Rosario Carrisi
Gianvito Campeggio

Cittadino Digitale

Quali strumenti per una "cittadinanza digitale" consapevole

Prefazione di Marco Mancarella

Rosario Carrisi
Gianvito Campeggio

Cittadino Digitale

Quali strumenti per una
"cittadinanza digitale" consapevole

Prefazione di Marco Mancarella

Gli autori svolgono abitualmente seminari in tutta Italia
su questi temi e altri argomenti.
Per contatti e informazioni scrivere a rosario@carrisi.it

Copertina di Alessandro Carrisi

Giugno 2022

“Ben informati, gli uomini sono dei cittadini;
mal informati diventano sudditi.”

Alfred Sauvy

“… il digitale non è lo scopo, ma il mezzo.”

Marco La Diega

Indice

Prefazione

di Marco Mancarella[1]

Nel panorama editoriale italiano sussiste, da sempre, una duplice necessità. Innanzitutto, la presenza di un testo che sia in grado di fornire una visione esaustiva, scientificamente corretta, del concetto, non ancora normativamente definito, di "cittadinanza digitale" e, al contempo, uno sguardo proiettato sulla futura veste della Pubblica Amministrazione, destinata sempre più a trasformarsi da "struttura fondata sulla carta" a "struttura fondata sui bit", ovvero su quelle unità elementari dell'informazione senza le quali il mondo elettronico non potrebbe esistere, determinando in tal modo, finalmente, il passaggio definitivo dall'odierna situazione di "informatica parallela", caratterizzata da una costante sovrapposizione di processi cartacei e digitali, ad una situazione di "informatica pura", ove il processo cartaceo divenga solo un ricordo e l'agere digitale la sola certezza.

[1] Professore Associato di Informatica giuridica presso UniSalento. Avvocato, già Coordinatore del Tavolo permanente per l'Amministrazione Digitale - TAD di UniSalento, Direttore dell'Osservatorio Mediterraneo sulla Cultura Digitale – MODiCT, componente del Consiglio Scientifico di @LawLab presso la LUISS – Guido Carli di Roma, componente del Direttivo ANDIG (Associazione Nazionale Docenti di Informatica Giuridica), Consulente di I livello del FORMEZ – Presidenza del Consiglio dei Ministri, Amministratore Unico di LiquidLaw s.r.l. – Azienda spinoff UniSalento (www.liquidlaw.it) e componente nel 2019 del tavolo di confronto con il Gruppo di lavoro AGID per le nuove Regole tecniche/Linee guida del Codice dell'Amministrazione Digitale.

A tale prima necessità editoriale, come detto, se ne affianca però un'altra, ovvero l'esigenza di un testo che ad un approccio normativo-dottrinario sia in grado di affiancare una chiara vis pratica. Un testo, in definitiva, che possa offrire un supporto anche operativo, per chi già lavora all'interno di una Pubblica Amministrazione. Ma, al contempo, un testo comunque accessibile al cittadino curioso di approfondire la sua nuova veste e identità: quella digitale.

Stefano Rodotà, indimenticato primo Garante privacy nel nostro Paese e fine interprete del cambiamento, giustamente sottolineava: "I cittadini mostrano di preoccuparsi assai del loro "corpo elettronico", di una esistenza sempre più affidata alla dimensione astratta del trattamento elettronico delle loro informazioni. Le persone sono ormai conosciute da soggetti pubblici e privati quasi esclusivamente attraverso i dati che le riguardano, e che fanno di esse una entità disincarnata. Con enfasi riduzionista, per molti versi pericolosa, si dice che "noi siamo le nostre informazioni". La nostra identità viene così affidata al modo in cui queste informazioni vengono trattate, collegate, fatte circolare".

Il testo di Rosario Carrisi e Gianvito Campeggio riesce a soddisfare la duplice necessità su delineata, offrendo al lettore un quadro organico della normativa e prassi dell'agere amministrativo digitale e, conseguentemente, della nuova visione del cittadino moderno e dei suoi diritti. Uno sforzo, quest'ultimo, che detiene un carattere di unicità nel panorama dottrinario italiano, da sempre sin troppo legato ad una visione classica del concetto di cittadinanza. Potremmo definirla "analogica", ora quasi del tutto superata da quella "digitale".

Il lavoro degli Autori è stato rivolto, essenzialmente, a fornire al lettore un quadro semplificato della Pubblica Amministrazione digitale, attraverso una puntuale ricostruzione della normativa di settore, oggetto quotidianamente di modifiche da oltre un ventennio. La cd. era digitale nella quale oramai siamo immersi ha aggravato tale lavoro, con l'introduzione negli ultimi anni di una notevole quantità di riforme strutturali e organizzative nella Pubblica Amministrazione, fornendo però notevoli spunti di riflessione al giurista, al dipendente pubblico e allo stesso cittadino.

Oggigiorno è divenuto una sorta di "imperativo categorico" doversi confrontare con tematiche quali la validità del documento informatico e della sua sottoscrizione elettronica, la posta elettronica certificata, il domicilio digitale, gli strumenti di identificazione digitale ed i servizi telematici più evoluti per il cittadino e molto altro ancora. Chi rifiuta il confronto appare sempre più estromesso dall'evoluzione tecnologica pubblica, dalla stessa, oramai quasi del tutto avverata, Amministrazione digitale. Cosa ancor più grave, chi rifiuta il confronto appare, inoltre, incapace di far valere nelle adeguate sedi il proprio diritto soggettivo all'utilizzo delle tecnologie informatiche nei rapporti con la Pubblica Amministrazione, come sancito e giudizialmente assicurato dall'art. 3 del Codice dell'Amministrazione Digitale.

Il futuro è oggi e questo testo intende costituire un utile ed agile strumento di lettura del cambiamento in atto per permettere, a chi il confronto con il cambiamento ancora non lo abbia avviato, di approcciarsi, senza timori, ad esso.

Lecce, 10 giugno 2022 Marco Mancarella

Introduzione

Internet e le tecnologie hanno cambiato la vita e le abitudini delle persone.

Le nuove tecnologie stanno cambiando anche il rapporto tra cittadini e uffici pubblici rendendolo più semplice e trasparente.

Per questo motivo ai cittadini sono riconosciuti una serie di "diritti digitali" che compongono la "Carta della cittadinanza digitale". La carta della cittadinanza digitale è contenuta nel Codice dell'Amministrazione Digitale (CAD)[2] che costituisce il nucleo minino di diritti che le amministrazioni devono garantire a cittadini ed imprese.

Nella nostra società si moltiplicano le occasioni e la necessità di un rapporto costante e più diretto, di confronto e collaborazione, fra istituzioni pubbliche e cittadini (singoli o associazioni).

Sul fronte europeo, il rafforzamento e l'introduzione di nuove forme di partecipazione dei cittadini sono riconosciuti come importanti elementi del processo di ammodernamento delle istituzioni democratiche e di inclusione sociale. In tutto il mondo, stanno crescendo le iniziative dei governi democratici per favorire la partecipazione dei cittadini, di fronte alla maggiore complessità in cui agiscono gli attori pubblici, da un lato, e alla ricchezza delle esperienze e delle competenze

[2] Decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217

depositate presso i singoli cittadini, le associazioni, le comunità locali e professionali, dall'altro.

Il livello locale è fondamentale per il sostegno di questo processo di rinnovamento, data la caratteristica prossimità fra istituzioni locali e cittadini e la possibilità di un controllo ravvicinato sui processi decisionali e sui loro effetti.

Il cittadino per essere in condizione di dialogare con l'amministrazione ed esercitare i propri diritti deve poter essere favorito con interventi di alfabetizzazione digitale intervenendo su più versanti, a partire dalle pre-condizioni della partecipazione (accesso all'informazione, inclusione sociale, elettorato passivo ed attivo, iniziativa diretta), passando attraverso varie forme di consultazione dei cittadini nel corso dei processi di decisione, fino al coinvolgimento nella fase finale dei processi decisionali (voto).

Per realizzare questa "nuova" forma di partecipazione cittadina in modalità telematica ai processi decisionali delle istituzioni pubbliche, è necessario che la Pubblica Amministrazione sia fornita di strumenti utili per realizzare, in maniera efficiente ed efficace, gli obbiettivi richiesti, ovvero rispondere alle esigenze della società civile.[3] Si tratta di una doppia sfida per il Paese, non declinabile, rivolta sia ai cittadini che alla Pubblica Amministrazione.

L'allargamento della cittadinanza al digitale non passa solo attraverso la rete, le piattaforme informatiche, gli strumenti. La sfida più impegnativa è quella delle competenze (digitali) che i cittadini così come il personale dell'amministrazione devono acquisire e tenere costantemente aggiornate.

[3]https://temi.camera.it/leg18/temi/tl18_informatizzazione_delle_pubbliche_amministrazioni.html

La competenza digitale è sempre più centrale per una cittadinanza attiva e consapevole.

La diffusione delle tecnologie dell'informazione e comunicazione e la capillare disponibilità di connessione alla rete ha modificato lo scenario pubblico e privato dei cittadini. [4]

Le opportunità offerte dalle tecnologie richiedono una riflessione sull'inclusione digitale, ovvero la possibilità per tutti i cittadini di usufruire dei vantaggi derivati dall'uso delle tecnologie. L'inclusione digitale si tende a misurare in termini di accesso alle tecnologie, anche se non avviene esclusivamente tramite il possesso di mezzi tecnologici ma grazie alle conoscenze che si hanno per utilizzare tali mezzi.

Il traguardo della "Carta della Cittadinanza Digitale"[5], per alcuni arrivato troppo tardi, in realtà rischia di arrivare in maniera precipitosa (e a volte temuta) nella routine di molti altri. Per questo è necessaria una strategia di accompagnamento al cambiamento, di educazione a questa nuova dimensione della cittadinanza.

Perché la città digitale prenda forma e sia accogliente, è necessario ricordare a noi stessi che essere cittadini del XXI secolo vuol dire apprendere ed aggiornarsi ogni giorno.

La strategia 2025

Nel luglio 2020 è stato varato il **Piano triennale per l'informatica della pubblica amministrazione 2020-2022**[6] che prosegue e integra le linee di azione del Piano 2019-2021 e del Piano 2017-2019.

[4]http://www.cittadinanzadigitale.eu/wp-content/uploads/2015/11/digcomp_Ferrari_Troia.pdf
[5] http://www.cittadinanzadigitale.eu/blog/2015/10/29/carta-della-cittadinanza-digitale-nuove-sfide-per-cittadini-e-pa/
[6] https://www.agid.gov.it/it/agenzia/piano-triennale

L'attuazione del Piano, monitorata sul sito del **Dipartimento per la trasformazione digitale**[7], focalizza sulla realizzazione delle azioni previste dai piani precedenti ed è volto in particolare a:

- favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della pubblica amministrazione che costituisce il motore di sviluppo per tutto il Paese;
- promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale;
- contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

Nell'arco del triennio sono state definite circa 200 azioni: a carico di AgID e Dipartimento per la trasformazione digitale, altre a carico di PA centrali e locali.

Nel dicembre 2019, il Ministro per l'innovazione tecnologica e la digitalizzazione ha presentato il documento "**2025 - Strategia per l'innovazione tecnologica e la digitalizzazione del Paese".**[8]

La strategia di innovazione è articolata in tre "sfide" principali: la digitalizzazione della società, l'innovazione del Paese e lo sviluppo sostenibile e etico della società nel suo complesso. Il piano descrive un processo di trasformazione strutturale del Paese, dalle infrastrutture digitali, ai servizi della Pubblica Amministrazione, alla collaborazione tra pubblico e privato nel generare innovazione.

[7] https://innovazione.gov.it/dipartimento/
[8] https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf/

Piano nazionale Triennale per riformare l'Informatica nella P.A.

Il **Piano nazionale di riforma 2020**[9], presentato dal Governo alle Camere nel luglio 2020, include nell'area prioritaria l'innovazione e la digitalizzazione della pubblica amministrazione, individuando le misure necessarie per rispondere alle raccomandazioni in materia trasmesse dal Consiglio europeo e attuare gli Obiettivi di sviluppo sostenibile (SDGs) dell'Agenda 2030 delle Nazioni Unite.

Già nelle Raccomandazioni del 2019, il Consiglio sottolineava la necessità di *"migliorare l'efficienza della pubblica amministrazione, in particolare investendo nelle competenze dei dipendenti pubblici, accelerando la digitalizzazione e aumentando l'efficienza e la qualità dei servizi pubblici locali"* (Raccomandazione n. 3).

La Commissione Europea, nella Relazione per Paese relativa all'Italia 2020 (cd. Country Report) del febbraio 2020 ha riconosciuto che si sono verificati alcuni progressi nell'aumentare l'efficienza e la digitalizzazione della pubblica amministrazione.

Per quanto riguarda in modo specifico l'attuazione della succitata Raccomandazione n. 3 del 2019, la Commissione registra alcuni progressi nel miglioramento del livello di efficacia e digitalizzazione della pubblica amministrazione (Decreto Concretezza, disegno di legge sull'occupazione nel settore pubblico, creazione del ministero dell'innovazione e della digitalizzazione, avvio dell'applicazione IO, ecc.).

Il report si sofferma in modo particolare sulla digitalizzazione dei servizi pubblici, riconoscendo che

[9] https://temi.camera.it/leg18/dossier/OCD18-13873/programma-nazionale-riforma-2020-sezione-iii-del-def-2020-e-allegati-5.html

l'Italia sta lentamente migliorando la sua performance nell'offerta di servizi pubblici digitali per i cittadini e le imprese.

Nelle Raccomandazioni specifiche all'Italia il Consiglio europeo del 20 maggio 2020, invita l'Italia ad adottare provvedimenti, nel 2020 e nel 2021, volti a realizzare "un'infrastruttura digitale rafforzata per garantire la fornitura di servizi essenziali" (Raccomandazione n. 3) e a "migliorare […] il funzionamento della pubblica amministrazione" (Raccomandazione n. 4).

Tali Raccomandazioni trovano fondamento nella considerazione che *"un'amministrazione pubblica efficace è cruciale per garantire che le misure adottate per affrontare l'emergenza e sostenere la ripresa economica non siano rallentate nella loro attuazione".* Il Consiglio ritiene basso il livello di digitalizzazione e scarsa la capacità amministrativa, sottolineando che "Prima della crisi la digitalizzazione nelle amministrazioni pubbliche era disomogenea. L'interazione online tra le autorità e la popolazione era modesta e rimane bassa la percentuale di procedure amministrative gestite dalle regioni e dai comuni che possono essere avviate e portate a termine interamente in modo elettronico. La crisi ha inoltre messo in luce la mancanza di interoperabilità dei servizi pubblici digitali" (punto 24 dei considerando premessi alle Raccomandazioni).

Il Governo nel PNR 2020 sottolinea in primo luogo che il Piano di Rilancio e, al suo interno, il Recovery Plan, si baseranno su un incremento della spesa, tra cui quella per l'innovazione e la digitalizzazione.

La modernizzazione del Paese, intesa anzitutto, come disponibilità a disporre di una Pubblica Amministrazione efficiente, digitalizzata, ben organizzata e sburocratizzata, veramente al servizio del cittadino, costituisce una delle tre linee strategiche attorno a cui è costruito il Piano di rilancio

(assieme a Transizione ecologica e Inclusione sociale e territoriale, parità di genere).

Il volano per la creazione di una PA connessa con cittadini e imprese è costituito dal piano Italia 2025. Strategia per l'innovazione tecnologica e la digitalizzazione del Paese, presentato nel dicembre 2019 dal Ministro per l'innovazione tecnologica e la digitalizzazione.

La strategia di innovazione è articolata in tre "sfide" principali, mutuate dagli Obiettivi di Sviluppo Sostenibile (SDGs) delle Nazioni Unite:

- la digitalizzazione della società;
- l'innovazione del Paese;
- lo sviluppo sostenibile e etico della società nel suo complesso.

Al fine di rilanciare la semplificazione mediante il rafforzamento dell'utilizzo delle tecnologie digitali per l'accesso ai servizi delle Pubbliche Amministrazioni, il Governo intende potenziare l'offerta di servizi in rete e il sistema di identità digitale anche attraverso la promozione dell'uso delle stesse ai fini dell'identificazione degli utenti, consentendo l'accesso ai servizi on line previa identificazione attraverso il sistema **SPID** e la **Carta di Identità Elettronica (CIE**) dove si è aggiunto anche il **Progetto IO,** che cambierà radicalmente il modello di interazione tra cittadini e amministrazione.

Le sfide che la P.A. deve affrontare

Dal 1° marzo 2021 gli strumenti Sistema Pubblico di Identità Digitale (SPID), Carta d'identità elettronica (CIE) e Carta nazionale dei servizi (CNS) sono le uniche "chiavi" che i cittadini potranno utilizzare per accedere ai servizi telematici della pubblica amministrazione (Agenzia delle Entrate, Enti Locali, INPS, INAIL, ecc).

In linea con quanto previsto dal Decreto Semplificazione 2020 (DL n. 76/2020), infatti, dal 1° marzo non è più possibile ottenere credenziali proprie da parte della pubblica amministrazione ed entro il 30 settembre 2021 quelle già in uso sono progressivamente dismesse.

E' quindi necessario dotarsi di una delle tre modalità di identificazione e autenticazione, SPID, CIE o CNS, riconosciute per i servizi on line di tutte le Pubbliche amministrazioni. Tutte le modalità per poter ottenere lo SPID sono disponibili sul sito istituzione predisposto dall'Agenzia per l'Italia Digitale (AgID) e dal Dipartimento per la trasformazione digitale (www.spid.gov.it).

Nel capitolo terzo (Le piattaforme abilitanti) ne parliamo in dettaglio di questi importanti strumenti.

Italia Digitale 2026

Il Piano Nazionale di Ripresa e Resilienza (PNRR)[10] destina il 27% delle risorse totali alla transizione digitale, i cui obiettivi e le cui iniziative sono regolati dalla **Strategia per l'Italia digitale 2016,** elaborata dal MITD – Ministro per l'innovazione tecnologica e la transizione digitale.

All'interno del Piano la Strategia si sviluppa in due assi: il primo riguarda le infrastrutture digitali e la connettività a banda ultra larga a cui saranno destinati 6,71 miliardi di euro in reti ultraveloci; il secondo riguarda tutti quegli interventi volti a trasformare la Pubblica Amministrazione (PA) in chiave digitale e potrà contare su una dotazione di 6,74 miliardi di euro.

La digitalizzazione delle infrastrutture tecnologiche e dei servizi pubblici è un impegno non più rimandabile per **far diventare la PA un vero "alleato" di cittadini e imprese**. Il

[10] https://assets.innovazione.gov.it/1620284306-pnrr.pdf

digitale è la soluzione in grado di accorciare drasticamente le "distanze" tra enti e individui e ridurre i tempi della burocrazia.

La strategia **Italia digitale 2026** include importanti investimenti per garantire la copertura di tutto il territorio con reti a banda ultra-larga, condizione necessaria per consentire alle imprese di catturare i benefici della digitalizzazione e più in generale per realizzare pienamente l'**obiettivo di gigabit society**. Una Pubblica Amministrazione (PA) efficace deve saper supportare cittadini e imprese con **servizi sempre più performanti e universalmente accessibili**, di cui il digitale è un presupposto essenziale.

***

La digitalizzazione, se fatta bene, riduce i costi, aumenta la velocità, permette una maggiore trasparenza, aiuta a formalizzare le procedure togliendo le ambiguità e l'arbitrio del singolo. Una PA digitalizzata in modo corretto può contrastare con estrema efficacia la corruzione e restituisce così ai cittadini i diritti che troppo spesso una burocrazia asfittica e prepotente nega loro.[11]

Lo scopo di questo testo è contribuire alla trasformazione digitale, cercando di aumentare in tutti la consapevolezza digitale, perché la trasformazione che va attuata è soprattutto culturale!

Infine per coloro che vogliono approfondire il tema della digitalizzazione possono consultare il progetto "**Italia login – la casa del cittadino**" attuato dall'Agenzia per l'Italia Digitale (AgID), con il supporto di Formez, che prevede la realizzazione di numerose attività a sostegno della trasformazione digitale nella PA, orientata a favorire il dialogo e l'interazione tra Stato, cittadini e imprese nel segno della semplificazione e dell'usabilità.

[11] COPPOLA P., Più Digilae Meno Corruzione Più Democrazia, Maggioli 2022

Capitolo primo

La cittadinanza digitale

1.1. Il concetto di cittadinanza digitale

Per **Cittadinanza digitale** si intende la capacità di un individuo di partecipare alla società online. Come ogni attore di una società, il cittadino digitale diviene portatore di diritti e doveri, fra questi quelli relativi all'uso dei servizi dell'amministrazione digitale.

Quindi è comprensibile che questa nuova tipologia di cittadinanza non è un'alternativa opposta a quella classica, ma, invece, la "*cittadinanza digitale*", non è altro che l'estensione naturale, il completamento e l'interpretazione globale delle nuove forme di interazione e di vita sociale e politica.[12] È quell'insieme, quindi, di diritti/doveri che, grazie al supporto di una serie di strumenti (l'identità, il domicilio, le firme digitali) e servizi, è diretta a semplificare il rapporto tra cittadini, imprese e pubblica amministrazione utilizzando le tecnologie digitali.

Le ultime novità in fatto di cittadinanza digitale si sono avute con il **D.lgs. n. 217 del 13 dicembre 2017**, pubblicato in Gazzetta ufficiale il 12 gennaio 2018 con il quale sono state emanate le disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al **codice dell'amministrazione digitale**, risalente al 2005, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124,

[12] Media, Tecnologie e Scuola. Per una nuova Cittadinanza Digitale. Pier Paolo Limone.

in materia di riorganizzazione delle amministrazioni pubbliche, chiamato proprio Carta della cittadinanza digitale.[13]

La Carta della cittadinanza digitale ha lo scopo di *"…. garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici…."*

Il termine cittadinanza digitale è espressione sempre più usata negli ultimi anni all'interno del dibattito sulle nuove tecnologie e la vita quotidiana, e ora anche a scuola. Assieme a "Costituzione" e "Sviluppo sostenibile", rappresenta uno dei tre assi della macro-categoria dell'Educazione civica.

L'istituto della cittadinanza, può essere letto come la capacità del cittadino di partecipare alla vita online dalla quale deriva una condizione di appartenenza a uno Stato, che di conseguenza rende l'individuo legato ad esso da diritti e doveri che tale relazione comporta». È la risultante di tre processi differenti: il rapporto intercorrente fra potere e cittadino all'interno di un preciso ordinamento politico; la partecipazione attiva del cittadino alla vita pubblica, il rapporto fra individuo e collettività. In particolare:

- **Rapporto fra il cittadino e lo Stato**: include tematiche quali la possibilità di accedere a servizi online, ottenere certificati, dialogare con la Pubblica Amministrazione, effettuare pagamenti, e di conseguenza l'introduzione a nuovi strumenti come l'identità digitale e il domicilio digitale del cittadino (ossia la possibilità di essere riconosciuti univocamente dall'Amministrazione Pubblica e avere un

[13] https://www.diritto.it/la-cittadinanza-digitale-e-i-diritti-digitali/

domicilio - una mail certificata ad esempio - identificato per la ricezione di comunicazioni);

- **Rapporti fra il cittadino e le aziende:** in digitale richiede spesso di uscire dai confini nazionali, visto che in Rete si usufruisce di servizi di aziende e multinazionali che si rifanno a legislazioni differenti. Entrano in gioco in questo caso competenze relative alla gestione dei propri dati personali (e alla possibilità di verificare come tali dati siano utilizzati dalle aziende), la gestione della privacy, l'accesso all'informazione e alla possibilità di definire quali siano i reali obiettivi dell'informazione con cui si entra in contatto (ad esempio imparare a differenziare una comunicazione che ha finalità commerciali ma che trasmette informazioni di cronaca, come un articolo sulle prestazioni di un motore sponsorizzato dall'azienda stessa);
- **Rapporti fra gli stessi cittadini**: include la possibilità di avere relazioni di lavoro o studio, culturali o di svago all'interno della Rete anche al di là dei confini dello stato.

Alla base delle tre direttrici vi è l'accesso a Internet quale diritto che favorisce l'esercizio di altri diritti fondamentali - dalla libertà di espressione a quella di informare ed essere informati, dall'iniziativa economica alla possibilità di innovare - è condizione necessaria per il pieno sviluppo individuale e sociale, come indicato dalla **Dichiarazione dei Diritti in Internet**[14] e sancito da numerose organizzazioni sovranazionali (fra cui ONU, G8 e UE).

Il percorso di digitalizzazione della pubblica amministrazione, anche per l'impulso della "**Carta della cittadinanza digitale**" (art. 1 della Legge 124/2015 di riforma

[14] https://www.interno.gov.it/it/notizie/dichiarazione-dei-diritti-internet-nuova-cittadinanza-sulla-rete

della PA), ha visto in questi ultimi anni delinearsi due assi principali:

- l'emanazione del **Piano triennale per l'informatica nella PA (2020-2022)**, documento di indirizzo anche economico, che definisce la strategia operativa di sviluppo dell'informatica pubblica;
- l'aggiornamento del **Codice dell'Amministrazione Digitale**, sempre più orientato ad essere norma di indirizzo generale delegando alle Linee guida la regolamentazione tecnico-operativa.

1.2. Riferimenti normativi per la trasformazione digitale

La trasformazione digitale della pubblica amministrazione in Italia è partita molto dopo rispetto agli altri paesi europei. A maggior ragione, questo processo di trasformazione di lungo periodo deve avvenire con una forte *governance* politica e con competenze tecnologiche, servizi e gestione di processi. Pertanto è necessario creare nuove opportunità di crescita, semplificare la burocrazia e rendere la politica più trasparente ed efficace per meglio contestualizzare il dibattito cittadino (al centro) e amministrazione.

Il **Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022** è frutto della stretta collaborazione tra l'Agenzia per l'Italia Digitale e il Dipartimento per la Trasformazione Digitale[15] e rappresenta il primo documento di indirizzo strategico approvato dal Presidente del Consiglio con DPCM 31 maggio 2017 per

[15] https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/index.html

promuovere la trasformazione digitale della Nazione, in particolare della Pubblica Amministrazione.

Il Piano fissa gli obiettivi ed individua i principali interventi di sviluppo e gestione dei sistemi informativi delle P.A. in attuazione dell'articolo 14-bis, comma 2, lettera b) del Codice dell'Amministrazione Digitale (CAD), secondo cui l'AgID svolge, tra l'altro, *"funzioni di programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella pubblica amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche"*.

Il Piano Triennale, approvato con DPCM 17 Luglio 2020, rappresenta la naturale evoluzione delle precedenti versioni 2017-2019 e 2019-2021.

La terza versione (2020-2022) del Piano è finalizzata alla realizzazione di linee strategiche, quali:

a) favorire lo sviluppo di una società digitale, in cui i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della Pubblica amministrazione, che costituisce il motore di sviluppo per tutto il Paese;
b) promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale;
c) contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.[16]

[16] https://pianotriennale-ict.italia.it/

L'aggiornamento 2021-2023 del Piano rappresenta la naturale evoluzione dei tre Piani precedenti. Laddove la prima edizione (2017-2019) poneva l'accento sull'introduzione del Modello strategico dell'informatica nella PA e la seconda edizione (2019-2021) si proponeva di dettagliare l'implementazione del modello, il Piano triennale 2020-2022 era focalizzato sulla realizzazione delle azioni previste e sul monitoraggio dei risultati.

Nell'arco del triennio sono state definite circa 200 azioni: a carico di AGID e Dipartimento per la trasformazione digitale, altri soggetti istituzionali e, altre a carico di PA centrali e locali.

L'aggiornamento 2021 – 2023 rappresenta la naturale evoluzione della precedente edizione. In particolare:

- consolida l'attenzione sulla realizzazione delle azioni previste e sul monitoraggio dei risultati;
- introduce alcuni elementi di novità connessi all'attuazione PNRR e alla vigilanza sugli obblighi di trasformazione digitale della PA.

1.3. Diritti soggettivi digitali

Nel 2015 una commissione di studio della Camera dei Deputati, la Commissione per i diritti e i doveri in Internet, ha redatto la Carta dei diritti di Internet, un documento che dà un fondamento costituzionale ai princìpi e ai diritti connessi alla dimensione virtuale e, in generale, alla nostra "vita online". [17]

Il digitale non è una moda!

Accedere a Internet è un diritto fondamentale della persona. Cresce e si consolida la considerazione di Internet come

[17] www.generazioniconnesse.it

una dimensione essenziale per le società per la crescita, il libero confronto, la produzione e condivisione della conoscenza. Ne è dimostrazione la Dichiarazione dei Diritti in Internet. "*L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale*" è quanto si legge nella Dichiarazione dei Diritti in Internet, approvata dalla Commissione e pubblicata il 28 luglio 2015. Per la prima volta in Italia si è istituita in sede parlamentare una Commissione di studio su questi temi.

Alla classica suddivisione dei diritti umani in tre generazioni quale frutto di una concezione dinamica del diritto e, in fondo, della società e del pensiero umano, se ne è aggiunta una quarta generazione dei diritti che trae origine dalla nuova dimensione tecnologica della comunicazione e dell'informazione.

Di fronte all'avvento della nuova economia, delle nuove tecniche di acquisizione e trattamento delle informazioni e di diffusione e trasmissione delle stesse (da Internet alla rete satellitare), si sono venuti configurando i c.d. diritti della società tecnologica.

"*Ogni persona ha diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali."* (Stefano Rodotà, La Repubblica 28 Luglio 2015, intervista di Arturo Di Corinto).

Il **Codice dell'Amministrazione Digitale (CAD)** è sicuramente un provvedimento che prevede che le Pubbliche Amministrazioni cambino il loro modello organizzativo. In questo senso il CAD non è una legge sull'informatica nel settore pubblico, bensì una legge sui procedimenti amministrativi.

La lettura del CAD è quindi rivolta ai cambiamenti che una Pubblica Amministrazione deve programmare per rispondere alle prescrizioni dettate dal legislatore.

Il CAD è soprattutto una legge che governa i rapporti "digitali" tra cittadino e pubblica amministrazione.

Un'amministrazione digitale si caratterizza, quindi, per essere un'amministrazione semplificata e trasparente, un'amministrazione accessibile in rete, un'amministrazione che eroga servizi in rete, un'amministrazione che corrisponde quindi ad un nuovo modello di relazione con i cittadini e le imprese che danno vita ad una serie di diritti/doveri.[18]

Gli ultimi Decreti correttivi hanno ulteriormente ampliato e rafforzato tale gamma di diritti in capo ai cittadini e imprese introducendo nuove forme di tutela degli stessi nel caso di inadempimento da parte delle Pubbliche Amministrazioni.

A tal proposito si ricorda:

art. 3-bis. Uso della telematica, introdotto dalla L. 11 febbraio 2005, n. 15

"Per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati".[19]

art. 3. Diritto all'uso delle tecnologie - *D.Lgs. n. 82/2005*

"Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2 [Pubbliche Amministrazioni], anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo,

[18] https://www.diritto.it/la-cittadinanza-digitale-e-i-diritti-digitali/
[19] https://www.camera.it/parlam/leggi/05015l.htm

fermi restando i diritti delle minoranze linguistiche riconosciute".[20]

art. 3-bis Identità digitale e domicilio digitale *- D.Lgs n.82/2005*

01."Chiunque ha il diritto di accedere ai servizi on-line offerti dai soggetti di cui all'articolo 2, comma 2, lettere a) e b), tramite la propria identità digitale".

1."I soggetti di cui all'articolo 2, comma 2, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese hanno l'obbligo di dotarsi di un domicilio digitale……"

Dalla lettura dell' art. 3-bis D.Lgs n.82/2005 emergono due istituti necessari per interfacciarsi con le pubbliche amministrazioni:

a) **Domicilio digitale:** tutti i cittadini potranno dialogare direttamente con le pubbliche amministrazioni attraverso il proprio indirizzo di posta elettronica certificata (o altro sistema conforme alla normativa in vigore). Il cittadino può indicare al Comune di residenza un domicilio digitale come mezzo esclusivo di comunicazione con l'amministrazione;
b) **Identità digitali:** per poter usufruire dei servizi online della P.A. sarà possibile accedere ai siti web ed ai portali di qualunque pubblica amministrazione attraverso le identità digitali uniche per ciascun cittadino, con il nuovo sistema SPID (Sistema Pubblico di Identità Digitale).

Il Codice dell'Amministrazione Digitale (CAD) si caratterizza per la disciplina di nuovi diritti dei cittadini digitali quali:

[20] https://www.camera.it/parlam/leggi/deleghe/testi/05082dl.htm

- il diritto all'uso di soluzioni e di tecnologie per potere colloquiare in modalità digitale con le Amministrazioni (art.3, CAD);
- il diritto alla identità digitale (art. 3,1-quinquies);
- il diritto di accesso telematico ai dati, alle informazioni e ai documenti (art. 52, CAD);
- il diritto di conoscere in rete la situazione relativa alle proprie istanze (art. 3, 1-quater, CAD);
- il diritto all'amministrazione digitale (art.2, 3 e ss.;12, 40, 41, 53, 64 e 65, CAD);
- il diritto alla sicurezza informatica dei propri dati personali e del patrimonio informativo pubblico (dlgs 196/2003; art. 51, CAD);
- il diritto alla qualità dei servizi erogati in rete (art. 7, CAD);
- il diritto alla partecipazione democratica elettronica (art. 9, CAD)[21]

1.4. Strumenti di tutela dei diritti digitali

La rivoluzione digitale ha ridefinito il nostro modo di comunicare, di informarci e di lavorare, cambiando ogni aspetto della nostra vita e dotando ognuno di noi di un nuovo passaporto: quello di **cittadino digitale**.

Il cittadino digitale come ogni attore della società diviene portatore di diritti e doveri fra questi quelli relativi all'uso dei servizi dell'amministrazione digitale.

Si ricorda, infatti, che l'art. 1 della Carta della cittadinanza digitale sancisce il diritto dei cittadini e delle imprese "*anche*

[21] https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2018-09-28/index.html

attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione (...) di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale (...) al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici".

Al fine di garantire ai cittadini e alle imprese, **nel caso in cui le amministrazioni non consentano loro di esercitare i loro diritti di cittadinanza digitale**, il Codice di Amministrazione Digitale (CAD) ha previsto appositi strumenti di tutela:

L'articolo 7, ultimo comma del CAD, prevede che i cittadini che vedono violati i propri "diritti" digitali possono ricorrere al difensore civico digitale oppure alla *class action*[22].

Difensore civico digitale[23]

Il **difensore civico**[24] è una figura di garanzia a tutela del cittadino e si prefigge il compito di creare il "ponte" tra il

---

[22] L'art. 7. co. 4, del CAD afferma che: "*In caso di violazione del diritto a servizi on-line semplici e integrati, gli utenti, hanno il diritto di rivolgersi al difensore civico digitale di cui all'articolo 17 comma 1 quater del CAD[22]"*. Ancora *"Il ricorrente può agire in giudizio anche nei termini e con le modalità stabilite nel decreto Legislativo n. 198/2009, notificando una diffida all'organo di vertice dell'amministrazione o del concessionario affinché effettui, entro il termine di novanta giorni, gli interventi utili alla soddisfazione degli interessati. (art. 3). Sono escluse dall'applicazione del presente decreto le autorità amministrative indipendenti, gli organi giurisdizionali, le assemblee legislative e gli altri organi costituzionali nonché la Presidenza del Consiglio dei Ministri.(art. 1, co. 1 ter)".*

[23] https://www.agid.gov.it/it/agenzia/difensore-civico-il-digitale.

[24] Il Difensore civico per il digitale è una figura introdotta nel Codice dell'amministrazione digitale (CAD) – art. 17, comma 1 quater – dal cd. Decreto Madia (D. Lgs 26 agosto 2016, n.179) recita testualmente: "*È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della*

cittadino e la pubblica amministrazione che non eroga un servizio.

Per il cittadino è molto più difficile contestare un ente che rappresenta il bene comune senza cadere in una posizione di egoismo inaccettabile e censurabile.

Da qui l'esigenza di modificare il rapporto tra Pubblica Amministrazione e cittadino, mettendo l'accento sul dialogo anziché che sul rapporto di autorità.

Sia per evitare che i pubblici uffici abusino del potere loro conferito, sia per evitare che aumenti il distacco tra cittadino e istituzioni e manchi uno dei principi fondamentali dello stato di diritto, vale a dire il senso civico nel rispetto delle regole e della convivenza pacifica.

Nulla cambia con l'introduzione del Codice dell' Amministrazione digitale (CAD) che prevede e disciplina la figura del Difensore civico per il digitale nella sua funzione di garante e di tutela dei diritti di cittadinanza digitali.

La figura del Difensore civico per il digitale è in parte mutuata da quella del Difensore civico, la quale è stata introdotta dalla L. 142/1990 e successivamente nel Dlgs. 18 agosto 2000, n 267, (il Testo Unico sull'ordinamento degli Enti Locali) e per altro non obbligatoria (anche se ormai la quasi totalità delle Regioni/Province Autonome lo ha istituito).

Le due figure sono in parziale sovrapposizione, visto che, almeno in principio, si può ricorrere al Difensore civico anche

---

pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni. Le decisioni del difensore civico sono pubblicate in un'apposita area del sito Internet istituzionale. Il difensore segnala le inadempienze all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione".

nel caso di problematiche legate all'inadempienza della PA relativamente al CAD.[25]

L'istituzione di un Difensore civico per il digitale, però, non pare superflua, tenuto in considerazione la generale scarsa conoscenza del Codice.

La figura del Difensore civico per il digitale, prevista in precedenza presso ogni amministrazione, è ora prevista a livello unico nazionale. L'Ufficio del Difensore civico per il digitale è istituito presso AgID, dando attuazione alle disposizioni dell' articolo 17 comma 1-quater del CAD.

A tal proposito l'art.17, comma1-quater del CAD rubricato "Strutture per l'organizzazione, l'innovazione e le tecnologie", come di recente modificato, disciplina puntualmente oltre la figura del responsabile della transizione digitale anche l'istituzione di un difensore civico per il digitale cui..... *"chiunque può inviare segnalazioni e reclami relativi ad ogni presunta violazione del Codice e di ogni altra norma in materia* di *digitalizzazione ed innovazione della Pubblica Amministrazione. Se tali segnalazioni sono fondate, il difensore civico per il digitale invita l'ufficio responsabile della presunta violazione a porvi rimedio tempestivamente e comunque nel termine di trenta giorni. Il difensore segnala le inadempienze all'ufficio competente per i procedimenti disciplinari"*.[26]

---

[25] https://www.agendadigitale.eu

[26] Il Difensore civico per il digitale è una figura introdotta nel Codice dell'amministrazione digitale (CAD) – art. 17, comma 1 quater – dal cd. Decreto Madia (D. Lgs 26 agosto 2016, n.179) recita testualmente: "*È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre*

Per la prima volta, infatti, esiste una figura, un ufficio, un soggetto – terzo, imparziale, competente e autonomo per legge – al quale cittadini e imprese potranno rivolgersi, in maniera agile, semplice e immediata, senza formalità, intermediari professionali né carte da bollo per segnalare gli ostacoli che incontrano nell'esercizio dei loro diritti di cittadinanza digitale e/o gli inadempimenti di amministrazioni e concessionari di pubblici servizi.

Il Difensore civico per il digitale a garanzia dei diritti digitali di cittadini e imprese, ha una duplice funzione:

1. raccoglie le segnalazioni relative alle presunte violazioni del Codice dell'Amministrazione Digitale (CAD) o di ogni altra norma in materia di digitalizzazione ed innovazione, (art.17, comma 1 quater del CAD),
2. in caso di contestazione sulla dichiarazione di accessibilità o di esito insoddisfacente del monitoraggio decide in merito alla corretta attuazione della legge sulla accessibilità agli strumenti informatici per le persone con disabilità. In caso di reclami di utenti relativi a dichiarazioni di accessibilità dispone eventuali misure correttive. (art.3-quinquies della legge n.4/2004).

L'istituto prevede due percorsi differenti di comunicazione con il Difensore Civico per il digitale in base alle funzioni che lo stesso è chiamato a svolgere:

Percorso Funzione A: Presunte violazioni del CAD

Per le segnalazioni che riguardano le presunte violazioni del CAD si può inviare direttamente la segnalazione al Difensore

trenta giorni. Le decisioni del difensore civico sono pubblicate in un'apposita area del sito Internet istituzionale. Il difensore segnala le inadempienze all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione".

compilando il modulo all'interno dell'area dedicata sul sito istituzione di AgID.[27]

Prima di inviare una segnalazione ricordarsi di:

a) circostanziare e dettagliare l'evento, indicando tutti gli elementi informativi necessari all'esame da parte del difensore;
b) fare una segnalazione per ogni amministrazione che si ritiene coinvolta nelle presunte violazioni.

Il difensore esamina le segnalazioni e, qualora le ritenga fondate, invita il soggetto responsabile a porvi rimedio tempestivamente e pubblica la relativa decisione online.

AgID ci dice cosa non è e cosa non fa il Difensore Civico per il Digitale. Nella sezione del sito a lui dedicata è riportato esplicitamente:

- **non risolve o media eventuali controversie fra cittadino e PA;**
- **non può sostituirsi alla PA** nell'attività richiesta dal cittadino;
- **non fornisce assistenza agli utenti** su malfunzionamenti di soluzioni applicative o servizi online offerti dalle PA;
- **non sostituisce l'URP** delle Amministrazioni.

L'ufficio costituito ha il compito di raccogliere i casi segnalati da cittadini e imprese, verificarne la fondatezza, contattare la PA accusata della presunta violazione ed esortarla alla tempestiva osservanza delle norme, pena il trasferimento del fascicolo al competente ufficio del personale per l'eventuale apertura di un'azione disciplinare nei confronti dei responsabili.

Percorso Funzione B: Dichiarazioni di accessibilità

[27] https://www.agid.gov.it/it/form/difensore-civico-digitale

L'art.3 quater, comma 2, lett. c) della legge n. 4/2004 sull'accessibilità, prevede che l'utente possa segnalare - tramite l'apposito link reso disponibile sui siti istituzionali dei soggetti erogatori (PA, Ente pubblico economico, ecc.) - al Difensore civico per il digitale eventuali risposte ritenute insoddisfacenti o mancate risposte da parte degli stessi.

I dati sulle attività concluse verranno pubblicate sul web.

Le dichiarazioni di accessibilità sono rese disponibili:

- nel footer, per i siti web,
- nella sezione dedicata alle informazioni generali riportate nell'app-store, per le applicazioni mobili.[28]

Class action e ricorso al Tribunale Amministrativo Regionale (TAR)

Il Decreto legislativo 20 Dicembre 2009, n. 198[29] traduce in disposizioni di dettaglio i principi contenuti nell'art. 4 della legge delega n. 15 del 2009 (riforma Brunetta) in materia di efficienza della pubblica amministrazione. In attuazione di tale decreto dal 1° gennaio 2010 è divenuta operativa la *class action* nel settore pubblico.

In pratica, per garantire una elevata performance delle pubbliche amministrazioni nei confronti della collettività, si consente nei confronti delle stesse un controllo esterno di tipo giudiziale sulla qualità, tempestività ed economicità dei servizi resi.

---

[28] https://www.agid.gov.it/it/agenzia/difensore-civico-il-digitale.

[29] Il Decreto Legislativo n. 198 del 20 dicembre 2009. Attuazione dell'art. 4 della Legge 4 Marzo 2009, n. 15, in materia di ricorso per l'efficienza delle amministrazioni e dei concessionari di servizi pubblici. Tale atto introduce la possibilità per i cittadini e per le associazioni che tutelano gli interessi dei propri associati, di ricorrere alla Class Action nei confronti della Pubblica Amministrazione nel caso in cui si verifichino inefficienze nell'erogazione del servizio richiesto.

I destinatari di una possibile *class action* sono tutte le amministrazioni dello Stato, da quelle nazionali a quelle regionali e comunali.

L'azione può essere promossa:

- nei confronti delle Pubbliche Amministrazioni e dei concessionari di servizi pubblici che abbiano violato:
  - gli standard di qualità ed economici fissati;
  - le modalità ed i tempi di erogazione indicati nelle carte dei servizi;
  - termini fissati.

Oppure

- nei confronti di amministrazioni e concessionari di servizi pubblici che:
  - non hanno emanato atti amministrativi. Non tutti gli atti amministrativi però, ma quelli generali obbligatori e non aventi contenuto normativo. Cioè quegli atti da emanarsi obbligatoriamente entro e non oltre un termine fissato da una legge o da un regolamento
  - non esercitano poteri di vigilanza, controllo o di sanzione.

La class action può essere promossa da:

- Il cittadino che, a seguito delle suddette violazioni, ritiene di aver subito una lesione diretta concreta ed attuale dei propri interessi;
- Le associazioni a tutela degli interessi dei propri associati.

Una volta verificata l'esistenza di un disservizio è necessario presentare una diffida all'amministrazione:

- L'amministrazione ha 90 giorni di tempo per ripristinare il servizio. L'obiettivo della diffida è che si instauri un procedimento volto a responsabilizzare i dirigenti competenti o gli organi di indirizzo e di controllo.
- Scaduti i 90 giorni, se il servizio non è stato ripristinato o il concessionario non ha provveduto (o ha provveduto solo in parte ad eliminare la situazione denunciata), l'interessato (o le associazioni o i comitati che tutelano gli interessi dei propri associati) hanno tempo un anno per promuovere un ricorso dinnanzi al Giudice Amministrativo.
- Il ricorso sarà pubblicizzato sul sito istituzionale del Ministero della Pubblica Amministrazione e dell'Innovazione e su quello dell'Amministrazione interessata.
- Entro 20 giorni prima dell'Udienza fissata, possono intervenire tutti i cittadini che si trovano nella medesima situazione.
- Il TAR può accogliere o meno il ricorso.
- La Sentenza del Giudice, nel caso in cui il ricorso sia ammesso, si baserà nell'ordinare alla Pubblica amministrazione o al concessionario del servizio di attivare tutte quelle misure per porre rimedio al disservizio riscontrato. E' escluso il risarcimento del danno che si potrà, invece, ottenere facendo riferimento alle vie giudiziarie ordinarie.

1.5. Sanzioni per le PA che violano le norme sulla digitalizzazione

Il Decreto Semplificazione del luglio 2020 ha previsto l'inserimento nel Codice dell'Amministrazione Digitale di

una **norma sanzionatoria** che nelle intenzioni del legislatore potrà assicurare più celermente l'attuazione dell'Agenda digitale italiana ed europea, la digitalizzazione dei cittadini, delle pubbliche amministrazioni e delle imprese.[30]

Il Decreto in questione ha novellato il CAD introducendo l'art. 18 bis rubricato "violazione degli obblighi di transizione digitale". La norma conferisce all'Agenzia per l'Italia Digitale ("AGID") **il potere di vigilanza, verifica, controllo e monitoraggio** sul rispetto non solo delle disposizioni del CAD ma anche *"di ogni altra norma in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione, ivi comprese quelle contenute nelle Linee guida e nel Piano triennale per l'informatica nella pubblica amministrazione"*.

Infatti, l'AgID potrà procedere, d'ufficio o su segnalazione del Difensore Civico Digitale, all'accertamento delle relative violazioni da parte delle pubbliche amministrazioni, gestori di servizi pubblici e società a controllo pubblico. Nell'esercizio dei poteri di vigilanza, verifica, controllo e monitoraggio, l'AgID potrà quindi richiedere e acquisire presso i soggetti interessati dati, **documenti e ogni altra informazione strumentale e necessaria**.

Ove venga accertata la sussistenza delle violazioni contestate, Agid assegna al trasgressore un congruo termine perentorio, proporzionato rispetto al tipo e alla gravità della violazione, **per conformare la condotta agli obblighi previsti** dalla normativa vigente, segnalando le violazioni all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione, nonché ai competenti organismi indipendenti di valutazione. Le predette segnalazioni sono pubblicate a cura dell'AgID su apposita area del proprio sito internet istituzionale.

[30] https://www.agendadigitale.eu/documenti/semplificazioni-bis-nel-cad-sanzioni-per-le-pa-che-violano-le-norme-sulla-digitalizzazione-cosa-si-rischia/ - Luglio 2021

L'art. 18bis del CAD indica **al comma 5** le ipotesi tassative in cui Agid irroga la sanzione amministrativa pecuniaria che oscilla tra il minimo di euro 10.000 ed il massimo di euro 100.000 qualora il soggetto pubblico non ottemperi all'obbligo di conformare la condotta entro il termine assegnato:

- In caso di **mancata ottemperanza** alla richiesta di dati, documenti o informazioni di cui al comma 1, ultimo periodo, ovvero di trasmissione di informazioni o dati parziali o non veritieri;
- **violazione degli obblighi previsti dall'art. 5 CAD** concernenti la messa a disposizione della piattaforma per i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i micro-pagamenti e quelli basati sull'uso del credito telefonico;
- violazione **degli obblighi previsti dall'art. 50-ter, comma 5, CAD** concernenti il trasferimento dei dati nella Piattaforma Digitale Nazionale Dati ed il divieto di modifica della titolarità del dato.
- violazione degli obbighi previsti dall'art. 64, comma 3-bis, CAD concernente l'utilizzo delle identità digitali ai fini dell'identificazione degli utenti dei propri servizi on-line.
- violazione degli obblighi previsti dall'art. 64-bis CAD concernente la fruizione da parte degli utenti dei servizi in rete tramite punto di accesso nonché la progettazione e sviluppo dei sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi per ogni servizio le relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità e l'adozione degli strumenti di analisi individuati dall'AgID con le Linee guida.
- violazione degli obblighi previsti dall'articolo 65, comma 1, del decreto legislativo 13 dicembre 2017, n.

217 concernente il riconoscimento del diritto all'identità digitale ed al domicilio digitale

- violazione **degli obblighi previsti dall'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179,** convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, concernenti la migrazione dei centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici verso l'infrastruttura sviluppata presso la Presidenza del Consiglio di Ministri o in alternativa verso infrastruttura avente analoghe caratteristiche o il cloud compatibilmente con i livelli minimi di sicurezza, affidabilità capacità e risparmio energetico fissato dal regolamento di Agid d'intesa con la struttura della Presidenza del Consiglio dei Ministri.

Il legislatore non ha escluso l'ipotesi di ulteriore inerzia dell'amministrazione inadempiente prevedendo contestualmente all'irrogazione della sanzione nei casi di violazione delle norme specificamente indicate al comma 5 e di cui si è fatto menzione la segnalazione da parte di Agid della violazione **alla struttura della Presidenza del Consiglio dei ministri competente** per l'innovazione tecnologica e la transizione digitale, ricevuta la segnalazione, che diffida ulteriormente il soggetto responsabile a conformare la propria condotta agli obblighi previsti dalla disciplina vigente entro un congruo termine perentorio, proporzionato al tipo e alla gravita' della violazione, avvisandolo che, in caso di inottemperanza, potranno essere esercitati i poteri sostitutivi del Presidente del Consiglio dei ministri o del Ministro delegato.

In tal caso, decorso inutilmente il termine, il Presidente del Consiglio dei ministri o il Ministro delegato per l'innovazione tecnologica e la transizione digitale, valutata la gravità della violazione, **può nominare un commissario ad acta** incaricato di provvedere in sostituzione.

L'Agenzia per l'Italia Digitale (AgID) ha disciplinato con un proprio regolamento **le procedure di contestazione, accertamento, segnalazione e irrogazione delle sanzioni** per le violazioni di cui alla presente disposizione.[31]

La modifica del CAD introdotta dal Decreto Semplificazioni bis deve essere letta in stretta connessione con i compiti e le responsabilità del Responsabile per la Transizione Digitale (RTD) **figura istituita per la prima volta con l'art. 17** di cui ogni PA deve dotarsi tra le figure professionali interne dotate di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico.

1.6. Il Responsabile per la Transizione Digitale

Al Responsabile per la Transizione Digitale (RTD) viene affidata dall'art. 17 del Codice dell'Amministrazione Digitale il compito di guidare l'amministrazione verso la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità e che sono declinati nel:

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

[31] Determinazione n. 611/2021 del 29 novembre 2021 - *Adozione del Regolamento recante le procedure di contestazione, accertamento, segnalazione delle violazioni in materia di transizione digitale e di esercizio del potere sanzionatorio ai sensi dell'art.18-bis, del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche*

b. indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c. indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 CAD;
d. accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
e. analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
f. **cooperazione alla revisione della riorganizzazione dell'amministrazione** ai fini di cui alla lettera e);
g. indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h. **progettazione e coordinamento delle iniziative** rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i. promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei

Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j. **pianificazione e coordinamento del processo di diffusione**, all'interno dell'amministrazione, **dei sistemi di identità e domicilio digitale**, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis. – J-bis. pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

L'art. 18 Bis descritto precedentemente prevede che "*Le violazioni accertate dall'AgID rilevano ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comportano responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165*" colmando di fatto una lacuna normativa del CAD che non aveva previsto alcuna disciplina specifica nel caso di inosservanze gravi all'attuazione della trasformazione digitale. Si tratta di una previsione che serve da monito per le amministrazioni e che **coinvolge personalmente i dirigenti apicali**.

Capitolo secondo

Gli strumenti dell'Amministrazione Digitale

2.1 Firma elettronica e firma digitale

Firmare digitalmente un documento significa garantire riservatezza, confidenzialità, autenticità, integrità e non ripudio del suo contenuto.

Sono passati ormai più di venti anni da quando la firma elettronica è diventata una realtà (il primo regolamento è il D.P.C.M. 8 febbraio 1999)[32]. Continua, però, ad aleggiare una gran confusione sull'argomento **firma digitale** e, soprattutto, sulla differenza tra **firma elettronica semplice (FES)**, **firma elettronica avanzata (FEA)** e **firma elettronica qualificata (FEQ).**

Spesso si parla di firma elettronica e firma digitale utilizzandole come sinonimi o senza capirne le differenze e il relativo valore probatorio. Occorre fare un po' di chiarezza!

La normativa in materia di firma elettronica ha subito negli ultimi anni un ingente processo di riforma, dal momento che il Regolamento eIDAS (Regolamento UE n. 910/2014)[33], ha

[32] D.P.C.M. 8 febbraio 1999, *Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513.*

[33] Regolamento (UE) 910/2014, il cosiddetto *Regolamento eIDAS*.; https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN#d1e2367-73.

proceduto all'abrogazione della previgente Direttiva 1999/93/CE[34], il cui limite era quello di non fornire un quadro transfrontaliero e transettoriale completo per la realizzazione di transazioni elettroniche sicure, affidabili e di facile impiego.

Con l'entrata in vigore del Regolamento eIDAS, il legislatore italiano, con alcuni interventi normativi nel 2016 e nel 2017, ha proceduto ad adeguare la normativa contenuta all'interno del Codice dell'amministrazione digitale a quella comunitaria, assegnando alle firme elettroniche valori giuridici differenziati rispetto al precedente quadro normativo.

Nell' ordinamento italiano sono presenti quattro diverse tipologie di firme. Alcune di queste, come la firma elettronica (FE), la firma elettronica avanzata (FEA) e la firma elettronica qualificata (FEQ), hanno derivazione comunitaria[35], mentre la firma elettronica digitale è definita dal nostro Codice dell'Amministrazione Digitale.

Analizziamo nel dettaglio le diverse tipologie di firme previste dal Codice dell'Amministrazione Digitale e le differenze a livello legale.

Le firme legali si dividono in:

- Firma elettronica Semplice
- Firma Elettronica Avanzata
- Firma Elettronica Qualificata
- Firma Digitale.

---

[34] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche. La presente direttiva era volta ad agevolare l'uso delle firme elettroniche e a contribuire al loro riconoscimento giuridico. Essa istituiva un quadro giuridico per le firme elettroniche e taluni servizi di certificazione al fine di garantire il corretto funzionamento del mercato interno.

[35] Regolamento (UE) 910/2014.

La firma elettronica semplice (FES)

La firma elettronica è costituita da *"un insieme dei dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati dal firmatario per firmare"*[36].

Il Regolamento eIDAS stabilisce la non discriminazione dei documenti elettronici rispetto ai documenti cartacei. A livello nazionale le firme elettroniche introdotte da eIDAS non mutano sostanzialmente il quadro di riferimento, non vi saranno disagi per gli attuali possessori di firme digitali.

Mentre nel codice dell'amministrazione digitale (CAD - Decreto Legislativo 7 marzo 2005, n. 82) la firma elettronica viene definita come un insieme di dati in forma elettronica utilizzati come metodo di identificazione informatica, nel Regolamento eIDAS, al Capo I Art. 3, la firma elettronica è descritta come dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

La locuzione *"utilizzati dal firmatario per firmare"* ha una funzione prettamente identificativa, comportando un rafforzamento della funzione dichiarativa (cioè la manifesta adesione al contenuto del documento firmato) e della funzione probatoria[37].

[36] Regolamento (UE) 910/2014, art. 3 paragrafo 10.
[37] cfr. art. 21 del CAD.

L'efficacia giuridica delle firme elettroniche		
	Firma elettronica	**Firma elettronica avanzata, qualificata o digitale**
CAD	Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21).	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. (art.21).
eIDAS	Non sono negati effetti giuridici per via della sua forma elettronica. Spetta al diritto nazionale dei singoli Paesi europei definire gli effetti giuridici delle firme elettroniche (art. 25).	Ha un effetto giuridico equivalente a quello di una firma autografa. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri (mutuo riconoscimento).

La firma elettronica semplice rappresenta una qualsiasi connessione di dati utile per l'autenticazione informatica su un documento elettronico.

Uno strumento che dal punto di vista della sicurezza non offre molte garanzie, dal momento che non rispetta i requisiti previsti per le firme elettroniche più forti. Infatti, la firma elettronica semplice non riesce ad assicurare i tre fondamentali

obiettivi che le altre tipologie di firma elettronica perseguono, cioè:

- autenticità;
- non ripudio;
- integrità del documento.

Esempi sono: codice PIN o le credenziali di accesso ai siti web.

Bisogna affermare, tuttavia, che *"a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate"*[38].

La firma elettronica avanzata (FEA)

La firma elettronica avanzata è definita come *"un insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati"*[39].

Il suo utilizzo soddisfa determinati requisiti:

- è connessa unicamente al firmatario;
- è idonea a identificare il firmatario;
- 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;

[38] Regolamento (UE) 910/2014, art. 25 paragrafo 1.
[39] Regolamento (UE) 910/2014, art. 3, paragrafo 11 e art. 26.

- è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati[40].

Riassumendo questi punti, la Firma Elettronica Avanzata può essere definita come una Firma Elettronica che:

- permette di identificare il firmatario;
- garantisce la connessione univoca con il firmatario;
- è creata tramite l'utilizzo di dati sui quali il firmatario conserva un controllo esclusivo;
- è collegata a questi dati in modo che il firmatario possa rilevare eventuali modifiche successive.

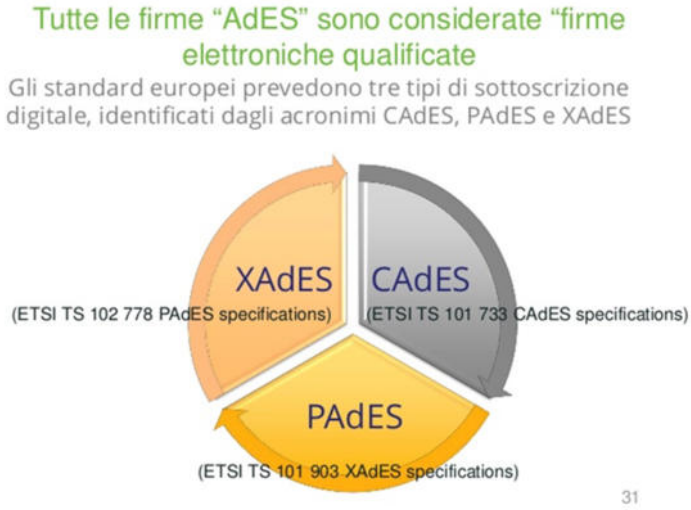
Sebbene simili, la firma elettronica avanzata e la firma elettronica sono due strumenti differenti e diversamente affidabili. Nello specifico, *"l'elemento che differenzia in modo sostanziale un firma elettronica avanzata da una firma elettronica è la capacità della FEA di rilevare le eventuali modifiche apportate ad documento dopo la sottoscrizione, che rassicura il firmatario riguardo all'integrità e immodificabilità delle dichiarazioni ivi prodotte"*[41]. Un' analoga differenziazione è rilevabile anche a livello delle piattaforme utilizzabili per realizzare tipologie di firme. Infatti, *"una piattaforma FEA, ... oltre a consentire l'uso dei mezzi di intensificazione più sicuri…, deve essa stessa garantire nel tempo l'integrità e l'immodificabilità del documento firmato digitalmente, indipendentemente dal sistema nel quale esso viene memorizzato e gestito"*[42].

[40] Regolamento (UE) 910/2014, art. 26, paragrafo 1, lett. a), b), c) e d).
[41] PIGLIAPOCO S., *Progetto Archivio Digitale. Metodologia Sistemi Professionalità*; Torre del Lago (LU), Civita editoriale, 2016.
[42] PIGLIAPOCO S., *Progetto Archivio Digitale. Metodologia Sistemi Professionalità*; Torre del Lago (LU), Civita editoriale, 2016.

Esempio sono: c.d. firma grafometrica, che, per il tramite di un pennino, viene apposta su tablet ed è molto diffusa nel settore bancario e nel settore assicurativo[43].

Gli standard europei[44] prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES e XAdES, modalità di sottoscrizione adottate anche in Italia.

Questi tipi di sottoscrizione appartengono alla famiglia di formati di firme digitale chiamata AdES, acronimo di Advanced Electronic Signatura, cioè firma elettronica avanzata.



Come scegliere il formato da utilizzare?

La differenza tra i formati consiste soprattutto nel modo in cui si presenta il file al soggetto che vuole verificare quella firma.

[43] Dizionario enciclopedico Treccani, "Informatica giuridica e diritto dell' informatica", Diritto on line, 2013, su https://www.treccani.it/enciclopedia/informatica-giuridica-e-diritto-dell-informatica_%28Diritto-on-line%29/#4lefirmeelettroniche-1.
[44] Decisione della Commissione europea 2011/130/EU.

A. La firma CAdES - p7m

Nel formato CAdES, composto da C-AdES che sta per *"Cryptographic message syntax"* della famiglia AdES, la busta crittografica che racchiude il documento, la firma prendono e il certificato, assumono il formato "p7m".

Pregi	Difetti
• può essere apposta su qualsiasi tipo di file, file di testo (Microsoft Word, OpenOffice Writer, semplici file di testo, etc.), fogli di calcolo (Microsoft Excel, OpenOffice Calc), file immagine (JPEG, GIF, PNG, etc.), PDF.	• per potere aprire la busta "p7m" è necessario avere a disposizione un software specifico, come DiKE, File Protector, ArubaSign, che riesca che si trova all'interno di un lettore/scrittore di smart card. • per effettuare più firme sullo stesso documento è necessario re-imbustare in una nuova busta CAdES la prima "busta" contenente la firma con un effetto detto "matrioska". • non è possibile aggiungere una firma grafica visibile sul documento[45].

B. La firma PAdES - pdf

Nel formato PAdES, composto da P-AdES che sta per "PDF" della famiglia AdES, la busta crittografica assume un estensione ".pdf".

Nel nostro ordinamento è stata introdotta nel 2006 a seguito di un protocollo di intesa tra Adobe e l'allora CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione).

[45] https://www.agid.gov.it; si veda anche Gruppo di Lavoro Firma Digitale. (2018). *Breve Guida sulle Firme Elettroniche.* Roma: Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili.

Nel 2011 la Commissione Europea nella decisione 2011/130/EU[46] ha imposto il suo utilizzo nei documenti firmati elettronicamente nel mercato interno avendo risolto alcuni difetti della firma CAdES.

La busta PAdES è un formato particolarmente idoneo quando è necessario apporre una nuova firma al documento dopo la prima sottoscrizione digitale.

Pregi	Difetti
• non è necessario alcun tipo di software e lettore specifico per aprire la busta che si apre in PDF • è possibile firmare un documento senza l'effetto matrioska e senza invalidare le sottoscrizioni precedentemente apposte. • è possibile aggiungere una firma grafica visibile sul documento, oltre quella digitale, potendo quindi essere inserita nel punto desiderato del documento	• è possibile firmare solo PDF.

In conclusione, la busta PAdES è un formato particolarmente idoneo quando è necessario apporre una nuova firma al documento dopo la prima sottoscrizione digitale[47].

C. La firma XAdES - xml

[46] 2011/130/UE: Decisione della Commissione, del 25 febbraio 2011 , che istituisce requisiti minimi per il trattamento transfrontaliero dei documenti firmati elettronicamente dalle autorità competenti a norma della direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno [notificata con il numero C(2011) 1081] Testo rilevante ai fini del SEE.

[47] https://www.agid.gov.it; si veda anche Gruppo di Lavoro Firma Digitale. (2018). *Breve Guida sulle Firme Elettroniche.* Roma: Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili.

Il formato XAdES, che sta per "XML" della famiglia AdES, è lo standard per la sottoscrizione elettronica dei documenti in formato XML.

Pregi	Difetti
• non necessita di imbustamento/sbustamento • può accedere ai "metadati" , cioè quelle informazioni contenute nei tag xml, formato utilizzato per elaborazioni numeriche. • è possibile firmare un documento senza l'effetto matrioska e senza invalidare le sottoscrizioni precedentemente apposte	• i file xml sono di difficile lettura.

La firma elettronica qualificata (FEQ)

La firma elettronica qualificata è una peculiare tipologia di firma avanzata, *"creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche"*[48].

La firma elettronica qualificata garantisce in modo univoco l'identificazione del titolare, e, dal punto di vista dell'efficacia giuridica, equivale ad una firma autografa, come statuito dall'art. 25 del Regolamento eIDAS[49].

Dalla definizione di firma elettronica qualificata emergono due elementi[50]:

[48] Regolamento (UE) 910/2014, art. 3, punto 1, n. 12.
[49]Regolamento (UE) 910/2014, art. 25, com.3 prescrive che: *"Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri"*.
[50] AGID – Firma elettronica qualificata.

1. dispositivo per la creazione della firma elettronica qualificata;
2. certificato qualificato per firme elettroniche.

Il Regolamento eIDAS è d'ausilio fornendo i relativi significati:

"dispositivo per la creazione della firma elettronica qualificata"

Software o hardware configurato che è utilizzato per creare una firma elettronica, la quale deve soddisfare i requisiti di cui Allegato II[51] del Regolamento eIDAS[52]:

- assicurare la riservatezza dei dati per la creazione di una firma elettronica, nonché questi compaiano in pratica una sola volta;
- assicurare che i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;
- assicurare che i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi;
- assicurare che i dati non siano alterati;
- assicurare che sia impedita la presentazione di tali dati siano presentati al firmatario prima della firma.

[51] Allegato II contiene analiticamente i requisiti per i dispositivi per la creazione di una firma elettronica qualificata.
[52] A tal proposito si faccia riferimento al Regolamento (UE) 910/2014, art. 3, paragrafi 22 e 23.

"certificato qualificato per firme elettroniche"

Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica, confermando almeno il nome o lo pseudonimo di tale persona, oltre a essere sia rilasciato da un prestatore di servizi fiduciari qualificato, sia conforme ai requisiti di cui all' Allegato I[53] del Regolamento eIDAS[54]:

- un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;
- un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito, nonché il nome, se del caso, il numero di registrazione quali figurano nei documenti ufficiali (se si tratta di persona giuridica), oppure il nome della persona (nel caso di persone fisica);
- almeno il nome del firmatario, o uno pseudonimo, qualora sia usato uno pseudonimo;
- i dati di convalida della firma elettronica che corrispondono ai dati per la creazione di una firma elettronica;
- l'indicazione dell'inizio e della fine del periodo di validità del certificato;
- il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

[53] Allegato I contiene analiticamente i requisiti per i dispositivi per la creazione di una firma elettronica qualificata.
[54] A tal proposito si faccia riferimento al Regolamento (UE) 910/2014, art. 3, paragrafi 14 e 15.

- la firma elettronica avanzata o sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato, nonché il luogo in cui questo è disponibile gratuitamente;
- l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;
- qualora i dati per la creazione di una firma elettronica connessi ai dati di convalida della firma elettronica siano ubicati in un dispositivo per la creazione di una firma elettronica qualificata, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento autorizzato.

La normativa italiana prevede che *nel certificato di firma elettronica qualificata può essere inserito il codice fiscale*[55] del titolare del certificato, eventualmente indicando il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza (o in sua mancanza un altro codice identificativo, purché univoco) per quei soggetti residenti all'estero e a cui non è stato attribuito il codice fiscale.

Esempio: card con chip che contiene alcuni dati anagrafici e il codice fiscale, come la Tessera Sanitaria.

La firma digitale

La firma digitale viene definita dal D.Lgs. 82/2005 come *"un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata (crittografia asimmetrica), 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*

[55] D.Lgs. 82/2005, art. 28, com. 2.

informatico o di un insieme di documenti informatici"[56]. A differenza della firma elettronica, in questo caso si rende necessario un sistema di chiavi crittografiche asimmetriche che permette di riconoscere univocamente il firmatario di un qualsiasi documento digitale.

Nell'ordinamento italiano, questa tipologia di firma è riconosciuta come "alter ego" digitale della firma autografa e conferisce, di conseguenza, pieno valore legale ai documenti firmati. In questo modo se ne riconosce l'autenticità e l'integrità.

Per ogni utente, le due chiavi vengono generate da un *apposito algoritmo* con la garanzia che la chiave privata sia la sola in grado di poter decifrare correttamente i messaggi cifrati con la chiave pubblica associata e viceversa. Lo scenario in cui un mittente vuole spedire un messaggio a un destinatario in modalità sicura è il seguente: il mittente utilizza la chiave pubblica del destinatario per la cifratura del messaggio da spedire, quindi spedisce il messaggio cifrato al destinatario; il destinatario riceve il messaggio cifrato e adopera la propria chiave privata per ottenere il messaggio "in chiaro".

Ulteriori indicazioni sulla Firma Digitale sono contenute nell'Art. 24 del CAD e in particolare il comma 2 stabilisce che: *"l'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente"*.

La disciplina della firma digitale è stata apportata dal D.P.R. n. 513 del 1997, emanato in attuazione dell'art. 15 della Legge 15 marzo 1997, n. 59[57], che fornì per primo una disciplina organica per il documento informatico, rinviando ad un

[56] D-Lgs. 82/2005, art. 1, com. 1, lettera s).

[57] Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.

D.P.C.M. (poi adottato l'8 febbraio del 1999) per l'emanazione delle relative regole tecniche. La disciplina, confluita poi nel D.P.R. n. 445 del 2000[58], è stata più volte modificata per consentire il pieno recepimento dell'allora vigente normativa comunitaria (Direttiva 1999/93/CE). Come già detto, tuttavia, tale tipologia di firma è prevista solamente a livello nazionale e non comunitario[59]. Al riguardo, si può osservare come il legislatore italiano abbia in passato attribuito una rilevanza giuridica nettamente prevalente alla firma digitale rispetto agli altri tipi di firma previsti a livello comunitario, e ciò in ragione dell'elevato livello di sicurezza garantito dall'utilizzo di tale soluzione tecnica.

L'art. 24, comma 1 del CAD, prescrive che la firma digitale si riferisca in maniera univoca ad un solo soggetto ed al documento cui è stata apposta o associata, affinché a quest'ultimo possa essere attribuita l'efficacia di cui al 2702 c.c. ed il soddisfacimento del requisito della forma scritta.

Anche la firma digitale si basa su un certificato qualificato, il quale deve essere rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato o che comunque, se stabilito in uno Stato non comunitario, rispetti le condizioni di cui all'art. 24, comma 4-ter del CAD, e che non deve essere né scaduto, né revocato, né sospeso al momento della sottoscrizione, per non far risultare il documento informatico sostanzialmente privo di sottoscrizione. Le informazioni obbligatoriamente incluse all'interno del certificato sono elencate all'art. 24, comma 4, che rimandando alle Linee Guida (attualmente occorre far riferimento alle regole

[58] D.P.R. n. 445 del 2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.*

[59] Del resto questo stretto legame tra elementi contenuti nel *Regolamento eIDAS* e quelli presenti nel *Codice dell'Amministrazione Digitale* è rinvenibile, direttamente proprio nel CAD, laddove all'art.1, com. 1-bis, si asserisce che *"ai fini del presente Codice, valgono le definizioni di cui all''art. 3 del Regolamento eIDAS"*.

tecniche di cui al D.P.C.M. 22 febbraio 2013[60]), ne individua un nucleo minimo costituito dall'indicazione esplicita della propria validità, dagli elementi identificativi del titolare di firma digitale e del prestatore di firma elettronica qualificata, nonché dagli eventuali limiti d'uso.

Cresce l'utilizzo della firma che consente di scambiare in rete documenti con piena validità legale. Dalla partecipazione a bandi di gara e concorsi, alla firma di contratti e la modifica di assetti societari, dal sistema di fatturazione ai documenti sanitari. Sono molti gli utilizzi della firma digitale così come diffuso è il suo utilizzo.

Secondo il monitoraggio che AgID effettua sui dati forniti dai certificatori accreditati, a dicembre 2019 (e da maggio 2014) sono + di 20 milioni le utenze attive di firma digitale (e di conseguenza i certificati qualificati). Di queste l'80% si basa su firma digitale remota (che non richiede l'utilizzo di smart card o token). Sempre nel 2019, sono + di 3 miliardi le firme digitali remote generate.

Armonizzata nel quadro europeo dal Regolamento eIDAS del 2014, la firma digitale offre numerosi vantaggi, tra cui il risparmio di tempo e costi, e incentiva la dematerializzazione dei documenti in molti settori della pubblica amministrazione; garantendo l'autenticità del firmatario, l'integrità, la piena validità legale del documento sottoscritto e il suo riconoscimento in tutti i Paesi europei[61].

Tra le novità del 2020, la possibilità di acquisire la firma remota autenticandosi con il Sistema Pubblico di Identità digitale SPID, senza doversi necessariamente registrare per usufruire del servizio.

---

[60] D.P.C.M. 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*.

[61] NICOTRA M. *Firma digitale, come cambierà in Italia dopo eIDAS.* Tratto da Forum PA. 2016.

Tutti i certificatori di firma digitale possono implementare e utilizzare SPID per riconoscere online un utente, generare un certificato qualificato di firma remota e far firmare documenti informatici generando una firma elettronica qualificata[62].

Riassumendo questi punti, la Firma Digitale può essere definita come una Firma Elettronica che:

- è l'equivalente elettronico della firma autografa su carta, in quanto è associata al documento elettronico sulla quale è apposta;
- ne attesta l'integrità, l'autenticità e la non ripudiabilità;
- necessita dell'utilizzo di un apposito dispositivo di firma che si presenta sotto forma di una smart card da inserire in un apposito lettore, o di una chiavetta USB corredato da un software di firma rilasciato da un'Autorità di certificazione

Esempio: la Carta Nazionale dei Servizi (CNS) della Camera di Commercio.

Efficacia probatoria dei documenti sottoscritti con Firma Elettronica.

A secondo del differente livello di sicurezza presentato dalle diverse tipologie di firme, differente sarà anche l'efficacia probatoria dei documenti informatici sottoscritti, nonché la loro capacità di soddisfare il requisito della forma scritta.

Sulla base di quanto riportato nel Regolamento Europeo eIDAS[63], nel CAD[64] e nel Codice Civile[65] si può affermare che:

- a livello nazionale, l'art. 20, comma 1-bis, del Codice di Amministrazione Digitale, un *"documento informatico*

[62] https://www.agid.gov.it/it.
[63] Regolamento (UE) 910/2014 – eIDAS.
[64] Codice dell'Amministrazione Decreto Legislativo 7 marzo 2005, n. 82.
[65] Si analizzano in particolare gli artt. 1350 e 2702 c.c.

soddisfa il requisito della forma scritta e ha efficacia prevista dall' art. 2702 del c.c."[66], se vi è apposta una tipologia di firma ritenuta univocamente sicura, oppure se è stato formato attraverso un processo di identificazione informatica tale da soddisfare particolari requisiti.

La sottoscrizione degli atti deve farsi per iscritto ai sensi dell' art. 1350 c.c., ma esiste una differenziazione tra le differenti tipologie di firme utilizzabili per sottoscrivere le varie categorie di atti. Nello specifico, *"salvo il caso di sottoscrizione autentica, le scritture private di cui all' art. 1350, primo comma, numeri da 1 a 12, del c.c.*[67]*,se fatte con documento informatico, sono sottoscritte a pena di nullità, con firma elettronica qualificata o firma digitale"*[68]*,* mentre maggiore libertà di azione è consentita per gli atti di cui all' art. 1350, primo comma, numero 13, del c.c., che *"redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale"*[69].

Variabile a seconda della tipologia di firma elettronica adottata è anche la riconducibilità al titolare della firma dell'utilizzo del dispositivo utilizzato per apporla. Ne caso di utilizzo di firma elettronica qualificata o digitale, si determina un'inversione dell'onere della prova, e *"l'utilizzo del dispositivo di firma elettronica qualificata*

---

[66] Il verificarsi di tali circostanze fa sì che il documento informatica, assumerebbe l' efficacia di una scrittura privata, la *quale "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"* (art. 2720 c.c.).

[67] I primi dodici punti dell' art. 1350 c.c. individuano una serie di atti che devono farsi per atto pubblico o scrittura privata, sotto pena di nullità.

[68] D.lgs. 82/2005, art. 20, comm. 1-bis.

[69] D.lgs. 82/2005, art. 21, comm. 2-bis.

o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria".[70]

Per quel che riguarda la data e l'ora di formazione del documento informatico, queste sono opponibili ai terzi, esclusivamente se sono state apposte conformemente alle Linee guida di cui all'art. 71 del CAD.[71]

- A livello comunitario, gli effetti giuridici delle firme elettroniche sono specificati nell' art. 25 del Regolamento (UE) 910/2014.
  Indipendentemente dalla particolare firma elettronica considerata, a questa *"non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate"*[72]. L'effetto giuridico ottenibile aumenta se si considera la firma elettronica qualificata, dato che questa *"ha effetti giuridici equivalenti a quelli di una firma autografa"*[73]. Se poi questa è anche basata su di un certificato qualificato che è stato rilasciato in uno Stato membro dell' Unione europea, allora dovrà essere riconosciuta come firma elettronica qualificata anche in tutti gli altri Stati membri[74].

Di seguito uno schema riassuntivo della valenza giuridica delle varie tipologie di firme secondo la normativa nazionale e comunitaria:

---

[70] D.lgs. 82/2005, art. 20, comm. 1-ter.

[71] A tal riguardo si faccia riferimento al D.lgs. 82/2005, art. 20, comm. 1-bis.

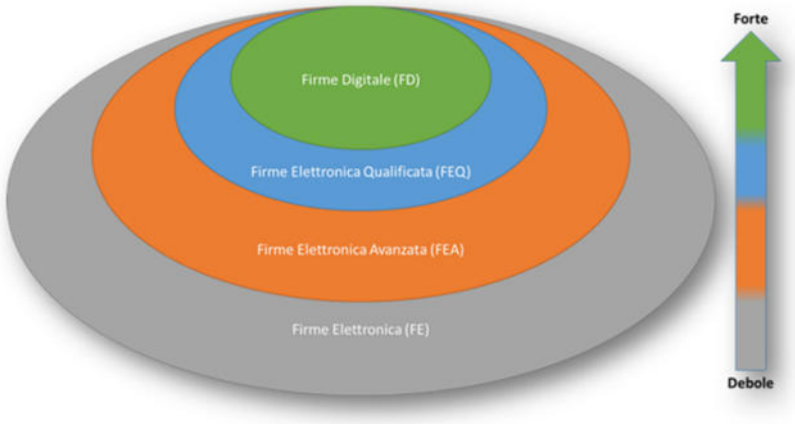
[72] Regolamento (UE) 910/2014, art. 25, paragrafo 1.

[73] Regolamento (UE) 910/2014, art. 25, paragrafo 2.

[74] A tal proposito si faccia riferimento al Regolamento (UE) 910/2014, art. 25, paragrafo 3.

Tipo di firma	Italia (D.lgs. 82/2005)	Comunitaria (Reg. UE 910/2014)
Firma elettronica	• Ammissibile come prova in procedimenti giudiziali, ma liberamente valutabile dal giudice	• Ammissibile come prova in procedimenti giudiziali
Firma elettronica avanzata	• Soddisfa il requisito della forma scritta e ha efficacia prevista dall'articolo 2702 del Codice Civile (ex art. 20, c.1-bis del CAD) • Utilizzabile per la sottoscrizione degli Atti di cui al Codice Civile, art. 1350, comma 13 (ex Art. 21, c.2-bis del CAD)	• Ammissibile come prova in procedimenti giudiziali
Firma elettronica qualificata	• Soddisfa il requisito della forma scritta e ha efficacia prevista dall'articolo 2702 del Codice Civile (ex art. 20, c.1-bis del CAD) • Utilizzabile per la sottoscrizione degli Atti di cui al Codice Civile, art. 1350, comma 13 (ex Art. 21, c.2-bis del CAD) • Si presume riconducibile al titolare della firma, salvo che questi dia prova contraria (inversione dell'onere della prova) – (ex art. 20, c.1-ter del CAD)	• Ha effetti giuridici equivalenti a quelli di una firma autografa
Firma digitale		NON APPLICABILE *E' un particolare tipo di firma elettronica qualificata presente esclusivamente nell'ordinamento italiano.*

Pensando ad uno schema, le varie firme esaminate possono essere rappresentate come:



I sigilli elettronici.

Il **sigillo elettronico** è ancora oggi relativamente poco utilizzato. Eppure, emerge quando si parla di documenti digitali.

A tal proposito, il regolamento (UE) definisce sigillo elettronico i *"dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi"*[75]. Analogamente a quanto previsto nell'ambito della firma elettronica, il Regolamento eIDAS prevede che ci sia un creatore del sigillo ovvero *"una persona giuridica che crea un sigillo elettronico"*[76], utilizza dei dati unici in forma elettronica[77] per

[75] Regolamento (UE) 910/2014, art. 3, paragrafo, 25.
[76] Regolamento (UE) 910/2014, art. 3, paragrafo, 24.
[77] Come previsto dall' art. 3, paragrafo 24 del Regolamento (UE) 910/2014, si tratta dei cosiddetti "dati per la creazione di un sigillo elettronico", ovvero dei dati unici utilizzati da creatore del sigillo elettronico per creare un sigillo elettronico.

creare il sigillo elettronico, realizzando l'associazione con i dati del documento elettronico che si vuole "sigillare" al fine di garantirne l'integrità e la paternità. Si tratta, dunque, di uno *"strumento da utilizzare per certificare la qualità e l''affidabilità dei dati gestiti da una persona giuridica e rilasciati a un cittadino, un'impresa, o trasmessi da un sistema a un altro con i meccanismi dell' interoperabilità e cooperazione applicativa"*[78].

Esistono due grandi tipologie, che variano secondo i requisiti di sicurezza intrinseci, di sigillo elettronico. Nello specifico:

- avanzato;
- qualificato.

Sigillo elettronico avanzato

Un sigillo elettronico avanzato è tale se presenta quattro caratteristiche fondamentali:

1) Connessione esclusiva, univoca e diretta con il creatore del sigillo;
2) Idoneità a identificare il creatore;
3) Creazione di un sigillo elettronico che possa essere controllato/utilizzato esclusivamente dal titolare;
4) Collegamento a dati grazie ai quali è possibile garantirne l'originalità e l'integrità[79].

Sigillo elettronico qualificato

Un sigillo elettronico qualificato è *"un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo*

[78] PIGLIAPOCO S., *Progetto Archivio Digitale. Metodologia Sistemi Professionalità*; Torre del Lago (LU), Civita editoriale, 2016.
[79] Regolamento (UE) 910/2014, art. 36, paragrafo, 1, lett. a),b),c) e d).

elettronico qualificato e basato su un certificato qualificato per sigilli elettronici"[80] (che, quindi, presenti le quattro caratteristiche sopra indicate).

Un certificato di sigillo elettronico si considera qualificato se contiene (come si può leggere nell'Allegato III del regolamento eIDAS):

1) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di sigillo elettronico;
2) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali, per una persona fisica: il nome della persona;
3) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;
4) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;
5) l'indicazione dell'inizio e della fine del periodo di validità del certificato;
6) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;
7) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

[80] Regolamento (UE) 910/2014, art. 3, paragrafo, 27.

8) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui al numero 7) è disponibile gratuitamente;
9) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;
10) qualora i dati per la creazione di un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

A questo punto è necessario evidenziare cosa intende il legislatore europeo con le espressioni *"certificato qualificato di sigillo elettronico"* e *"dispositivo per la creazione di un sigillo elettronico qualificato"*.

Per *"certificato qualificato di sigillo elettronico"*[81], si intende un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica confermando il nome di tale soggetto, che è rilasciato da un prestatore di servizi fiduciari qualificato nonché che è conforme a particolari requisiti, che indicano quali sono gli elementi che tali certifica e devono obbligatoriamente contenere. Nello specifico questi sono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di sigillo elettronico;
b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

[81] A tal proposito si veda il Regolamento (UE) 910/2014, art. 3, paragrafi 29 e 30, nonché Allegato III.

- per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,
- per una persona fisica: il nome della persona;

c) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;
d) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;
e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;
f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;
g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;
h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;
i) dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;
j) un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato[82].

Per *"dispositivo per la creazione di un sigillo elettronico qualificato"*[83], invece, si intende un software o hardware configurato utilizzato per creare un sigillo elettronico; he soddisfa *mutatis mutandis* i requisiti di cui all'Allegato II del Regolamento eIDAS, già previsti nella firma elettronica qualificata.

[82] Regolamento (UE) 910/2014, Allegato III, paragrafo 1.
[83] A tal proposito si rinvia al regolamento (UE) 910/2014, art. 3, paragrafi 31 e 32, nonché Allegato II.

Effetti giuridici dei sigilli elettronici.

I sigilli elettronici nel nostro ordinamento non sono definiti direttamente, ma vengono recepiti dal diritto comunitario (Regolamento (UE) 910/2014).

Pertanto per comprendere e conoscere i loro effetti giuridici dobbiamo ricondurci alla normativa europea.

L'inserimento del comma 1-bis dell'art.1 CAD dal D.Lgs. 179/2016 dove si evidenzia come *"ai fini del presente Codice, valgono le definizioni di cui all' articolo 3 del regolamento eIDAS"*[84] si legge esplicitamente il legame che lega il Codice dell' Amministrazione Digitale al Regolamento eIDAS. Dunque, le definizioni che valgono ai fini del CAD sono date dalla sommatoria di quelle presenti nel Regolamento eIDAS e di quelle contenute nel CAD stesso.

Gli effetti giuridici dei sigilli elettronici sono disciplinati nell'art.35del Regolamento (UE) 910/2014. Indipendentemente dal particolare sigillo elettronico considerato, a questo "*non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati"*[85]. Il livello di tutela sale se si considera il sigillo elettronico qualificato. Il quale, in aggiunta, *"gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato"*[86]. Se il sigillo, poi, si basa su di un certificato

[84] Regolamento (UE) 910/2014, art. 3, paragrafo 1.
[85] Regolamento (UE) 910/2014, art. 35, paragrafo 1.
[86] A tal proposito si rinvia al Regolamento (UE) 910/2014, art. 35, paragrafo 3.

qualificato che è stato rilasciato in uno Stato membro dell' UE, questo sarà riconosciuto anche negli altri Stati membri.

In tabella gli effetti giuridici dei sigilli elettronici secondo la normativa nazionale e comunitaria.

Tipo di sigillo	Italia	UE
Sigillo elettronico	Tale strumento non direttamente presente nell'ordinamento italiano, di completa derivazione dal diritto comunitario	Ammissibile come prova in procedimenti giudiziali
Sigillo Elettronico avanzato	Tale strumento non direttamente presente nell'ordinamento italiano, di completa derivazione dal diritto comunitario	Ammissibile come prova in procedimenti giudiziali
Sigillo elettronico qualificato	Tale strumento non direttamente presente nell'ordinamento italiano, di completa derivazione dal diritto comunitario	Gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato

Sigillo elettronico e firma digitale

Fino a questo punto, sembra che il sigillo elettronico e la firma digitale possano essere considerati, di fatto, equivalenti (visto che, in sostanza, anche le due definizioni sono, di fatto, analoghe). In realtà, tra i due strumenti sussistono delle precise differenze. Differenze da conoscere bene per sapere quale dei due strumenti utilizzare a seconda di circostanze e necessità.

Sigillo elettronico	Firma digitale
Garantisce l'origine e l'integrità dei documenti digitali	Garantisce l'identità del firmatario di un documento digitale e conferisce piena validità legale a un documento digitale
Si riferisce a una persona giuridica (un organismo unitario composto da una pluralità di individui o un complesso di beni, al quale vengono riconosciuti diritti e doveri)	Si riferisce a una persona fisica (un soggetto di diritto, dotato di capacità giuridica, con degli obblighi e dei diritti fin dalla sua nascita)

In conclusione, si può dire che la firma digitale è uno strumento indicato per le persone, mentre il sigillo elettronico è a uso (quasi) esclusivo di enti o aziende.

2.2 Il documento informatico

Il documento informatico è l'elemento centrale per la digitalizzazione delle pratiche amministrative.

Il Regolamento eIDAS n. 910/2014 fornisce una definizione molto estesa di **documento elettronico** inteso come "*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva*". Secondo la normativa europea, la qualifica di documento elettronico è intrinsecamente determinata dalle modalità di rappresentazione di un qualsiasi contenuto, che non possono prescindere dall'utilizzo di una forma (o formato) elettronico.[87]

[87] CICLOSI F., *I documenti informatici dopo le nuove Linee guida AgiD – Formazione, gestione e conservazione*, Maggioli, 2021

La vigente versione del Codice dell'Amministrazione Digitale (CAD) fornisce ulteriori elementi di qualificazione racchiusi nella definizione di **documento informatico**, inteso come "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"[88], in contrapposizione al **documento analogico** ("*rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*").

Una difficoltà è quella di distinguere tra le diverse tipologie di documenti informatici utilizzati, considerando che, per alcuni di essi, la vigente normativa impone l'obbligo di attestarne la conformità.

Possiamo distinguere diverse tipologie di documenti informatici:

a) **Documento informatico (nativo digitale)**
b) **Copia per immagine su supporto informatico di documento analogico (cartaceo)**
c) **Duplicato informatico**
d) **Copia informatica di documento informatico**

[88] Cfr art. 1, comma 1 lettera p) del Codice dell'Amministrazione Digitale – D.lgs 82/2005

Proviamo a spiegare e chiarire le differenze esistenti tra queste diverse tipologie di documenti informatici.

2.2.1 Documento informatico (nativo digitale)

Riferimento normativo: **art. 20 D.Lgs. 7 marzo 2005 n. 82**

Quando si parla di documento informatico è naturale associare l'idea di documento a quella di *file*. Vi è però da dire che la tradizione giuridica italiana, tradizionalmente di stampo più umanistico che informatico, ha influenzato il Legislatore e nelle definizioni normative, dapprima dell'art. 22 Legge 241/90 al cui par. 1 lett d) si intende per "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" e successivamente nell'abrogato art. 9 del dpr 455/2000 secondo cui "gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge". [89]

[89] DONGIOVANNI F. *"La formazione del documento informatico alla luce delle nuove Linee Guida AgID", 2021*

Nel Codice dell'Amministrazione Digitale (di seguito CAD), la naturale derivazione del concetto di documento informatico è pervenuta nell'art. 1, lettera p) del D.Lgs 82/2005, secondo cui sono documenti informatici quei *file* che contengano una «***rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti***».

Si può pertanto riscontrare, che le definizioni citate si rifanno alla teoria formulata da Carnelutti secondo cui il documento «*è una cosa rappresentativa di un fatto giuridicamente rilevante»* od anche «*qualsiasi oggetto, cosa idonea a far conoscere un fatto, diversa dal testimone, che è una persona, e non una cosa che rappresenta*»[90].

2.2.2 Copia per immagine su supporto informatico di documento analogico

Riferimento normativo: **art. 22 D.Lgs. 7 marzo 2005 n. 82**

Nel CAD la copia per immagine su supporto informatico di documento analogico nell'art. 1, comma 1, lett. I-bis) è definita come "il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto" e sempre nell'art. 1, comma 1, i ter) la copia informatica di documento analogico è "il documento informatico, avente contenuto identico a quello del documento analogico da cui è tratto". Sempre il CAD all'art. 22 comma 1-bis ricorda come deve essere prodotta la copia per immagine su supporto informatico di documento analogico, ovvero "*mediante processi e strumenti che assicurano 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*

[90] Si veda F. CARNELUTTI, Documento – Teoria moderna, in Nov. Digesto Italiano, VI, Torino, 1957, pag. 85 e segg.

.

in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia"[91].

Sempre in base all'art. 22 del CAD le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, in base alle Linee guida AgID, diversamente le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico formate in base alle Linee guida AgID mantengono la stessa efficacia probatoria se non disconosciute in giudizio.

Le copie formate nelle predette modalità sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo diverse disposizioni di legge[92].

All'interno delle nuove Linee guida risiedono importanti novità come la specificazione che la certificazione di processo deve essere considerata nel caso di esigenze di dematerializzazione massiva dei documenti analogici[93], attraverso le regole tecniche indicate nell'allegato 3 alle Linee guida (disciplinanti la certificazione di processo). Vengono inoltre aggiornate le modalità per assicurare la conformità delle copie per immagine mediante "l'apposizione della firma digitale o firma elettronica qualificata a firma elettronica avanzata…, ovvero sigillo elettronico qualificato o avanzato da parte di chi

[91] Per una dettagliata disciplina della "certificazione di processo" vedasi *Linee guida sulla formazione, gestione dei documenti informatici* All. 3 "Certificazione di processo".
[92] Sui documenti analogici non suscettibili di conservazione digitale si veda il comma 5 dell'art 22 del CAD.
[93] Vedasi *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.2 "Copie per immagine su supporto informatico di documenti analogici".

effettua il raffronto". Quindi la conformità della copia per immagine è garantita in base a quanto disposto dall'art. 20 comma 1 bis del CAD, ovvero "previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi (delle Linee guida AgID) con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore".

Inoltre, in continuità con quanto previsto dal CAD, le Linee guida stabiliscono che il documento informatico contenente l'attestazione di pubblico ufficiale è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato[94]. Tale attestazione di conformità avviene mediante dichiarazione allegata o asseverata al documento informatico da notaio o altro pubblico ufficiale a ciò autorizzato[95]. L'attestazione di conformità potrà essere inserita nel documento informatico o essere prodotta come separato documento informatico contenente un riferimento temporale e l'impronta di ogni copia per immagine. Le copie originali dei documenti potranno essere distrutte conformemente a quanto previsto dall'art. 22 comma 2 e 5 del CAD[96].

2.2.3 Duplicato informatico

Riferimento normativo: **art. 23bis comma 1 D.Lgs. 7 marzo 2005 n. 82**

Nel mondo analogico, una copia di un atto cartaceo è ontologicamente diversa dall'originale mentre in ambito

[94] Ibidem.
[95] Sulla definizione di attestazione di conformità vedasi *Linee guida sulla formazione, gestione dei documenti informatici* All.1 "Glossario"
[96] Vedasi *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.2 "Copie per immagine su supporto informatico di documenti analogici".

informatico la copia di un file informatico è identica all'originale. Si assiste pertanto nel C.A.D. alla nascita di un *terzo tipo* documentale, denominato "***duplicato informatico***", disciplinato dall'art. 1 lettera i-quinquies) del CAD secondo cui esso è un *"documento informatico ottenuto mediante la, memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario"*, e che translittera nella terminologia giuridica il concetto di copia adoperato in informatica. Infatti in informatica un file presenta rispetto alla sua copia sia contenitore che il contenuto esattamente identici in quanto strutturato in una stessa identica sequenza di bit. In questo caso vi è la piena coincidenza tra i due documenti informatici sia per il contenuto che per la sequenza dei valori binari che costituisce la loro rappresentazione informatica.[97]

Nell'ambito del duplicato informatico nelle Linee guida si specifica che esso ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica[98], sullo stesso dispositivo o su dispositivi diversi. Un esempio pratico di duplicato informatico descritto dalle Linee guida è la formazione di quest'ultimo mediante copia da un PC ad una pen-drive di un documento nel medesimo formato[99].

2.2.4 Copia informatica di documento informatico

Riferimento normativo: **art. 23bis comma 2 D.Lgs. 7 marzo 2005 n. 82**

---

[97] DONGIOVANNI F. *"La formazione del documento informatico alla luce delle nuove Linee Guida AgID", 2021*

[98] Per evidenza informatica, secondo quanto stabilito dalle Linee guida al paragrafo 2.3 "Duplicati, copie ed estratti informatici di documenti informatici" si fa riferimento a una "sequenza finiti di bit che può essere elaborata da una procedura informatica".

[99] Vedasi *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.3 "Duplicati, copie ed estratti informatici di documenti informatici".

La *copia informatica* di documento informatico è definita nell'art. 1, comma 1, lett. i-quater) del CAD come *"il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari"*. Il tratto distintivo si evidenzia pertanto in una coincidenza con il contenuto a fronte di una divergenza nella sequenza dei valori binari. Nell'ambito del concetto di copia di un documento di un documento informatico, le Linee guida specificano che questa è "un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto" e "l'estratto 'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto"[100].

La validità del documento informatico per copie e/o estratti di documenti informatici è consentita tramite il raffronto dei documenti o la certificazione di processo, assicurando in entrambi i modi il ricorso "la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine"[101].

Nelle Linee guida, il valore probatorio di tali documenti è subordinato al fatto che vi sia o meno un'attestazione di conformità redatta da un pubblico ufficiale.

Nel primo caso pertanto la piena efficacia probatoria si ha a patto che la produzione delle copie o degli estratti

[100] Ai fini della rappresentazione di tali concetti nelle Linee guida si fa l'esempio di un documento informatico con estensione ".doc" trasformato in altro documento informatico con estensione ".pdf" come creazione della copia di un documento informatico, poiché il primo e il secondo documento avranno il medesimo contenuto, ma una differente sequenza di bit (Vedasi Linee guida sulla formazione, gestione dei documenti informatici, par. 2.3 "Duplicati, copie ed estratti informatici di documenti informatici").

[101] Vedasi *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.3 "Duplicati, copie ed estratti informatici di documenti informatici".

conformemente ai dettami delle Linee guida, insieme al verificarsi alternativamente delle seguenti condizioni:

a) la conformità all'originale in tutte le sue componenti attestata da un pubblico ufficiale autorizzato a farlo;
b) il non espresso disconoscimento della conformità;
c) la conservazione dell'originale informatico da cui sono tratte la copia o l'estratto (nei casi in cui è espressamente previsto).

Nel secondo caso in cui non vi sia l'attestazione di un pubblico ufficiale, ai fini di recepire le previsioni contenute nel Regolamento eIDAS e CAD, la conformità della copia o dell'estratto informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto. In linea con le disposizioni del DPCM 13 novembre 2014, l'attestazione della conformità delle copie o dell'estratto informatico di un documento informatico, può avvenire tramite inserimento nel documento informatico contenente la copia o l'estratto, o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico che contiene l'attestazione dovrà essere "sottoscritto con firma o con firma elettronica qualificata o digitale avanzato del notaio o del pubblico ufficiale a ciò autorizzato"[102].

[102] Ibidem.

2.3 Il documento informatico nelle Nuove Linee Guida AgID[103]

Il 30 settembre 2020 l'Agenzia per l'Italia Digitale (di seguito AgID) con determinazione n. 407 del 9 settembre 2020 ha adottato le nuove "*Linee guida sulla formazione, gestione e conservazione dei documenti informatici*"[104], le quali diventeranno obbligatorie il 01.01.2022[105], e abrogano in toto il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici", il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione", e quasi del tutto il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico"[106].

Le Linee Guida sono state adottate ai sensi dell'art. 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes* secondo quanto stabilito dal Consiglio di Stato nel parere n. 2122 del 10.10.2017[107].

Per ciò che concerne le modalità di formazione del documento informatico si osserva una sostanziale continuità con

---

[103] DONGIOVANNI F. *"La formazione del documento informatico alla luce delle nuove Linee Guida AgID", 2021*

[104] Si veda comunicazione nella Gazzetta Ufficiale della Repubblica Italiana, serie generale n. 259 del 19 ottobre 2020. Le Linee guida diventeranno obbligatorie il 01.01.2022 secondo quanto stabilito

[105] Con determinazione n. 371 /2021 AgID ha posticipato l'obbligatorietà delle linee guida al 01.01.2022, confermando che i DPCM oggetto di abrogazione saranno ancora in vigore sino a tale data.

[106] Gli articoli del DPCM 3 dicembre 2013 sul protocollo informatico ancora in vigore riguardano l'art. 2 comma 1, Oggetto e ambito di applicazione; l'art. 6, Funzionalità; l'art. 9, Formato della segnatura di protocollo; l'art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici; l'art. 20, Segnatura di protocollo dei documenti trasmessi; l'art. 21, Informazioni da includere nella segnatura.

[107] Per un riferimento al citato parere e per consultare il documento originale si consulti il sito https://www.giustizia-amministrativa.it/cons.-st.-comm.-spec.-10-ottobre-2017-n.-2122.

quanto contenuto nel predetto DPCM 13 novembre 2014, prevedendo inoltre la possibilità di creare il documento informatico tramite l'utilizzo di strumenti software ed anche attraverso l'adozione di servizi cloud qualificati[108].

Le Pubbliche Amministrazioni e i soggetti di cui all'art. 2 commi 2 e 3 del CAD formano i documenti informatici secondo le seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità, e la cui *immodificabilità e integrità* sono garantite da:
   - apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
   - memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza ICT di AgID del 2017 e del Reg. UE 679/2016;
   - trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato valido ai fini delle comunicazioni elettroniche aventi valore legale[109];
   - versamento ad un sistema di conservazione;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico, e la cui *immodificabilità e integrità* sono garantite da:

[108] Si vedano *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.1.1 sulla "formazione del documento informatico".

[109] Come specificato nel Regolamento Europeo 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS).

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale;
- versamento ad un sistema di conservazione;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente, e la cui *immodificabilità e integrità* sono garantite da:
   - apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
   - registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
   - produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica, e la cui *immodificabilità e integrità* sono garantite dall'applicazione delle misure di cui ai punti precedenti.

Le nuove Linee guida rispetto alle precedenti regole tecniche chiariscono che il documento informatico deve essere identificato in modo univoco e persistente nel tempo[110], e nel caso delle Pubblica Amministrazione l'univocità del documento

[110] Vedasi *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.1.1 sulla "formazione del documento informatico".

può avvenire in modalità differente a seconda che il documento informatico sia soggetto a registrazione di protocollo o meno.

Nel caso il documento sia soggetto a registrazione di protocollo l'identificazione è rappresentata dalla segnatura di protocollo associata in maniera univoca al documento, mentre nel caso il documento non sia soggetto alla registrazione di protocollo l'identificazione viene affidata alle funzioni del sistema di gestione informatica dei documenti[111].

2.4 Posta Elettronica Certificata (PEC)

Che cos'è la PEC?

L'art. 1, comma 1, lettera v-bis, del CAD definisce la PEC come un **sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi**[112].

Per utilizzare un linguaggio corrente possiamo definirla un tipo speciale di email che consente di inviare e ricevere messaggi di testo e allegati con lo stesso **valore legale** di una raccomandata con avviso di ricevimento. È per questo che la PEC è uno degli **strumenti chiave per digitalizzare il lavoro delle amministrazioni pubbliche**.

- **Chi ha mandato il messaggio?**
  colui che nella e-mail figura come mittente.

- **Quando è stato mandato il messaggio?**

[111] Nel caso di registrazione non soggette a registrazioni di protocollo l'identificazione può essere soggetta anche mediante associazione al documento di una sua impronta crittografica generata da algoritmi di hash ritenuti crittograficamente sicuri (vedasi *Linee guida sulla formazione, gestione dei documenti informatici*, par. 2.1.1 sulla "formazione del documento informatico".).

[112] Art. 1, comma 1, lettera v-bis, CAD (d.lgs. n. 82 del 7 marzo 2005).

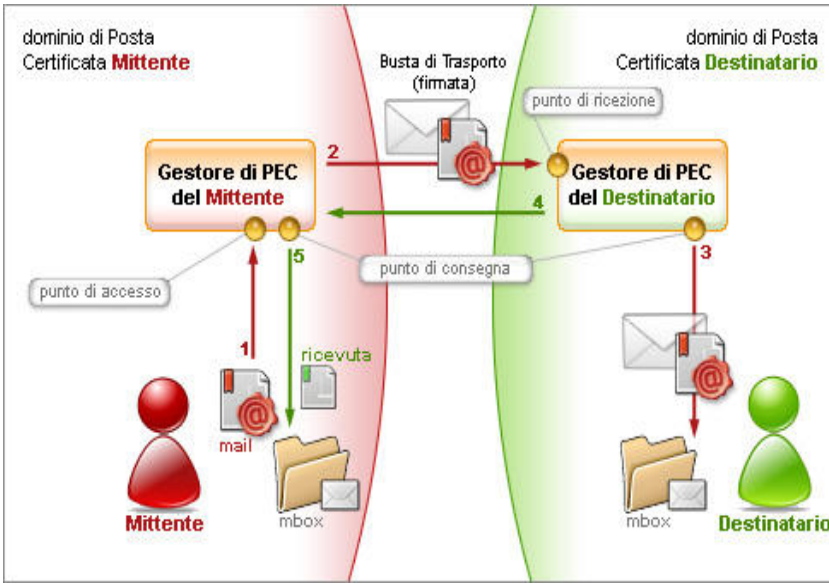
all'ora indicata dalla e-mail.

- **Cosa voleva dirmi il mittente?**
  ciò che è contenuto nella e-mail o negli allegati.

Il sistema di posta elettronica certificata risolve alcune carenze intrinseche della raccomandata tradizionale, ossia la conoscibilità certa della casella mittente (mentre non è tracciabile colui che spedisce una raccomandata); e la possibilità di legare in maniera certa ed opponibile ai terzi la trasmissione con il documento trasmesso, possibilità preclusa con la raccomandata.

La funzionalità della PEC è garantita dai gestori del servizio, i quali, infatti, sono tenuti a sottoscrivere le ricevute di accettazione e consegna mediante una firma elettronica che consente di rendere manifesta la provenienza, ed assicurare l'integrità e l'autenticità delle ricevute stesse; mentre la busta di trasporto è sottoscritta con una firma elettronica che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata[113].

[113] Art. 9, commi 1 e 2, DPR n. 68/2005.



Diverse tipologie di PEC:

- quelle per professionisti ed imprese (ma, ora, anche per i cittadini);
- quella per i cittadini (ma solo verso la PA, la c.d. CECPAC – Casella Elettronica Certificata Pubblica Amministrazione e Cittadini, chiusa dal 18 settembre 2015);
- la PEC-ID, disciplinata dal DPCM del 27 settembre 2012.

I riferimenti normativi principali della PEC sono:

- il CAD (d.lgs. n. 82 del 7 marzo 2005);
- il D.P.R. dell'11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata";
- il Decreto Ministeriale del 2 novembre 2005, recante "Regole tecniche per la formazione, la trasmissione e la

validazione, anche temporale, della posta elettronica certificata".

2.5 Domicilio digitale dei professionisti, imprese e P.A.

2.5.1 INdicePA

L'indice dei domicili digitali delle pubbliche amministrazioni (IPA) è una banca dati di libera consultazione dove è possibile trovare informazioni per comunicare con le Pubbliche Amministrazioni e i Gestori di Pubblici Servizi. Se si hanno rapporti contrattuali con le Pubbliche Amministrazioni in IPA è possibile trovare i riferimenti necessari per la fatturazione elettronica e per gli ordini elettronici[114].

I contenuti di IPA sono strutturati in tre macro livelli:

1. informazioni di sintesi sull'Ente;
2. informazioni sugli uffici di protocollo (Aree Organizzative Omogenee - AOO)
3. informazioni sui singoli uffici (Unità Organizzative – UO), sulla struttura organizzativa e gerarchica.

Gli Enti iscritti in IPA sono responsabili della gestione dei dati pubblicati e sono tenuti ad aggiornare i contenuti pubblicati

[114] L'IPA è una banca dati di libera consultazione in cui puoi trovare i riferimenti per comunicare con le Pubbliche Amministrazioni e i Gestori di Pubblici Servizi. Se hai rapporti contrattuali con le Pubbliche Amministrazioni in IPA trovi i riferimenti necessari per la fatturazione elettronica e per gli ordini elettronici.

con cadenza almeno semestrale. Le linee guida IPA[115], emesse ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 (CAD), adottate con Determinazione n. 97/2019, definiscono:

- le informazioni che gli Enti dovranno inserire all'interno dell'IPA, tra cui l'indicazione del proprio **domicilio digitale**, come previsto dall'art. 6-ter del CAD[116];
- le regole tecniche che gli Enti dovranno seguire per pubblicare i propri riferimenti;
- le modalità di gestione dei contenuti informativi all'interno dell'Indice.

Come ricercare il Codice IPA.

Per poter trovare i dati di cui si necessita ed anche un codice IPA o un domicilio digitale, nella schermata home è possibile utilizzare una barra di ricerca. Questa, una volta digitato ciò che si cerca, condurrà a ciò che effettivamente si vuol trovare. Per farlo, basta scegliere tre parole presenti nel nome dell'ente o in qualsiasi altro documento e cliccare su cerca.

Le azioni dunque sono queste:

1. cliccare nella barra di ricerca;
2. digitare tre parole presenti all'interno del documento o dell'ente;
3. cliccare su cerca.

Dopo aver effettuato queste azioni, sarà poi possibile usufruire dell'elenco codici IPA e di tutte le informazioni di cui si necessita. La barra di ricerca però non è l'unica possibilità per trovare ciò che si cerca, ci sono infatti anche verso il basso della

[115] https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_ipa.pdf.
[116] C.A.D. Codice dell'Amministrazione Digitale: art. 6-ter "*Indice degli indirizzi delle pubbliche amministrazioni e dei gestori di pubblici servizi*", art. 47 "*Trasmissione dei documenti tra le pubbliche amministrazioni*".

home page, delle icone che categorizzano tutte le tipologie di ricerche.

2.5.2 INI-PEC

INI-PEC è l'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata istituito dal Ministero dello Sviluppo Economico[117].

INI-PEC raccoglie tutti gli indirizzi di PEC delle Imprese e dei Professionisti presenti sul territorio italiano ed è pensato per chiunque abbia la necessità di ottenere l'indirizzo di PEC di un professionista o di un'impresa che desidera contattare.

L'istituto è stato pensato con l'intento di semplificare la comunicazione tra cittadini, imprese, professionisti e istituzioni raccogliendo gli indirizzi di posta elettronica certificata delle imprese e dei professionisti di tutta Italia e trova disciplina nell' articolo 6-bis del decreto legislativo 7 marzo 2005, n.82 concernente "Codice dell'amministrazione digitale" introdotto dall'articolo 5, comma 3 del decreto legge 18 ottobre 2012 n.179, convertito con modificazioni dalla legge 17 dicembre 2012, n.221[118].

---

[117]Decreto 19 Marzo 2013. Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti (INI-PEC). http://www.inipec.gov.it.

[118] Art. 6bis - Indice nazionale degli indirizzi PEC delle imprese e dei professionisti, recita: *"Al fine di favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito, entro sei mesi dalla data di entrata in vigore della presente disposizione e con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico.*
L'Indice nazionale di cui al comma 1 è realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali, in

INI-PEC è la prova che l'innovazione passa anche attraverso azioni semplici, come mettere a disposizione in un luogo digitale gli indirizzi di posta elettronica certificata: un fatto all'apparenza scontato che però cambia la pratica quotidiana di migliaia di cittadini, e pubbliche amministrazioni, consentendo di risparmiare tempo e denaro.

Senza bisogno di autenticazione o di programmi aggiuntivi, chiunque può accedere alla sezione di ricerca del portale e cercare l'indirizzo di posta elettronica certificata di proprio interesse.

Se l'azienda o il professionista cercato è presente nell'indice, INI-PEC fornisce all'utente l'indirizzo richiesto, semplificando la vita di tutti.

L'indice viene puntualmente aggiornato con i dati provenienti dal Registro Imprese e dagli Ordini e dai Collegi di appartenenza, nelle modalità stabilite dalla legge.

---

attuazione di& quanto previsto dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2.
L'accesso all'INI-PEC è consentito alle pubbliche amministrazioni, ai professionisti alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini tramite sito web senza necessità di autenticazione. L'indice è realizzato in formato aperto, secondo la definizione di cui all'articolo 68, comma 3.
Il Ministero per lo sviluppo economico, al fine del contenimento dei costi e dell'utilizzo razionale delle risorse, sentita l'Agenzia per l'Italia digitale, si avvale per la realizzazione e gestione operativa dell'Indice nazionale di cui al comma 1 delle strutture informatiche delle Camere di commercio deputate alla gestione del registro imprese e ne definisce con proprio decreto, da emanare entro 60 giorni dalla data di entrata in vigore della presente disposizione, le modalità di accesso e di aggiornamento.
Nel decreto di cui al comma 4 sono anche definite le modalità e le forme con cui gli ordini ei collegi professionali comunicano all'Indice nazionale di cui al comma 1 tutti gli indirizzi PEC relativi ai professionisti di propria competenza e sono previsti gli strumenti telematici resi disponibili dalle Camere di commercio per il tramite delle proprie strutture informatiche al fine di ottimizzare la raccolta e aggiornamento dei medesimi indirizzi".

Il reperimento delle informazioni di tutti gli operatori economici che per legge devono possedere un proprio indirizzo PEC è ora più agevole ed efficace grazie ad INI-PEC.

2.5.3 INAD

In futuro, a completare il sistema, è prevista l'istituzione dell'**INAD**, l'Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro Imprese. Per ora, le modalità di realizzazione e gestione operativa dell'INAD sono contemplate dalle Linee Guida adottate ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005), che sono state oggetto di una consultazione pubblica sino al 10 luglio 2020.

L'INAD verrà realizzato e gestito dall'AGID ("Gestore INAD") che vi provvederà avvalendosi di InfoCamere S.c.p.A. quale struttura informatica delle Camere di commercio già deputata alla gestione dell'elenco INI-PEC.

In questo elenco pubblico verranno iscritti i domicili digitali eletti ai sensi dell'art. 3-bis, commi 1-bis e 1-ter, CAD destinati alle comunicazioni aventi valore legale effettuate dai soggetti privati o dai soggetti di cui all'art. 2, comma 2, CAD e, con riferimento a questi ultimi, altresì alle comunicazioni connesse al conseguimento di finalità istituzionali (si pensi agli avvisi di pagamento, alle notifiche, alle multe).

In particolare, potranno eleggere il proprio domicilio digitale mediante iscrizione nell'INAD:

- le persone fisiche che avranno compiuto il 18° anno di età e capaci di agire;
- gli enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro delle imprese e, quindi,

all'iscrizione del proprio domicilio digitale negli elenchi INI-PEC o IPA.

2.6 Il protocollo informatico ed i flussi documentali

Il Legislatore definisce il **protocollo informatico** come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti'', ovvero tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali[119].

L'attività di protocollazione è quella fase del processo amministrativo che certifica provenienza e data di acquisizione del documento identificandolo in maniera univoca per mezzo dell'apposizione di informazioni numeriche e temporali. La protocollazione della comunicazioni in entrata e in uscita deve avvenire attraverso un sistema automatizzato (art. 40-bis CAD, art. 50 D.P.R. n. 445/2000) e costituisce, pertanto, un passo obbligato per tutti i flussi documentali che intercorrono tra le Amministrazioni ed all'interno di esse.

L' introduzione del concetto di protocollo informatico nella pubblica amministrazione italiana risale, quindi, al DPR n. 445 del 28 dicembre 2000, il TU sulla documentazione amministrativa (anche detto TUDA) che ha reso obbligatoria per le Pubbliche Amministrazioni la registrazione di tutti i flussi documentali. In particolare, l'art. 61 del Decreto dispone che ciascuna Amministrazione debba istituire un servizio per la tenuta del protocollo informatico, della gestione dei flussi

[119] Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR 445/2000, art.1).

documentali e degli archivi per ciascuna delle Aree Organizzative Omogenee (AOO)[120] in cui essa si sviluppa.

La normativa si completa con il DPCM3 dicembre 2013, recante le regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del CAD, che sostituiscono le precedenti di cui al DPCM 31 ottobre 2000.

Come funziona il protocollo informatico.

Parlare di come funziona il protocollo informatico significa spiegare cosa sia la **registrazione di protocollo**:

L'insieme di metadati che devono essere memorizzati dal registro di protocollo, al fine di tenere traccia di tutti i contenuti che vengono spediti o ricevuti da una pubblica amministrazione. L'associazione di queste informazioni (i metadati) ai documenti è permanente e non modificabile.

In altre parole, la registrazione di protocollo, associando determinate informazioni (i metadati) a un documento, tiene traccia di tutti i documenti in entrata e in uscita da una data Area organizzativa omogenea in una data pubblica amministrazione.

Obiettivi

Gli obiettivi che si intendono perseguire sono:

- eliminare i registri cartacei, diminuire gli uffici di protocollo, razionalizzare il flusso documentale;
- implementare gli strumenti che favoriscono un effettivo esercizio del diritto di accesso allo stato dei procedimenti ed ai relativi documenti da parte dei soggetti interessati (cittadini ed imprese) al fine di migliorare la trasparenza dell'azione amministrativa.

[120] L'Area Organizzativa Omogenea (AOO) è definita come un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'"articolo 50, comma 4, del DPR 28 dicembre 2000, n. 445.

Gestione dei flussi documentali.

Successivamente al DPR n. 445/00, l'assetto normativo è stato rimodulato sulla base del CAD, il quale, pur non contenendo la completa disciplina del protocollo informatico, in parte ancora mantenuta nel DPR n. 445/00, ne completa alcuni aspetti e, soprattutto, contiene la definizione legislativa aggiornata di gestione informatica dei documenti, al cui interno si colloca il protocollo informatico.

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

Le Linee guida AgID riguardanti la **gestione documentale**[121], per la precisione nel capitolo 3, introducono ulteriori specifiche per quanto riguarda il protocollo informatico.

Il protocollo informatico a norma dell' art. 52 del DPR. n.445/00 deve:

A. assicurare
   - il tracciamento e la storicizzazione di qualsiasi operazione, comprese quelle di annullamento, e l'attribuzione all'operatore;
   - l'immodificabilità delle informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo;
   - la modificabilità solo delle informazioni relative all'assegnazione interna all'amministrazione e alla classificazione;

[121]https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/20253150222O__OLinee+Guida+sul+documento+informatico+.pdf.

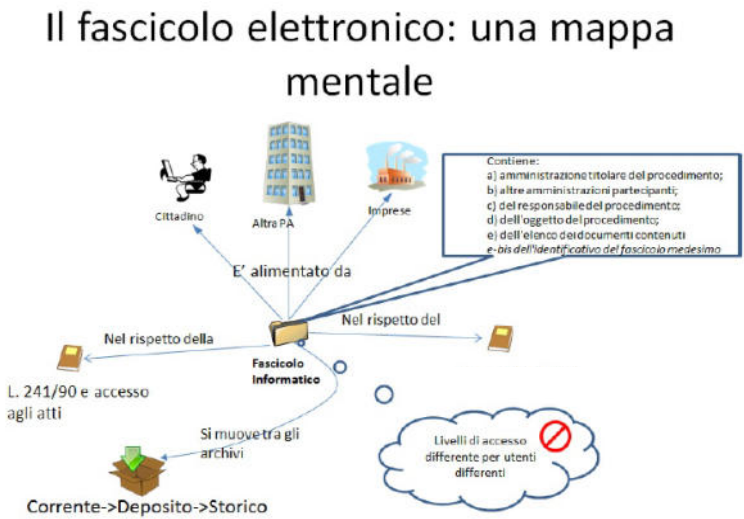
- la storicizzazione delle informazioni annullate attraverso le informazioni oggetto della stessa;
- la storicizzazione di tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili.

B. garantire
   - identificazione e autenticazione di tutti gli utenti;
   - l'accesso alle informazioni unicamente agli utenti o ai gruppi di utenti autorizzati a farlo;
   - il tracciamento permanente di qualsiasi operazione di modifica;
   - l'individuazione del soggetto che ha effettuato le eventuali operazioni di modifica.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto[122].

Il Codice dell'Amministrazione Digitale (CAD), inoltre, deve prevedere che le pubbliche amministrazioni siano tenute – per ciascun procedimento di loro competenza – a raccogliere in un **fascicolo informatico** gli atti e i documenti da chiunque formati, rendendoli direttamente consultabili da tutte le amministrazioni coinvolte nel procedimento.

[122] "Istruzioni per la produzione e conservazione del registro giornaliero di protocollo", emanate dall'AGID per aiutare le Pubbliche Amministrazioni a rispettare l'obbligo, a partire dall'11 ottobre 2015, di inviare in conservazione il registro giornaliero di protocollo entro la giornata lavorativa successiva.



Il **D.Lgs. 217/2017** ha poi introdotto **la pari accessibilità al fascicolo da parte di tutti gli interessati** attraverso il sistema documentale di ricerca ed il punto di accesso telematico ai servizi della PA.

A norma dell'art. 41 comma 2-ter del CAD, così come modificato dall'ultimo correttivo, il fascicolo informatico deve recare l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) delle altre amministrazioni partecipanti;
c) del responsabile del procedimento;
d) dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
f) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida.

Come accennato, il D.Lgs. 217/20217 ha introdotto l'art. 40-ter del CAD che ha previsto il Sistema pubblico di ricerca documentale. Si tratta di un sistema "volto a facilitare la ricerca dei documenti soggetti a obblighi di pubblicità legale, trasparenza o a registrazione di protocollo ai sensi dell' art. 53 del DPR n. 445/00, e di cui all' art. 40-bis e dei fascicoli dei procedimenti di cui all'art. 41, nonché a consentire l'accesso *on-line* ai soggetti che ne abbiano diritto ai sensi della disciplina vigente".

Le amministrazioni sono tenute, dunque, ad integrare il proprio servizio di gestione documentale con il sistema di ricerca documentale, al fine di consentire la ricerca dei documenti soggetti ad obblighi di pubblicità legale nonché la consultazione e l'alimentazione dei fascicoli informatici da parte delle amministrazioni coinvolte nei procedimenti dei soggetti interessati.

Ai sensi dell' art. 56 del DPR n. 445/00, le operazioni di **registrazione** e le operazioni di **segnatura di protocollo** nonché le operazioni di **classificazione** costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle Pubbliche Amministrazioni, ossia quella che viene considerata la **funzionalità minima del protocollo informatico**.

Le due attività più importanti sono, quindi, la registrazione del protocollo e la segnatura di protocollo.

La prima è effettuata per ogni documento ricevuto o spedito dalle Pubbliche Amministrazioni mediante la memorizzazione delle seguenti informazioni:

a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;

b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili;
e) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Invece, la segnatura di protocollo consiste nell'apposizione o associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile e le informazioni minime previste sono:

a) il progressivo di protocollo;
b) la data di protocollo;
c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata.

In base al comma 2 dell'art. 55 TUDA, l'operazione di segnatura di protocollo va effettuata contemporaneamente all'operazione di registrazione di protocollo.

Il DPCM 3 dicembre 2013, inoltre, prevede che le Pubbliche Amministrazioni individuino obbligatoriamente le Aree Organizzative Omogenee e i relativi uffici di riferimento, nominino, in ciascuna delle Aree Organizzative Omogenee individuate, il **responsabile della gestione documentale**, e un suo vicario, per casi di vacanza, assenza o impedimento del

primo, adottino il manuale di gestione, definiscano i tempi, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico.

Al servizio della gestione dei flussi documentali deve essere preposto un **dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi formazione definiti secondo le procedure prescritte dalla disciplina vigente** (art. 61, co. 2, DPR n. 445/2000). È comunque raccomandabile che tale figura venga ricoperta dal soggetto preposto all'archivio dell'ente in quanto è il soggetto più indicato ad assumersi la responsabilità di garantire l'operatività ed il rispetto delle norme in materia di conservazione.

Con la riforma 2016 del CAD, attuata con il D.Lgs. n. 179, il Legislatore pare avere superato la distinzione di figure tra il Responsabile per la gestione e il Responsabile per la conservazione digitale, di cui appresso meglio si dirà. Nel nuovo art. 44 del CAD si individua, infatti, un **unico responsabile per il "sistema di gestione e conservazione dei documenti informatici"**. La norma del CAD è ovviamente di rango superiore rispetto a quella contenuta nei DPCM in tema di gestione e conservazione digitale, quindi prevalente. Ma la reale portata di tale novità normativa potrà essere compresa solo nel tempo e con le nuove regole tecniche di prossima emanazione. Di certo l'"avere accomunato le due fasi, gestione e conservazione, e riconosciuta la necessità di un solo responsabile è in linea, oggi, con quanto avviene con i principali applicativi e nelle Amministrazioni, ove si tende ad avere soluzioni informatiche che in un solo cruscotto mettano insieme le due fasi sotto la responsabilità di un unico soggetto (che

quindi al contempo è Responsabile per il protocollo e la gestione informatica e Responsabile per la conservazione digitale).

Un dubbio classico all'interno delle Amministrazioni è quello connesso al **"cosa", nella realtà della pratica quotidiana, occorra protocollare**: l'Amministrazione, a norma dell'art. 53, comma 5, del DPR n. 445/2000 ha l'obbligo di provvedere alla registrazione di protocollo per tutti i documenti ricevuti o spediti. Sono **esclusi** da tale obbligo gli atti infraprocedimentali tra i quali, a titolo esemplificativo, rientrano le circolari scolastiche. Non è, altresì, obbligatorio protocollare documenti come le offerte commerciali, le comunicazioni augurali, le newsletter e altri casi similari. Occorre sottolineare che le istruzioni relative alle comunicazioni sottratte alla protocollazione, in conformità con le norme di legge, devono essere sempre indicate nel manuale di gestione del protocollo informatico.

Per quanto attiene le PEC e PEO (Posta Elettronica Ordinaria), l'art. 40-bis del CAD impone alle Amministrazioni la loro protocollazione. In particolare, dovranno formare oggetto di registrazione di protocollo, sia in entrata che in uscita:

a) i messaggi Posta Elettronica Ordinaria inviati tra Pubbliche Amministrazioni;
b) i messaggi Posta Elettronica Ordinaria contenenti comunicazioni tra Amministrazione e dipendenti;
c) i messaggi di Posta Elettronica Certificata in genere.

2.7 Conservazione dei documenti informatici

Che cos'è la conservazione digitale?

La conservazione digitale è l'attività volta a proteggere nel tempo gli archivi di documenti informatici e i dati[123]. Il sistema ha l'obiettivo di impedire la perdita o la distruzione dei

[123] https://www.agid.gov.it/it/piattaforme/conservazione

documenti e di garantirne autenticità, integrità e accesso controllato ai fini amministrativi e di ricerca come previsto dal comma 1-ter dell'art.44 del CAD[124].

Chi deve conservare?

- Le pubbliche amministrazioni
- I privati, nel caso di obblighi normativi

Quali documenti conservare?

- I documenti amministrativi, fiscali e contabili, i fascicoli, i registri e i repertori informatici predisposti secondo le seguenti possibili forme:
- Documenti di testo, fogli di calcolo, schemi XML redatti tramite l'utilizzo di appositi strumenti software;
- Documenti acquisiti per via telematica o su supporto informatico, e-mail, documenti acquisiti come copia per immagine di un documento analogico;
- Registrazioni informatiche di transazioni o processi informatici, dati forniti dall'utente attraverso la compilazione di moduli o formulari elettronici;
- Insiemi di dati, provenienti da una o più basi dati, raggruppati secondo una struttura logica determinata (viste).

Quali strumenti servono per conservare i documenti a norma?

Conservazione digitale significa quindi sostituire i documenti cartacei, con lo stesso documento in formato digitale la cui valenza legale di forma, contenuto e tempo è testimoniata con una firma digitale e una marca temporale.

[124] Art. 44 comma 1-ter prevede che: **"**Il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida".

Il processo di conservazione:

A) comprende automaticamente:

- la firma digitale, ossia quella firma elettronica che si applica ai documenti informatici, esattamente come la firma tradizionale (autografa) viene apposta sui documenti cartacei;
- la marca temporale, ossia una successione di caratteri che rappresentano una data e/o un orario per assodare l'effettivo avvenimento di un'attività/evento.

L'unione della firma digitale alla marca temporale consente di mantenere invariati nel tempo l'autenticità , la reperibilità , il valore legale, la sicurezza, la leggibilità, l'integrità dei documenti conservati.

Il trasferimento dell'oggetto di conservazione nel sistema di conservazione avviene generando un *Pacchetto di Versamento (PdV)* nelle modalità e con il formato previsti dal manuale di conservazione.

B) prevede:

a. l'acquisizione da parte del sistema di conservazione del PdV per la sua presa in carico;
b. la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell' allegato 2 "Formati di file e riversamento" relativo ai formati;
c. il rifiuto del PdV, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie. Il numero massimo di rifiuti è stabilito nell'ambito di un contratto o convenzione e non può essere inferiore a 3, oltre il quale il conservatore non è più tenuto ad accettare quell'oggetto in conservazione. Tale misura serve a

sensibilizzare il Produttore nella fase di predisposizione del PdV;

d. la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;

e. l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata o avanzata apposta dal responsabile della conservazione o dal responsabile del servizio di conservazione, ove prevista nel manuale di conservazione;

f. la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o dal responsabile del servizio di conservazione con il sigillo elettronico qualificato o avanzato del titolare dell'oggetto di conservazione o del conservatore accreditato e la gestione del pacchetto di archiviazione, sulla base delle specifiche della struttura dati contenute nell'allegato 4 "Standard e specifiche tecniche" e secondo le modalità riportate nel manuale di conservazione;

g. la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione, oppure l'apposizione del sigillo elettronico qualificato o avanzato, secondo le modalità indicate nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;

h. ai fini della interoperabilità tra sistemi di conservazione, i pacchetti di distribuzione possono contenere parte, uno o più i pacchetti di archiviazione;

i. la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle presenti linee guida;

j. la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 "Formati di file e riversamento";

k. l'eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del Titolare dell'oggetto di conservazione e le procedure descritte nel successivo paragrafo 4.12;

l. nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIBAC rilasciata al Titolare dell'oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia.

Nel caso di affidamento a terzi del servizio di conservazione le modalità sono indicate nei manuali del Titolare dell'oggetto di conservazione e del conservatore accreditato e concordate tra le parti[125].

[125]https://docs.italia.it/AgID/documenti-in-consultazione/lg-documenti-informatici docs/it/bozza/conservazione.html#processo-di-conservazione.

Quali sono le figure professionali coinvolte?

Per la conservazione *in-house*, interviene la figura interna del responsabile della conservazione[126].

Per la conservazione *in outsourcing*, oltre al responsabile della conservazione del soggetto affidatario, un responsabile del servizio di conservazione del soggetto che lo eroga.

Mentre le regole tecniche sul protocollo informatico stabiliscono che il responsabile della gestione documentale deve essere interno alla PA, è possibile nominare un responsabile della conservazione che sia esterno all'ente, ma, in questo caso la scelta è limitata a soggetti accreditati scelti nell'albo tenuto dall'Agenzia per l'Italia Digitale: "la PA deve sempre e comunque nominare al suo interno un responsabile di conservazione, questo ultimo principio non è strettamente obbligatorio per le aziende private"[127].

Chiarire questo punto è molto importante: il responsabile della conservazione può delegare (tramite contratto) un soggetto terzo, ma non può privarsi della sua responsabilità nei termini di *culpa in eligendo e vigilando*.

---

[126] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

[127] http://www.agendadigitale.eu/identita-digitale/due-responsabili-distinti-per-conservazione-e-gestionedocumentale-come-possono-collaborare_1708.htm.

Come conservare i documenti?

In-house – i documenti vengono conservati all'interno della propria struttura organizzativa. I soggetti devono rispettare quanto previsto dalle Linee Guida AgID.

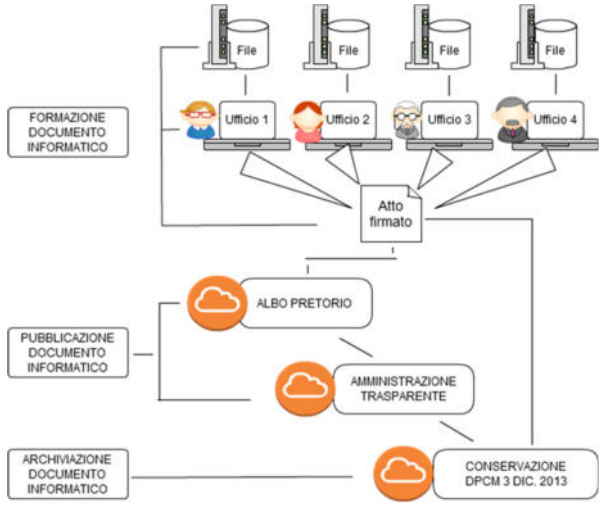
In outsourcing – i documenti vengono conservati da soggetti esterni alla struttura organizzativa. Le PA che affidano a terzi la conservazione hanno l'obbligo di rivolgersi a conservatori qualificati da AgID.

Qual è la differenza tra archiviazione e conservazione?

Con **archiviazione documentale** si fa riferimento alla memorizzazione di un documento (digitale dall'origine o scansionato) su un supporto idoneo (es. Sistema Documentale, CD).

Con **conservazione digitale** si intende la sostituzione della conservazione su carta con quella digitale anche per documenti cartacei all'origine.

Il processo di conservazione quindi è successivo all'eventuale archiviazione, infatti solo a seguito della procedura di conservazione digitale è possibile liberarsi della copia cartacea.



Quali sono i vantaggi e i benefici?

Efficienza gestionale	**Riduzione** (tempi e costi)
• rapidità nel reperimento dei documenti e delle informazioni in esso contenute; • efficienza dell'organizzazione in termini di modernità organizzativa e gestionale, rapidità e disponibilità; • maggiore controllo dei processi documentali.	• costi (diretti ed indiretti) sui processi operativi; • spazi dedicati all'archivio dei documenti; • tempo dedicato alla gestione, con recupero di personale ed attività produttive; • tempi di svolgimento delle attività relative ai documenti; • impatto organizzativo delle visite ispettive da parte degli organi competenti. • Ecologico: nessuna stampa, risparmio di carta e toner, risparmio energetico.

Capitolo terzo

Le piattaforme abilitanti

3.1 Piattaforme abilitanti

Le piattaforme abilitanti sono soluzioni che offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa[128].

Le Piattaforme attraverso i loro strumenti consentono di ridurre il carico di lavoro delle pubbliche amministrazioni, sollevandole dalla necessità di dover realizzare ex novo funzionalità, riducendo i tempi e i costi di attuazione dei servizi, garantendo maggiore sicurezza informatica ed alleggerendo la gestione dei servizi della pubblica amministrazione. Si tratta quindi di piattaforme tecnologiche che nascono per supportare la razionalizzazione dei processi di *back-office* della PA, al fine di migliorare l'efficienza e generare risparmi economici, per favorire la semplificazione e la riduzione degli oneri amministrativi a carico di imprese, professionisti e cittadini, nonché per stimolare la creazione di nuovi servizi digitali.

Infine, il concetto di piattaforma cui fa riferimento il Piano Triennale per l'Informatica della P.A. comprende non solo piattaforme abilitanti a livello nazionale e di aggregazione territoriale, ma anche piattaforme che possono essere utili per più tipologie di amministrazioni o piattaforme che raccolgono e

[128] https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/capitolo-3-piattaforme/obiettivi-e-risultati-attesi-2.html

riconciliano i servizi delle amministrazioni su differenti livelli di competenza. È il caso, ad esempio, delle piattaforme di intermediazione tecnologica sui pagamenti disponibili sui territori regionali che si raccordano con il nodo nazionale pagoPA.

Il documento originale NON si identifica in quello cartaceo, MA è informatico. Questo comportamento dev'essere rispettato per *alfabetizzazione cittadini e dipendenti alle competenze di «informatica giuridica»* in armonia con le disposizioni previste sia negli artt:

Art. 23-ter. Documenti amministrativi informatici - CAD

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

Art. 8. Alfabetizzazione informatica dei cittadini- CAD

1. Lo Stato e i soggetti di cui all'articolo 2, comma 2, promuovono iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo.[129]

[129] DECRETO LEGISLATIVO 13 dicembre 2017, n. 217 Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.

Il Piano 2020-2022 e il successivo Piano 2021-2023 promuovono l'avvio di nuove piattaforme che consentono di razionalizzare i servizi per le amministrazioni ed i cittadini.

Perché abilitanti?

Perché rendono disponibili alla cittadinanza digitale tutti gli strumenti e sistemi che abilitano e/o semplificano il rapporto fra cittadini e imprese con la Pubblica Amministrazione, ma anche perché abilitano la PA all'operatività richiesta dal Codice dell'Amministrazione Digitale.[130] [131]

Alcune piattaforme, infatti, hanno come destinatari i cittadini e le imprese (identità digitale SPID, pagamenti informatici e fatturazione elettronica, per esempio), altre sono rivolte in via principale alla PA, ma sono ugualmente "abilitanti", come nel caso dell'Anagrafe Nazionale della Popolazione Residente (ANPR).

Secondo il Decreto Semplificazioni (decreto legge n. 76/2020), entro il 28 febbraio 2021 tutte le amministrazioni locali e centrali, gli enti pubblici e le agenzie dovevano:

- integrare nei propri sistemi informativi SPID (Sistema Pubblico di Identità Digitale) e CIE (Carta d'Identità Elettronica) come unico sistema di identificazione per l'accesso ai servizi digitali;
- integrare la piattaforma pagoPA nei sistemi di incasso per la riscossione delle proprie entrate;
- avviare i progetti di trasformazione digitale necessari per rendere disponibili i propri servizi sull'App IO.[132]

[130] Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni, su docs.italia.it. URL consultato il 24 luglio 2020.
[131] Art. 64. Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni, su docs.italia.it.
[132] https://innovazione.gov.it/dipartimento/focus/linee-guida-decreto-semplificazione/

3.2 Sistema Pubblico d'Identità Digitale (SPID)

Riferimento normativo: art. 64 Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82);

SPID, il Sistema Pubblico di Identità Digitale, permette di accedere ai servizi online della Pubblica Amministrazione con un'unica coppia utente/password. Un sistema di credenziali a cui si aggiunge anche una password temporanea da generare al momento via app o da ricevere via sms (cosiddetto OTP), per entrare nei siti (o app) delle diverse amministrazioni pubbliche. Sino ad oggi si era costretti ad attivare un account per ciascuna amministrazione (cosa che richiede di solito un passaggio di persona a uno sportello fisico).

Presentato come "la password pigliatutto", obiettivo di SPID è quello di favorire l'offerta di servizi online per cittadini e persone giuridiche da parte di imprese e Pubbliche Amministrazioni. Viene gestito dall'Agenzia per l'Italia Digitale (AgID) con il coordinamento del Dipartimento per la Trasformazione digitale.[133] [134]

SPID ha lo stesso valore di un qualsiasi documento d'identità nello svolgimento di pratiche amministrative online: non sarà più necessario allegare fotocopie di documenti di identità.

Per il cittadino

- è un sistema di accesso semplice e sicuro ai servizi digitali.
- Il processo di identificazione è assicurato da protocolli stabiliti da AgID a cui i gestori di identità devono aderire rispettando la privacy.

[133] https://www.spid.gov.it/
[134] https://www.agid.gov.it/it/piattaforme/spid

- I dati personali comunicati non possono essere utilizzati per scopi commerciali e non possono essere utilizzati e ceduti a terze parti senza l'autorizzazione dell'utente.
- Con SPID gli italiani possono accedere anche ai servizi europei dei Paesi membri.

Per le pubbliche amministrazioni

- è una piattaforma di semplificazione tecnologica che consente di ridurre i costi di gestione legati a sistemi di identificazione gestiti autonomamente, offrendo ai cittadini un servizio omogeneo su tutto il territorio nazionale;
- ha elevati standard di sicurezza e identificazione sia in fase di autenticazione che di accesso ai servizi;
- si basa su un solido schema architetturale che rispetta degli standard di design e di sicurezza garantiti dai gestori di identità (identity provider) che sono soggetti accreditati da AgID e da essa vigilati.
- L'accesso ai servizi, inoltre, può avvenire scegliendo fino a tre livelli progressivi di sicurezza.

3.3 Carta d'Identità Elettronica (CIE) e Carta Nazionale dei Servizi (CNS)

Riferimento normativo: art. 66 Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82)

Carta d'Identità Elettronica (CIE)

La carta d'identità elettronica italiana, emessa dal Ministero dell'Interno, è un documento di riconoscimento previsto in Italia che ha sostituito la carta d'identità in formato cartaceo nella Repubblica Italiana.[135] [136]

[135] https://www.cartaidentita.interno.gov.it/
[136] https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi

L'introduzione della CIE è volta a incrementare i livelli di sicurezza mediante l'adeguamento delle caratteristiche del supporto agli standard internazionali di sicurezza e a quelli anticlonazione e anticontraffazione in materia di documenti elettronica.

La crescita del numero di CIE è fisiologica per il progressivo scadere delle carte di identità cartacee, che andranno sostituite con le CIE. Il Decreto Semplificazioni 2020 permette ora di richiedere la sostituzione della carta di identità cartacea anche prima della scadenza naturale. Entro il 2026 tutti dovremmo avere sostituito la carta di identità cartacea con quella elettronica e di conseguenza Istituto Poligrafico e Zecca dello Stato, con il Ministero dell'Interno, si sta muovendo massicciamente per la sua adozione.

Per il cittadino

- una chiave di accesso ai servizi online pubblici e privati aderenti, da qualsiasi dispositivo: computer, tablet e smartphone.
- un'unica identità digitale valida in tutta Europa;
- uno strumento di verifica dell'identità del cittadino protetto dai tentativi di contraffazione;
- un accesso veloce ai servizi online (es.: CIE come badge identificativo). CIE garantisce un sistema di accesso semplice e sicuro in tutti gli scenari di utilizzo. È lo Stato italiano che certifica e garantisce l'identità del possessore dalla CIE e grazie ad elevate soluzioni di sicurezza, i dati contenuti nel documento sono inalterabili e protetti.

Per le pubbliche amministrazioni

- è lo strumento di identità digitale rilasciato dal Ministero dell'Interno che consente di ridurre i costi di gestione legati a sistemi di identificazione gestiti autonomamente.

- Con la CIE è possibile accedere ai servizi online della pubblica amministrazione (e non solo) in condizioni di massima sicurezza, in quanto conforme al "livello di garanzia elevato", il più alto previsto dal Regolamento eIDAS (Reg. UE 910/2014) che definisce le norme in materia di strumenti di identificazione digitale rilasciati dagli Stati dell'UE.
- La CIE, come documento di identità, permette di verificare con certezza l'autenticità del documento e l'identità del titolare durante svolgimento di procedure amministrative presso uffici pubblici (ad es. per il rilascio di certificati e documenti).
- L'app IDEA (Identity Easy Access), scaricabile gratuitamente per i dispositivi Android e presto disponibile anche per iOS, consente di leggere e visualizzare i dati contenuti nel microprocessore della CIE, compresa la foto del titolare, e verificarne l'autenticità rafforzando così a tutti i livelli, l'azione di contrasto ai fenomeni di contraffazione e furto di identità.

La CIE permette di avere anche una firma elettronica avanzata (FEA) (art. 61 DPCM del 22 febbraio 2013). La carta può essere utilizzata per firmare atti e documenti della pubblica amministrazione, costituendo una funzionalità abilitante per lo sviluppo dei servizi collegati all'identità dei cittadini.[137]

Carta Nazionale dei Servizi (CNS)

La Carta Nazionale dei Servizi (CNS) equivale alla tessera sanitaria di ultima generazione, rilasciata con il chip sul fronte della scheda, denominata anche TS-CNS (o TS-CRS).

[137] https://innovazione.gov.it/dipartimento/focus/linee-guida-decreto-semplificazione/

Tale carta consente l'accesso ai servizi che richiedono la Carta Nazionale dei Servizi per l'autenticazione, non dovendo quindi accreditarsi con le tradizionali username e password. I titolari di partita IVA che si iscrivono alla Camera di commercio possono richiedere una diversa tipologia di CNS, identica sotto il profilo tecnico a quella per i privati cittadini ma utilizzabile per la gestione di pratiche sulla partita IVA e su altri servizi a questa riservati.

Su entrambe le schede è presente un chip che contiene un certificato personale, utilizzabile come metodo di autenticazione sicuro.

Per poter utilizzare la tessera sanitaria come carta CNS occorre richiedere il PIN (di 8 cifre) presso l'ASL competente territorialmente.[138] Al fine del riconoscimento dell'identità personale da parte della ASL competente sarà sufficiente indicare un documento d'identità in corso di validità, la tessera sanitaria e un indirizzo di posta elettronica (non necessariamente certificata). Terminata la fase di registrazione, lo sportello fornirà direttamente una parte del PIN e le restanti cifre del PIN verranno inviate all'indirizzo di posta elettronica indicato.[139]

3.4 PagoPA: effettuare pagamenti con modalità informatiche

Riferimenti normativi: art. 5 Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82)

[138] Inserendo in un motore di ricerca le parole chiave "CNS ASL" seguite dalla regione d'appartenenza, si ottiene un
elenco delle ASL presso cui è possibile attivare la CNS.

[139] Per riferimenti ed informazioni si rinvia alla pagina dedicata del sito web istituzionale di AgID

PagoPA[140] è la piattaforma che rende più semplice, sicuro e trasparente qualsiasi pagamento verso la Pubblica Amministrazione, configurandosi come una nuova modalità per eseguire, presso i Prestatori di Servizi di Pagamento (PSP) aderenti, i pagamenti verso gli Enti pubblici in modalità standardizzata, sia online che offline.[141]

Per il cittadino la possibilità di:

- scegliere tra molteplici canali e metodi di pagamento: direttamente sul sito o dall'app di un Ente oppure dai canali fisici e online della propria banca (es: sportelli ATM e home banking) e di altri Prestatori di Servizi di Pagamento come gli uffici postali o i punti vendita Mooney e Lottomatica, o ancora attraverso gli strumenti digitali più innovativi sul proprio smartphone nel rispetto delle normative europee (Payment Service Directives 1 e 2);
- avere la completa visibilità dei costi di commissione associati a ciascun metodo di pagamento (quindi già esistenti prima dell'adozione della piattaforma pagoPA da parte di un Ente), in totale trasparenza;
- avere sempre la certezza del debito dovuto, grazie all'attualizzazione automatica dell'importo (se l'importo varia nel tempo per interessi di mora o saldi parziali, su pagoPA viene sempre aggiornato).
- avere un'esperienza di pagamento nei confronti della PA più economica, efficiente e digitale.

Per le pubbliche amministrazioni:

[140] pagoPA è attualmente gestito dalla società PagoPA S.p.A. Il nuovo sito dedicato al progetto è raggiungibile all'indirizzo www.pagopa.gov.it
[141] https://www.pagopa.gov.it/

- di ottenere efficienza e risparmi economici mediante la gestione dei pagamenti in modo centralizzato, con un significativo risparmio nei costi di gestione;
- il controllo e il monitoraggio, in tempo reale, di tutti gli incassi avendo certezza che le somme dovute allo Stato da parte dei cittadini siano state davvero pagate ed incassate;
- la possibilità di effettuare ipotesi efficienti di politiche di spesa;
- la riduzione dei costi di incasso;
- la riduzione dei costi indiretti derivanti da una non corretta gestione dei pagamenti (pagamento in contanti, spostamenti, recupero del credito, sanzioni, etc.);
- la diminuzione dell'uso del contante a favore dei pagamenti con moneta elettronica, anche grazie a una maggiore apertura degli Enti verso il mercato bancario;
- la riconciliazione automatica del pagamento rispetto alla posizione debitoria;
- l'immediatezza.

3.5 App IO

Riferimenti normativi: articolo 64bis del Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82)

Ideato e sviluppato dal Team per la Trasformazione Digitale e oggi gestito da PagoPA S.p.A., ha l'obiettivo di facilitare l'accesso dei cittadini a tutti i servizi digitali della Pubblica Amministrazione e ai diritti che questi servizi garantiscono. La peculiarità di questo progetto è e che è un unico canale attraverso cui tutti gli Enti, locali e nazionali (Comuni,

Regioni, agenzie centrali) offrono i propri servizi al cittadino, in modo semplice e personalizzato, direttamente su smartphone.[142]

L' App IO esprime, in questo modo, una nuova visione dei servizi pubblici, completamente centrata sui bisogni dell'utente. E introduce un modo diverso di fare innovazione per e con i cittadini, seguendo dinamiche di sviluppo tipiche di una startup.

Per i cittadini permette di:

- ricevere tutti i messaggi della Pubblica Amministrazione sul proprio smartphone, personalizzati, con la possibilità di gestirli in un archivio;
- gestire i propri contatti di recapito da un unico punto, con la facoltà di scegliere in ogni documento da quali servizi farsi contattare;
- essere sempre aggiornati sulle scadenze e gestire gli avvisi in modalità "integrata" (aggiungendo i promemoria nel proprio calendario personale con un clic);
- ricevere avvisi di pagamento, con la possibilità di pagare servizi e tributi dalla app in pochi secondi;
- effettuare pagamenti verso la Pubblica Amministrazione attraverso pagoPA, in perfetta sicurezza e con diversi metodi di pagamento supportati (carte di credito, bancomat, PayPal, ecc.);
- portare sempre con sé lo storico delle operazioni e le relative ricevute di pagamento;
- ricevere e conservare documenti, ricevute, certificati direttamente nel proprio smartphone e condividerli con un ufficio pubblico in pochi clic;

[142] https://innovazione.gov.it/dipartimento/focus/linee-guida-decreto-semplificazione/#app-io

- eleggere direttamente dalla app il proprio domicilio digitale (ad esempio per ricevere le raccomandate a valore legale presso un indirizzo PEC);
- richiedere bonus e sconti, legati a iniziative o programmi specifici.
- una maggiore conoscenza dei servizi, con una riduzione drastica della burocrazia.
- Inoltre in molti casi IO permette un risparmio alla Pubblica Amministrazione, che può tradursi in un costo minore per i cittadini per la fruizione dei servizi.

Per le pubbliche amministrazioni di:

- inviare comunicazioni ai cittadini tramite messaggi di notifica in app, semplicemente conoscendo il loro codice fiscale (senza dover chiedere un indirizzo di contatto);
- comunicare e gestire le scadenze e ricevere pagamenti elettronici con maggiore facilità;
- inviare, ottenere e gestire documenti (atti, notifiche, certificati) in modo semplice e efficiente;
- gestire le preferenze di ogni cittadino in modo centralizzato;
- ridurre i costi di gestione (delle notifiche, dei pagamenti, ecc.);
- facilitare i pagamenti e ridurre i costi di recupero dei crediti.[143]

3.6 Istanze e dichiarazioni telematiche

Riferimenti normativi: art. 65 Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82)

[143] https://innovazione.gov.it/progetti/app-io-cittadinanza-digitale/

La presentazione di istanze e dichiarazioni per via telematica, sono considerate valide dalle amministrazioni riceventi ed equivalenti a quelle sottoscritte con firma autografa apposta innanzi all'addetto al procedimento, se rispettano uno dei seguenti requisiti:

- sono sottoscritte con firma digitale;
- il richiedente o il dichiarante sono identificati con il Sistema Pubblico di Identità Digitale (SPID) o con la carta d'identità elettronica (CIE) o la con la carta nazionale dei servizi (CNS);
- sono formate tramite il punto di accesso telematico[144] per i dispositivi mobili **App IO**;
- sono sottoscritte e presentate insieme alla copia del documento d'identità;
- con invio telematico dal domicilio digitale dell'istante o del dichiarante.

Le persone fisiche possono altresì eleggere il domicilio digitale[145] avvalendosi dell'applicazione mobile IO.

Per quanto riguarda le comunicazioni (presentazione di istanze, di dichiarazioni, di dati e lo scambio di informazioni e documenti, anche a fini statistici) tra le imprese e le amministrazioni pubbliche si fa presente che le stesse avvengono esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione.

Sempre con le modalità telematiche le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.

[144] Decreto Legislativo 7 marzo 2005, n.82 s.m.i., art. 64-bis, funzione prevista dal CAD e al momento non attiva.
[145] Decreto Legislativo 7 marzo 2005, n.82 s.m.i., art.3-bis, comma 1-ter.

Le comunicazioni tramite i domicili digitali sono effettuate agli indirizzi PEC inseriti negli elenchi previsti dal CAD (INI-PEC e iPA).

Qualora l'amministrazione destinataria dell'istanza o della dichiarazione telematica formata in base all'art. 65 del CAD non la ritenga valida[146], è possibile inviare una segnalazione al Difensore Civico Digitale.

3.7 Anagrafe Nazionale della Popolazione Residente (ANPR)

L'Anagrafe Nazionale della Popolazione Residente (ANPR) è il progetto di anagrafe unica a livello nazionale che raccoglie i dati e i servizi demografici degli italiani nella quale sono confluite le anagrafi comunali ed è istituita presso il Ministero dell'Interno. Oltre ad evitare duplicazioni nelle informazioni, grazie ad ANPR i cittadini possono verificare e modificare facilmente i propri dati demografici e fruire dei servizi anagrafici in un unico luogo, indipendentemente dal comune di residenza.

Collegandosi alla piattaforma del Ministero dell'Interno[147] si possono consultare e rettificare i dati anagrafici, richiedere certificati, e formulare richieste di rettifica e dal 1febbraio 2022 è attivo il servizio per il cambio di residenza o dimora.

Si possono scaricare i seguenti 14 certificati per proprio conto o per un componente della propria famiglia, dal proprio computer senza bisogno di recarsi allo sportello:

- Anagrafico di nascita
- Anagrafico di matrimonio
- di Cittadinanza

[146] Decreto Legislativo 7 marzo 2005, n.82, art. 65, comma 1-ter.
[147] https://www.anagrafenazionale.interno.it/

- di Esistenza in vita
- di Residenza
- di Residenza AIRE
- di Stato civile
- di Stato di famiglia
- di Residenza in convivenza
- di Stato di famiglia AIRE
- di Stato di famiglia con rapporti di parentela
- di Stato Libero
- Anagrafico di Unione Civile
- di Contratto di Convivenza.

Per i certificati digitali non si dovrà pagare il bollo e saranno quindi gratuiti (e disponibili in modalità multilingua per i comuni con plurilinguismo). Potranno essere rilasciati anche in forma contestuale (ad esempio cittadinanza, esistenza in vita e residenza potranno essere richiesti in un unico certificato). Attraverso ANPR si possono raggiungere i seguenti obiettivi:

- attuare la circolarità anagrafica, tramite la fruizione dei dati presenti in ANPR da parte delle amministrazioni pubbliche, i gestori dei servizi pubblici e le società a controllo pubblico che hanno diritto di accesso ai dati ANPR;
- rendere disponibile un servizio di accesso ai propri dati anagrafici (visura anagrafica) a tutti i cittadini;
- rendere disponibili servizi digitali per la certificazione anagrafica per tutti i cittadini.

3.8 Il cassetto digitale dell'imprenditore

Il "**cassetto digitale dell'imprenditore**" è il servizio offerto dalle Camere di commercio ai cittadini imprenditori per accedere ai documenti ufficiali della propria impresa.

Impresa.italia.it mette a disposizione di ogni titolare e legale rappresentante visure, bilanci, fascicolo d'impresa ed altri documenti ufficiali del Registro imprese certificati dalle Camere di commercio. Il servizio permette di controllare anche lo stato delle pratiche presentate a 3.500 Sportelli Unici delle attività produttive e di entrare in contatto con le start-up e PMI innovative italiane. Si accede in modo facile, sicuro e veloce con le credenziali SPID o con la Carta Nazionale dei Servizi (CNS) da qualsiasi dispositivo: pc, smartphone e tablet.

3.9 Piattaforma Notifiche Digitali (PND)

La Piattaforma, istituita dal legislatore nel 2019, è pensata per semplificare le notifiche digitali sia per le amministrazioni (che potranno servirsi di un servizio reso da PagoPA) sia per cittadini e imprese (che potranno ricevere notifiche e comunicazioni in modo più semplice e affidabile). Con l'entrata in vigore dal 21 giugno 2022 del regolamento[148] che ne stabilisce il funzionamento, si compie un passo avanti decisivo per la realizzazione della Piattaforma notifiche della Pa.

[148] Decreto 8 febbraio 2022, n. 58, del ministro per l'innovazione tecnologica e la transizione digitale, pubblicato sulla Gazzetta ufficiale n. 130 del 6 giugno

Per i destinatari sprovvisti di recapiti digitali con certificato idoneo, il gestore invierà una raccomandata con avviso di ricevimento. In caso di indirizzo inesistente saranno svolti accertamenti per individuare un recapito alternativo. In ultima battuta, l'addetto al recapito postale depositerà l'avviso di avvenuta ricezione sulla Piattaforma e lo renderà così disponibile al destinatario.

Capitolo quarto

La trasparenza amministrativa e i diritti di accesso[149]

4.1 La trasparenza amministrativa

La trasparenza dell'azione amministrativa rappresenta un'esigenza fondamentale degli ordinamenti democratici e rende possibile la partecipazione dei governati all'esercizio del potere pubblico da parte dei governanti.

Questa nozione di trasparenza evoca la nota immagine, cara a Filippo Turati, della Pubblica Amministrazione "casa di vetro", all'interno della quale, tutto è sempre e costantemente visibile.

«E' solo dagli anni 90 che il legislatore ha cominciato a fare della trasparenza lo strumento per superare le disuguaglianze nella conoscenza (asimmetrie informative) facendo proprio della conoscenza (resa possibile dalla trasparenza) un importante strumento di riequilibrio delle disuguaglianze» (D. Donati).

[149] Capitolo tratto dal libro Carrisi R. "*Bilanciamento tra trasparenza amministrativa e privacy nella Pubblica Amministrazione*", 2020 I edizione – pagg 9-29

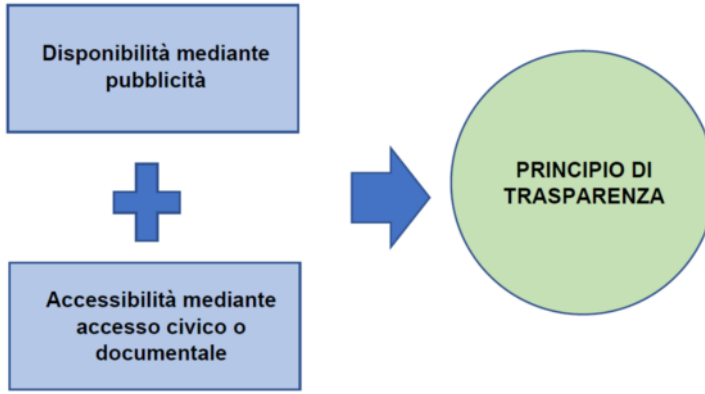
"Gli ultimi anni hanno inciso in modo particolarmente significativo sulla legislazione in materia di trasparenza: in particolare il d.lgs. 97/2016, noto come FOIA, ha introdotto con prepotenza nel nostro ordinamento una rinnovata concezione di trasparenza nella pubblica amministrazione, imponendo agli enti non soltanto precisi obblighi di pubblicazione, ma anche delle novellate tipologie di accessibilità, anche informativa, la cui omissione o il cui non corretto adempimento sono significativamente tutelati da responsabilità e conseguenti sanzioni."[150]

Nelle inevitabili difficoltà operative che quotidianamente si palesano agli operatori delle pubbliche amministrazioni proprio a causa dello scontro tra la trasparenza e la privacy, questo lavoro analizzerà non solo le sentenze più rilevanti della magistratura amministrativa ma soprattutto i provvedimenti del Garante per la protezione dei dati personali.

Si è passati da un accesso documentale o procedimentale, di cui alla legge n. 241/1990, esercitabile dagli individui che vantano una posizione soggettiva giuridicamente rilevante e che presentano un interesse diretto, concreto e attuale; al decreto legislativo n. 33/2013 (decreto trasparenza), che ha introdotto un accesso civico di portata generale, previsto all'art. 5, il quale esplica la trasparenza in funzione di una "accessibilità totale" alle informazioni per le quali è prevista la pubblicazione, senza la necessaria sussistenza dei suddetti requisiti.

L'innovazione radicale ha però riguardato l'introduzione nel nostro ordinamento dell'accesso civico generalizzato, disciplinato dal d. lgs. n. 97/2016, che modifica il decreto trasparenza, equivalente al FOIA. Tale tipo di accesso consente a chiunque di accedere a tutti i dati e ai documenti detenuti dalle amministrazioni con i soli, ovvi, limiti legali.

[150] Tessaro T. – Bertin M., *Come cambia la trasparenza amministrativa dopo il GDPR e il nuovo Decreto Privacy*, Santarcangelo di Romagna, Maggioli, 2019



In sintesi gli strumenti della trasparenza amministrativa sono:

Trasparenza proattiva	Realizzata grazie alla pubblicazione sui siti istituzionali dei documenti, informazioni e dati indicati dalla legge • **Obblighi di pubblicazione** → d.lgs. 33/2013 modificato dal d.lgs. 97/2016
Trasparenza reattiva	In risposta alle istanze di conoscenza avanzata dagli interessati. • **Diritto di accesso agli atti** → legge 241/91 • **Diritto accesso civico semplice** → d.lgs. 33/2013 • **Diritto accesso civico generalizzato** → d.lgs. 33/2013
Trasparenza attiva	Collegamento tra trasparenza e apertura • **Open data** → d.lgs. 82/2005 e d.lgs. 33/2013 modificato dal d.lgs. 97/2016

4.2 La legge 241/1990

La legge 7 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" ha disciplinato due istituti giuridici intesi ad ampliare l'ambito dei poteri attribuiti al cittadino nei confronti della pubblica amministrazione.

Il primo è quello di partecipazione al procedimento amministrativo, diretto a tutelare i soggetti "nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti" e "quelli che per legge debbono intervenirvi": soggetti cioè caratterizzati dalla titolarità di una situazione giuridicamente differenziata, che, tra l'altro, li abilita ad agire in via giurisdizionale. In questo ambito, l'art. 10 della legge prevede "di prendere visione degli atti del provvedimento, salvo quanto previsto dall'articolo 24 (Esclusione dal diritto di accesso[151])".[152]

Il secondo istituto è quello del diritto di accesso ai documenti amministrativi come "*il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi*" (art. 22, comma 1, lett. a)) diretto in modo indifferenziato nei confronti di "chiunque vi abbia interesse", in quanto finalizzato ad assicurare la trasparenza dell'attività amministrativa e favorirne lo svolgimento imparziale, ferme, tuttavia, le ragioni di riservatezza e tutela dei terzi, tra cui le imprese, le quali incontrano, però, un limite nella necessità

[151] Legge 241/1990 - Art. 24 – Comma 6 lettera d) "*quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorchè i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono*"

[152] Tessaro T. – Bertin M., *Come cambia la trasparenza amministrativa dopo il GDPR e il nuovo Decreto Privacy*, Santarcangelo di Romagna, Maggioli, 2019 – Pag. 28-29

assoluta di ordine costituzionale di garantire agli interessati di prendere "visione degli atti relativi ai procedimenti amministrativi, la cui conoscenza sia necessaria per curare o per difendere i loro interessi giuridici".

L'accesso ai documenti amministrativi disciplinato dalla legge 241/1990 è condizionato dalla titolarità in capo all'istante, di "*un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso*" (art. 22, comma 1), essendo espressamente escluso che il suo esercizio possa avvenire per finalità di mero "controllo generalizzato dell'operato delle pubbliche amministrazioni" (art. 24, comma 3). Le condizioni affinché la richiesta di accesso sia accolta consistono nell'esistenza di un interesse giuridicamente rilevante che qualifiche e supporti la domanda.

Pertanto i documenti amministrativi possono essere oggetto di accesso solamente a favore di chi sia detentore, potendolo dimostrare, di una posizione giuridica qualificata e differenziata.[153]

In altri termini, una volta che il richiedente dimostri di essere portatore di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento del quale è chiesto l'accesso, la pubblica amministrazione deve limitarsi, al massimo, ad un esame oggettivo dell'istanza, ma non può né deve condizionare l'esibizione alla dimostrazione della pendenza di un giudizio, né, qualora ciò sia, ipotizzarne l'esito o valutare l'utilità o l'efficacia del documento richiesto ai fini dell'accoglimento delle ragioni dell'istante.[154]

---

[153] Cons. Stato, sez. III, 12 marzo 2018, n. 1578 e sez. IV, 19 ottobre 2017, n. 4838
[154] Tessaro T. – Bertin M., *Come cambia la trasparenza amministrativa dopo il GDPR e il nuovo Decreto Privacy*, Santarcangelo di Romagna, Maggioli, 2019 – Pag. 31-33

In questo, molto chiaramente, la giurisprudenza ha affermato che "*Il diritto di accesso agli atti della pubblica amministrazione, a prescindere dalla necessità dei suddetti atti per la predisposizione del ricorso giurisdizionale, non costituisce una pretesa meramente strumentale alla difesa in giudizio della situazione sottostante, essendo in realtà diretto al conseguimento di un autonomo bene della vita… In altri termini, non spetta a chi riceve l'istanza di accesso ai documenti amministrativi valutare l'utilità ai fini difensivi degli atti di cui si richiede l'accesso*".[155]

4.3 La pubblicità per finalità di trasparenza

Il D.Lgs. 33/2013

Con il d. lgs. 14 marzo 2013 n. 33 intitolato "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*" il legislatore – in attuazione della delega contenuta nella legge 6 novembre 2012, n. 190, recante: "*Disposizioni per la prevenzione e la repressione della*

[155] TAR Campania, Napoli, sez. VI, 13 giugno 2018, n. 3961

corruzione e dell'illegalità nella pubblica amministrazione" (art. 1, commi 35 e 36) – ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzione di dati, informazioni, atti e documenti sui siti web istituzionali dei soggetti obbligati.

A tal fine la trasparenza è definita come "*l'accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*" (art. 1, comma 1). Inoltre è precisato che oggetto del decreto è l'individuazione degli obblighi di trasparenza *"concernenti l'organizzazione e l'attività delle pubbliche amministrazioni"* e che "*tutti i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7"* (art. 2, comma 1, e art. 3).[156]

La tipologia dei predetti obblighi di pubblicazione per finalità di trasparenza concernenti l'organizzazione e l'attività delle pubbliche amministrazioni è schematicamente riassunta nell'allegato al d.lgs. n. 33/2013 che individua la "struttura delle informazioni sui siti istituzionali" e che precisa come la sezione dei siti istituzionali denominata "*Amministrazione trasparente*" deve essere organizzata in sotto-sezioni all'interno delle quali devono essere inseriti i documenti, le informazioni e i dati previsti dal decreto (art. 48 e allegato al d.lgs.).

[156] Garante per la protezione dei dati personali, "*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*" (Pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014) – pag. 25

I principi e la disciplina di protezione dei dati personali[157] – come peraltro previsto anche dagli artt. 1, comma 2, e 4 del d. lgs. n. 33/2013 – devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.

La diffusione dei dati personali da parte di soggetti pubblici è ammessa unicamente quando la stessa è prevista da una specifica legge o da regolamento. Pertanto le P.A. prima di mettere a disposizione sui siti web istituzionali atti o documenti che contengono dati personali devono verificare che la normativa in materia di trasparenza preceda tale obbligo. Laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione è necessario selezionare i dati personali da inserire in tali atti o documenti da pubblicare, verificando caso per caso se ricorrono i presupposti per l'oscuramento di determinate informazioni. Infatti l'art. 4, comma 4, del d. lgs. n. 33/2013 ricorda di "*rendere […] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione"*, nel rispetto del principio di "minimizzazione dei dati" previsto dall'art. 5 del Reg. UE 679/2016.[158] E' invece sempre vietata la diffusione dei dati personali idonei a rivelare lo "stato di salute" e la "vita sessuale" (art. 4, comma 6, del d.lgs. n. 33/2013).

---

[157] «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, comma 1 Reg. UE 679/2016)

[158] L'art. 5 Reg. UE 679/2016 comma 1 recita *"I dati personali sono: […] c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); […*]"

L'accesso civico semplice

L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.

Tanto che si parla del diritto di accesso civico connesso agli obblighi di pubblicazione come di un *diritto di diffida* nei confronti delle PA inadempienti.[159]

Il diritto di accesso civico che può essere esercitato, anche telematicamente, in forma gratuita e senza necessità di particolare motivazione, con riferimento ai dati oggetto di pubblicazione obbligatoria, costituisce forse una delle più importanti innovazioni delle norme in materia in quanto ha dotato la società civile di uno strumento forte di controllo e di stimolo alla trasparenza nella gestione e amministrazione della cosa pubblica.

L'istanza va indirizzata al **responsabile della prevenzione della corruzione e della trasparenza dell'ente (RPCT),** in base al c.1 dell'art. 5 del 33/2013. Il RPCT deve rispondere, motivatamente, entro 30 giorni, pubblicando i dati

[159] Cfr. Decreto legislativo n. 33 del 2013, art 46 Responsabilità derivante dalla violazione delle disposizioni in materia di obblighi di pubblicazione e di accesso civico *"1. L'inadempimento degli obblighi di pubblicazione previsti dalla normativa vigente e il rifiuto, il differimento e la limitazione dell'accesso civico, al di fuori delle ipotesi previste dall'articolo 5-bis) costituiscono elemento di valutazione della responsabilità dirigenziale, eventuale causa di responsabilità per danno all'immagine dell'amministrazione e sono comunque valutati ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili. 2. Il responsabile non risponde dell'inadempimento degli obblighi di cui al comma 1 se prova che tale inadempimento è dipeso da causa a lui non imputabile."*

mancanti o incompleti e indicando al richiedente il collegamento ipertestuale nella sezione «Amministrazione trasparente.»[160]

4.4 Accesso civico generalizzato

La normativa sull'accesso civico generalizzato, contenuta nel decreto legislativo 14 marzo 2013, n. 33 come modificato dal decreto legislativo 25 maggio 2016, n. 97 e nota come **FOIA (Freedom of Information Act)**, garantisce a chiunque il diritto di accedere ai dati e ai documenti posseduti dalle pubbliche amministrazioni, con il limite degli interessi pubblici o privati indicati dalla legge.[161]

Giornalisti, organizzazioni non governative, imprese, cittadini italiani e stranieri possono richiedere dati e documenti, così da svolgere un ruolo attivo di controllo sulle attività delle pubbliche amministrazioni. L'obiettivo del FOIA è anche favorire una maggiore trasparenza nel rapporto tra le istituzioni e la società civile e incoraggiare un dibattito pubblico informato su temi di interesse collettivo.

L'accesso civico generalizzato differisce dalle altre due principali tipologie di accesso già previste dalla legislazione.

A differenza del diritto di accesso procedimentale o documentale, che in base agli artt. 22 e seguenti della legge n. 241/1990 tutela soltanto il richiedente con un interesse diretto, concreto e attuale, l'accesso civico generalizzato garantisce al cittadino la possibilità di richiedere dati e documenti alle

[160] Cfr. Decreto legislativo n. 33 del 2013, Art. 5. Accesso civico a dati e documenti, comma 1 *"L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione".*

[161] Fonte FOIA - Centro di competenza nazionale – Dipartimento della Funzione Pubblica, www.foia.gov.it

pubbliche amministrazioni senza dover dimostrare di possedere un interesse qualificato.

A differenza, invece, del diritto di accesso civico "semplice", che in base all'art. 5, co. 1 del decreto legislativo n. 33/2013 (c.d. Decreto trasparenza), consente di accedere esclusivamente alle informazioni che rientrano negli obblighi di pubblicazione previsti dal Decreto trasparenza, l'accesso civico generalizzato si estende a tutti i dati e i documenti in possesso delle pubbliche amministrazioni, con il solo limite degli interessi pubblici e privati indicati dalla legge.

E' stata adottata dal Ministro per la Pubblica Amministrazione la circolare n. 1/2019 sulla "**Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)",** con l'obiettivo di fornire indirizzi e chiarimenti alle amministrazioni sugli aspetti organizzativi, procedimentali e tecnologici connessi ad una efficiente gestione del FOIA.

Inoltre la Circolare n. 2/2017 del Ministro per la semplificazione e la pubblica amministrazione contiene raccomandazioni operative per l'attuazione della disciplina dell'accesso civico generalizzato. La Circolare, adottata dal Dipartimento della funzione pubblica nell'esercizio della sua funzione generale di "coordinamento delle iniziative di riordino della pubblica amministrazione e di organizzazione dei relativi servizi" (art. 27, n. 3, legge n. 93 del 1983), è rivolta a tutte le pubbliche amministrazioni.

Infine in materia di accesso civico generalizzato, l'Autorità nazionale anticorruzione (A.N.AC.) ha adottato, d'intesa con il Garante per la protezione dei dati personali, le linee guida recanti indicazioni operative per l'applicazione delle

esclusioni e dei limiti all'accesso civico generalizzato (delibera n. 1309 del 28 dicembre 2016).[162]

Al fine di stabilire quando è necessario rifiutare l'accesso generalizzato per evitare un pregiudizio concreto alla protezione dei dati personali, le pubbliche amministrazioni possono richiedere un parere al Garante per la protezione dei dati personali (art. 5, comma 7, d.lgs. n. 33 del 2013).

4.5 Accesso ai dati personali (privacy)

Uno dei fondamentali diritti dell'interessato garantiti dal **Regolamento generale sulla protezione dei dati (RGPD o GDPR)[163]** è sicuramente il diritto di accesso che viene disciplinato dall'art. 15 laddove viene sancito che l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso ai dati e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

[162] Autorità Nazionale Anticorruzione , *"Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co.2 del d. lgs. n. 33/2013"* (determinazione n. 1309 del 28/12/2016), disponibile sul sito www.anticorruzione.it

[163] REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo ad un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il titolare del trattamento deve fornire all'interessato le informazioni relative all'azione intrapresa riguardo ad una richiesta di accesso, ai sensi degli articoli da 15 a 20, senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato per un massimo di altri due mesi, se necessario, tenuto conto della complessità della richiesta e del numero di richieste.

Qualora si applichi la proroga, l'interessato è informato dei motivi del ritardo entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta in formato elettronico, le informazioni sono fornite, ove possibile, in formato elettronico, salvo indicazione diversa dell'interessato.

Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi

dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.[164]

Fig 1: Riepilogo dei tipi di accesso

Caratteristiche	Accesso L. 241	Accesso Civico	Accesso privacy
Chi	Soggetti privati	Chiunque (pubblico o privato)	La persona a cui si riferiscono i dati
Che cosa	Documenti amministrativi	Documenti e dati	Dati personali
Motivazione	Necessaria – tutela interesse diretto concreto e attuale corrispondente a situazione giuridicamente tutelata	Non necessaria	Non necessaria
Tutela	Ricorso o al TAR difensore civico o Commissione per l'accesso	Riesame responsabile per la trasparenza o ricorso al difensore civico/TAR	Reclamo al Garante per la Protezione dei dati personali

[164] M. IASELLI, *Privacy: i diritti dell'interessato nell'ottica del GDPR*, articolo pubblicato sulla rivista online www.altalex.it in data 16/11/2017

4.6 Pubblicità per altre finalità nella Pubblica Amministrazione

Accanto agli obblighi di pubblicazione per finalità di trasparenza permangono altri obblighi di pubblicità online di dati, informazioni e documenti della p.a. – contenuti in specifiche disposizioni di settore diverse da quelle approvate in materia di trasparenza – come, fra l'altro, quelli volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (es.: pubblicità integrativa dell'efficacia, dichiarativa, notizia). Si pensi, a titolo meramente esemplificativo, alle pubblicazioni ufficiali dello Stato, alle pubblicazioni di deliberazioni, ordinanze e determinazioni sull'albo pretorio online degli enti locali (oppure su analoghi albi di altri enti, come ad esempio le Asl), alle pubblicazioni matrimoniali, alla pubblicazione degli atti concernenti il cambiamento del nome, alla pubblicazione della comunicazione di avviso deposito delle cartelle esattoriali a persone irreperibili, ai casi di pubblicazione dei ruoli annuali tributari dei consorzi di bonifica, alla pubblicazione dell'elenco dei giudici popolari di corte d'assise, etc..

In tutti i casi, indipendentemente dalla finalità perseguita, laddove la pubblicazione online di dati, informazioni e documenti, comporti un trattamento di dati personali, devono essere opportunamente contemperate le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali, nonché la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

In tale quadro, è opportuno evidenziare che le decisioni, assunte dalle amministrazioni pubbliche o dagli altri soggetti onerati, in ordine all'attuazione degli obblighi di pubblicità sui siti web istituzionali di informazioni, atti e documenti contenenti

dati personali sono oggetto di valutazione da parte del Garante al fine di verificare che siano rispettati i principi in materia di protezione dei dati personali.[165]

4.7 Albo pretorio on line

Per Albo Pretorio si intende il luogo e lo spazio dove vengono affissi tutti quegli atti per i quali la legge impone la pubblicazione in quanto debbono essere portati a conoscenza del pubblico, come condizione necessaria per acquisire efficacia e quindi produrre gli effetti previsti. L'attività dell'albo pretorio consiste quindi, nella pubblicazione di tutti quegli atti sui quali viene apposto il "referto di pubblicazione":

- deliberazioni, ordinanze, determinazioni, avvisi, manifesti, gare, concorsi e altri atti del Comune e di altri enti pubblici, che devono essere portati a conoscenza del pubblico come atti emessi dalla pubblica amministrazione;
- avvisi di deposito alla casa comunale di atti finanziari e delle cartelle esattoriali;
- provvedimenti tipo piani urbanistici, del commercio, del traffico, ecc. ecc.
- particolari atti riguardanti privati cittadini, come il cambio di nome e/o cognome.

Nel referto di pubblicazione viene indicato l'avviso di pubblicazione e di deposito dell'atto, con l'indicazione di chi l'ha emesso o adottato, l'oggetto, la data, il numero e la

---

[165] Garante per la protezione dei dati personali, *«Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati»* (in G.U. n. 134 del 12 giugno 2014 e in www.gpdp.it, doc. web n. 3134436), pag. 10

precisazione dell'ufficio presso il quale il documento e gli allegati sono consultabili.

La legge n. 69 del 18 giugno 2009, perseguendo l'obiettivo di modernizzare l'azione amministrativa mediante il ricorso agli strumenti informatici riconosce l'effetto di pubblicità legale agli atti e ai provvedimenti amministrativi pubblicati dagli Enti Pubblici sui propri siti informatici. All'art. 32, comma 1, la legge 69/2009 dispone che "*a far data dal 1 gennaio 2010 gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione sui propri siti informatici da parte delle amministrazioni e degli enti pubblici obbligati*". [166]

Nell' Albo pretorio on line va a confluire tutta la documentazione prodotta dall'ente come delibere, provvedimenti conclusivi di procedimenti amministrativi, atti amministrativi di carattere generale, determinazioni dirigenziali, pubblicazioni matrimoniali, avvisi elettorali, varianti al piano regolatore, elenco degli abusi edilizi, ordinanze e avvisi provenienti dagli uffici comunali, pubblicazioni di atti insoluti o non notificati, istanze di cambio nome, elenco oggetti smarriti, bollettino lotterie nazionali, avvisi vendite all'asta, licenze commerciali, bandi di concorso, gare d'appalto, avvisi disponibilità di alloggi in affitto, atti vari su richiesta di altri enti.

L'albo pretorio contiene diversi provvedimenti che devono essere pubblicati per legge e che possono, a volte, fare menzione di alcuni dati sensibili strettamente indispensabili. Nel predisporre i documenti da affiggere, però, fermo restando il rispetto degli obblighi di legge sulla trasparenza

[166] Legge 18 giugno 2009, n. 69 *"Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile"* pubblicata sulla GU n.140 del 19-6-2009 - Suppl. Ordinario n. 95.

delle deliberazioni adottate, occorre comunque rispettare la riservatezza degli interessati. La pubblicazione indiscriminata di informazioni personali può porsi, infatti, in contrasto con la normativa sulla protezione dei dati quando ciò non sia necessario al raggiungimento delle finalità per le quali i dati sono stati raccolti.

Questo è quanto ribadito dal Garante per la protezione dei dati personali che nelle sue decisioni ha richiamato le amministrazioni ad adeguare alla normativa il trattamento dei dati personali contenuti nei documenti destinati alla pubblicazione sull'albo pretorio, nel rispetto del principio di pertinenza e non eccedenza delle informazioni di carattere personale da includere negli atti destinati all'affissione.

4.8 Il controinteressato: profilo soggettivo della riservatezza

La tutela dei controinteressati è un momento rilevante sia nell'accesso documentale (Legge 241/1990) sia nell'accesso civico generalizzato disciplinato dall'articolo 5 del decreto legislativo n. 33/2013 così come modificato dal decreto legislativo n. 97/2016.

La circolare n. 2/2017 del Ministro per la semplificazione e la pubblica amministrazione, emanata dopo le Linee guida adottate dall'ANAC con la delibera n. 1309 del 28 dicembre 2016, stabilisce che, per ciascuna domanda di accesso generalizzato, così come per l'accesso documentale previsto dalla legge 241/90, l'amministrazione debba **verificare l'eventuale esistenza di controinteressati**; verifica che – però – non è evidentemente necessaria quando la richiesta di accesso civico abbia ad oggetto delibere, documenti o, in generale, dati la cui pubblicazione è prevista dalla legge come obbligatoria, essendo stata, in questo caso, effettuata a monte una valutazione

da parte del legislatore al momento della imposizione della prescrizione di diffusione sui siti.

L'art. 5, comma 1, del d.lgs. 33/201, nel sancire l'obbligo dell'amministrazione, cui è indirizzata la richiesta di accesso, di dare comunicazione ai controinteressati individuati, fa – comunque – salvi i casi di obbligazione obbligatoria.

Appendici

Il Piano Triennale per l'Informatica nella Pubblica Amministrazione

Il Piano Triennale per l'informatica nella Pubblica Amministrazione (Piano Triennale o Piano) è uno strumento essenziale per promuovere la trasformazione digitale del Paese e, in particolare, quella della Pubblica Amministrazione italiana.

Coerentemente con gli obiettivi definiti dal Legislatore e dall'Agenzia per l'Italia Digitale, tra i quali rientrano anche quelli definiti all'interno del PNRR, il Piano ha l'obiettivo di dare una accelerazione al processo di semplificazione amministrativa e di digitalizzazione nelle relazioni con i cittadini e le imprese, promuovendo l'uso competitivo delle tecnologie dell'informazione e della comunicazione (ICT) e la ricerca di un miglioramento continuo dei processi interni della Pubblica Amministrazione .

Strategia e principi guida

La strategia è volta a:

- favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della pubblica amministrazione che costituisce il motore di sviluppo per tutto il Paese,
- promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale,

- contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

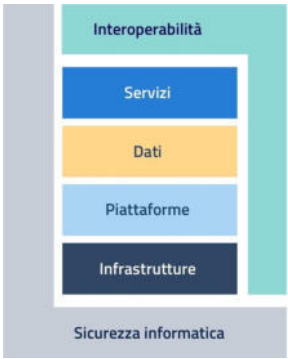
I principi guida del Piano sono:

- **digital & mobile first per i servizi**, che devono essere accessibili in via esclusiva con sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;
- **cloud first** (cloud come prima opzione): le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;
- **servizi inclusivi e accessibili** che vengano incontro alle diverse esigenze delle persone e dei singoli territori e siano interoperabili by design in modo da poter funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- **sicurezza e privacy by design**: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- **user-centric, data driven e agile**: le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo e rendono disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti secondo il principio transfrontaliero by design
- **once only**: le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;

- **dati pubblici un bene comune**: il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- **codice aperto**: le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

Strategia e principi guida

L'aggiornamento 2021-2023 del Piano triennale ha come obiettivo il consolidamento e l'aggiornamento dell'edizione 2020-2022, sempre basandosi sulla rappresentazione semplificata del Modello strategico di evoluzione ICT della PA, che descrive in maniera funzionale la trasformazione digitale, attraverso: due livelli trasversali relativi a interoperabilità e sicurezza informatica e, quattro livelli verticali per servizi, dati, piattaforme ed infrastrutture.



L’aggiornamento 2021-2023

L’aggiornamento 2021-2023 del Piano Triennale, in continuità con la precedente edizione, consolida l’attenzione sulla realizzazione delle azioni previste e sul monitoraggio dei risultati raggiunti nel raggiungimento degli obiettivi predefiniti.

La struttura dell’aggiornamento 2021-2023 mantiene la suddivisione in tre parti:

- **PARTE I – IL PIANO TRIENNALE** Composta da un’introduzione, seguita dalla descrizione della strategia e un approfondimento sui principi guida dell’Agenzia.
- **PARTE II – LE COMPONENTI TECNOLOGICHE** suddivisa in 6 capitoli corrispondenti ai livelli rappresentati nel Modello strategico.
- **PARTE III – LA GOVERNANCE** suddivisa in 3 capitoli che descrivono la governance da attuare per la trasformazione digitale del Paese e le azioni in carico alle amministrazioni.

Italia Digitale 2026

Strategie e iniziative per il digitale del Piano Nazionale di Ripresa e Resilienza[167]

Il Piano nazionale di ripresa e resilienza

Il 27% delle risorse totali del **Piano nazionale di ripresa e resilienza** (PNRR)[168] sono dedicate alla transizione digitale.

All'interno del Piano si sviluppa su due assi la nostra strategia per l'Italia digitale.

Il primo asse riguarda le infrastrutture digitali e la connettività a banda ultra larga. Il secondo riguarda tutti quegli interventi volti a trasformare la Pubblica Amministrazione (PA) in chiave digitale.

I due assi sono necessari per garantire che tutti i cittadini abbiano accesso a connessioni veloci per vivere appieno le opportunità che una vita digitale può e deve offrire e per migliorare il rapporto tra cittadino e pubblica amministrazione rendendo quest'ultima un alleato nella vita digitale dei cittadini.

[167] https://innovazione.gov.it/dipartimento/focus/italia-digitale-2026/ (aggiornamento agosto 2021)
[168] https://assets.innovazione.gov.it/1620284306-pnrr.pdf

Assi di intervento

La digitalizzazione delle infrastrutture tecnologiche e dei servizi pubblici è un impegno non più rimandabile per **far diventare la PA un vero "alleato" di cittadini e imprese**. Il digitale è la soluzione in grado di accorciare drasticamente le "distanze" tra enti e individui e ridurre i tempi della burocrazia.

La strategia **Italia digitale 2026** include importanti investimenti per garantire la copertura di tutto il territorio con reti a banda ultra-larga, condizione necessaria per consentire alle imprese di catturare i benefici della digitalizzazione e più in generale per realizzare pienamente l'**obiettivo di gigabit society**.

Una Pubblica Amministrazione (PA) efficace deve saper supportare cittadini e imprese con **servizi sempre più performanti e universalmente accessibili**, di cui il digitale è un presupposto essenziale.

Gli obiettivi Italia digitale 2026

L'importante piano di investimenti e riforme previsto dal Piano nazionale di ripresa e resilienza vuole mettere l'Italia nel gruppo di testa in Europa entro il 2026.

Per fare ciò pone cinque ambiziosi obiettivi:

1. **Diffondere l'identità digitale**, assicurando che venga utilizzata dal 70% della popolazione;
2. **Colmare il gap di competenze digitali**, con almeno il 70% della popolazione che sia digitalmente abile;
3. Portare circa il 75% delle PA italiane a utilizzare **servizi in cloud**;
4. Raggiungere almeno l'80% dei **servizi pubblici essenziali erogati online**;
5. Raggiungere, in collaborazione con il Mise, il 100% delle famiglie e delle imprese italiane con **reti a banda ultra-larga**.

Obiettivo 1 - Identità e cittadinanza digitale

"Diffondere l'identità digitale, assicurando che venga utilizzata entro il 2026 dal 70% della popolazione"

La trasformazione dell'architettura digitale della Pubblica Amministrazione (PA), dall'infrastruttura cloud all'interoperabilità dei dati, è accompagnata da investimenti mirati a migliorare i servizi digitali offerti ai cittadini.

Obiettivo 2 - Competenze digitali

"Colmare il gap di competenze digitali, con almeno il 70% della popolazione che sia digitalmente abile"

Le iniziative di trasformazione digitale di infrastrutture e servizi sono arricchite da interventi di supporto alle competenze digitali dei cittadini, per garantire un sostegno robusto e pervasivo al compimento del percorso di alfabetizzazione digitale del Paese. In questo ambito il Piano nazionale di ripresa e resilienza nel suo complesso prevede diverse linee di azione, tra loro sinergiche, che coprono tutti gli snodi del percorso educativo.

Obiettivo 3 - Cloud e infrastrutture digitali

"Portare entro il 2026 circa il 75% delle PA italiane a utilizzare servizi in cloud"

La trasformazione digitale della Pubblica Amministrazione (PA) segue un approccio "cloud first", orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni verso un ambiente cloud.

Obiettivo 4 - Servizi pubblici online

"Raggiungere entro il 2026 almeno l'80% dei servizi pubblici essenziali erogati online"

Il gap digitale della PA italiana comporta una ridotta produttività e uno spreco di risorse. Cittadini e imprese ad oggi sono costretti ad accedere alle diverse amministrazioni come silos verticali, non interconnessi tra loro. Con Italia digitale 2026 si vuole superare questo ostacolo.

Obiettivo 5 - Reti ultraveloci

"Raggiungere entro il 2026 il 100% delle famiglie e delle imprese italiane con reti a banda ultra-larga"

La nuova strategia europea Digital Compass stabilisce obiettivi impegnativi per il prossimo decennio: deve essere garantita entro il 2030 una connettività a 1 Gbps per tutti e la piena copertura 5G delle aree popolate. L'ambizione dell'Italia è di raggiungere gli obiettivi europei di trasformazione digitale in netto anticipo sui tempi, portando connessioni a 1 Gbps su tutto il territorio nazionale entro il 2026.

Cybersecurity

Nel suo complesso, la digitalizzazione aumenta il livello di vulnerabilità della società da minacce cyber su tutti i fronti: ad esempio frodi, ricatti informatici o attacchi terroristici.

Cronoprogrammi

Di seguito vengono riportati tutti i cronoprogrammi previsti dagli investimenti del Piano nazionale di ripresa e resilienza.

DATI E INTEROPERABILITA'

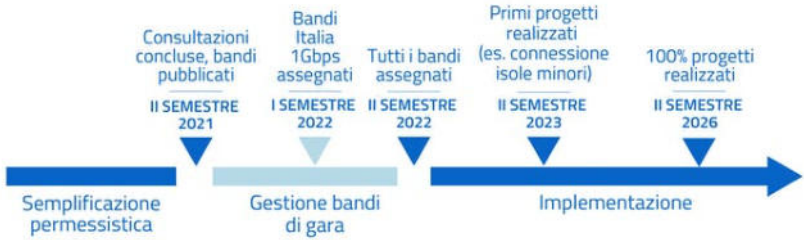
SERVIZI DIGITALI E CITTADINANZA DIGITALE

CYBERSECURITY

DIGITALIZZAZIONE DELLE GRANDI AMMINISTRAZIONI CENTRALI

COMPETENZE DIGITALI DI BASE

RETI ULTRAVELOCI



Bibliografia

AA.VV., *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno: commento al regolamento UE 910/2014*, Giappichelli, 2017;

AGID, *Linee guida sulla formazione, gestione e conservazione dei documenti informatici (e relativi allegati)*, Roma, 2020

BUFFA F., *Firme elettroniche e grafometriche. Dalla Direttiva CE/1999/93 al regolamento EIDAS 2014/910/UE, in vigore dall'1.7.2016*, Key Editore, 2016;

CARNELUTTI F., *Documento – Teoria moderna*, in Nov. Digesto Italiano, VI, Torino, 1957;

CARUCCI P., MESSINA M., *Manuale di archivistica per l'impresa*, Carucci, 1998;

CICLOSI F., *Le nuove Linee guida AgID e il sistema di conservazione*, Sicurezza ICT. Maggioli, 2020;

CICLOSI F., *I documenti informatici dopo le nuove Linee guida AgiD – Formazione, gestione e conservazione*, Maggioli, 2021;

CONTESSA C. (a cura di), *Il Codice dell'Amministrazione Digitale* , La Tribuna, 2018;

COPPOLA P., *Più Digitale Meno Corruzione Più Democrazia – La trasformazione digitale della pubblica amministrazione*, Maggioli, 2022;

DEODATI M., *Il nuovo procedimento amministrativo digitale*, gennaio 2017

D'AVANZO W., *Introduzione all'e-government*, in Blog di consulenza legale ed informazione giuridica (consulenzalegale.altervista.org), 2019

DONGIOVANNI F., *"La formazione del documento informatico alla luce delle nuove Linee Guida AgID", 2021*

FRANCHINI C., MINAZZI F., *Dalla carta al digitale. La nuova gestione documentale nella PA dopo la riforma del CAD (D.Lgs. 179/2016)*, Maggioli, 2016

GIANNOTTA M., SOLOMBRINO E. (a cura di), *Le istituzioni intelligenti nei processi multilivello dell'agenda digitale*, Tamgram Edizioni Scientifiche, 2017

Gruppo di Lavoro Firma Digitale. *Breve Guida sulle Firme Elettroniche.* Roma: Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili. 2018

GUARNACCIA E. - MANCARELLA M., *Il Codice dell'Amministrazione Digitale 2018,* Giugno 2018

GUERCIO M., *Archivistica informatica. I documenti in ambiente digitale*, Carocci, 2019

GUERCIO M., *Conservare il digitale: principi, metodi e procedure per la conservazione a lungo termine di documenti digitali*, Roma, Laterza, 2013

LA DIEGA M., *The switcher – Trasformazione e passaggio al Digitale nella Pubblica Amministrazione*, 2017

MANCARELLA M., *Lineamenti di informatica giuridica*, agosto 2017

MASUCCI A., *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Giappichelli Editore, Torino, 2011

NICOTRA, M. (2016, aprile 26). *Firma digitale, come cambierà in Italia dopo eIDAS*. Tratto da Forum PA.

PIGLIAPOCO S., *Progetto Archivio Digitale. Metodologia Sistemi Professionalità*, Torre del Lago (LU), Civita editoriale, 2016

Garante per la protezione dei dati personali, *Parere sullo schema di "Linee guida sulla formazione, gestione e conservazione dei documenti informatici (nr. 32 del 13/02/2020"*, [doc web 9283921], Roma, 2020

D. Lgs. 7 marzo 20015 n. 82, "Codice dell''Amministrazione Digitale", così come modificato dal D.L. 16 luglio 2020 n. 76, poi convertito con modifiche dalla L. 11 settembre 2020, n. 120, Gazzetta Ufficiale della Repubblica Italiana, 2005

Agenzia per l'Italia Digitale – *Guida di riepilogo dei diritti di cittadinanza digitali previsti dal Codice dell'Amministrazione Digitale e relativa pubblicazione* - Determinazione n. 57/2022

Sitografia

- Agenzia per l'Italia digitale, il regolamento UE n. 910/2014 – eIDAS, in www.agid.gov.it
- AgID, "*Nuove Linee Guida sulla formazione, gestione e conservazione dei documenti informatici",* https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico_.pdf
- www.agid.gov.it
- https://avanzamentodigitale.italia.it/it
- www.agendadigitale.eu/cittadinanza-digitale
- https://avanzamentodigitale.italia.it/it
- http://consulenzalegale.altervista.org/ll-regolamento-eidas/
- www.inipec.gov.it
- www.indicepa.gov.it
- www.innovazione.gov.it
- italiadomani.gov.it
- padigitale2026.gov.it
- www.agid.gov.it/it/agenzia/progetti-pon-governance/italia-login-casa-del-cittadin o/informazione-formazione-transizione-digitale (*Progetto Italia Login - Informazione e formazione per la transizione digitale*)
- https://docs.italia.it
- https://www.competenzedigitali.gov.it/

Breve informazione sugli autori

Dott. Rosario Carrisi
rosario@carrisi.it

Consulente di management certificato CMC - Certified Management Consultant (Certificazione ICMCI – International Council of Management Consulting Institutes, ora CMC-Global) nell'area sistemi Informativi ed organizzazione aziendale.

Dal 1982 si occupa di ICT. Ha lavorato presso società di informatica a carattere nazionale svolgendo attività di progettazione, sviluppo software e avviamento di sistemi informativi aziendali mettendo a frutto un background multidisciplinare in organizzazione aziendale, ICT e security.

Perfezionamento post-laurea in "Sicurezza informatica ed investigazioni digitali", "Digitalizzazione Documentale e Privacy" e "Governance, management, e-government delle pubbliche amministrazioni".

Dal 1996 svolge attività di consulenza organizzativa e direzionale.

Consulente privacy e Responsabile Protezione dei dati (Data Protection Officer) certificato UNI 11697 in organizzazioni private, amministrazioni locali e strutture sanitarie. Da oltre 20 anni si occupa di supporto specialistico agli enti pubblici sui temi della trasformazione digitale.

Docente in materia di privacy, sicurezza delle informazioni e applicazione del CAD (protocollo informatico e flussi documentali, conservazione, DR e Business Continuity). Interviene come relatore in numerosi seminari sui temi della privacy, sicurezza delle informazioni e trasformazione digitale.

Componente del comitato tecnico scientifico del Mediterranean Observatory on Digital Culture and Tourism (MODICT) dell'Università del Salento.

Socio fondatore ed amministratore del **Centro Studi & Progetti Srl e Carrisi Consulting Srls.**

Responsabile dei servizi GDPR/Protezione Dati e servizi di supporto alla transizione digitale presso la società di consulenza **PA 3.26 Srl** *(www.pa326.it)*.

Avv. Gianvito Campeggio
gianvitocampeggio@hotmail.com

Avvocato del Foro di Lecce. Esperto di tecniche normative.

Assistente alla Didattica del Corso di Istituzioni di Diritto Pubblico Dipartimento di Scienze Politiche - Università LUISS.

Collaboratore presso il Centro di Ricerca Euroamericano sulle Politiche Costituzionali (CEDEUAM), centro associato alla Red CLACSO. Referente per l'area di ricerca relativa alle Tecniche normative e ricercatore nella sezione Ecologia Costituzionale – Tecniche e stili di normazione presso l'Università del Salento.

Collaborazione alla didattica col "Laboratorio sulle tecniche di redazione degli atti normativi e amministrativi" - Università LUISS.

Diploma Scuola di Specializzazione per le Professioni Legali (SSPL) – Università del Salento.

Componente del Consiglio Direttivo dell'Associazione Italiana Giovani Avvocati (AIGA), sez. Lecce.

Consulente presso l'Associazione per la Difesa e l'Orientamento dei Consumatori (ADOC), sez. Lecce.

Internet e le tecnologie hanno cambiato la vita e le abitudini delle persone.

Le nuove tecnologie stanno cambiando anche il rapporto tra cittadini e uffici pubblici rendendolo più semplice e trasparente.

Per questo motivo ai cittadini sono riconosciuti una serie di "diritti digitali" che compongono la "Carta della cittadinanza digitale". La carta della cittadinanza digitale è contenuta nel Codice dell'Amministrazione Digitale (CAD) che costituisce il nucleo minino di diritti he le amministrazioni devono garantire a cittadini ed imprese.

Per realizzare questa "nuova" forma di partecipazione cittadina in modalità telematica ai processi decisionali delle istituzioni pubbliche, è necessario che la Pubblica Amministrazione sia fornita di strumenti utili per realizzare, in maniera efficiente ed efficace, gli obbiettivi richiesti, ovvero rispondere alle esigenze della società civile. Si tratta di una doppia sfida per il Paese, non declinabile, rivolta sia ai cittadini che alla Pubblica Amministrazione.

L'allargamento della cittadinanza al digitale non passa solo attraverso la rete, le piattaforme informatiche, gli strumenti. La sfida più impegnativa è quella delle competenze (digitali) che i cittadini così come il personale dell'amministrazione devono acquisire e tenere costantemente aggiornate.

Copertina di Alessandro Carrisi

€ 26,00