UNIVERSITÀ DEGLI STUDI "MAGNA GRAECIA DI CATANZARO"
Corso di **INFORMATICA GIURIDICA**
DOCENTE: Avv. Prof. FABRIZIO SIGILLÒ - A.A. 2025/2026

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Sommario

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

LA FIRMA DIGITALE (IN GENERALE)

Gli **articoli 24 e 25 del CAD** sono quindi dedicati alle tipologie di firme digitali, strumento che con- sente lo scambio di documenti aventi validità legale al pari di quella tradizionalmente ascritta al documento analogico completo della firma analogica.

È in questo caso che deve farsi ricorso ad una firma digitale così come definita dalla Legge e da essa regolamentata.

La firma digitale si fonda su un concetto affatto recente: la crittografia dal greco κρυπτός (kryptós) "nascosto" e γραφία (graphía) "scrittura" e consiste, pertanto, nel cercare di nascondere la scrittura ma renderla leggibile conoscendone la chiave che lo consente.

Sembra che già ai tempi degli antichi Greci esistessero già elementari sistemi di crittografia e tra questa la cosiddetta *scitala* che si rinviene anche nella storia romana antica e viene realizzata nella forma del c.d. *cifrario di Cesare*. Si tratta di un sistema ingegnoso quanto semplice (e quindi esposto a svelare il segreto attraverso cui funziona). Intorno ad un bastone di legno viene avvolto una lunga cintura in pelle su cui vengono incise le parole. Solo facendo partire la cintura da un certo punto e facendo quindi coincidere le parole in un certo modo l'intera frase sarebbe risultata leggibile. Si tratta di un sistema ingegnoso quanto semplice (e quindi esposto a svelare il segreto attraverso cui funziona).

È durante le due guerre che si sviluppano sistemi di crittografia elaborati che trovano uno strumento affidabile nella macchina Enigma, apparentemente una macchina da scrivere ma con due tastiere: la prima normale alla cui digitazione corrispondeva però una vocale o una consonante differente. Solo chi conosceva questa corrispondenza avrebbe potuto leggere quel che il documento conteneva.

La macchina fu poi modificata dando vita a diverse funzioni basata su sistemi similari e si dovette attendere il dopo guerra per reperire un sistema di crittografia particolare basata sul ***cifrario VIC***, caratterizzato dalla complessità ma anche da una particolarità: esso era basato cioè sull'uso di carta e penna.

Giungiamo agli anni '70 con l'attivazione dei sistemi di **crittografica basata su chiavi** di cui una pubblica e quindi conoscibile e l'altra privata quindi nascosta. La novità apportata all'epoca fu di sostituire l'utilizzo di una stessa **chiave detta simmetrica** perché usata sia dal

mittente che dal destinatario con quella **asimmetrica** in cui si utilizza una coppia di chiavi correlate matematicamente in maniera che ognuna consente di decifrare la cifratura eseguita con l'altra. L'una viene definita **privata**, che deve rimanere segreta mentre l'altra è quella **pubblica**, che può essere quindi liberamente distribuita senza alcuna necessità di utilizzare un canale sicuro. Fino a che la chiave privata resta segreta, la chiave pubblica può essere distribuita a tutti e per un tempo indefinito senza compromettere la sicurezza del sistema.

Questo il sistema adottato nella cifratura della firma digitale.

Tutte le persone fisiche (in esso comprendendosi anche amministratori e dipendenti di società e pubbliche amministrazioni) possono richiedere il rilascio del certificato di firma digitale a particolari soggetti espressamente autorizzati denominati "***certificatori***" e preventivamente accreditati dall'AgID (cfr. art. 1 Cad) che garantiscono l'identità dei soggetti che utilizzano la firma digitale e che dall'Agid stessa sono controllati.

LE FINALITÀ SVOLTE DAL CERTIFICATO DI FIRMA DIGITALE

Una volta acquisito il certificato di firma esso potrà espletare le due finalità a cui è demandato:

- autenticazione;
- certificazione;

benché la prima delle due non sia ritenuta propria della firma digitale perché sostituibile con altre modalità (es. carta d'identità elettronica; carte di accesso ai servizi e, più di recente, SPID).

Prerogativa della firma digitale è invece la possibilità di sottoscrivere una dichiarazione ottenendo garanzia di integrità dei dati che vengono sottoscritti ed autenticità delle informazioni relative al sottoscrittore che resistono a querela di falso ma non anche alla modifica del testo originale che, se variato anche in una piccola parte (una virgola, un punto, una parola) verrà rilevata e visibile.

SOSTANZIALI DIFFERENZE TRA LA FIRMA ANALOGICA E DIGITALE

Sul concetto di firma digitale si impongono una serie di precisazioni che muovono dalla premessa sopra riportata che la vede quale equivalente elettronico della tradizionale firma

autografa su carta.

Inutile pretendere di individuare un'assoluta similitudine tra l'una e l'altra poiché:

- la firma analogica ha una componente grafica che nella firma digitale è meramente eventuale;
- due originali di firme analogiche relative allo stesso atto presumibilmente non saranno identiche perché rispondenti ad alcune componenti fisiche destinate ad essere differenti (la stessa firma analogica apposta dalla stessa persona difficilmente sarà identica da un'altra apposta anche all'interno dello stesso documento; due firme potranno differire a seconda della maggiore o minore pressione della penna da parte dell'autore od ancora da un diverso suo stato psicologico; finanche l'uso del tipo di pennino o le caratteristiche della penna usata potrebbero determinare una diversità);
- di una firma si può ipotizzare il tentativo di riproduzione (copia) non necessariamente da parte della stessa firma si pula firma analogica potrà essere riprodotta (copiata) più o meno esattamente rispetto all'originale (e l'accertamento sull'esatta rispondenza non sarà percepibile se non attraverso specifica indagine grafologica);
- la firma analogica potrebbe perdere la sua visibilità (ad esempio se scolorita).

Di contro potrà dirsi che:

- la firma digitale deve ritenersi più affidabile (più agevole falsare una firma autografa, so- stanzialmente impossibile falsarne una digitale);
- la firma digitale rimarrà sempre identica ed inalterabile senza risentire dello stato fisico od anche solo dell'umore del firmatario;
- la firma digitale elimina l'esigenza della presenza personale del firmatario e quindi agevola lo scambio di atti e contratti;
- la firma digitale assicura la convivenza con l'atto a cui essa viene apposta (non potrà cioè esserci il rischio che venga persa una o più pagine dell'atto e comunque la firma si intenderà applicata all'intero documento);
- se la firma autografa ha una durata legata alla vita della persona che la appone e mantiene la riconducibilità all'autore vita natural durante, la firma digitale ha una durata predeterminata decorsa la quale essa perde la sua efficacia e richiede un sistema di

conservazione dell'atto digitalmente firmato con modalità specifiche.

Tecnicamente la firma digitale può dirsi consistente di un chip al cui interno sono contenuti i dati di riferimento del suo titolare. Il chip può essere apposto su una card tipo bancomat; su una card perfettamente identica a quella utilizzata per i telefonini mobili od anche affidata ad un sistema esterno al firmatario e gestita in remoto.

Ognuno dei sistemi porta con sé

VANTAGGI E SVANTAGGI.

In linea di principio può dirsi che nel caso di firma "tipo bancomat" o "tipo sim card" la firma (il chip) che contiene il relativo certificato è generata da uno strumento di cui il titolare dispone (per l'appunto la smartcard o il c.d. token USB). Con la firma digitale remota la firma viene generata dal certificatore (colui che cioè fornisce la firma digitale all'utente) attraverso altro strumento che as- socia i parametri per l'autenticazione (di solito una serie di 8 numeri) e li comunica sul dispositivo di cui l'utente dispone.

Nel sistema "tipo bancomat" gli svantaggi non sono legati tanto e solo alle dimensioni comunque limitate del supporto, quanto alla necessità che per la lettura della firma e per la sua apposizione necessiti un apposito lettore di quel tipo di card.

Nel sistema "tipo sim card" generalmente inserito in una semplice pennina USB e quindi identica ad essa (tant'è che con essa si dispone di memoria – limitata - utile a salvaguardare documenti foto o musica), il vantaggio è rappresentato dalla sostanziale mancanza di limiti all'utilizzo del supporto (denominato "token") stante la diffusione degli ingressi USB disponibili su moltissimi (pressoché tutti) strumenti elettronici. Vi è di contro l'eventualità (non frequente ma possibile) che il contatto USB possa non essere improvvisamente funzionante (rischio insito nella natura di strumento tecnologico).

Nel sistema "remoto" il vantaggio è rappresentato dalla possibilità di apporre la firma senza neanche necessità di disporre di un computer in quanto il sistema associa. Di contro il profilo di sicurezza aumenta in relazione alla possibilità che il supporto possa essere perso rendendolo così parzialmente utilizzabile anche da soggetto diverso dal suo titolare.

L'assegnazione del certificato di firma digitale (che può essere richiesta da chiunque) viene rilasciato da un soggetto particolare (**il certificatore**) rispondente a livelli di

affidabilità e sicurezza particolarmente elevati ed appositamente annotato nell'apposito registro pubblico gestito dall'AGID (cfr. art. 1 CAD).

La procedura di apposizione della firma digitale è poi molto semplice e richiede il preventivo inserimento del certificato nel lettore o nella presa USB (a seconda della tipologia del token) ed all'inserimento di una password che è consegnata insieme al certificato ma che dovrebbe essere cambiata e personalizzata con un equivalente più affidabile, questo perché la disponibilità della password (la cui cura è affidata obbligatoriamente al titolare di firma) rende possibile applicare la firma digitale ad ogni documento senza possibilità che venga disconosciuta la sua riconducibilità al titolare del certificato e non a chi illecitamente l'abbia utilizzato.

Sul piano squisitamente tecnico/informatico può dirsi che nel momento in cui si appone la firma digitale si realizzano una serie di passaggi che consistono: della creazione di un file, definito "busta crittografica", al cui interno si trovano il documento originale, la c.d.

"EVIDENZA INFORMATICA DELLA FIRMA" (C.D. "*HASH*")

e la chiave per la verifica della stessa che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore.

Nella pratica quindi il documento originale firmato digitalmente avrà queste componenti

1. documento originale;
2. hash (ovverosia una versione ridotta del certificato);
3. firma dell'utente (che contiene pochi dati di riferimento quali il nome e cognome e il codice fiscale);
4. firma del certificatore (che non può che coincidere con il soggetto in tal senso autorizzato e presente ne registri AGID).

STANDARD DI FIRMA (CADES, PADES, XADES)

Sempre sul piano tecnico è utile sapere che così come nella firma analogica la sua apposizione può essere apposta indifferentemente con la penna nera o blu, nella firma digitale si individuano 3 differenti standard europei denominati **CAdES, PAdES e XadES.**

L'apposizione di una di queste firme resta trasparente all'autore che dovrà operare sempre nello stesso modo (l'inserimento delle proprie credenziali) selezionando

preventivamente uno dei tipi di firma. In alcuni casi però è necessario che la firma rispetti uno degli standard richiesti così come accade nel processo telematico laddove mentre in quello civile sono ammissibili tanto le firme Cades quanto quelle Pades, non è così nel processo amministrativo che invece impone l'utilizzo esclusivo del formato Pades).
Anche in questo caso vantaggi e svantaggi.

Il documento firmato **Cades** condurrà all'elaborazione di un nuovo documento che conterrà la sua originaria denominazione (prova.doc) aggiungendovi l'estensione **p7m** (e quindi prova.doc.p7m) che indicherà, per l'appunto, la presenza di una firma digitale e potrà però essere letto con appositi programmi.

Il formato **Pades** è applicabile ai soli file in formato PDF ma, al tempo stesso, il file firmato con questa modalità rimarrà leggibile da qualsiasi programma abilitato alla lettura dei file PDF e con- sentirà (se adeguatamente impostato) anche la verifica sull'esistenza della firma e renderà visibili i dati del suo autore.

Il documento firmato digitalmente potrà essere assoggettato ad una verifica che restituirà i dati anagrafici del firmatario ma, soprattutto, la data di validità del certificato che, una volta scaduto, rende la firma eventualmente apposta come non riconducibile al suo autore.

LA RILEVANZA GIURIDICA DELLA FIRMA DIGITALE

Sul piano giuridico si è detto che il documento sottoscritto con firma digitale ha nel nostro ordinamento piena efficacia giuridica, a condizione che non sia modificato dopo l'apposizione della firma.

Il CAD nella sua ultima versione ha apportato una particolare variazione modificando la sua impostazione iniziale che individuava la presenza di più tipi di documento informatico (firmato o non firmato) ma anche di firme (autografa; elettronica; elettronica digitale; qualificata).

Con la recente revisione del 2016 si è proceduto ad allineare le firme ad un unico criterio valido in tutta Europa e determinante il mutuo riconoscimento tra i vari paesi che ne fanno parte, in osservanza a quanto disposto dal **regolamento eIDAS (articolo 25,3)** a norma di cui ***Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno***

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri (e la firma elettronica indicata nel regolamento corrisponde alla firma digitale italiana).

Viene quindi mantenuta la differenza tra tipologie di firma ma se ne limita la elencazione alle due forme della:

a) **firma elettronica** (generica) realizzabile con qualsiasi strumento (password, PIN, digitalizza- zione della firma autografa, tecniche biometriche, ecc.) pur in grado di conferire un certo li- vello di autenticazione a dati elettronici;
b) **firma elettronica avanzata**, più sofisticata, idonea ad identificare in modo univoco il firmatario, a garantire la visibilità di modifiche intervenute successivamente alla firma digitale apposta.

Può allora dirsi che **a norma dell'art. 21 il documento informatico sottoscritto con firma elettronica ha valore di forma scritta**, con la precisazione che la firma elettronica se **avanzata** conferirà al documento la presunzione di validità assoluta mentre quelle "**semplice**" sarà sottoposta alla libera valutazione del giudice chiamato a decidere sulla sua rilevanza probatoria.

CARATTERISTICHE GENERALI DELLA FIRMA SECONDO LE INDICAZIONI DEL CAD

La sezione dedicata alla firma digitale si completa con l'indicazione delle sue caratteristiche generali elencate nello stesso ordine esposto dalla Legge.

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 di cui all'arti- colo 71, **la validità** del certificato stesso, nonché **gli elementi identificativi del**

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

titolare e del certificatore e gli eventuali limiti d'uso.

4-bis. **L'apposizione** a 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**, **salvo che lo stato di sospensione sia stato annullato**. 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.

REGOLAMENTO EIDAS 1

L'intento di unificare la normativa a livello europeo è stato realizzato mediante l'approvazione del Regolamento comunitario nr. 910/2014 denominato eIDAS (acronimo di "Electronic Identification, Authentication and Trust Services") in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Tale Regolamento si riproponeva di fornire una "base normativa comune sul livello di sicurezza delle interazioni elettroniche e sulla gestione dei servizi elettronici e delle transazioni del commercio elettronico, in sintesi consentire ai cittadini, alle imprese e alle pubbliche amministrazioni di lavorare online in modo sicuro attraverso strumenti di identificazione elettronica riconosciuti in tutti gli Stati membri.

La sua approvazione comporta l'adeguamento di alcune parti del CAD che, ad esempio, nella nuova versione dell'**art. 24 4-ter** sancisce l'efficacia delle firme elettroniche basate su un certificato qualificato anche se **rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea** sia pur subordinandolo ad una serie di condizioni ben definite: a) **il certificatore possiede i requisiti previsti dal regolamento eIDAS ed è qualificato in uno Stato membro**; b) **il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui al medesimo regolamento**; 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.**

Ulteriore aggiornamento interessa l'**art. 25** nella parte in cui attribuisce valenza giuridica **ai sensi dell'articolo 2703 cod. civ. alla firma elettronica o qualsiasi altro tipo di firma elettronica avanzata se autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato**.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

La modalità di attestazione è regolata dal comma 2 e consiste nella dichiarazione 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. Significativo il riferimento ad una delle tradizionali forme della firma che potrà essere assoggettato all'attestazione ove richiesta: **l'acquisizione digitale della sottoscrizione autografa**.

IL CERTIFICATORE

Abrogati gli artt. 26 e 27 con spostamento delle regole che definiscono la figura del **certificatore al successivo art. 28 e prosegue fino all'art. 37 (peraltro abrogato)**, delineando alcune componenti di questo soggetto ma anche del titolare del certificato che, ai sensi dell'**art. 32 impone obblighi del titolare e del prestatore di servizi di firma elettronica qualificata** e precisa che **Il titolare del certificato di firma è tenuto ad assicurare la custodia** del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad **adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri**; è altresì tenuto **ad utilizzare personalmente il dispositivo di firma**.

All'altro soggetto (il certificatore) sono invece destinate una serie di regole a cui attenersi nella fase di svolgimento della sua attività.

Vige, anche per questi, il generale obbligo di **adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi** che parte dalla fase di rilascio del certificato, in cui il certificatore dovrà **provvedere con certezza all'identificazione della persona che fa richiesta** della certificazione (egli è infatti **responsabile dell'identificazione del soggetto che richiede** il certificato qualificato di firma anche se tale attività è delegata a terzi); **rilasciare e rendere pubblico il certificato elettronico; procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico, di perdita del possesso o della compromissione del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma**, di **provvedimento dell'autorità**, di acquisizione della conoscenza di **cause limitative della capacità del titolare**, di **sospetti abusi o falsificazioni**; assicurare la **precisa determinazione della data e dell'ora**

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

di rilascio, di revoca e di sospensione dei certificati elettronici; **non copiare, né conservare, le chiavi private di firma** del soggetto cui il certificatore ha fornito il servizio di certificazione.

L'attività di verifica e controllo sull'operato del prestatore di servizi è affidata ad Agid che attraverso una procedura espressamente regolata (che prevede ovviamente la possibilità audizione del fornitore) può irrogare sanzioni economiche tra 4.000,00 e 40.000,00 euro (fermo restando risarcimento danno) per la violazione delle disposizioni e che si estendono fino all'eventualità che il responsabile venga cancellato dall'elenco dei prestatori di servizi.

REGOLAMENTO EIDAS 2

L'ulteriore aggiornamento del Regolamento eIDAS è contenuto nel c.d. eIDAS 2.0 (UE 2024/1183 dell'11 aprile 2024 ed entrato in vigore a maggio 2024) che mira alla creazione di un sistema unico di identità digitale per tutta l'Unione Europea anche attraverso procedure di gestione e conservazione dei documenti informatici che sotto il vigore della precedente normativa, venivano affidati alla totale autonomia legislativa da parte dei singoli stati membri.

Si tratta di un processo che mira semplificare l'accesso a servizi telematici (prestiti bancari, partecipazione a pubblici concorsi) attraverso l'uso dei **wallet (portafogli) digitali europei** denominati **EUDIW – European digital identity wallet**, e che nell'eliminare barriere tecnologiche, garantirà elevatissimi livelli di sicurezza e protezione dei dati.

Elemento chiave in questa procedura sarà l'utilizzo di **attributi** riepilogativi di qualsiasi informazione legata a una persona (tradizionali nome, età, titolo di studio ma anche livello di merito creditizio o stato di salute) e che al momento sono ripartiti attraverso differenti strumenti (la carta di identità, la patente) ma che potranno essere integrati in un portafoglio digitale, previa certificazione affidata a soggetti specialistici che hanno già a disposizione questi dati (si pensi alle università per il titolo di studio od al medico di famiglia per quel che attiene lo stato di salute).

Questi dati saranno presenti nel wallet di ogni cittadino che li potrà quindi utilizzare alla bisogna.

Ogni Paese membro dovrà predisporre il proprio portafogli entro il 2026. In **Italia** un primo passo è stato realizzato con il D.L. 19/2024 che ha **introdotto l'IT wallet**, necessitante di pervenire al superamento di elementi tecnici e delle procedure di accreditamento dei fornitori che dovranno essere in grado di capire le modalità che consentiranno il concreto adeguamento tecnico alla normativa.

FORMAZIONE GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Con il **capo III** il CAD apre la sezione dedicata alla **formazione, gestione e conservazione dei documenti informatici** che si apre, per l'appunto con l'**art. 40**

espressamente riferito alla **Formazione di documenti informatici già citato in precedenza in queste note e che ribadiscono il concetto generale che impone alle pubbliche amministrazioni la formazione degli originali dei propri documenti**, inclusi quelli inerenti ad albi, elenchi e pubblici registri, **con mezzi informatici** e che secondo si completa con la successiva previsione di cui all'**art. 41. (Procedimento e fascicolo informatico)** che affida alla **gestione dei procedimenti amministrativi delle P.A. all'utilizzo delle tecnologie dell'informazione** e della comunicazione mediante raccolta in un fascicolo informatico di atti, documenti e dati che lo compongono **e che sarà** realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento **e recherà l'indicazione dei seguenti dati:**

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

b) le altre amministrazioni eventualmente partecipanti;

c) il responsabile del procedimento;

d) l'oggetto del procedimento;

e) l'elenco dei documenti contenuti;

e-bis) l'identificativo del fascicolo medesimo.

In questo contesto interviene il disposto dell'**art. 42.**

DEMATERIALIZZAZIONE DEI DOCUMENTI DELLE PUBBLICHE AMMINISTRAZIONI

che affida alle amministrazioni la **valutazione (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**.

La scelta dovrà rispettare le regole tecniche di cui all'art. 71 **al fine di garantire la conformità dei documenti agli originali** e, per come disposto dal **comma 1-bis, se conservato da uno dei soggetti** di cui all'articolo 2 esonera cittadini ed imprese dal conservare gli originali che potranno essere richiesti.

Non manca ovviamente il riferimento alla sorte dei **documenti originali cartacei che potranno essere archiviati nel loro formato originale e conservati in modo permanente**

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

con modalità digitali.

Le disposizioni per la

CONSERVAZIONE

sono indicate all'art. 44 ed impongono un sistema che assicuri:

- l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione;
- **la sicurezza e l'integrità del sistema e dei dati e documenti presenti;**
- **la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;**
- **la raccolta di informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati;**
- **l'agevole reperimento delle informazioni riguardanti i documenti registrati;**
- **l'accesso, in condizioni di sicurezza, alle informazioni del sistema, nel rispetto delle disposizioni in materia di tutela dei dati personali;**
- **lo scambio di informazioni con sistemi di gestione documentale di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi;**
- **la corretta organizzazione dei documenti nell'ambito del sistema di classificazione adottato;**
- **l'accesso remoto, in condizioni di sicurezza, ai documenti e alle relative informazioni di registrazione tramite un identificativo univoco;**

j) il rispetto delle regole tecniche di cui all'articolo 71.

Nel sistema di conservazione digitale a norma assume un ruolo particolare ed importante, sul lato soggettivo, il **responsabile per la gestione e conservazione dei documenti informatici** che opera d'intesa con il dirigente dell'ufficio, il responsabile del trattamento dei dati personali, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici.

L'attività di conservazione richiede il preventivo riconoscimento pubblico dato che, ai sensi dell'**art. 44-bis, i soggetti pubblici e privati che svolgono attività di conservazione** dei documenti informatici e di **certificazione dei relativi processi** anche per conto di terzi (e

che devono avere un capitale sociale non inferiore a 200.000 euro) **chiedono l'accreditamento presso AgID.**

Il **capo IV del CAD** è dedicato alla

TRASMISSIONE INFORMATICA DEI DOCUMENTI

e si apre, anche questa volta, con un principio di carattere generale.

Art. 45 I documenti trasmessi da soggetti giuridici 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.

La stessa norma descrive la **procedura di perfezionamento della trasmissione** che **si intende spedita 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.

P.E.C. (POSTA ELETTRONICA CERTIFICATA)

È il sistema di funzionamento della **Posta Elettronica Certificata (**di seguito **P.E.C.)** regolata dal **d.P.R. 11 febbraio 2005, n. 68** ed a cui il CAD affida il compito di trasmettere telematicamente le comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna (art. 48 CAD) con conseguente equivalenza equivale alla notificazione per mezzo della posta (art. 48 sub 2).

Al pari della notifica ma anche della raccomandata postale **la data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso a mezzo PEC sono – ai sensi dell'art. 48 sub 3) opponibili ai terzi**[1] (sempre che siano eseguite nel rispetto del d.P.R. 68/2005 e delle solite regole tecniche).

Il funzionamento della PEC non differisce più di tanto da quello della posta elettronica ordinaria, consistendo anche essa, al pari di quest'ultima, della trasmissione o della ricezione di un messaggio ad uno specifico account.

[1] **Opponibilità ai terzi** può tradursi nella possibilità che un atto possa produrre effetti sia nei confronti tra le parti che ne hanno dato causa (e questo è scontato) che nei confronti di coloro che non vi hanno partecipato (e questo è appunto il concetto di opponibilità)

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Particolarità afferiscono al sistema di rilascio dell'account di PEC alle modalità pratiche preordinate a darne valenza giuridica ed al suo funzionamento pratico.

Caratteristica peculiare della PEC è la sua esclusiva applicazione sul territorio nazionale italiano. La circostanza comporta ovviamente che, così come funziona, esso non possa garantire la stessa por- tata giuridica oltre il territorio nazionale e che pertanto il particolare valore riconosciuto alla PEC dalla legge italiana (che riconosce ad essa prova dell'invio e della consegna del messaggio) non varrà in altri paesi europei ed extra europei.

L'acquisizione della PEC non si discosta dall'apertura di un indirizzo di posta elettronica ordinaria. Tutti possono cioè diventare titolari di un indirizzo di posta certificata che potrà però essere rilasciata solo dai gestori autorizzati.

Il funzionamento della PEC può essere paragonato ad un servizio postale tradizionale in cui vi è un ufficio (ovviamente virtuale) che riceve, rilascia la ricevuta, consegna e dà la ricevuta di ritorno al mittente.

Il servizio può funzionare solo tra PEC e PEC. Non che il messaggio di PEC non giunga ad un indirizzo di posta ordinaria ma in questo caso esso non porterà con sé gli effetti giuridici che discendono dall'utilizzo di questo sistema.

RICEVUTA DI ACCETTAZIONE E DI CONSEGNA

La procedura prevede quindi che il titolare di una PEC invii ad altra PEC un messaggio (che può ovviamente contenere anche un allegato), ricevendosi immediatamente un messaggio di risposta: la **RICEVUTA DI ACCETTAZIONE** che sostanzialmente null'altro dice che il servizio di PEC del mittente (es. Lextel, Aruba, Poste) ha accettato di procedere alla spedizione del messaggio al destinatario. Ad essa segue la **RICEVUTA DI CONSEGNA** che in questo caso attesta invece che il nostro postino ha consegnato al servizio di PEC del destinatario il nostro messaggio depositandolo nella casella di posta di quest'ultimo.

Questa seconda fase (generalmente le due coincidono temporalmente) è il momento di perfezionamento della trasmissione del messaggio PEC che si intenderà ricevuto dal destinatario proprio nel momento in cui il mittente disporrà della ricevuta di consegna.
Sebbene il funzionamento riproponga quello in uso presso il servizio postale (in cui il postino porta a destinazione quel che al suo ufficio postale è pervenuto da altro ufficio presso cui la

busta è stata depositata) vi è però una differenza che rende la PEC particolare.

Perché la consegna al destinatario si perfezioni non è necessario che questi effettivamente ne abbia visione o apra la casella di posta elettronica e men che meno che egli legga l'eventuale allegato ma sarà sufficiente che il suo "postino" abbia trasmesso la ricevuta di consegna al destinatario perché è in quel momento che il messaggio si intenderà ricevuto.

UTILITÀ E PROBLEMATICHE CONNESSE ALL'USO DELLA P.E.C.

Da questa procedura derivano una serie di vantaggi ma anche di incertezze.

Premessa l'equiparazione della PEC alla raccomandata postale con ricevuta di ritorno, può dirsi che il sistema presenti un vantaggio sul piano economico dato che al di là del costo (risibile) annuale per il mantenimento della PEC la trasmissione è assolutamente gratuita e con essa può viaggiare una serie di formati dei più vari (es. documenti, fotografie, messaggi vocali) senza che il peso dell'allegato influisca sul costo della spedizione, così come avverrebbe se ci si rivolgesse al servizio postale ordinario.

Trasmissione e ricezione della PEC può essere eseguita in ogni ora del giorno senza sottostare agli orari di funzionamento dell'ufficio e, allo stesso modo, la sua trasmissione ma anche la sua lettura prescinde dalla disponibilità di un computer perché potrà essere ricevuta sul cellulare o sul tablet o su un computer portatile.

La ricezione è immediata e quindi non esiste l'obbligo di compiuta giacenza altrimenti richiesta per la consegna con il servizio postale tradizionale (si consideri che peraltro è alla PEC che è affidata anche la possibilità di notificare atti giudiziari e non solo posta)

Diminuisce l'ipotesi del rifiuto volontario del messaggio nel senso che se si è titolari di una PEC a quell'indirizzo io potrò trovarti senza che – come accade per la posta elettronica – la spedizione debba perfezionarsi con la consegna al portiere o ad un altro che convive con il destinatario.

L'intero percorso del messaggio resta tracciato presso il fornitore che ha l'obbligo di trattenere presso di sé per un certo tempo (30 mesi) il log (gli eventi associati a invii e ricezioni).

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Meno frequente (sia pure in linea di principio) è la sicurezza del messaggio dato che è a carico del fornitore l'obbligo di garantire il rispetto delle misure di sicurezza previste dal Codice dei dati per- sonali e la sicurezza della comunicazione evitando che possano viaggiare nelle linee della PEC an- che virus digitali.

Di contro la PEC si espone a suoi **limiti** in qualche modo congeniti.

In primo luogo il fatto – di cui si è già detto – che la PEC è qualcosa di esclusivamente italiano. Essa non è riconosciuta come standard internazionale e quindi il suo valore giuridico (è uguale alla raccomandata) non può essere riconosciuto al di fuori del nostro Paese.

Se dal lato mittente c'è indubbiamente il vantaggio di perfezionare immediatamente la spedizione e la ricezione, dal lato destinatario vi è l'obbligo di tenere sempre sotto controllo l'account di posta certificata in quanto che nei suoi confronti il perfezionamento sarà contestuale al rilascio della ricevuta di consegna e quindi sarà il caso che controlli quotidianamente se è arrivata posta.

Non si trascuri di considerare come il sistema di PEC sia ormai utilizzato nel processo civile, nel processo amministrativo e nel processo tributario con l'effetto che eventuali decorrenze di termini inizieranno a scadere dal momento in cui giungeranno alla casella di posta certificata del destinatario.

La PEC richiede una certa attenzione (sia pure ordinaria) perché la cancellazione del messaggio dal server del fornitore rende non più recuperabile il messaggio. È pur vero che c'è l'obbligo di conservazione dei log da parte del fornitore ma questo non significa avere a disposizione l'intero messaggio di posta che sia stato inavvertitamente cancellato.

In un contesto informatizzato è scontato che si predisponga un sistema idoneo ad assicurare la massima sicurezza ai dati ma anche alla loro disponibilità.

È quel che viene disposto all'**art. 51, dedicato, per l'appunto, alla SICUREZZA DEI DATI, DEI SISTEMI E DELLE INFRASTRUTTURE DELLE PUBBLICHE AMMINISTRAZIONI.**

Esso si sviluppa mediante la predisposizione di un Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica che viene attuato da AgID in raccordo con le altre autorità competenti

in materia e mira ad assicurare, tralaltro, la **custodia ed il controllo dei documenti informatici delle pubbliche amministrazioni 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**.

È in questa sezione del CAD che viene normato il profilo più innovativo della informatizzazione della pubblica amministrazione informatizzata

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

I DATI APERTI (OPEN DATA)

Il concetto di dato aperto è ben sintetizzato nella norma citata e si riferisce a **dati e documenti pubblicati dalle amministrazioni senza l'espressa adozione di una licenza e che si intendono quindi 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**.

Rimandando per il momento alla definizione di dato aperto, si indirizza l'attenzione del lettore sull'elemento qualificativo dei dati che, salve le eccezioni richiamate nell'ultima parte (... *motivata ai sensi delle linee guida nazionali…*), impongono l'utilizzo di **dati privi di licenza.**

Non è un caso che la parte introduttiva del corso di informatica giuridica sia stata dedicata, tralaltro, all'illustrazione del concetto di licenza che proprio qui (oltre che in ambito privatistico) trova la sua piena attuazione.

I dati pubblicati dalla P.A. devono quindi essere privi di alcuna licenza. La scelta ha un fine ben preciso: rendere il dato utilizzabile e riutilizzabile da tutti senza necessità cioè di disporre di un preciso programma proprietario che ne limiti la disponibilità.

È anche in relazione all'accesso ai dati pubblicati della P.A. che si impone anche il rispetto di alcuni requisiti ai **siti internet degli enti pubblici**.

In tal senso **l'art. 53 del CAD** prevede il rispetto di principi di accessibilità, elevata usabilità e reperibilità. Il sito, in definitiva, deve essere facile da usare ed i suoi contenuti completi e facili da reperire anche da parte dei portatori di disabilità.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Anche in questo caso le regole tecniche di cui all'art. 71 contribuiscono a meglio determinare la portata dell'obbligo di legge.

Tra le disposizioni successive del CAD vi sono alcuni aspetti apparentemente significativi anche se consistenti di interventi non realizzati o mal realizzati.

È un esempio quello di cui all'**art. 62** dedicato alla

COSTITUZIONE DELL'ANAGRAFE NAZIONALE DELLA POPOLAZIONE RESIDENTE (ANPR).

Si tratta, in particolar modo, di una banca dati nazionale destinata ad accogliere le anagrafi comunali in modo da rendere disponibili dati, atti e strumenti per lo svolgimento delle loro attività istituzionali.

Il condizionale sarebbe stato giustificato dai risultati della prima tornata di acquisizione dei relativi dati che alla data del 21 marzo 2017 annoveravano un numero limitato di comuni (3 ed anche piccolissimi) che avevano completato il subentro e 240 quelli che avevano appena iniziato i propedeutici al subentro.

Il dato è però significativamente aumentato di recente (complice l'utilizzo dei sistemi telematici imposti dall'emergenza sanitaria) ed a novembre 2022 restituiscono un risultato di tutto rispetto (68.009.849 cittadini presenti in ANPR.

ANPR avrebbe dovuto costituire anche un sistema integrato idoneo a consentire ai Comuni di svolgere i servizi anagrafici ma anche di consultare o estrarre dati, monitorare le attività, effettuare statisti- che in maniera più rapida perché permetterà di evitare duplicazioni di comunicazione con le Pubbliche Amministrazioni; garantire maggiore certezza e qualità al dato anagrafico; semplificare le operazioni di cambio di residenza, emigrazioni, immigrazioni, censimenti, e molto altro ancora.

Nuove però le problematiche che si addensano sulla effettiva utilità in relazione ad una circolare (115 del 31 ottobre 2022) con la quale il Dipartimento per gli Affari Interni e Territoriali del Ministero degli Interni ha precisato che "*è esclusa la possibilità per il richiedente di acquisire, accedendo alla piattaforma ANPR con la propria identità digitale, certificati relativi a soggetti terzi*".

Trattasi di fatto di una incoerente visione di quel che è tradizionalmente possibile mediante il ricorso al sistema tradizionale esperibile presso gli uffici d'anagrafe dei Comuni italiani e

preclude invece il più comodo ma anche meno impegnativo sistema introdotto dall'attivazione dell'ANPR.

Di fatto quindi, mentre è possibile chiedere ad un Comune il certificato di anagrafe di un terzo (a patto di conoscere la data di nascita) la stessa operazione non è invece esperibile con modalità telematiche.

Difficilmente comprensibile il fondamento della circolare anche in considerazione del fatto che seppur costituenti dati personali, essi sono e rimangono di conoscenza pubblica e quindi esposti a quella disponibilità che pare incompatibile con le ragioni esposte dal Ministero ("…*impatto ed implicazioni, rischi per i diritti e la libertà degli interessati*…" e della presenza di dati di minori).

Più comprensibili piuttosto le ragioni sottostanti al rigetto della richiesta di convenzione per l'utilizzo del servizio ANPR, che il Ministero riconduce all'approfondimento di specifiche indagini sui sistemi degli enti che avevano inoltrato quelle richieste e che sembrerebbero non essere in regola con i criteri di sicurezza informatica più adeguate. La ragione, ancorché compatibile con lo spiegato diniego alle convenzioni, lascia impregiudicato il motivo della accessibilità tramite i sistemi istituzionali che quei criteri di sicurezza devono obbligatoriamente rispettare.

Per favorire poi la diffusione dei servizi in rete e agevolare l'accesso ad essi è istituito, a norma dell'**art. 64 CAD il**

SISTEMA PUBBLICO PER LA GESTIONE DELLE IDENTITÀ DIGITALI (PIÙ SEMPLICEMENTE SPID).

SPID permette di accedere a tutti i servizi online della Pubblica Amministrazione (es. prenotazioni sanitarie, iscrizioni scolastiche, accesso alla rete wi-fi pubblica) con un'unica Identità Digitale (username e password) con un sistema che prescinde dalla disponibilità di uno strumento ulteriore (come avviene per la funzione di autenticazione offerta dalla firma digitale) ma è facilmente utilizzabile anche mediante tablet o smartphone.

SPID è il nuovo sistema di login che permette a cittadini e imprese di accedere con un'unica identità digitale, da molteplici dispositivi, a tutti i servizi online di pubbliche amministrazioni e imprese aderenti.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

L'uso dello SPID si caratterizza dal superamento del legame a password, chiavi e codici e si bada su un sistema di credenziali con caratteristiche differenti in base al livello di sicurezza richiesto per l'accesso.

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

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

Per ottenere un'identità SPID l'utente deve farne richiesta al gestore che preferisce (anche in questo caso il fornitore del servizio è individuato nell'apposito registro nazionale) e che, dopo aver verificato i dati del richiedente, emette l'identità digitale rilasciando le credenziali all'utente.

L'uso dello SPID ha ricevuto una definitiva estensione dall'attuazione della L. 11 settembre 2020, n.120, che ha reso efficaci le disposizioni del decreto "Semplificazione e innovazione digitale" mirando ad incrementare quel passaggio (che si è detto non sempre lineare) verso un'unica identità digitale e valida in ogni sede degli stati membri aderenti alla Comunità europea.

Dalla data del 1 ottobre 2021 l'accesso ai siti delle amministrazioni pubbliche è possibile solo attraverso i servizi digitali con SPID e Carta d'Identità Elettronica con conseguente abbandono delle tradizionali procedure che associano l'accesso all'accoppiata username-password per ognuno di detti servizi.

I SERVIZI IN RETE DELLA P.A.

L'**art. 64 bis** del CAD sembrerebbe orientato a rendere praticamente esecutivo quel generale principio che vuole le Pubbliche amministrazioni disponibili ad intrattenere rapporti mediante i sistemi telematici, sancendo un principio ben chiaro: **I soggetti di cui all'articolo 2, comma 2, rendono fruibili i propri servizi in rete, in conformità alle regole tecniche di cui all'articolo 71, tramite il punto unico di accesso telematico attivato presso la**

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Presidenza del Consiglio dei ministri, senza nuovi o maggiori oneri per la finanza pubblica.

Il principio viene meglio delineato nell'art. successivo (**art. 65**) intitolato

ISTANZE E DICHIARAZIONI PRESENTATE ALLE PUBBLICHE AMMINISTRAZIONI PER VIA TELEMATICA

e che, altrettanto chiaramente prescrive che "***Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministra-zioni e ai gestori dei servizi pubblici ai sensi dell'articolo 38, commi 1 e 3, del d.P.R. 28 dicembre* 2000, n. 445[2],** sono valide:

- ***a)*** se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore qualificato;
- ***b)*** ovvero, **quando l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID)**, nonché attraverso uno degli altri strumenti di cui all'articolo 64, comma 2-novies, nei limiti ivi previsti;
- ***c)*** ovvero sono sottoscritte e presentate unitamente alla copia del documento d'identità;

c-bis) ovvero ***se trasmesse dall'istante o dal dichiarante 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*** *…*"

La rilevanza dei principi che precedono viene assistita dall'attuazione di un sistema sanzionatorio che colpisce di **responsabilità dirigenziale e disciplinare il titolare dell'ufficio competente nel caso** in cui non venga dato corso al procedimento attivato con istanza o dichiarazione inviate ai sensi e con quelle modalità (art. 65 1-ter).

È anche a questo fine che vengono preventivate strutture preordinate ad agevolare il rapporto con l'amministrazione e, tra esse, la

CARTA D'IDENTITA' ELETTRONICA E LA CARTA NAZIONALE DEI SERVIZI

predestinata ad essere utilizzate per l'autenticazione del soggetto che voglia usufruire dei ser- vizi forniti dalle pubbliche amministrazioni.

---

[2] **Art. 38 d.P.R. 28 dicembre 2000, n. 445** – Modalità di invio e sottoscrizione delle istanze

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

LA CARTA D'IDENTITÀ ELETTRONICA

può ritenersi come una elaborazione anche grafica del corrispondente cartaceo (che continua ad esistere) ma se ne differisce sia per la presenza di alcune componenti di sicurezza (ologrammi, sfondi di sicurezza, micro scritture) che per l'incorporazione di un chip anch'esso di sicurezza per la protezione dei dati anagrafici che dentro sono memorizzati ma soprattutto destinato a consentire l'autenticazione in rete da parte del cittadino che voglia ac- cedere ai servizi della pubblica amministrazione.

Una serie di difficoltà di carattere tecnico (la prima versione era destinata a sfaldarsi pressoché immediatamente) i tempi lunghi (comunque non immediati) per richiederlo e conseguirla e, per- ché, anche i costi superiori rispetto alla carta tradizionale non hanno agevolato lo sviluppo della carta d'identità elettronica che, a marzo 2017 risulta acquisita da 300 mila cittadini di 199 Comuni.

Garantisce un livello di sicurezza elevato (c.d. "sicurezza 3") e viaggia oggi di pari passo con lo SPID. Questo costituisce – come detto in precedenza - la chiave unica di accesso ai servizi pubblici, men- tre la Carta d'Identità Elettronica (CIE) certifica l'identità" ma nelle previsioni quest'ultima, se dotata di pin, dovrebbe consentire l'accesso ai medesimi servizi consentiti dall'uso dello SPID.

LA CARTA NAZIONALE DEI SERVIZI

è il documento con il quale ogni Ente erogatore di servizi assume una serie di impegni nei confronti della propria utenza riguardo i propri servizi, le modalità di erogazione, gli standard di qualità e l'informativa sulle modalità di tutela previste.

Il suo utilizzo è rimesso alla disponibilità di una smartcard ma anche di una chiavetta USB contenenti il certificato di firma digitale e consente di accedere ai servizi online della Pubblica Amministrazione.

La finalità di autenticazione mediante CNS esperita mediante il certificato di firma digitale dovrebbe, nelle intenzioni del legislatore, perdere questo carattere in favore dell'uso dello SPID ma sia l'una che l'altra resta affidata alla diffusione del sistema e, soprattutto, all'adesione degli enti ed all'erogazione dei servizi.

Si è detto delle indicazioni genericamente destinate ad assicurare un utilizzo

ragionato del software all'interno della pubblica amministrazione, prevalentemente fondato sulla convenienza economica.

Il principio viene regolamentato al **Capo VI** dedicato, per l'appunto, allo

SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI

e meglio specificato all'**art. 68** quale indicazione dedicata alla **fase di acquisizione di programmi informatici o parti di essi e da operarsi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica** e **previa la valutazione comparativa di tipo tecnico ed economico** tra diverse soluzioni:

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**; c-bis) software **fruibile in modalità cloud computing**; d) software **di tipo proprietario mediante ricorso a licenza d'uso**; e) **combinazione** delle precedenti soluzioni.

Sulla scorta di queste linee guida l'amministrazione pubblica, prima di prima di procedere all'acquisto, viene richiesta all'effettuazione di una serie di valutazioni comparative delle diverse soluzioni disponibili sulla base di diversi criteri:

- costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;
- 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;
- 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.

È solo nel caso in cui questa valutazione riveli l'impossibilità (che la pubblica amministrazione dovrà motivare) di accedere ad una delle soluzioni **è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso**.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

È in questa fase che può essere attuata anche una sorta di collaborazione tra le varie amministrazioni e tali che se una ha fatto realizzare soluzioni e programmi informatici su sue specifiche indicazioni essa dovrà obbligatoriamente rendere pubblico e gratuito il sorgente per fare in modo che anche altre pubbliche amministrazioni o soggetti privati possano utilizzarle.

FORMATO DEI DATI DI TIPO APERTO

È in questo capo del CAD che si rinviene l'esatta definizione di dati aperti di cui si era letto nel con- testo dell'art. 52 e che vengono così descritti dall'**art. 68 comma 3**.

Si intende 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.

Sono intesi **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 soggetti giuridici, anche per finalità commerciali, in formato disaggregato** (ovverosia separatamente dall'elenco in cui essi sono contenuti. Potrò cioè utilizzare soltanto la parte che mi interessa dei dati e dovrò essere in condizione di farlo)

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.

L'accesso fa riferimento evidentemente a reti come internet in cui questi dati devono essere resi disponibili per come disposto da altre leggi come ad esempio quelle sull'anticorruzione.

Per **metadato** deve intendersi letteralmente un'informazione resa sotto forma di struttura in modo che la ricerca delle informazioni sia più efficace ed anche rapida.

Un esempio può aiutare in questo senso mediante riferimento al catalogo di una biblioteca. Nel catalogo ci sono ulteriori informazioni (il contenuto, la posizione di un libro) che consentono una ricerca più rapida (ovverosia se il dato esiste e dove esso si trovi, modalità che ne agevolino l'individuazione; indicazione sulla sua effettiva disponibilità).

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

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** fatta salva l'eventualità che per motivi specifici possano essere individuate tariffe superiori ai costi marginali.

Il **Capo VII** del CAD sembrerebbe dedicato alla sezione più rilevante del codice stesso in quanto vi è una miriade di norme che rimandano **alle**

REGOLE TECNICHE INDICATE ALL'ART. 71

Rimarrà disilluso quindi chi si troverà a leggere il contenuto della norma citata che così recita:

1. Con decreto del Ministro delegato per la semplificazione e la pubblica amministrazione, su proposta dell'AgID, di concerto con il Ministro della giustizia e con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e il Garante per la protezione dei dati personali nelle materie di competenza, sono adottate le regole tecniche per l'attuazione del presente Codice.

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."

Può quindi dirsi che, anche in questo caso, l'art. 71 ancorché componente determinante per la piena attuazione del CAD, consista di fatto in un precetto comprensivo di principi, di criteri e requisiti non immediatamente determinati (e quini non operativi) e richiedente, per la loro applicazione pratica, l'intervento politico/governativo, quel decreto ministeriale destinato a fissare, per tutti casi in cui viene imposto il rinvio alle regole tecniche, lo specifico contenuto di quelle regole.

Il rischio che questo intervento manchi di organicità è sussistente e comprensibilmente sentito da - gli studiosi della materia in quanto, in mancanza di un testo unico che riunisca la variegata congerie di discipline da regolamentare e le "regoli" in maniera univoca è ipotizzabile una serie di provvedimenti scollegati tra di loro e caoticamente coesistenti.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE (2.a parte)

INDICE

Dovrà essere una procedura che muova dalla posizione del destinatario del CAD che non è certo solo e soltanto la Pubblica amministrazione ma il cittadino, il professionista, le imprese rendendo concretamente utilizzabile il sistema di interazione con gli strumenti telematici.

Si dovrà lavorare di interventi mirati alla diffusione delle nuove tecnologie e, ancor di più, all'alfabetizzazione del cittadino.

Dovrà evitarsi che, per il sol fatto di dover provvedere alla predisposizione dei regolamenti si creino incertezze e dubbi in una materia che, a dire il vero, semplice e di immediata percezione non lo è tra gli operatori del settore, le pubbliche amministrazioni e anche i cittadini e che non gradirebbero quindi tecnicismi normativi non facili da comprendere.