INFORMATION TECHNOLOGY LAW

DISPENSE

(Ignazio Zangara)

… … …

SEZIONE III

PUBBLICA AMMINISTRAZIONE DIGITALE

IL QUADRO NORMATIVO

La trasformazione digitale che stiamo vivendo in Italia è costituita da competenze che iniziano a delinearsi e da strumenti che stanno cambiando il modo di gestire la cosa pubblica e i rapporti tra gli enti pubblici, i cittadini e le imprese.

Il processo di informatizzazione nella pubblica amministrazione si può dire che abbia avuto inizio negli anni Novanta ed ha avuto travagliate vicende di sviluppo. Sebbene una buona parte delle norme giuridiche orientate all'amministrazione digitale siano pienamente operative da oltre un ventennio, le incompetenze da parte degli operatori hanno comportato ritardi applicativi gravi con conseguenze di ordine economico ed inefficienze che hanno tenuto la gran parte del territorio italiano in uno stato di arretratezza amministrativo-funzionale. Solo da un decennio si iniziano ad apprezzare gli sforzi di semplificazione e di snellimento delle procedure amministrative che il legislatore aveva previsto a suo tempo.

Per questioni di opportunità mi limiterò qui a citare i provvedimenti normativi principali che hanno spinto, spesso solo nelle intenzioni, il passaggio in Italia da un'amministrazione di carte ad una in bit.

La legge n. 241 /1990, intitolata "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", e il D.Lgs. n. 29/1993, dal titolo "Razionalizzazione dell'organizzazione delle amministrazioni pubbliche e revisione della disciplina in materia di pubblico impiego, a norma dell'articolo 2 della legge del 23 ottobre 1992 n. 421", rappresentano il punto di partenza del processo di innovazione del nostro sistema pubblico; processo che ha avuto la sua definitiva consacrazione con l'emanazione delle leggi Bassanini 1 e 2 (n. 59 e 127 del 1997).

In particolare, la legge n. 241/1990 ha introdotto rilevanti innovazioni nel modo di organizzare il procedimento amministrativo, definendone sia i termini di durata sia la struttura sequenziale in un'ottica di razionalizzazione ed innovazione. I conseguenti e fondamentali principi della trasparenza dell'azione amministrativa e dell'accesso agli atti dell'amministrazione da parte dei cittadini sono figli del provvedimento normativo in parola. Con la stessa legge, infine, è stato previsto, sia pure implicitamente, l'utilizzo dell'informatica nel settore pubblico per la redazione dei documenti amministrativi, come vedremo meglio tra breve.

Il D.Lgs. n. 29/1993 ha operato una vera e propria rivoluzione per l'amministrazione pubblica disciplinando nuovi criteri di gestione e di valutazione dei risultati dell'agire amministrativo. Con esso è stata istituita l'Autorità per l'informatica nella pubblica amministrazione (AIPA), un'autorità indipendente dal controllo del Governo alla quale è stato affidato il compito di armonizzare il processo di informatizzazione nella PA per evitare il prevalere di interessi privati e abusi di potere da parte degli stessi amministratori. Nel 2001, è stato istituito il Ministero per l'Innovazione e le Tecnologie che ha assunto buona parte delle funzioni che in precedenza erano state delegate all'AIPA. Nel 2003, l'AIPA è stata sostituita con il Centro nazionale per l'informatica nella PA (CNIPA), non più quale autorità indipendente, ma soggetta al controllo della Presidenza del Consiglio dei ministri. Con funzioni analoghe, nel 2009, è stata istituita DigitPA in sostituzione del CNIPA che, infine (almeno fino ad oggi), nel 2012, è stata trasformata in Agenzia per l'Italia digitale (AgID) con l'obiettivo di contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica del paese. Come spesso accade nel nostro ordinamento, il susseguirsi di provvedimenti normativi ha

modificato natura e indirizzo dell'organo ora descritto, quasi a dimostrare che i risultati raggiunti – a onor del vero, neanche così onorevoli – sono da ricondurre ad un certo Governo piuttosto che ad una reale esigenza di cambiamento.

Nel 1995 è stata creata la Rete Unitaria della Pubblica Amministrazione (RUPA) con lo scopo di garantire ed assicurare l'interoperabilità e la cooperazione delle infrastrutture informatiche e telematiche delle pubbliche amministrazioni. In tal modo, tramite la rete dedicata, è stato possibile connettere qualsiasi terminale pubblico ad un qualsiasi altro computer collegato alla medesima rete. In buona sostanza, con la RUPA ha avuto inizio il processo di interoperabilità tra sistemi informatici presso le PPAA, sia centrali che periferiche, che prima d'allora non potevano scambiare dati e informazioni.

Dalla RUPA, nel 2005, si è passati al Sistema pubblico di connettività (SPC), disciplinato compiutamente dal Codice dell'amministrazione digitale (CAD). Il Codice all'articolo 73 definisce il Sistema pubblico di connettività, al primo comma, quale "insieme di infrastrutture tecnologiche e di regole tecniche che assicura l'interoperabilità tra i sistemi informativi delle pubbliche amministrazioni, permette il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e tra queste e i sistemi dell'Unione europea ed è aperto all'adesione da parte dei gestori di servizi pubblici e dei soggetti privati" e, al secondo comma, gli attribuisce il compito di garantire "la sicurezza e la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascun soggetto aderente". La condivisione e lo scambio di dati e di informazioni tra le amministrazioni statali, regionali e locali ha lo scopo di favore la collaborazione tra tutti gli uffici pubblici e lo svolgimento, in cooperazione informatica, dei procedimenti amministrativi connessi, garantendo efficienza, sicurezza e riservatezza delle informazioni.

Con l'istituzione del Sistema pubblico di connettività è nata anche la Rete internazionale delle pubbliche amministrazioni (RIPA) finalizzata a rendere interoperabili anche i sistemi utilizzati negli uffici italiani all'estero.

Il CAD, emanato con D.Lgs. del 5 marzo 2005, n. 82, ha rappresentato una pietra miliare nel percorso di informatizzazione seguito dall'Italia, ha riordinato norme esistenti (in parte già accorpate dal legislatore nel DPR del 28 dicembre 2000, n. 445: Testo Unico delle disposizioni legislative in materia di documentazione amministrativa) e ne ha introdotte di altre per nuovi servizi e nuove opportunità. Contiene le disposizioni per garantire il diritto di ogni cittadino di usufruire dei servizi della PA anche online e l'obbligo per la PA di snellire le procedure e di rendere tutti i servizi e le comunicazioni interne ed esterne per via telematica.

Il CAD è ancora oggi uno strumento ambizioso che ha dato luogo a moltissime discussioni in dottrina ed ha suscitato numerose critiche. In conseguenza di ciò e dell'incessante progresso tecnologico, il testo normativo ha subito diverse modifiche e integrazioni che ne hanno reso ancor più complesso il recepimento e la concreta applicazione.

Non è sufficiente che una nuova tecnologia sia valida e disponibile perché possa essere utilizzata legittimamente nell'amministrazione pubblica; occorre una puntuale e definita previsione normativa che consenta di operare con i singoli strumenti informatici. In altri termini, lo Stato pubblicando le norme giuridiche autorizza misure e comportamenti al fine di orientare tutti gli operatori, pubblici e privati, verso una convergenza di scopi con le tecniche più adeguate per realizzarli. Nel caso dell'utilizzo degli strumenti informatici un elemento di complessità ulteriore è dato dall'elevato analfabetismo telematico degli operatori e dalla mancanza di una formazione adeguata che rallentano oltremodo l'applicazione del CAD.

Nel prosieguo della sezione sono descritti, per sommi capi, gli strumenti digitali più significativi contenuti nel CAD e nelle altre norme correlate.

IL DOCUMENTO AMMINISTRATIVO ELETTRONICO

Il documento amministrativo elettronico è il primo strumento significativo nel processo di dematerializzazione della PA. Il provvedimento con il quale viene riconosciuto nell'ordinamento giuridico potrebbe essere individuato all'art. 22 della legge n. 241/90, che al secondo comma definisce il documento amministrativo come "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti anche interni formati dalle pubbliche amministrazioni o comunque utilizzati ai fini dell'attività amministrativa". Tale nozione, se da un lato sancisce il principio della libertà delle forme che l'atto può assumere in quanto oggettivazione dell'attività amministrativa, dall'altro acclara la piena ammissibilità nel sistema giuridico-amministrativo della tecnica elettronica.

Prima dell'emanazione della legge n. 59/1997 (c.d. legge Bassanini 1) a livello normativo si distingueva tra atto amministrativo ad elaborazione elettronica ed atto in forma elettronica. L'art. 3 del D.Lgs. del 12 febbraio 1993 n. 39, infatti, disciplinava tanto l'atto amministrativo ad elaborazione elettronica (intendendosi con tale locuzione l'atto amministrativo predisposto elettronicamente mediante l'utilizzo di processi di elaborazione elettronica e poi stampato su carta), quanto l'atto in forma elettronica (intendendosi con tale espressione l'atto amministrativo redatto e perfezionato elettronicamente attraverso l'apposizione della firma digitale).

La legge Bassanini 1, all'art. 15, comma 2, stabilì che "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti ad ogni effetto di legge".

Il successivo regolamento, emanato con DPR n. 513/1997, ha poi fissato la definizione di documento informatico come rappresentazione di atti, fatti o dati giuridicamente rilevanti. Con tale regolamento sono stati introdotti nell'ordinamento giuridico criteri di amplissima portata validi sia per il settore pubblico che per quello privato. Per la prima volta, infatti, sono stati indicati i criteri giuridici oggettivi ai quali dovranno sottostare i documenti informatici e le modalità con cui i contratti dovranno essere posti in essere. Il quadro normativo italiano è stato successivamente completato con l'emanazione del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR n. 445/2000) che ha stabilito che per documento informatico deve intendersi la mera rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti a prescindere dal riferimento a qualsivoglia sottoscrizione elettronica.

È interessante segnalare l'art. 40 del CAD, che disciplina la formazione dei documenti informatici da parte della PA: "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". L'articolo riprende il concetto espresso all'art. 3[1] del D.Lgs. n. 39/93 che ha segnato un netto capovolgimento rispetto al passato: non c'è soltanto un pieno riconoscimento del documento informatico, intendendo quello nato in originale in forma elettronica, ma addirittura ormai questo costituisce la regola per le pubbliche amministrazioni, mentre il documento cartaceo in originale è ridotto ad eccezione, motivata da particolari ragioni storiche o archivistiche. Si è voluta cioè affermare una posizione di principio, che tende ad accelerare il più possibile il cambiamento e l'innovazione.

LE FIRME ELETTRONICHE

Prima di entrare nel vivo delle firme elettroniche è utile comprendere cosa si intende per sottoscrizione di un documento. La sottoscrizione è la scrittura del proprio nome e cognome di proprio pugno in calce ad un documento. Troviamo una definizione nel codice di procedura penale all'art. 110, il quale recita al primo ed al secondo comma: "Quando è richiesta la sottoscrizione di

[1] Il comma in parola, abrogato nel 2016, aveva previsto che gli atti amministrativi adottati da tutte le pubbliche amministrazioni dovevano di norma essere predisposti tramite i sistemi informativi automatizzati.

un atto, …, è sufficiente la scrittura di propria mano, in fine dell'atto, del nome e cognome di chi deve firmare. Non è valida la sottoscrizione apposta con mezzi meccanici o con segni diversi dalla scrittura". Quest'ultimo punto asserisce che se la sottoscrizione è apposta, ad esempio, con un timbro meccanico o dattilografico o con un disegno il documento non si ha per sottoscritto. In relazione al valore probatorio di un documento sottoscritto, è utile richiamare l'articolo 2702 del codice civile che recita: "La scrittura privata 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". In sostanza, nel caso di firma non autenticata, se un soggetto disconosce una firma su un documento attribuito a sé o ad altri, sarà suo l'onere di dare la prova della falsità della firma (un brocardo latino ricorda che *onus probandi incumbit in ei qui dicit*[2]). Lo strumento giuridico di ordine penale per verificare al falsità dell'atto è la 'querela di falso'. Diverso è il caso della firma autenticata in quanto in tale circostanza siamo in presenza di un notaio o un altro pubblico ufficiale, quindi un soggetto a cui è attribuita fede pubblica, che attesta l'autenticità della sottoscrizione, apposta appunto in sua presenza.

Le firme elettroniche, ed in particolare la firma digitale, per certi versi, ampliano il concetto di sottoscrizione autografa.

Il merito del citato DPR n. 513/1997 non sta solo nell'aver fissato la definizione di documento informatico, ma anche nell'aver introdotto il concetto di firma digitale come "il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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". Questa definizione di firma digitale prevede, pertanto, che l'applicazione della stessa possa avvenire solamente con l'utilizzo di un sistema di crittografia "a chiavi asimmetriche". Il sistema – basato sull'utilizzazione di una chiave privata e quindi segreta e di una chiave pubblica reperibile in appositi elenchi pubblici – garantisce contemporaneamente fino a quattro requisiti dell'atto sottoscritto: 1) provenienza (paternità); 2) irrifiutabilità (non ripudio); 3) immodificabilità; 4) segretezza. La combinazione delle due chiavi consente di codificare e decodificare il documento.

Il legislatore europeo con la direttiva 1999/93/CE ha ampliato la nozione di firma elettronica prevedendone quattro tipologie differenti: la firma elettronica semplice, la firma elettronica avanzata, la firma elettronica qualificata, la firma digitale.

Il Codice dell'amministrazione digitale ha armonizzato la normativa e ha dettato definitivamente la disciplina del documento informatico e delle firme elettroniche.

L'articolo 1 del CAD definisce il 'documento informatico' come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" e all'articolo 20 ne mette in evidenza l'idoneità a soddisfare il requisito della forma scritta e la sua valutabilità in giudizio tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità.

Il valore probatorio del documento informatico è determinato secondo una scala decrescente. Se è sottoscritto con firma digitale o altra firma elettronica qualificata o avanzata l'efficacia probatoria sarà più forte; se è possibile identificare un soggetto tramite una procedura informatica semplice (firma elettronica semplice) l'efficacia probatoria sarà più debole.

La firma elettronica semplice è costituita da un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica. Non essendoci alcun riferimento al termine 'documento', la firma elettronica semplice può essere rappresentata da un insieme di dati usato per autenticarsi, come ad esempio una utenza con *user id* e *password* che dà accesso ad un servizio e permette di operare all'interno di un sistema protetto (*email*, *social network, intranet*).

[2] Il principio generale prevede dunque che l'onere della prova incombe su colui che afferma qualcosa.

La firma elettronica avanzata è definita come l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la sua connessione univoca al firmatario e consente di rilevare se i dati stessi siano stati successivamente modificati. Dal documento così sottoscritto è permesso identificare in maniera certa il firmatario e, inoltre, rilevare se il documento stesso è stato modificato dopo la firma. Il firmatario, ovviamente, deve avere il controllo esclusivo sui mezzi per apporre questo tipo di firma. Un esempio di tale firma è il processo di firma grafometrica che soddisfa i requisiti prescritti dalle regole tecniche di cui al DPCM del 22 febbraio 2013 (si pensi ai dispositivi grafometrici delle banche o delle assicurazioni, degli alberghi). Senza entrare troppo nei particolari, e premesso che possono esistere diverse soluzioni di firma grafometrica, un principio generale di queste tipologie di firma è che esse collezionano dati biometrici del firmatario (es. pressione, velocità di firma, tratto, ecc.) e li fondono in maniera permanente con il documento firmato. La legge riconosce alla firma elettronica avanzata un ambito di applicabilità inferiore a quello della firma digitale, in quanto la firma elettronica avanzata non può essere usata per i contratti che trattano vendite o locazioni di immobili e hanno valenza solo nei rapporti tra firmatario e controparte che gli ha proposto di usare quella particolare soluzione di firma; non ha cioè una valenza verso tutti (*erga omnes*) come avviene per la firma digitale. Questo motivo la rende non adatta per i rapporti con la pubblica amministrazione.

La firma elettronica qualificata è un particolare tipo di firma elettronica avanzata, basata su un certificato qualificato, e realizzata mediante un dispositivo sicuro per la creazione della firma. Sono presenti due elementi addizionali rispetto alle firme che abbiamo descritto finora: un certificato rilasciato da un'autorità di certificazione (CA[3]), accreditata presso AgID, ed un dispositivo fisico sicuro per la creazione della firma. Il certificato è un documento informatico contenente un'attestazione dell'identità, proveniente da un soggetto terzo fiduciario (CA), dotato di specifici criteri di affidabilità, che permette di riporre fiducia nel meccanismo di sottoscrizione. Quanto al dispositivo si tratta di un dispositivo sicuro (un *token usb*, una *smart card* o un sistema di *one time password – otp*, nel caso della firma remota[4]) che, inserito nel *device*, permette di perfezionare l'operazione di firma su un documento informatico. In questi casi, i dispositivi devono garantire la conformità ai requisiti di sicurezza molto stringenti, fissati dalla normativa vigente, per assicurare il controllo esclusivo del firmatario sulla propria firma.

La firma digitale è basata su un certificato qualificato e su un sistema di chiavi crittografiche asimmetriche, una pubblica e una privata, correlate tra loro. Il sistema a doppia chiave consente, come accennato poco sopra, al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di assicurare provenienza, non ripudio, integrità e segretezza di un documento informatico o di un insieme di documenti informatici. Il complesso sistema crittografico presente nella firma digitale si aziona con l'incrocio della chiave pubblica e della chiave privata che ciascun soggetto firmatario possiede.

La chiave pubblica del titolare della firma digitale è disponibile a tutti (gli elenchi delle chiavi pubbliche sono disponibili presso le CCAA) e con essa è possibile verificare che il documento sia stato effettivamente firmato dal soggetto che afferma di esserne l'autore e non sia stato alterato nel tempo. La chiave privata è, ovviamente, conosciuta soltanto dal soggetto titolare della firma digitale e consente di sottoscrivere i documenti e, se lo desidera, secretarli.

[3] L'autorità di certificazione, dopo aver riconosciuto tramite valido documento di identità, il richiedente la firma digitale, emette un certificato digitale riportante i dati del titolare della firma, la scadenza della validità del certificato stesso e la chiave pubblica attribuitagli. In alcuni casi, il certificato può riportare anche limiti di firma sia di ordine economico sia di ordine temporale sia in relazione alla tipologia di atti che è possibile sottoscrivere.

[4] La firma digitale remota non necessita l'installazione di nuovo hardware (lettori di smart card) o l'inserimento di token usb nel *device* che si utilizza per la sottoscrizione ed il meccanismo di firma digitale sui documenti si completa esclusivamente per via telematica, anche tramite verifica con otp ottenuto con lo smartphone.

La cifratura non viene applicata su tutto il testo, ma soltanto ad una parte di esso, cioè sull'impronta (*digest*) del documento stesso, estratta automaticamente dal testo da parte del software di firma. Il sistema quindi crea l'impronta del testo da sottoscrivere con una funzione di *hash* e su quella (che è costituita da un numero di caratteri fisso indipendentemente dal numero dei caratteri che compone il documento) viene esercitata la cifratura all'atto della sottoscrizione.

Con il Regolamento europeo *electronic IDentification Authentication and Signature* (eIDAS), del 2014, sia la firma elettronica qualificata che la firma digitale hanno acquisito pieno valore in tutto il territorio dell'Unione, essendoci regole tecniche comuni in tutti gli Stati membri.

Il CAD prevede, inoltre, un meccanismo automatico di apposizione di firma a seguito di una particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo, al fine di sottoscrivere flussi copiosi di documenti (cd. "firma massiva") di *routine*, come ad esempio i certificati in cui la discrezionalità sul contenuto è del tutto assente.

In generale, la firma digitale può essere apposta tramite software di firma dedicati e si distingue in tre tipologie: 1) la firma CAdES (*Cryptographic Message Syntax Advanced Electronic Signature*) produce una estensione "p7m" al file e sigilla in una busta digitale il contenuto del documento insieme al certificato di firma. Un qualunque software di firma (validato dall'AgID) consente l'estrazione dalla busta del file firmato; 2) la firma PAdES *(PDF Advanced Electronic Signatures*) può essere apposta ai documenti in formato "pdf", i quali conserveranno la medesima estensione. I file firmati in questo modo potranno essere letti, e potrà verificarsi la firma, con qualunque software pdf-*reader*. Questo formato permette, inoltre, di apportare modifiche al documento con ulteriori firme senza che venga persa la traccia del file firmato in origine. Infine, può apporsi un segno grafico sul documento per rappresentare l'avvenuta sottoscrizione; 3) la firma XAdES (*XML Advanced Electronic Signature*), come per i pdf, non prevede la creazione di una busta, non modifica l'estensione del file e permette di accedere ai metadati contenuti all'interno del documento (informazioni contenute nei *tag* xml) in modo da consentire anche alle macchine l'accesso alle informazioni (*machine readable form*). Con quest'ultima tipologia di firma vi è la possibilità di sottoscrivere singole parti del documento, ad esempio, nei casi in cui il documento sia stato scritto a più mani e ciascuno debba firmare solo la propria parte.

IL TIMBRO DIGITALE

Il timbro digitale è un codice grafico bidimensionale impresso nel documento originale elettronico che permette anche dopo la stampa di conservare le garanzie di autenticità e di verificarne l'eventuale alterazione. La previsione all'art. 23, comma 2-bis, del CAD puntualmente recita: "Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le 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". La norma consente, ad esempio, di emettere certificati senza la necessità di utilizzare supporti speciali, quali carta filigranata, timbri a secco, firme autografe, ecc., per garantirne l'autenticità.

L'esigenza tutelata dalla previsione del CAD riguarda l'ottimizzazione della vita dei documenti prodotti in originale in formato elettronico con firma digitale. Infatti, in questo caso, anche se il documento informatico sottoscritto con firma digitale viene stampato, la presenza del timbro digitale fa sì che non si interrompa la catena di valore della firma digitale ivi apposta, poiché il contrassegno consente di verificare l'autenticità e quindi la validità del documento su carta.

La verifica deve poter essere effettuata in ogni momento attraverso appositi software. I programmi per effettuare tale verifica sono resi disponibili gratuitamente e mantenuti costantemente aggiornati da parte dei fornitori attraverso l'AgID che provvede a verificare in via preliminare la rispondenza dei suddetti software alle linee guida. Pertanto, per effettuare la verifica della corrispondenza della copia analogica al documento amministrativo informatico originale sarà possibile utilizzare direttamente i software disponibili sul sito dell'AgID o quelli messi a disposizione sui portali delle amministrazioni emananti.

Per effettuare la verifica della corrispondenza il software deve consentire: 1. l'interpretazione del codice che identifica la tipologia del contrassegno utilizzato; 2. la decodifica del contenuto del contrassegno e il salvataggio di tale contenuto da parte del soggetto che effettua la verifica; 3. nel caso in cui il contenuto del contrassegno sia sottoscritto con firma elettronica qualificata o firma digitale, la verifica della firma utilizzando l'apposito software messo a disposizione dal certificatore accreditato; 4. la visualizzazione in chiaro del contenuto del contrassegno per verificarne la corrispondenza con il contenuto della copia analogica.

LA MARCA TEMPORALE

Un altro strumento disciplinato dal Regolamento europeo eIDAS è la marca temporale che è possibile applicare su un documento o su una serie di documenti. Consiste nella generazione, da parte di una terza parte fidata (CA), di una firma digitale sul documento (anche aggiuntiva rispetto a quella del sottoscrittore originario) a cui è associata l'informazione relativa ad una data e ad un'ora certa.

La marcatura temporale consente quindi di stabilire l'esistenza di un documento informatico o di un gruppo di documenti informatici a partire da un certo istante temporale e di opporlo ai terzi.

Il tempo, cui fanno riferimento le marche temporali, è riferito al Tempo Universale Coordinato (UTC) ed è assicurato da un ricevitore radio sintonizzato con il segnale emesso dall'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino. L'apposizione della marca temporale non incide sul contenuto del documento e non ne modifica la sua firma originaria.

LA POSTA ELETTRONICA CERTIFICATA

Il servizio di posta elettronica certificata (PEC) consente di spedire qualunque tipo di documento prodotto con strumenti informatici da un *server* ad un altro in maniera certa e sicura. La PEC, infatti, è un sistema di posta elettronica avanzato, idoneo a fornire al mittente documentazione elettronica con valenza legale attestante l'invio e la consegna di documenti informatici. Certificare l'invio e la ricezione del documento significa, da un lato, fornire al mittente da parte del proprio gestore di PEC una ricevuta che è prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione, dall'altro, con riferimento all'arrivo del messaggio al destinatario, fornire al mittente, da parte del gestore di PEC del destinatario e dello stesso mittente, la ricevuta di avvenuta o mancata consegna con precisa indicazione temporale. Questa possibilità è finalizzata a garantire l'utente nell'ipotesi di un contenzioso, laddove si richieda la documentazione attestante l'invio e la ricezione di un messaggio. Semplificando, la PEC rappresenta una evoluzione informatica del tradizionale servizio postale di raccomandata con avviso di ricevimento.

La disciplina della PEC risale ad una legge del 2003, ripresa poco dopo dal CAD che ha regolato la materia introducendo il concetto di domicilio digitale equivalente in tutto e per tutto a quello fisico (art. 6), precisando poi che la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata (art. 48). Il destinatario di un messaggio di PEC non può negare l'avvenuta ricezione, posto che la ricevuta di avvenuta consegna, firmata ed inviata al mittente dal gestore di PEC scelto dal destinatario, riporti le indicazioni della data e dell'ora in cui il messaggio è stato consegnato nella casella di PEC del destinatario, certificandone l'avvenuta consegna.

Siffatta certificazione è possibile solamente nel caso in cui entrambi gli interlocutori dispongano di caselle PEC, sia pure appartenenti a gestori diversi. Alcuni *provider* PEC consentono di inviare mail ad indirizzi non PEC, ma ovviamente questo tipo di scambio documentale non soddisfa la previsione di cui all'art. 48 del CAD.

L'art. 49 del CAD dispone che "gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche", ribadendo in tal modo il principio di segretezza della corrispondenza costituzionalmente garantito all'art. 15.

I gestori di questo tipo di servizio firmano digitalmente tutto quanto da loro generato: ricevute, buste di trasporto e avvisi e hanno l'obbligo di registrare tutte le operazioni relative alle proprie PEC nel *log* del proprio sistema, di estrarre le registrazioni con cadenza giornaliera, apponendo una marca temporale e di conservarle per almeno trenta mesi, nel rispetto delle norme di legge in materia di conservazione.

Il registro di *log* deve contenere le seguenti informazioni: il codice identificativo univoco assegnato al messaggio originale (*message-id*), la data e l'ora dell'evento, il mittente del messaggio originale, i destinatari del messaggio originale; l'oggetto del messaggio originale, il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.), il codice identificativo (*message-id*) dei messaggi correlati generati (ricevute, errori, ecc.), il gestore mittente.

Il citato Regolamento eIDAS, oltre ad intervenire in materia di firme elettroniche, ha istituito il Servizio elettronico di recapito certificato (SERC), che costituisce un'alternativa alla PEC. Il Regolamento eIDAS definisce il Servizio elettronico di recapito certificato come "un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, tra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate"; nello specifico vengono definiti altresì i "servizi elettronici di recapito qualificato certificato" quelli che "soddisfano i requisiti seguenti: a) sono forniti da uno o più prestatori di servizi fiduciari qualificati; b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente; c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati; d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati; e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi; f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata. Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati".

Il decreto legge n. 185/08, convertito nella legge n. 2 del 28/01/2009, ha introdotto l'obbligo per società, professionisti e PPAA di istituire una versione virtuale della sede legale, tramite PEC, presso cui potranno essere recapitati con valore legale atti e documenti.

LE CARTE ELETTRONICHE

Già con il primo piano di azione per l'e-Government, orientato alla digitalizzazione della PA, risalente al 2000, era stata prevista la diffusione di strumenti di autenticazione in rete, quali la carta d'identità elettronica (CIE) e la carta nazionale dei servizi (CNS), per l'accesso ai servizi telematici erogati dalle PPAA. Il CAD, all'art. 66, ne disciplina compiutamente i contenuti, demandando le specifiche tecniche ai decreti attuativi ed alle relative linee guida.

La CIE, invero, nasce con la legge Bassanini 2 del 1997, la n. 127, intitolata "Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo", la quale,

all'art. 2, demanda al governo la definizione delle modalità per il rilascio ed il rinnovo della carta di identità su supporto magnetico. Successivamente, l'art. 1 del D.Lgs. n. 10/2002 definisce la CIE quale "documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare" e dispone anche l'istituzione della CNS, definendola "il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni".

Dal 2006 i Comuni avrebbero dovuto rilasciare la CIE ai richiedenti in sostituzione di quella cartacea, ma i costi per acquistare gli strumenti necessari per produrla e la scarsa utilità pratica della stessa (nella prima versione realizzata i servizi elettronici connessi erano assai ridotti) ne hanno rallentato notevolmente la distribuzione.

Le vicende traverse della CIE si sono sbloccate solo di recente quando sono stati implementati i servizi aggiuntivi che hanno suscitato una vera spinta all'utilizzo. Dal punto di vista applicativo la CIE si è sviluppata oggi in una carta ibrida, in quanto integra nel supporto in policarbonato anticontraffazione, mediante la tecnica del *laser engraving*, la fotografia e i dati del cittadino. Ai fini della sicurezza il supporto è corredato anche da ologrammi, sfondi di sicurezza, micro scritture, *guilloche*, ecc. e contiene un microprocessore a radiofrequenza (*near field communication*) con fattore abilitante per i servizi online e ai fini dell'acquisizione di identità digitali su Spid. La verifica dell'identità del titolare può essere effettuata sia in maniera tradizionale, essendo 'a vista' i dati anagrafici e la fotografia, sia tramite il processore con l'applicazione "ICAO MRTD", la stessa presente sul passaporto elettronico emesso da tutti i paesi europei. L'applicazione può contenere, altresì, a richiesta del titolare, l'indicazione del gruppo sanguigno, le opzioni di carattere sanitario previste dalla legge, alcuni dati biometrici, con esclusione, in ogni caso, del DNA. I dati riportati sono firmati digitalmente dal Ministero dell'Interno. L'accesso alle impronte digitali è permesso solo a chi è in possesso di specifiche autorizzazioni (le forze dell'ordine, la polizia di frontiera). È escluso che un qualunque dispositivo possa leggere i dati personali contenuti nella CIE all'insaputa del titolare. Tutta la conversazione tra la CIE e i lettori è cifrata con delle chiavi che vengono cambiate ad ogni sessione con algoritmi standard che ne impediscono l'intercettazione.

Al fine di razionalizzare, semplificare l'azione amministrativa e per accedere a servizi online della PA il *chip* contiene una *user id* associata al codice di identificazione personale (pin) consegnato al titolare della carta.

La carta nazionale (o regionale) dei servizi (CNS), che in alcune regioni coincide con la tessera sanitaria, è, invece, una *smart card* che non ha funzione di documento di riconoscimento 'a vista', perciò non contiene la foto del titolare ed è provvista esclusivamente di un *microchip*.

La CNS contiene anch'essa un certificato di autenticazione (emesso, ovviamente, da una CA riconosciuta) consistente nell'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare della carta nazionale dei servizi, al pari di una firma digitale. Essa contiene i dati identificativi del titolare, il codice numerico di identificazione delle carte nonché le date del suo rilascio e della sua scadenza. Essa può eventualmente contenere informazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione dei servizi al cittadino, cui si può accedere tramite la carta. Occorre precisare che i dati personali che vengono forniti ai fini dell'accesso ai servizi sono utilizzabili esclusivamente al fine di identificare in rete il titolare della carta nazionale dei servizi e per verificare la sua legittimazione al servizio.

IL SISTEMA PUBBLICO DI IDENTITÀ DIGITALE - SPID

Il DPCM del 24 ottobre 2014 ha novellato l'art. 64 del CAD, prevedendo per i cittadini e le imprese il Sistema pubblico di identità digitale (Spid), quale strumento di accesso elettronico unico, sicuro e protetto ai servizi online erogati delle PPAA. L'identità digitale dei soggetti richiedenti (credenziali) è rilasciata da appositi gestori (*identity provider*), soggetti privati accreditati presso

l'AgID, nel rispetto delle regole emesse dalla stessa. È previsto che tutte le pubbliche amministrazioni devono rendere i propri servizi online accessibili tramite Spid al fine di favorire e di semplificare l'utilizzo dei servizi digitali. Spid è rivolto solo ai maggiorenni e non prevede costi, anche se i gestori di identità digitale possono proporre agli utenti, ed eventualmente aggiungere, servizi a pagamento. Il sistema prevede tre livelli di sicurezza: un primo, permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente; un secondo – necessario per servizi che richiedono un grado di sicurezza maggiore –, permette l'accesso attraverso un nome utente e una password scelti dall'utente, più la generazione di un codice temporaneo di accesso (otp); per attivare il servizio Spid con credenziali di terzo livello è necessario effettuare la procedura di riconoscimento utilizzando la carta nazionale dei servizi (CNS), la tessera sanitaria (sempre con CNS), la carta di identità elettronica (CIE) oppure un dispositivo di firma digitale o di firma remota. Con questo terzo livello di sicurezza è possibile ottenere servizi ed informazioni che necessitano di una sottoscrizione di livello pari alla firma digitale o che hanno ad oggetto anche categorie particolari di dati personali (ex art. 9 del regolamento europeo 679/2016 sul trattamento dei dati personali). Infatti, questo livello si basa su autenticazione informatica a due fattori basato su certificati digitali, al pari della firma digitale, e criteri di custodia delle chiavi private sui dispositivi locali o remoti, per soddisfare i requisiti di sicurezza previsti dalla legge comunitaria sulle firme elettroniche[5]. È utile qui sottolineare che Spid di terzo livello, essendo associato ad un altro strumento collegato al titolare, dovrà essere rinnovato quando lo strumento collegato (CIE, certificato di firma digitale, ecc) scade.

Anche i servizi digitali erogati dai privati possono essere resi accessibili tramite Spid in una logica di convergenza degli strumenti e di facilitazione agli utenti, sempre nel rispetto delle regole tecniche dettate dall'AgID. Ciascun soggetto – solo persone fisiche, al momento – può richiedere, se lo reputa opportuno in base alle proprie attività professionali, una o più identità digitali, anche con livelli di sicurezza differenti.

È bene notare che il proliferare di carte e sistemi elettronici (CIE, CNS e Spid) per il riconoscimento in rete dei cittadini è il frutto di una sequenza di norme che si sono succedute nel tempo e che hanno favorito la realizzazione del rapporto virtuale tra amministrazioni pubbliche e utenza.

IL SISTEMA DI PAGAMENTO 'PAGO PA'

A norma dell'art. 5 del CAD, tutte le pubbliche amministrazioni, i gestori di pubblici servizi e le società a partecipazione pubblica sono obbligati ad accettare i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i pagamenti di modico valore, quelli basati sull'uso del credito telefonico. L'AgID mette a disposizione, attraverso il Sistema pubblico di connettività, una piattaforma tecnologica – Pago PA – per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, al fine di assicurare, attraverso Spid, l'autenticazione dei soggetti interessati all'operazione in tutta la gestione del processo di pagamento.

Il sistema Pago PA permette di pagare tributi, tasse, utenze, rette, quote associative, bolli e qualsiasi altro tipo di debito verso le Pubbliche Amministrazioni centrali e locali ed anche verso

[5] In proposito, l'allegato 3 della direttiva comunitaria del 1999, elenca i requisiti relativi ai dispositivi per la creazione di una firma sicura. In particolare, i dispositivi per la creazione di una firma sicura, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che: a) i dati per la creazione della firma utilizzati nella generazione della stessa compaiano solo una volta e che sia ragionevolmente garantita la loro riservatezza; b) i dati per la creazione della firma utilizzati nella generazione della stessa non siano, entro limiti ragionevoli di sicurezza, derivati e la firma sia protetta da contraffazioni compiute con l'impiego di tecnologia attualmente disponibile; c) i dati per la creazione della firma utilizzati nella generazione della stessa siano sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi. E, inoltre, i dispositivi per la creazione di una firma sicura devono garantire di non alterare i dati da firmare né devono impedire che tali dati siano presentati al firmatario prima dell'operazione di firma.

altri soggetti, come le aziende a partecipazione pubblica, le scuole, le università, le ASL nonché verso società private, purché aderenti alle linee guida tecniche dettate dall'AgID, che forniscono servizi a pagamento verso i cittadini e le imprese. Il versamento può essere effettuato direttamente dal debitore attraverso il sito web dell'ente creditore o per il tramite dei prestatori di servizi di pagamento privati (PSP), principalmente, banche ed altri istituti di credito.

CONCLUSIONI

Dopo quasi trent'anni di norme varate e sperimentazioni, l'amministrazione digitale in Italia è tutt'altro che *smart*; troppo spesso si lavora ancora con i moduli e con fascicoli di documenti cartacei, si opera in tempi eccessivamente lunghi, ci si scontra con inefficienze gravi imputabili a smarrimenti di documenti e collocamenti errati di pratiche, lungaggini dovute alla gestione cartacea dei flussi documentali, oggi inaccettabili.

Di contro, ma i casi purtroppo non sono numerosi, si assiste a fenomeni di virtuosismo amministrativo in alcuni luoghi legati più alla illuminazione dei singoli che all'adeguatezza del contesto. Se le leggi sono al servizio dell'efficienza erra chi artificiosamente le interpreta con eccessiva prudenza per continuare a operare con una mentalità 'analogica' e decisamente obsoleta.

Il lato positivo sta nella considerazione che ancora moltissimo si può e si deve fare e in tal senso la tecnologia fornisce sempre stimoli interessanti.

Molti degli strumenti che sono stati descritti muteranno nei prossimi anni e la nostra vita pubblica e professionale si modificherà in continuazione. Si pensi alla tecnologia della *blockchain* – una forma di condivisione distribuita delle informazioni, in grado di garantire a tutti i componenti della catena la possibilità di verificare e controllare atti e informazioni, che vengono registrati in archivi e registri condivisi con caratteristiche di inalterabilità, di immodificabilità e di tracciamento di tutti gli interventi e, pertanto, dove corruzione e abusi di potere saranno certamente meno frequenti perché impossibili da attuare o, comunque, ben riconducibili ai responsabili – oppure qualcosa che le si rassomiglierà, che potrà essere utile nei procedimenti amministrativi, nel processo giurisdizionale telematico, nella gestione dei registri pubblici, nel rispetto dei vincoli sulla trasparenza e che potrà dare un forte contributo ai sistemi incentrati sulla fiducia, quali la PEC, la firma digitale, il timbro digitale e chissà quanto altro che oggi riusciamo soltanto ad immaginare.