuove tecnologie, diritto d'autore, open government, open data, PA digitale e privacy. Dottoranda di ricerca presso l'Università di Foggia, ha esercitato per anni come avvocato. Promotrice degli Stati Generali dell'Innovazione. Attualmente, lavora come responsabile di Azione del Fondo Europeo di Sviluppo Regionale presso la Regione Puglia. È docente e relatrice in convegni di settore, autrice di numerosi contributi su Altalex, LeggiOggi e IGED, e scrive di diritti digitali per Ninja Marketing, Leonardo.it, Pionero.it e MySolutionPost.

Luigi Rufo

Laureato in Giurisprudenza presso l'Università degli Studi di Pisa nel 2011, cultore della materia in Diritto dell'Informatica, ha conseguito a gennaio 2014 il Master in Diritto delle Nuove Tecnologie e Informatica Giuridica, organizzato dal CIRSFID, presso l'Università di Bologna. Attualmente è dottorando di ricerca in Diritto e Nuove Tecnologie (XXIX ciclo) presso l'Università di Bologna.

Sarah Ungaro

Avvocato, ha conseguito il diploma della Scuola di Specializzazione per le professioni legali. Collabora con il Digital & Law Department dello Studio Legale Lisi come consulente legale, occupandosi di diritto dell'innovazione digitale, di e-Government e della redazione di articoli e contratti.

Simonetta Zingarelli

Avvocato dal 2008 e Tesoriere di ANORC. Consulente senior del Digital & Law Department dello Studio Legale Lisi occupandosi di diritto dell'informatica, consulenza e formazione in materia di e-government e conservazione digitale dei documenti per

imprese e PA. Relatrice in numerosi convegni e autrice di pubblicazioni in materia di diritto delle nuove tecnologie.