DOCUMENTI INFORMATICI E FIRME ELETTRONICHE

Marco Mancarella

- Documento informatico e firme elettroniche

Il Codice dell'Amministrazione Digitale definisce il documento informatico all'articolo 1, comma 1, lett. p), come: "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Per "atto", in diritto, si deve intendere un fatto consistente in un comportamento umano rilevante per l'ordinamento giuridico, poiché volontario. Elemento costitutivo è dunque l'imputazione a un soggetto di diritto, che può essere la persona fisica che ne ha voluto l'accadimento o la persona giuridica per la quale detta persona fisica ha agito in qualità di organo, nonché la volontarietà che, a sua volta, implica la consapevolezza da parte di chi ha agito, ossia la sua capacità di comprendere e, quindi, liberamente volere. Esempi sono da considerarsi il testamento, la sentenza, il contratto, l'atto amministrativo.

Per "fatto" si deve intendere un accadimento che avviene nella realtà materiale ("fatto naturalistico") e non si concretizza in un comportamento umano. Se il fatto è considerato all'interno di una norma, allora il suo verificarsi diviene rilevante per l'ordinamento ("fatto giuridico"). E' lecito affermare che tutti i fatti giuridici sono altresì fatti naturalistici, mentre non è vero il contrario. Un esempio di fatto giuridico è il decorso del tempo.

Per "dato" si deve intendere una descrizione elementare, spesso codificata, di un'entità, di un fenomeno, di una transazione, di un avvenimento o di altro. Nasce dall'osservazione di aspetti e fenomeni elementari; esso permette di effettuare dei calcoli, risolvere un problema, caratterizzare un fenomeno o esprimere un'opinione. Il dato può divenire "informazione" per un soggetto solo se comporta un reale aumento di conoscenza.

Tale definizione è il frutto delle evoluzioni che si sono a lungo susseguite in questa materia, a partire dal D.P.R. n. 531/1997, e costituisce il punto centrale attorno a cui ruota gran parte del Codice e che, da ultimo, è stato oggetto della incisiva azione della normativa europea, con il **Regolamento del Parlamento e del Consiglio del 23 luglio 2014 n. 910, cd. Regolamento eIDAS (electronicIDentificationAuthentication and Signature)**. Risulterebbe difficile, in effetti, poter parlare di Pubblica Amministrazione digitale senza che la parte più corposa e rilevante della sua attività (vale a dire la formazione, la trasmissione e la conservazione della documentazione amministrativa) sia realizzata in forma elettronica.

Sul punto occorre però precisare che **l'introduzione della locuzione "documento elettronico" nella definizione del C.A.D. di "documento informatico"** (presente nel nostro ordinamento sin dagli anni '90 del secolo scorso) è stata essenzialmente dovuta alla necessità di **assolvere al Regolamento eIDAS** che, appunto, non definisce i documenti informatici ma quelli elettronici. In futuro tale riferimento all'elettronica potrebbe perdere di necessità e vigore, data la possibile realizzazione di computer quantici (o quantistici), volti quindi ad utilizzare i quanti e non gli elettroni, come già da tempo preannunciato da Google: ciò porterà all'abbandono del documento elettronico in favore del documento quantico.

Al di là delle doverose puntualizzazioni sull'introduzione della locuzione "documento elettronico", l'intero concetto di Amministrazione Digitale ruota di fatto intorno a quella che viene chiamata **"rappresentazione informatica"** e può essere definita non solo come il risultato della trasformazione in bit, e successiva memorizzazione su supporto informatico, di quegli atti, fatti o dati che possano avere rilevanza giuridica, ma anche come il contenuto elettronico vero e proprio, a prescindere da quale che sia la sua genesi.

Per cui "documento informatico" può essere **un file di testo, una foto, un video, un audio, che rappresenti informaticamente o conservi elettronicamente un atto, un fatto o un dato rilevanti giuridicamente.**

Il Regolamento eIDAS, infatti, dal canto suo, definisce "documento elettronico", qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Il C.A.D. dedica l'intero Capo II alla disciplina del documento informatico e delle firme elettroniche mentre il Regolamento eIDAS dedica il capo IV al documento elettronico e la sez. IV del capo III alle firme elettroniche (artt. 25-34)

Una volta stabilita la rilevanza giuridica del documento informatico-elettronico, è venuta meno la necessità di prevederlo espressamente.

La Sezione II del Capo II del C.A.D. è interamente dedicata alle firme elettroniche ed ai certificatori.

Volendo semplificare l'esposizione, per donare al lettore un facile quadro di riferimento, è possibile dire che il C.A.D. distingue due macro-categorie di firme:

1. **la firma elettronica (semplice**), definita nel Regolamento eIDAS(art. 3, comma 1, n. 10) come quei "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare";
2. **la firma elettronica avanzata(FEA)**, definita nel Regolamento eIDAS(art. 3, comma 1, n. 11) come "una firma elettronica che soddisfi i requisiti di cui all'articolo 26, ossia: a) è connessa

unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati";

- **la firma elettronica qualificata (FEQ)**, definita nel Regolamento eIDAS(art. 3, comma 1, n. 12) come "una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche";
- **la firma (qualificata) digitale**, definita nel C.A.D.(art. 1, comma 1, lett. s) come "un particolare tipo di firma qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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".

Le firme elettroniche di un documento informatico, e in particolare le firme elettroniche avanzate e qualificate, tra cui quella digitale, si propongono di soddisfare tre esigenze che non tutte le tipologie di firma elettronica però soddisfano:

- che il destinatario possa verificare l'identità del mittente **(autenticità)**;
- che il mittente non possa disconoscere un documento da lui firmato **(non ripudio)**;
- che il destinatario non possa inventarsi o modificare un documento firmato da qualcun altro **(integrità)**.

Volendo ora procedere alla disamina delle singole tipologie di firma elettronica e partendo da quelle più basilari, sotto il profilo pratico la categoria delle firme elettroniche semplici può essere definita come una **categoria residuale**, nella quale confluiscono tutte le tipologie di firma che non detengono caratteri tali da configurarle come firme avanzate. Un classico esempio di scuola di firma elettronica semplice è quello della firma elettronica contenuta in una normale email: le credenziali di accesso riconosciute dal fornitore del servizio, infatti, integrano gli estremi di una firma elettronica semplice e, nella normalità dei casi, non di una firma avanzata.

L'art. 26 del Reg. eIDAS, a sua volta, stabilisce che una firma può essere considerata avanzata se:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Con il **Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 dal titolo "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali"** le firme avanzate hanno trovato una precisa regolamentazione tecnica nel nostro ordinamento, che produrrà i suoi effetti sino all'approvazione delle prossime Regole tecniche del C.A.D. (nella forma di Linee guida AgID, come da D.Lgs. n. 217/2017).

Come su evidenziato, all'interno della categoria delle firme elettroniche avanzate è possibile distinguere un altro gruppo di firme aventi caratteristiche di particolare importanza, ovvero le **"firme qualificate"**, definite tali in quanto rilasciate da un **certificatore accreditato presso l'Agenzia per l'Italia Digitale**. Nella realtà pratica, i certificatori accreditati sono soggetti pubblici o privati che emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).

Tra le firme qualificate, grande importanza occupa la **"firma digitale"**, la quale è un **particolare tipo di firma qualificata basata 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 (differenziando per struttura le firme digitali, possiamo avere: CADES, apponibile a qualsiasi formato di file e ne modifica l'estensione rendendolo .p7m; PADES, apponibile solo sui file PDF e non modifica l'estensione; XADES, apponibile solo sui file XML e non modifica l'estensione). Quindi, le sue **caratteristiche tecniche più importanti** sono:

- la chiave pubblica (contenuta nel certificato qualificato);

- la chiave privata (custodita dal mittente).

In altre parole, il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra: da questa asimmetria nasce anche la definizione del meccanismo come "**crittografia asimmetrica**".

Affinché il sistema risulti sicuro, è necessario che solo l'utente che intende crittare il documento, e nessun altro, abbia accesso alla chiave privata: l'unica copia della chiave deve essere "in mano" all'utente, che deve impedirne l'accesso a terzi. Vi sono, però, soluzioni alternative, come l'uso di una "**firma digitale remota**", ovvero una tipologia di firma digitale, accessibile via Rete (Intranet e/o Internet), nella quale la chiave privata del firmatario viene conservata assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM - Hardware Security Module) da parte di un certificatore accreditato. Il firmatario viene identificato dal servizio e autorizza l'apposizione della firma tramite un meccanismo di sicurezza fra i quali:

- PIN firma di tipo statico, ovvero un codice numerico che consente l'uso di dispositivi elettronici solo a chi ne è a conoscenza;
- token OTP, ovvero un sistema che genera una password valida solo per una singola sessione di accesso o transazione;
- riconoscimento grafometrico della firma autografa;
- telefono cellulare (come OTP) seguito da PIN firma.

Il **meccanismo di firma digitale** è semplice, riassumibile nelle seguenti fasi:

a. l'utente, avviando lo strumento di firma digitale sul proprio computer, ricava innanzitutto **l'impronta digitale** del documento con l'ausilio di una **"funzione hash"** (pubblica), detta anche messagedigest: l'impronta digitale si concretizza in un file di dimensioni relativamente piccole (128, 160 o più bit), che contiene una sorta di codice di controllo relativo al documento stesso; la funzione hash è fatta in modo da rendere minima la probabilità che da testi diversi si possa ottenere il medesimo valore dell'impronta, inoltre, è one-way, a senso unico, questo significa che dall'impronta è impossibile ottenere nuovamente il testo originario, quindi questa è "non invertibile";

b. l'utente utilizza, poi, la propria **chiave privata per cifrare l'impronta digitale**: il risultato di questa codifica è la firma; la firma prodotta dipende dall'impronta digitale del documento e, quindi, dal documento stesso, oltre che dalla chiave privata dell'utente;

c. a questo punto **la firma viene allegata al documento** che si intende sottoscrivere, insieme alla chiave pubblica;

d. il destinatario del documento su cui è apposta una firma digitale può verificarne l'autenticità: per farlo, **decifra la firma del documento con la chiave pubblica del mittente**, ottenendo l'impronta digitale del documento, e quindi **confronta quest'ultima con quella che si ottiene applicando la funzione hash** al documento ricevuto; se le due impronte sono uguali, l'autenticità e l'integrità del documento sono garantite; si tratta, in realtà, di un'operazione sostanzialmente automatica svolta dal computer, quindi pressoché immediata e semplice da realizzare per il destinatario, previa installazione sul proprio device del software di verifica, scaricabile gratuitamente dal sito dell'Agenzia per l'Italia Digitale (AgID).

Nel loro uso combinato, dunque, le due chiavi servono a garantire e a verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

La firma digitale rappresenta l'equivalente elettronico della tradizionale firma autografa su carta ed è univocamente associata al documento elettronico sul quale è apposta, attestandone con certezza, l'integrità, l'autenticità, la non ripudiabilità.

L'utilizzatore di firma elettronica qualificata o di firma (qualificata) digitale deve prestare particolare attenzione ai casi di scadenza temporale del proprio certificato di firma, di revoca o sospensione dello stesso. Infatti, l'apposizione di una firma digitale con **certificato scaduto, revocato o sospeso equivale a mancata sottoscrizione**. È ciò che stabilisce **l'art. 24 comma 4-bis** del C.A.D., prevedendo per la validità della sottoscrizione l'utilizzo di un certificato qualificato in corso di validità, attraverso il quale si possano rilevare gli elementi identificativi del titolare e del certificatore. Normalmente il certificato di firma digitale, rilasciato dall'ente certificatore, ha una durata biennale e o triennale.

Nel caso in cui il certificato di firma digitale sia scaduto, è necessario rivolgersi al proprio ente certificatore al fine di procedere al **rinnovo, oppure dotarsi di nuovo certificato** presso uno dei soggetti abilitati dall'Agenzia per l'Italia Digitale.

Revoca o sospensione del certificato hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che di essa ne erano già a conoscenza tutte le parti interessate.

Per quanto attiene alla validità nel tempo di firme qualificate o digitali il cui certificato sia scaduto, revocato o sospeso, in base all'art. 62, comma 1, delle citate Regole tecniche del 2013 sulle firme avanzate **sono comunque da ritenersi valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato**. Detto in altre parole, gli odierni sistemi di firma digitale evidenziano, nella loro normalità, il campo signing time (momento della firma), inserendo in automatico data e ora di sottoscrizione nella busta crittografica della firma qualificata o digitale: tale indicazione di data e ora può essere ritenuta un riferimento temporale, considerando quest'ultimo come "l'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento" (Regole tecniche sul documento informatico – DPCM 13 novembre 2014). Riassumendo, **se il riferimento temporale generato dal meccanismo di firma qualificata o digitale è anteriore alla data e ora di scadenza, revoca o sospensione del certificato allora la firma detiene comunque validità nel tempo**.

Tra gli altri processi comunemente in grado di attribuire un riferimento temporale occorre citare, in base all'art. 41 del DPCM 22 febbraio 2013: le marche temporali, la segnatura del protocollo informatico, la conservazione digitale o l'utilizzo di PEC.

Una volta descritto il quadro delle firme elettroniche, anche nell'ottica comparativa con le firme analogiche, possiamo passare a descrivere le diverse ipotesi che si possono incontrare in base al tipo di firma elettronica apposta al documento informatico.

Occorre distinguere due situazioni tra loro differenti, ossia:
- **l'efficacia probatoria** del documento informatico;
- la sua capacità di soddisfare il **requisito della forma scritta**.

- Efficacia probatoria e requisito della forma scritta

Per quanto riguarda **l'efficacia probatoria** del documento informatico, essa è da intendersi come **la "forza" che determinati documenti hanno come prova di un fatto una volta assunti in un processo**; pertanto, è la capacità di quei determinati atti di provare il loro contenuto.
Volendo ora affrontare la questione del **requisito della forma scritta** di un documento, primariamente occorre sottolineare come la rappresentazione di un atto, fatto o dato può avere diverse forme (modalità di rappresentazione): scritta, orale, attraverso segnali ottici o sonori, ed altre ancora. La forma scritta, pertanto, è solo una delle possibili, visto il **principio di libertà delle forme** previsto nel nostro ordinamento, ma detiene una valenza fondamentale, perché solo ad essa, e quindi per esemplificare non ad un documento orale, è possibile riconoscere un particolare valore in determinate circostanze.
La forma scritta è posta soprattutto a tutela di una o di entrambe le parti in un rapporto negoziale (come un contratto), poiché serve ad attirare l'attenzione dei contraenti rispetto all'atto che stanno per compiere ed alla sua importanza. Inoltre, con l'atto scritto si certifica la volontà delle parti e si agevola la prova della sua esistenza.
Normalmente la forma scritta si riconduce nel nostro ordinamento a due concetti:
a) forma scritta **ad substantiam**("ai fini della sostanza"), richiesta per l'**esistenza** stessa del negozio (come per es. per un contratto di compravendita di una casa);
b) forma scritta **ad probationem**("ai fini della prova"), richiesta solo per **provare l'esistenza** del negozio giuridico (come per es. per un contratto di agenzia): nella generalità dei casi, un negozio giuridico può essere provato in giudizio mediante qualsiasi mezzo (ad es. mediante testimoni), accade però, che, in talune ipotesi, la legge, con disposizioni espresse, stabilisca che possa esser provato in giudizio solo mediante documenti, ossia per mezzo di atti aventi forma scritta; è necessario sottolineare che il negozio mancante della forma ad probationem è perfettamente valido ed efficace, ma, in caso di processo, l'unico modo per provare l'esistenza di quel particolare negozio sarà la forma che la legge richiedeva, salva la possibilità di ottenere una **confessione** (disciplinata dagli artt. 2730 e 2735 c.c..) o un **giuramento**(disciplinato dall'art. 2739 c.c..) in giudizio.

I privati possono convenzionalmente prevedere per i loro atti determinate forme, come nel caso in cui si stabilisca che la disdetta del contratto debba necessariamente avvenire per iscritto attraverso un telegramma; anche in questo caso è da ritenersi, salvo diversa volontà, che il mancato rispetto della forma prevista convenzionalmente comporti la nullità dell'atto.

Compresi i concetti di efficacia probatoria e requisito della forma scritta, occorre ora soffermarsi su quanto disciplinato a riguardo dal C.A.D. novellato con il D.Lgs. 217/2017.

In base all'art. 20, comma 1-bis, del C.A.D.: "Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".

Sotto il profilo dell'efficacia probatoria, il comma fa riferimento a quella prevista dall'art. 2702 del Codice Civile per la **scrittura privata** (alla quale, quindi, il documento informatico con firma digitale, elettronica qualificata, elettronica avanzata o identificazione informatica del suo autoreè parificato ai fini probatori): in base all'art. 2702 c.c. **la scrittura privata** (quindi il semplice atto redatto tra le parti senza particolari formalità) fa **piena prova, fino a querela di falso,** della provenienza delle dichiarazioni da chi l'ha sottoscritta:

- se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione;

- ovvero se questa è legalmente considerata come riconosciuta.

Circa l'esposta portata probatoria del documento informatico, si rende necessaria una riflessione.

Il Legislatore aggiunge poi che: "L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria".

Ciò significa che nel momento in cui un soggetto adopera un dispositivo di firma elettronica qualificata o digitale deve sempre prestare il massimo dell'attenzione: infatti, l'uso indebito del dispositivo da parte di un altro soggetto porrebbe il titolare in una posizione processualmente scomoda, in quanto sarebbe costretto a fornire lui la prova di essere stato spogliato del possesso del dispositivo.

Altra novità del 2017, il nuovo comma 1-quater dell'art. 20 in esame che fa salva, comunque, la specialità della normativa, anche regolamentare, oggi esistente in tema di deposito degli atti e dei documenti in via telematica in materia di processo telematico

- Copie di documenti e duplicati

Come detto, in genere, i documenti possono essere sia analogici che informatici.
Per entrambi, comunque, si pone il problema della circolazione del documento, che normalmente esiste anzitutto nella sua versione "originale".
Tuttavia, il documento originale può essere fatto circolare non direttamente, ma attraverso delle sue copie, appositamente realizzate.
Per quanto riguarda le varie ipotesi rinvenibili nel C.A.D., troviamo:
1) la **copia informatica di documento analogico** (ad esempio il caso di un documento originariamente cartaceo e il cui contenuto viene riportato interamente in bit o mediante l'utilizzo di strumenti OCR), definita dall'art. 1, comma 1, lettera i-bis, come "il documento informatico avente **contenuto identico** a quello del documento analogico da cui è tratto"; l'art. 22, comma 1, del C.A.D. stabilisce il valore legale di atti pubblici, scritture private o documenti in genere, ivi compresi gli atti e documenti amministrativi, originariamente su supporto analogico e poi rilasciati con copia informatica da un pubblico ufficiale o altro soggetto autorizzato, come un notaio, attribuendo loro **efficacia** (ai sensi degli artt. 2714 e 2715 c.c.), quando sia apposta la **firma digitale, altra firma elettronica qualificata, firma elettronica avanzata o previa identificazione informatica del suo autore (attraverso un processo avente i requisiti fissati dall'AgID con Linee guida) da parte del soggetto che le ha rilasciate, volta ad attestarne la conformità all'originale**; le copie così create **sostituiscono gli originali analogici ad ogni effetto di legge**, anche sotto il profilo dell'esibizione e produzione in giudizio e l'assoluzione degli obblighi di conservazione;
2) la **copia per immagine su supporto informatico di documento analogico** (ad esempio la scansione di un documento originariamente cartaceo o la fotografia digitale dello stesso), definita dall'art. 1, comma 1, lettera i-ter, come "il documento informatico avente **contenuto e forma identici** a quelli del documento analogico da cui è tratto"; l'art. 22, comma 1-bis e 2, del C.A.D. dispone che la copia per immagine su supporto informatico di un documento analogico debba essere prodotta mediante processi e strumenti in grado di assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano

adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia; tali copie hanno la stessa efficacia probatoria degli originali da cui sono tratte, se la loro **conformità all'originale** è attestata da un notaio o altro pubblico ufficiale autorizzato (come un funzionario), nel rispetto delle regole tecniche (future Linee guida AgID);

3) la **copia (o estratto) informatica di documento informatico** (ad esempio quando si genera copia di un file passando da un estensione .doc a una .pdf), definita dall'art. 1, comma 1, lettera i-quater, come "il documento informatico avente **contenuto identico** a quello del documento da cui è tratto su supporto informatico **con diversa sequenza di valori binari**"; l'art. 23-bis, comma 2, del C.A.D. dispone che tali copie hanno il medesimo valore giuridico dei documenti informatici da cui sono tratte, se prodotte in conformità alle regole tecniche (future Linee Guida AgID) e la loro **conformità all'originale** è attestata da un pubblico ufficiale autorizzato o se la loro conformità **non è espressamente disconosciuta**; in tali casi, se previsto, resta fermo l'obbligo di conservazione del documento originale informatico;

4) la **copia analogica di un documento informatico** (ad esempio, la stampa di un file gestito e conservato dall'Amministrazione); l'art. 23 del C.A.D. dispone che tali copie hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la **conformità all'originale** è attestata da un pubblico ufficiale autorizzato oppure se il documento informatico originale è conforme alle regole tecniche (future Linee Guida AgID) e la conformità all'originale **non sia disconosciuta**; in tali casi, se previsto, resta fermo l'obbligo di conservazione del documento originale informatico.

Altra figura, distinta rispetto alla copia, e peculiare per il documento informatico, è il cd. **duplicato informatico**, ossia il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della **medesima sequenza di valori binari del documento originario: si tratta quindi del caso in cui si genera la versione di un file mantenendo la stessa estensione (da un .pdf ad un .pdf).**

Il duplicato informatico, per espressa disposizione dell'art. 23-bis del C.A.D., ha il **medesimo valore giuridico**, ad ogni effetto di legge, **del documento informatico da cui è tratto**, se prodotto in conformità alle regole tecniche di cui all'articolo 71 (future Linee Guida AgID).

Le norme ora esposte in tema di copie e duplicati si applicano anche all'attività della Pubblica Amministrazione. Due possono essere i classici casi in un'Amministrazione, che di seguito richiamiamo applicando la normativa già enucleata.

Un primo caso può essere quello della richiesta di un cittadino di copia analogica di un documento originariamente informatico dell'Amministrazione.

In base al citato art. 23 C.A.D. si deve provvedere per mezzo del soggetto incaricato (che in tal caso svolge la funzione di pubblico ufficiale) alla **stampa del documento originario informatico e**

all'attestazione di conformità all'originale informatico del documento stampato, quindi apponendo il relativo timbro e firma. In questo modo la stampa di un documento originale informatico avrà la stessa efficacia del documento da cui è tratta.

Al fine di garantire la provenienza e conformità dell'atto alla sua versione originale, sulle copie analogiche dei documenti informatici che l'Amministrazione rilascia al cittadino è possibile apporre un **timbro digitale**, se l'applicativo lo consenta. Si tratta di un codice a barre bidimensionale (glifo), disciplinato dall'art. 23, comma 2-bis: "Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con Linee Guida, tramite il quale è possibile accedere al 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 del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I soggetti che procedono all'apposizione del contrassegno rendono disponibili gratuitamente sul proprio sito Internet istituzionale idonee soluzioni per la verifica del contrassegno medesimo". In altre parole, con la stampa di un documento amministrativo informatico è possibile l'apposizione automatica di un timbro digitale, tale da non necessitare la copia creata di una dichiarazione di conformità firmata dal Pubblico Ufficiale. Il Timbro digitale, ove previsto negli applicativi, permette quindi di snellire notevolmente la fase di creazione di copie conformi analogiche derivanti da un file.

Altro classico caso che si verifica nelle Amministrazioni è la **ricezione di documenti cartacei, di cui si rende poi necessaria la scansione e acquisizione della relativa copia per immagine**. In particolare, al fine di garantire al documento informatico così ottenuto la stessa efficacia del corrispettivo analogico è necessario che il soggetto incaricato (secondo quanto previsto dall'art. 22 del C.A.D.) vi apponga una firma digitale.

Come rilevato da tutta l'analisi effettuata, le riproduzioni di un documento informatico possono avere la medesima portata probatoria degli originali da cui sono tratti: perché identiche, nel caso dei duplicati informatici, o perché dichiarate conformi da un pubblico ufficiale, nel caso delle copie informatiche o analogiche. È giusto affermare, quindi, che si tratti di una "**capacità probatoria dipendente**", poiché "la portata oggettiva della riproduzione è condizionata dall'attitudine probatoria dell'originale riprodotto"(FRANCHINI, MINAZZI).

- Documento amministrativo informatico

L'art. 22, comma 1, lett. d), della Legge n. 241/1990 dal titolo "Nuove norme sul procedimento amministrativo", come novellato nel 2005, così definisce il documento amministrativo: "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".

Pertanto, documento amministrativo può essere considerato una rappresentazione informatica di atti, anche interni, formati o utilizzati dalla Pubblica Amministrazione. Detto in altre parole, il "documento amministrativo informatico" si configura come species del genus "documento amministrativo".

L'art. 23-ter del C.A.D. ha poi disciplinato gli atti formati dalle Pubbliche Amministrazioni mediante strumenti informatici.

In base alla norma, 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.

Sempre secondo il C.A.D., art. 40: "Le Pubbliche Amministrazioni **formano gli originali dei propri documenti**, inclusi quelli inerenti ad albi, elenchi e pubblici registri, **con mezzi informatici** secondo le disposizioni di cui al presente codice e le Linee Guida".

Il **DPCM 21 marzo 2013**, voluto dallo stesso C.A.D., ha poi elencato i (pochi) casi di "documento originale analogico unico", ovvero quei casi nei quali l'originale dell'atto deve necessariamente rimanere cartaceo e la cuiconservazione digitale è esclusa: tutti casi, quelli elencati dal DPCM, che comunque non impattano sul normale agere della generalità delle Amministrazioni(tra questi troviamo, a titolo di esempio, gli atti giudiziari, processuali o di polizia giudiziaria e gli atti notarili), confermando la regola generale, di cui all'art. 40, in base alla quale la "forma informatica" costituisce un obbligo generale.

Va sottolineato che formare gli originali significa non solo **redigere** il testo con l'ausilio degli strumenti informatici, ma anche **sottoscrivere** gli atti in modalità elettronica. Pertanto, l'art. 40 non attribuisce alle Amministrazioni un potenziale strumento per operare, il documento informatico, ma ne prescrive la totale e assoluta obbligatorietà, da ciò derivando una **nullità di eventuali atti amministrativi nel momento in cui non rispettino la forma informatica**. Il procedimento logico giuridico che conduce alla nullità deriva dal combinato dell'art. 40 C.A.D. e dell'art. 21-septies della Legge n. 241/1990 che prescrive: "È nullo il provvedimento amministrativo che **manca degli**

elementi essenziali, che è viziato da difetto assoluto di attribuzione, che è stato adottato in violazione o elusione del giudicato, nonché negli altri casi espressamente previsti dalla legge".

Per dottrina (PERONGINI) e giurisprudenza (Cons. Stato, Sezione VI, 14 luglio 1999, n. 948), **tra gli elementi essenziali, la cui mancanza comporta la nullità dell'atto, rientra anche la "forma"**, come quella informatica prescritta per tutti i documenti amministrativi dall'art. 40 C.A.D.. La mancanza di tale forma informatica, dunque, comporta la nullità dell'atto. Con particolare riferimento alla forma, infine, occorre precisare che non ogni carenza formale dell'atto porta alla nullità dello stesso: l'art. 21-octies della Legge n. 241/1990, infatti, esclude la "violazione di norme sulla forma degli atti" dallo stesso ambito dell'annullabilità, degradando il vizio relativo a mera irregolarità, almeno quando esso riguardi provvedimenti contenutisticamente vincolati. Pertanto, si avrà nullità del provvedimento amministrativo solo in mancanza della forma essenziale, intendendosi per forma essenziale l'insieme delle caratteristiche esteriori necessarie e sufficienti ad identificare un atto come proveniente da una Pubblica Amministrazione., oltre a renderne intelligibile il dispositivo. A parere di chi scrive, per forma essenziale è assolutamente lecito ritenere la "forma informatica" come prescritta dall'art. 40 C.A.D., posizione avvalorata dalla stessa semantica rigorosa e scevra da qualsivoglia possibile fraintendimento utilizzata dal Legislatore nella norma. In ogni caso, al momento in cui si scrive non vi sono arresti giurisprudenziali che abbiano preso una posizione definita a riguardo.

Da ultimo, del documento amministrativo informatico si è interessato il DPCM 13 novembre 2014, oggi ancora in vigore, contenente le "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle Pubbliche Amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale, di cui al decreto legislativo n. 82 del 2005".

Le regole tecniche dedicano il capo III alla disciplina del documento amministrativo informatico che presenta specifiche peculiarità rispetto al documento informatico disciplinato nei capi precedenti.

Nella formazione dei documenti amministrativi, difatti, assumono una particolare rilevanza:

a) **l'uso degli strumenti riportati nel manuale di gestione documentale** di ciascuna Amministrazione;

b) **l'acquisizione delle istanze, dichiarazioni e comunicazioni** di cui agli articoli 5-bis (comunicazioni tra imprese e Amministrazioni), 40-bis (protocollo informatico) e 65 (istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica) del C.A.D..

In altre parole, **in base alle regole tecniche i casi ora elencati alle lettere a) e b) generano documenti amministrativi informatici.**

Particolarmente importante è la specificazione secondo la quale il documento amministrativo informatico assume le caratteristiche di **immodificabilità e di integrità** anche con la sua semplice **registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti**, come richiesto dalla normativa di settore.

Ai fini della trasmissione telematica di documenti amministrativi informatici, le Pubbliche Amministrazioni pubblicano sui loro siti gli standard tecnici di riferimento, le codifiche utilizzate e le specifiche per lo sviluppo degli applicativi software di colloquio, rendendo eventualmente disponibile gratuitamente sul proprio sito il software per la trasmissione di dati coerenti alle suddette codifiche e specifiche.

Un interessante ambito di discussione dottrinaria (MASUCCI, DUNI, MARONGIU, COSTANTINO)è rappresentato da quello in tema di **"atto amministrativo automatizzato"**, ovvero la possibilità, o meno, degli odierni sistemi informatici di porre in essere atti, in toto o in parte, senza l'ausilio umano ma solo tramite l'elaborazione automatica dei dati inseriti sulla base delle istruzioni contenute nel software. Secondo alcuni sarebbe possibile e auspicabile giungere ad una totale automatizzazione di talune categorie provvedimentali. Ma la più attenta dottrina ha rilevato come, in realtà, anche in casi vincolati di azione amministrativa, dove l'esercizio del potere pubblico non può uscire da binari rigidi preventivamente tracciati dal Legislatore, la discrezionalità amministrativa è spesso solo latente e, in talune circostanze, risorge, minando alla base la sequenzialità logica di un possibile software di automatizzazione. Il problema è aperto ma, a parere di chi scrive, difficilmente troverà compimento nel prossimo futuro, visto che il carattere essenziale del diritto amministrativo è quello di trovare soluzioni contemperando di volta in volta interessi diversi, pubblici e privati, contemperazione che, in questa fase storica, non è gestibile tramite l'elaborazione automatica di un algoritmo.

- Atto pubblico e nullità

Per **atto pubblico** occorre intendere, in base all'art. 2699 del Codice Civile: "Un atto scritto, redatto interamente dal notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato".

Per **pubblico ufficiale**, in base all'art. 357 del Codice Penale, bisogna intendere chi esercita, anche temporaneamente, una funzione legislativa, amministrativa o giudiziaria con o senza rapporto di impiego con lo Stato o altro ente pubblico.

Secondo la dottrina e la giurisprudenza, però, la nozione penalistica di atto pubblico è più ampia di quella civilistica comprendendo, oltre ai documenti contemplati dall'art. 2699 c.c., **tutti quelli formati da un pubblico ufficiale o da un pubblico impiegato incaricato di pubblico servizio e compilati, con le prescritte formalità, per uno scopo di diritto pubblico**, inerente all'esercizio della propria funzione o del pubblico servizio, al fine di comprovare un fatto giuridico o di attestare fatti da lui compiuti o avvenuti in sua presenza ed aventi rilevanza giuridica. In definitiva, **nel concetto penalistico di atto pubblico, particolarmente ampio,** rientrano:

- tutti gli atti pubblici di cui all'art. 2699 del Codice civile;
- qualsiasi documento interno di un pubblico ufficio che possa assumere carattere probatorio e rilevanza esterna ai fini della documentazione di fatti inerenti all'attività dell'ufficio cui è addetto l'autore e la regolarità delle sue operazioni amministrative (ad esempio, sono stati considerati atti pubblici i registri di protocollo e i fogli di raccolta delle firme di presenza dei dipendenti pubblici);
- qualsiasi documento che costituisca corrispondenza ufficiale di organi della pubblica amministrazione;
- qualsiasi documento redatto da un pubblico impiegato incaricato di un pubblico servizio nell'esercizio delle sue attribuzioni.

L'interpretazione penalistica è quella maggiormente accolta in dottrina, se non altro perché i profili di responsabilità penale sono i più delicati per un Pubblico Ufficiale o incaricato di pubblico servizio, ragione legittimante la loro condivisione nell'interpretazione degli istituti giuridici.

Da ciò consegue che, ad esempio, in un Comune le delibere di Giunta, di Consiglio, le determine dirigenziali o gli atti di liquidazione sono da considerarsi "atti pubblici".

Compresa la definizione civilistica e penalistica di "atto pubblico", occorre ora **verificare se il nostro ordinamento richiede una forma specifica a pena di invalidità.**

Nello specifico, ex **art. 21 co. 2-ter C.A.D.**: "Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110 [atto pubblico informatico redatto dal notaio], **ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale**. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti".

Da quanto detto, gli atti pubblici**necessitano di una firma qualificata o digitale a pena di nullità ai sensi dell'art. 21 co. 2-ter C.A.D. su indicato e non di una semplice firma elettronica avanzata** (men che meno di una firma elettronica semplice).

- Procedimento amministrativo informatico

Dato l'impianto normativo su esplicato, il documento amministrativo informatico trova oggi una sua puntuale disciplina. Per il procedimento amministrativo informatico la situazione è più complessa.

Il "procedimento amministrativo", in senso lato, è da intendersi come una **sequenza di atti amministrativi che portano all'emanazione di un atto finale (il provvedimento)**, e che quindi concorrono al conseguimento di un interesse pubblico. Pertanto, il procedimento amministrativo rappresenta la forma esteriore attraverso la quale si dispiega l'azione amministrativa, ovvero quel particolare iter procedurale che rende l'atto efficace e perfetto, nel pieno rispetto dell'art. 97 della nostra Costituzione e della disciplina primaria di settore dettata dalla Legge n. 241/1990.

Compreso il concetto di "procedimento amministrativo" è giusto ora sottolineare come non esista una definizione normativa di "procedimento amministrativo informatico", né tantomeno una sua puntuale disciplina all'interno di un unico testo legislativo.

Infatti, la Legge n. 241/1990 sul procedimento amministrativo è stata ideata e scritta con obiettivi essenzialmente "analogici" (si pensi che non era ancora nata Internet come oggi la intendiamo), poi nel tempo integrata sempre più in senso "digitale". Si veda, ad esempio, l'art. 3-bis, introdotto con la Legge n. 15/2005, secondo il quale la Pubblica Amministrazione, per conseguire maggiore efficienza nella sua attività, deve incentivare l'uso della telematica, nei rapporti interni, tra le diverse Amministrazioni e tra queste e i privati. Ma, a parere di chi scrive, l'impianto di fondo della Legge n. 241/1990 rimane comunque "analogico", motivo per il quale autorevole dottrina ha giustamente sottolineato come il modello del "procedimento sequenziale" di tale legge, quindi ripartito per rigide fasi, sia in realtà in fase di totale superamento a causa del processo di informatizzazione pubblico, con un **passaggio al "procedimento a stella"**: "il concetto di procedimento a stella, alternativo al classico procedimento sequenziale, non è un'invenzione o una proposta dottrinale, ma una constatazione, derivante dalla scomparsa del fascicolo cartaceo che imponeva una sequenzialità legata alla necessità di disporre della documentazione cartacea per ogni intervento. La disponibilità in Rete del fascicolo informatico, contenente tutti gli elementi, consente di compiere le attività necessarie contemporaneamente, salvo il caso di diversa prescrizione legislativa o di palese inopportunità"(DUNI). Da questa riflessione scaturisce la convinzione di un

progressivo "impoverimento applicativo" della Legge n. 241/1990: ancora vigente, ma che prosegue il suo cammino lungo modelli procedimentali inadatti alla realtà digitale e, nella sua disciplina del diritto di accesso documentale, già superata dal nuovo diritto di accesso generalizzato di cui al D.Lgs. n. 33/2013, di cui appresso meglio si dirà.
Lo stesso Consiglio di Stato, con i rilievi allo schema del C.A.D. svolti dalla sezione consultiva per gli atti normativi (Adunanza del 7 febbraio 2005), richiamava l'attenzione del Legislatore sulla necessità di una "perimetrazione" del Codice con riferimento alla disciplina del procedimento amministrativo. Richiamo non considerato appieno dal Legislatore nel testo finale del C.A.D..
Ad oggi, quindi, una disciplina unica e puntuale sul procedimento amministrativo informatico, contenuta in un unico testo legislativo e al passo con una visione procedimentale a stella, non esiste. È fondata, comunque, la posizione in dottrina secondo la quale, in base alla normativa vigente (essenzialmente C.A.D. e DPR n. 445/2000), sia possibile oggi espletare e gestire il procedimento amministrativo esclusivamente in forma elettronica (MASUCCI). L'interprete, dunque, può oggi ricostruire una **disciplina compiuta del procedimento amministrativo informatico, ma sempre da una sommatoria di norme contenute in diversi testi normativi di settore**. Il C.A.D., probabilmente, poteva essere il luogo ideale ove ricostruire un'unica disciplina sul procedimento amministrativo informatico o, comunque, è auspicabile possa divenirlo in futuro.
Delle norme di interesse in tema di procedimento amministrativo e Web sono anche contenute nel cd. Decreto Trasparenza, ovvero il D.Lgs. n. 33/2013. Il suo art. 35, c. 1, lett. d) dispone che le Amministrazioni pubblichino nella sezione "Amministrazione trasparente", sotto-sezione di primo livello "Attività e procedimenti", sotto-sezione di secondo livello "Tipologie di procedimento", gli atti e i documenti da allegare alle istanze, oltre che la modulistica necessaria, compresi i fac-simile per le autocertificazioni.
Nella pubblicazione della modulistica sui siti istituzionali è innanzitutto necessario rispettare le disposizioni previste dalla citata L. n. 4/2004 in tema di accessibilità. Pertanto, i moduli pubblicati dovranno essere dei file accessibili. Una specifica accortezza, non richiesta dalla norma e quindi di rado considerata dalle Amministrazioni, è quella di pubblicare file editabili e salvabili, al fine di ridurre la mole di documenti cartacei in entrata.

- Fascicolo informatico e Sistema pubblico di ricerca documentale

Come già evidenziato, le Pubbliche Amministrazioni sono del tutto obbligate a formare gli originali dei propri atti come documenti informatici (art. 40, comma 1, D.Lgs. n. 82/2005), nel rispetto delle

disposizioni del C.A.D. e delle relative regole tecniche. Quindi, ogni documento amministrativo deve non solo nascere informaticamente ma anche essere gestito con le stesse modalità: l'**art. 41**, infatti, dispone che per la gestione amministrativa dei documenti occorre utilizzare le tecnologie dell'informazione e della comunicazione e, più nello specifico, occorre **raccogliere in un fascicolo informatico gli atti, i documenti e i dati di ogni procedimento amministrativo, da chiunque formati**.

Di conseguenza, l'unico fascicolo che l'ufficio deve creare è quello informatico avendo cura di inserire nello stesso sia i documenti digitali (ricevuti da privati-altre Amministrazioni o formati dall'Amministrazione) sia i documenti analogici acquisiti al sistema informatico (ad es., tramite scansione).

Il fascicolo informatico deve essere 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 devono essere 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.

In base al **comma 2-ter dell'art. 41** del C.A.D., il fascicolo informatico deve recare l'indicazione:

- dell'Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre Amministrazioni partecipanti;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il Sistema pubblico di ricerca documentale (di cui meglio appresso si dirà) nel rispetto delle Linee Guida AgID.

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. 241/1990, in primis quelli di accesso ai documenti.

Il fascicolo informatico deve essere sempre realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le Amministrazioni coinvolte nel procedimento e

dagli interessati, nei limiti ed alle condizioni previste dalla disciplina vigente, attraverso il Sistema pubblico di accesso documentale (art. 40-ter) e il Punto di accesso telematico dei servizi in rete delle Amministrazioni, attivato presso la Presidenza del Consiglio dei Ministri (art. 64-bis).
Normalmente, nelle Amministrazioni sono utilizzate le seguenti tipologie di fascicolo (PENZO DORIA):

- **per procedimento amministrativo**, nel momento in cui occorra conservare una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale;
- **per affare**, nel momento in cui occorra conservare i documenti relativi ad una competenza generalmente non proceduralizzata, per la quale, dunque, non è prevista l'adozione di un provvedimento finale, inteso come atto dotato di capacità di incidere nella sfera giuridica di terzi;
- **per attività**, nel momento in cui occorra conservare i documenti relativi ad una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque prevista l'adozione di un provvedimento finale (la differenza essenziale con il fascicolo di affare è che mentre quest'ultimo conserva in modo organico documenti relativi a un medesimo argomento e di norma non prende avvio con un'istanza di parte, il fascicolo di attività conserva documenti relativi ad argomenti diversi pressoché privi di organicità);
- **per persona**, fisica o giuridica, nel momento in cui occorra conservare documenti relativi a diversi procedimenti amministrativi, distinti affari o diverse attività, ma legati da un vincolo archivistico interno, relativo ad una persona (fisica o giuridica che sia).

Volendo ora chiarire la portata del Sistema pubblico di ricerca documentale, esso è da intendersi come un sistema promosso dalla Presidenza del Consiglio dei Ministri e volto a facilitare la ricerca da parte di cittadini e imprese dei documenti soggetti a obblighi di pubblicità legale, trasparenza o a registrazione di protocollo e dei fascicoli dei procedimenti, nonché a consentirne l'accesso on-line ai soggetti che ne abbiano diritto ai sensi della disciplina vigente (art. 40-ter).
Tale componente dovrebbe costituire una sovrastruttura di livello nazionale in grado di dialogare con i singoli sistemi delle Amministrazioni attraverso standard di interoperabilità con l'obiettivo di consentire, a soggetti autorizzati, il reperimento generalizzato di documenti e fascicoli procedimentali, ovunque prodotti.

- Carta di identità elettronica e carta nazionale dei servizi

Ad oggi, il nostro Legislatore affronta il tema dell'identificazione elettronica sotto i diversi aspetti in cui esso si declina: carte elettroniche, sistema per l'identità digitale (SPID) e anagrafe nazionale della popolazione residente (ANPR).

Tralasciando l'esame delle cosiddette "identità digitali deboli", utilizzate dagli operatori online per l'accesso a servizi digitali (email, social media, eCommerce) costituite, di norma, da nome utente e password, oltre a una serie di attributi funzionali alla fruizione del servizio, le quali non hanno una valenza univoca in un procedimento civile o penale, il C.A.D. si occupa delle diverse misure di identificazione digitale definite "forti".

Per quel che riguarda le **carte elettroniche,** il C.A.D. (sia nella vecchia che nella nuova versione) distingue due tipologie, delle quali dà una definizione all'art. 1, precisando:

- alla lettera c) cosa debba intendersi per **"carta d'identità elettronica"**(CIE), ovvero "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";
- alla lettera d) la **"carta nazionale dei servizi"**(CNS), ovvero " il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle Pubbliche Amministrazioni".

La disciplina applicativa di tali strumenti è poi contenuta negli artt. 64 e seguenti del suddetto Codice, recentemente oggetto di intervento riformatore, ove vengono specificate le caratteristiche tecniche che le carte elettroniche devono possedere e la funzione peculiare delle stesse. In particolare, è bene sin da subito chiarire che prima della novella del 2016 la CIE e la CNS costituivano gli strumenti cardine previsti dal Legislatore per consentire l'accesso dei cittadini ai servizi erogati in Rete dalle Pubbliche Amministrazioni, con specifica delimitazione alle attività per le quali era richiesta l'autenticazione informatica; oggi ad esse è stato affiancato, e reso preminente, lo SPID, il quale costituisce, insieme alle carte elettroniche, l'unico sistema di accesso ai servizi in Rete erogati da una Pubblica Amministrazione.

Pur essendo fortemente assimilabili, l'elemento discretivo che rende le citate carte elettroniche non sovrapponibili è dato dalla maggiore sicurezza garantita dalla CIE rispetto alla CNS: invero, la seconda non possiede alcune caratteristiche tecniche possedute dalla prima, come per esempio la foto del soggetto, la banda ottica, gli ologrammi di sicurezza, etc., che fanno sì da una parte che la CNS dia meno garanzie sull'identificazione del suo possessore, ma che, per converso, permettono una più agevole distribuzione dello strumento, indipendentemente dai canali istituzionali abilitati a rilasciare la CIE.

Se la CIE ha la funzione principale di sostituire il classico documento di riconoscimento cartaceo, utilizzando la CNS, inserita in un apposito lettore collegato ad un PC, si può fruire di numerosi servizi messi a disposizione dalle PA, quali la firma digitale, la tessera sanitaria, il codice fiscale, i pagamenti online, semplicemente accedendo da remoto agli uffici pubblici in Rete, in qualunque posto del territorio nazionale ci si trovi.

Non tragga in inganno la definizione della carta d'identità elettronica come documento per l'identificazione "**fisica**" del titolare.

Infatti, come appare evidente nella Sezione III del Capo V del C.A.D., intitolato "Identità digitali, istanze e servizi on-line", tanto la carta nazionale dei servizi quanto la carta di identità elettronica, insieme a SPID, costituiscono strumenti per l'accesso ai servizi erogati in Rete dalle Pubbliche Amministrazioni per i quali sia necessaria "l'identificazione **informatica**" (art. 64, comma 2-nonies, in particolare).

Con tale disposizione il Legislatore ha voluto chiaramente definire le suddette carte elettroniche come strumento forte per l'affermazione dell'identità digitale, codificando espressamente il loro utilizzo per poter ricevere i servizi delle Pubbliche Amministrazioni in un'ottica di informatizzazione amministrativa completamente equivalente al modello fisico/cartaceo.

Da ultimo è bene dare atto che, se ad oggi il cittadino italiano ha ancora facoltà di scelta tra la richiesta di rilascio di una carta di identità cartacea o di una carta di identità digitale, entro dicembre 2018 il documento digitale sostituirà definitivamente quello cartaceo, come prescritto dal Piano triennale per l'Informatica nella Pubblica Amministrazione 2017-2019 e, ancor prima, dalla **circolare del Ministero dell'Interno n. 18 del 19 ottobre 2016**, attraverso un piano di dispiegamento per l'abilitazione di tutti i comuni al rilascio della nuova CIE.

Tale nuova carta di identità porterà dei vantaggi rilevanti per i cittadini, in quanto è previsto che la stessa contenga anche il **codice fiscale** dell'intestatario, le **impronte digitali** e gli estremi dell'**atto di nascita**; ulteriore novità è costituita, poi, dalla possibilità di aggiungere alla memoria del microchip elettronico anche la volontà di essere **donatore di organi**, la propria tessera elettorale e l'abilitazione all'utilizzo dei servizi della Pubblica Amministrazione mediante l'inserimento della propria firma digitale.

L'art. 64 termina prescrivendo che, con futuro DPCM o DM, sarà stabilita la data a decorrere dalla quale i soggetti obbligati all'applicazione del C.A.D. (Pubbliche Amministrazioni, gestori di pubblici servizi e società a controllo pubblico) utilizzeranno **esclusivamente** le identità digitali ai fini dell'identificazione degli utenti dei propri servizi. Una disposizione, questa, che ricalca altre introdotte dal 2016 ad oggi e volte a dare un impulso finale al processo di digitalizzazione pubblico.

- Istanze e dichiarazioni telematiche

La normativa vigente in tema di digitalizzazione prevede, all'**art. 65** del C.A.D., che le istanze e le dichiarazioni presentate telematicamente dal cittadino alle Amministrazioni e ai gestori di pubblici servizi siano da considerarsi valide:

a) se sottoscritte mediante **una delle forme di cui all'art. 20**(a parere di chi scrive, il richiamo del Legislatore a tutte le forme indicate nell'art. 20 può essere fuorviante e male interpretabile in funzione dell'intero contenuto dell'art. 65: in realtà, è lecito supporre che il Legislatore intendesse fare riferimento alle firme elettroniche avanzate, qualificate e digitali, oltre agli strumenti di identificazione informatica che, in base allo stesso art. 20, saranno meglio disciplinati con le future Linee Guida AgID; con esclusione quindi delle firme elettroniche semplici, utilizzabili per le istanze e dichiarazioni online del cittadino, ma con l'integrazione di quanto chiesto al punto c) dell'art. 65, di seguito esposto);

b) ovvero, quando l'istante o il dichiarante è identificato attraverso il **sistema pubblico di identità digitale (SPID)**, nonché attraverso **carta di identità elettronica (CIE)** o **carta nazionale dei servizi (CNS)**: in tali casi l'istanza è da intendersi come se fosse stata sottoscritta con **firma avanzata** in base all'art. 61, comma 2, del DPCM 22 febbraio 2013 (Regole tecniche firme avanzate ancor oggi efficaci) (la norma tecnica in questione non considera anche lo SPID, poiché non ricompreso, al tempo, nell'art. 65 C.A.D. cui la stessa fa riferimento ma, a seguito della modifica dell'art. 65 avvenuta nel 2016, a parere di chi scrive, per analogia anche un'istanza o dichiarazione formulata con SPID deve oggi intendersi come se fosse stata sottoscritta con firma avanzata; conferma a tale impostazione deriva anche dal contenuto dell'art. 20 che affianca gli strumenti di identificazione informatica alle firme forti sotto il profilo della validità ed efficacia probatoria; è lecito supporre che, con le prossime Linee Guida AgiD in via di definizione, sarà chiarito espressamente questo punto);

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 o altro servizio elettronico di recapito certificato qualificato (domicilio digitale)** purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee Guida AgID, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato: in tali casi l'istanza è da intendersi come se fosse stata sottoscritta con **firma avanzata**in base all'art. 61, comma 1, del DPCM 22 febbraio 2013 (Regole tecniche firme avanzate ancor oggi efficaci). In tal caso, **la**

trasmissione costituisce elezione di domicilio speciale ai sensi dell'art. 47 c.c.: la dichiarazione del domicilio digitale vincola quindi il dichiarante e rappresenta espressa accettazione dell'invioda parte delle Pubbliche Amministrazioni, degli atti e dei provvedimenti che lo riguardano.

Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel **settore tributario**.

Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate validamente comporta **responsabilità dirigenziale e responsabilità disciplinare** dello stesso.

Le istanze e le dichiarazioni inviate con modalità telematiche sono da ritenersi **equivalenti** alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.

Un'importante novità è stata prevista in tema di ricevuta dell'istanza.

A partire dall'1 gennaio 2017 le Pubbliche Amministrazioni devono adeguarsi al nuovo art. 18-bis della L. n. 241/1990 (introdotto dal D. Lgs. n. 126/2016) in materia di istanze, segnalazioni e comunicazioni presentate alle pubbliche amministrazioni anche in via telematica.

La norma prevede che:

- la **data di protocollazione** dell'istanza, segnalazione o comunicazione non può comunque essere diversa da quella di effettiva presentazione;
- dell'avvenuta presentazione di istanze, segnalazioni o comunicazioni deve essere rilasciata **immediatamente**, anche in via telematica, una **ricevuta**, che attesta l'avvenuta presentazione dell'istanza, della segnalazione e della comunicazione e indica i termini entro i quali l'amministrazione è tenuta, ove previsto, a rispondere, ovvero entro i quali il silenzio dell'amministrazione equivale ad accoglimento dell'istanza.

Al fine di evitare eventuali illegittimità procedimentali, saggiamente il Legislatore prosegue nell'art. 18-bis specificando che le istanze, segnalazioni o comunicazioni **producono effetti anche in caso di mancato rilascio della ricevuta**, ferma restando la **responsabilità** del soggetto che avrebbe dovuto predisporla e non l'ha fatto. Se poi eventualmente l'istanza, segnalazione o comunicazione è stata inviata ad un **ufficio diverso** rispetto a quello effettivamente competente, i termini per la chiusura del procedimento decorrono comunque dalla ricezione da parte dell'ufficio competente.

Adeguarsi agli obblighi di cui all'art. 18-bis richiede di certo un'efficiente organizzazione dell'ufficio protocollo, e delle soluzioni informatiche di protocollo, ed un vero e proprio censimento delle istanze/segnalazioni/comunicazioni ricevute da ogni Pubblica Amministrazione ai fini della

predisposizioni di format di ricevuta per ciascuna di esse e alla definizione delle modalità per il rilascio contestuale alla presentazione.