LUISS

Dipartimento di Impresa e Management
Corso di laurea magistrale in Gestione d'Impresa
Cattedra Digital Business Transformation

La digital transformation nella Pubblica Amministrazione: L'Automobile Club d'Italia, un caso di successo

Prof.ssa Cristina Alaimo
RELATORE

Prof.ssa Maria Isabella Leone
CORRELATORE

Sofia Donvito
Matricola n. 716691
CANDIDATO

Anno Accademico 2020/2021

"*Sempre devi avere in mente Itaca.*

Raggiungerla sia il pensiero costante"

Questa tesi di laurea rappresenta uno dei traguardi più importanti della mia vita,

in quanto la stesura è avvenuta in un momento particolare, che in pochi hanno potuto capire cosa ha significato per me.

Vorrei ringraziare tutti voi, che mi avete sostenuto, non facendomi sentire sola mai.

A mamma e papà, che mi hanno permesso di portare a termine il mio percorso nel migliore dei modi e che mi sopportano ogni giorno sempre di più,

A mio fratello, l'altra parte di me,

A nonna e nonno, il mio punto di riferimento da sempre,

A Elena, Dalila, Erica, Martina e Michela, le migliori amiche che ho e che tutti vorrebbero avere (ma me le tengo strette)

A mia zia Pierina, colei che veramente sa ciò che Itaca vuole significare.

,

INDICE

CAPITOLO QUARTO: INTERVISTA A VINCENZO PENSA DELL'AUTOMOBILE CLUB D'ITALIA: UN CASO DI SUCCESSO DELLA DIGITALIZZAZIONE DELLA PUBBLICA AMMINISTRAZIONE

INTRODUZIONE

Quando parliamo di innovazione, ci riferiamo a "l'atto, l'opera di innovare, cioè di introdurre nuovi sistemi, nuovi ordinamenti, nuovi metodi di produzione. (…) In senso concreto, ogni novità, mutamento, trasformazione che modifichi radicalmente o provochi comunque un efficace svecchiamento in un ordinamento politico o sociale, in un metodo di produzione, in una tecnica"[1].

Se inventare quindi significa creare qualcosa di nuovo, l'innovazione si sviluppa in questo senso fondendo tecnologie e idee, andando a determinare un cambiamento radicale nella vita delle persone o delle aziende.

Si parla di innovazione e non di trasformazione. La differenza è qualitativa, ovvero la tecnologia non deve essere soltanto innovazione ma anche una forza trasformatrice rispetto alle organizzazioni e a alla società.

Portando un esempio, quando è emersa la fotografia digitale, non ha semplicemente sostituito una vecchia tecnologia con una nuova, migliore o più economica. Non ha creato una nuova proposta di valore per servire i clienti né ha aperto nuovi canali di distribuzione. Ha invece consentito l'emergere di nuovi comportamenti sociali rafforzati da una nuova e sempre più potente razza di aziende, che si basano su un diverso modello operativo e di business, che competono in modi diversi.

Questo ci permette di definire il concetto di "*digital disruption*", il cui fondatore fu Clayton Christensen, ideatore della teoria "*job to be done*". L'autore afferma che questo termine descrive un processo mediante il quale un prodotto o servizio attecchisce inizialmente in semplici applicazioni nella parte inferiore di un mercato e poi si muove inesorabilmente verso l'alto, sostituendo infine i concorrenti affermati. Quindi, l'innovazione dirompente si focalizza non sul prodotto, ma sul bisogno, ancora non soddisfatto, che il prodotto è chiamato a soddisfare.

Viene da sé che al centro del processo c'è l'individuo, pertanto è possibile affermare che la caratteristica principale della "*disruptive innovation"* è quella di essere legata non tanto a mutamenti tecnologici complessi, quanto alla capacità di definire e cogliere i bisogni di un individuo[2].

Nel campo della Pubblica Amministrazione, è possibile applicare lo stesso concetto andando ad esaminare nuovi modi, di certo meno costosi e più efficaci, quindi anche misurabili, per erogare i servizi pubblici. Possiamo pensare al concetto di innovazione della Pubblica Amministrazione nelle politiche di apertura dei dati, permettendo alle imprese di sviluppare applicazioni che possano giovare al cittadino informandolo in tempo reale sul servizio selezionato, come trasporto, turismo, scuola, lavoro oppure consentire al cittadino o ad un'azienda di accedere ad atti e documenti amministrativi.

Per innovare non servono tecnologie particolari, quanto una strategia di lungo termine che traini le attività quotidiane e di persone pronte a innovare continuamente se stesse e l'ecosistema che le circonda, identificando

[1] Treccani, il portale del sapere, https://www.treccani.it

[2] Clayton Christensen, Michael Raynor e Rory McDonald in "What Is Disruptive Innovation?" (HBR, dicembre 2015)

lo sviluppo come una mentalità diffusa. Le persone rappresentano la vera liquidità aziendale e investire nella loro innovazione e formazione rappresenta il punto cruciale. Questo deve concretizzarsi nella:

- Creazione di condizioni sociali e organizzative che favoriscono l'identificazione e l'adozione delle innovazioni di prodotto e di processo;
- Stimolazione dell'attività di leadership e dell'evoluzione culturale delle singole persone tali da favorire l'accettazione di nuove sfide;
- Orientamento allo sviluppo delle competenze al fine di creare valore in tutti i processi aziendali.

Nella Pubblica Amministrazione si stanno facendo pressanti due necessità, la prima è il recupero di risorse, dovuta alla necessità di contenere i costi a fronte di esigenze di qualità e livello di servizi crescenti, la seconda è la crescente istanza di semplificazione e de-burocratizzazione che ispira anche i più recenti provvedimenti legislativi. A partire dagli anni Novanta, ci si è iniziati a interrogare su modelli che permettessero alle realtà pubbliche di essere più efficienti, come per esempio il metodo "*Lean Thinking*", ossia "pensiero snello", teorizzato e sviluppato da James P. Womack e Daniel, T. Jones (1996). Più che di metodo, si dovrebbe parlare di una filosofia utile ad agevolare i cambiamenti attesi, innescando processi di miglioramento dell'efficienza che vedano più coinvolte e partecipi le persone. Oggi, come afferma l'autrice Caterina Ingrosso, il "*Lean Thinking*" nella pubblica amministrazione è possibile se la centralità dell'utente e delle sue aspettative, l'efficienza e l'efficacia dell'azione amministrativa, lo sviluppo e il coinvolgimento dei dipendenti pubblici, sono le chiavi di volta di un'amministrazione pubblica moderna, idonea a supportare la competitività del sistema[3].

Al giorno d'oggi ci si pone il quesito se le aziende, e in particolare la Pubblica Amministrazione, riusciranno a sfruttare il potere del digitale[4], la cui sfida risiede nel far convivere l'aspetto teorico e tecnologico dell'innovazione, con quello pratico della sua effettiva applicazione nel tessuto sociale ed economico, e delle relative implicazioni, anche in termini di valore pubblico. Questo implica avere un approccio dirompente, che faccia si che l'innovazione diventi non una questione di scelta, ma una necessità. Nel corso degli anni ci sono stati diversi cambiamenti finalizzati a creare strutture improntate verso la cultura dell'efficienza e dell'efficacia, due pilastri chiave per contestualizzare il tema della dematerializzazione nella Pubblica Amministrazione. Oggi infatti, molteplici forze stanno spingendo la Pubblica Amministrazione al cambiamento, alcune di queste sono frutto del "*decision making*", di leggi nazionali ed internazionali, intente a modificare in modo "formale la pubblica amministrazione", altre sono il frutto dei cittadini stessi, di coloro che effettivamente fruiscono del servizio offerto, che richiedono processi decisionali più inclusivi, efficaci ed efficienti.

[3] Caterina Ingrosso, "*Lean Thinking : Il "pensiero snello" nella Pubblica Amministrazione. Che cos'è? E' possibile?*", (2018).
[4] Nino Lo Bianco, "*È il momento di osare. Riusciranno le aziende a sfruttare il potere del digitale*?", OpenLab, (2020).

La nuova cultura di efficienza ed efficacia del cittadino, è stata sicuramente alimentata e accelerata dalla diffusione delle tecnologie ICT che hanno posto le premesse per creare un rapporto sempre più diretto tra istituzioni e cittadini, infatti nel contesto europeo sono state introdotte nuove forme di partecipazione che possano creare un link e agevolare l'interconnessione tra attori pubblici, singoli cittadini, associazioni, comunità locali e professionali.
La tecnologia è stata negli ultimi anni al centro della produzione normativa nazionale, rappresentando un processo volto a snellire le norme che orientano l'azione degli Enti. Le nuove norme sono orientate ad una sempre maggiore applicabilità, in linea con le disposizioni emanate dall'UE, verso la direzione dell'ampliamento dell'adozione delle tecnologie informatiche all'interno delle amministrazioni pubbliche, in particolare in materia di documento informatico e di riorganizzazione dei processi.
Infatti, ancora oggi in molte realtà della Pubblica Amministrazione, i documenti vengono trasmessi e archiviati in forma cartacea, producendo ingenti quantità di carta, difficile poi da smaltire. Vediamo quindi che l'impatto di una corretta gestione dei documenti, sia fondamentale per migliorare la qualità e il sistema della performance di un sistema ormai datato. In questo contesto l'utilizzo di tecnologie informatiche apporterebbe benefici considerevoli, motivo per cui negli ultimi anni, si è assistito a una forte spinta, sia organizzativa che normativa, per il passaggio dal documento cartaceo al documento informatico e alla maggiore efficienza dell'erogazione del servizio offerto.
Prima conseguenza della dematerializzazione è riscontrabile sicuramente in un risparmio economico ma può anche consentire di rinnovare totalmente le modalità di lavoro grazie all'introduzione dell'ICT all'interno delle organizzazioni. È in questo ambito che viene considerato necessario identificare una *road map* che permetta agli Enti di orientarsi al processo di dematerializzazione con un'ottica di lungo termine, che sia effettivamente praticabile, funzionale e coerente con una strategia di *e-government*.
Il lavoro si declina in quattro capitoli.

Nel primo capitolo verrà illustrato il concetto di *e-government* con i relativi ambiti di applicazione e le aree di trasformazione coinvolte. Attraverso le aree di erogazione di questo andremo a identificare i vantaggi e che questo può apportare alla pubblica amministrazione, nonché le opportunità, andando anche a interpretare la produzione normativa degli ultimi anni, volta a regolamentare l'adozione delle tecnologie informatiche all'interno delle amministrazioni pubbliche.
Nel secondo capitolo andremo ad analizzare la diffusione del *cloud computing*, nel contesto della dematerializzazione e digitalizzazione dei documenti, andando ad esaminare come un approccio "*paperless document*" possa giovare alle aziende pubbliche e private. Andremo a definire quella che è l'architettura del *cloud computing*, e le sfide della sicurezza che da essa derivano, nonché i modi utilizzati per ovviarle. Infine, analizzando il trend evolutivo di questa tecnologia negli ultimi tre anni, ci soffermeremo in particolar modo su come questa possa contribuire allo sviluppo della digitalizzazione della pubblica amministrazione.

Nel terzo capitolo si mostrerà il ruolo della crittografia nell'era digitale e le diverse tipologie di firme elettroniche. Si porrà maggiormente l'accento sulla firma grafometrica, identificata come quella firma in grado di supportare il processo di dematerializzazione dei documenti e che si basa su tecniche e algoritmi biometrici. Nonostante i rischi che potrebbero scaturire, si dimostrerà come la firma grafometrica in realtà si pone come soluzione abilitante per la digitalizzazione dei processi documentali cartacei assicurando piena *compliance* e validità legale, dando luogo a processi di digitalizzazione che permettono di dematerializzare il cartaceo, creando efficienza e contenimento dei costi di gestione

Infine, il quarto capitolo si concluderà con la descrizione di un caso studio di una pubblica amministrazione che è stata in grado di cogliere gli aspetti più innovativi della *digital transformation* automatizzando i processi per effettuare un passaggio completo dal cartaceo al digitale.

CAPITOLO PRIMO. EGOVERNMENT: VERSO UN AMMINISTRAZIONE DIGITALE

1.1 E-government: una definizione

La connettività digitale ha dato inizio a un nuovo tipo di competizione tra le organizzazioni, basata su informazione e tecnologia, che attiva un ordine di innovazioni dirompenti e cambiamenti bruschi e sediziosi. Viene da sé, che la conoscenza in ambito digitale rappresenta il fattore critico di successo per tutte le organizzazioni, mentre l'apprendimento, che emerge attraverso la cooperazione, è il processo più importante[5]. L'innovazione, pertanto, diventa un requisito fondamentale per le organizzazioni pubbliche e private che vogliano raggiungere un vantaggio competitivo.

Finora, come ha mostrato la letteratura esistente, gli strumenti ICT hanno permesso alle organizzazioni private di aumentare la loro efficienza operativa, grazie ad una riduzione dei costi e ad un aumento della qualità dei servizi offerti, mentre il settore pubblico è stato messo da parte a causa dei ritardi nell'adottare tecnologie innovative a reinvenzione del business. Tuttavia, l'avvento di Internet, la connettività digitale, l'esplosione e l'uso dell'e-commerce e dei modelli di e-business nel settore privato stanno spingendo il settore pubblico a ripensare i modelli organizzativi gerarchici e burocratici. Negli ultimi anni, numerose sono state le riforme del legislatore volte a valorizzare l'importanza dell'ICT nel settore pubblico e l'adozione di modelli e-business per migliorare la qualità e la reattività dei servizi che forniscono ai propri cittadini, ampliando la portata e l'accessibilità dei propri servizi e delle infrastrutture pubbliche e consentendo ai cittadini di sperimentare una forma più rapida e trasparente di accesso ai servizi governativi, che potrebbero condurre a forme innovative di consultazione pubblica e ad altre forme di partecipazione democratica[6].

Queste azioni e strategie, volte a innovare e reinventare il governo attraverso la tecnologia, passano sotto la nozione di "*eGovernment*", che rappresenta un enorme impulso per andare avanti nel ventunesimo secolo con servizi governativi di qualità superiore ed economici e una migliore relazione tra cittadini e governo[7]. L'impulso e i benefici che la tecnologia poteva apportare alle pubbliche realtà, era stato anche identificato già agli inizi degli anni novanta, infatti Tapscott e Caston[8] sostenevano che l'ICT poteva provare un "cambio di paradigma", che da burocratico e tradizionale, caratterizzato da efficienza produttiva interna, razionalità funzionale, dipartimentalizzazione, controllo gerarchico e gestione basata su regole, passava ad acquisire requisiti di economia competitiva quali: flessibilità, organizzazione di rete, integrazione orizzontale e verticale, imprenditorialità innovativa, apprendimento dell'organizzazione, accelerazione nell'erogazione dei servizi e strategia orientata al cliente.

---

[5] Lundvall e Johnson, "*The Learning Economy*", pp. 23-42 (1994)
[6] Lips, M., "*Digital Government: Managing Public Sector Reform in the Digital Era*", Routledge, (2020)
[7] Fang, Z.Y., "*E-Government in Digital Era: Concept, Practice and Development*". International Journal of the Computer, the Internet and Management, (2002)
[8] Tapscott, D. and Caston, "*A. Paradigm Shift: The New Promise of Information Technology*", McGraw-Hill: New York, (1993).

Questa *disruptive innovation* nel settore pubblico ha introdotto "l'era dell'intelligenza di rete", reinventando aziende, governi e individui[9].

Purtroppo, come per ogni innovazione, esistono vantaggi e svantaggi, infatti, se l'ICT da un lato offre un potenziale considerevole per lo sviluppo dell'*eGovernment*, dall'altro potrebbe rappresentare una sfida o un pericolo in sé. Qualsiasi organizzazione ignori il valore potenziale della tecnologia può subire svantaggi competitivi considerevoli, ma d'altro canto il successo dell'*eGovernment*, potrà essere riconosciuto solo una volta che l'adattamento a determinate condizioni sia avvenuto. In particolare, le sfide dell'*eGovernment* vanno ben oltre la tecnologia, richiedono strutture e competenze organizzative, nuove forme di leadership, trasformazione dei partenariati pubblico-privato[10].

Secondo World Bank[11], "l'*eGovernment* è il sistema di tecnologie dell'informazione e della comunicazione possedute o gestite dal governo che trasformano le relazioni con i cittadini, il settore privato e/o altre agenzie governative in modo da promuovere l'emancipazione dei cittadini, migliorare la fornitura di servizi, rafforzare la responsabilità, aumentare la trasparenza o migliorare l'efficienza del governo".

Il punto che scaturisce è che, definendo l'*eGovernment* semplicemente come un processo verso la transazione digitale o l'adozione di tecnologie volte a implementare un servizio offerto, si riduce di gran lunga la gamma di opportunità e prospettive che può offrire. Infatti, per comprendere al meglio la portata di questo termine e per progettare una vera strategia di successo, bisogna pensarlo come un concetto multidimensionale e complesso, che non può limitarsi ad un'unica definizione, o meglio ad un'unica metodologia.

Utilizzare una prospettiva tecnologica, porta a teorizzare, in maniera troppo semplificativa, la portata che questo nuovo modello può avere, bisogna piuttosto considerarla come una variabile che possa agire pari passo e in maniera co-dipendente ad altri elementi organizzativi come le persone, le infrastrutture e i processi[12].

È possibile concludere pertanto che sebbene gli effetti delle tecnologie possano impattare in maniera significativa nel settore pubblico, non possono reputarsi l'elemento chiave e non possono prescindere da altri fattori, non di natura tecnologica, sia all'interno che all'esterno dell'Amministrazione.

Pertanto, si possono individuare tre aree critiche di trasformazione dell'*eGovernment*[13]:

1. Aree di trasformazione (interna, esterna, relazionale);
2. Utenti, clienti, attori e loro interrelazioni (cittadini, imprese, organizzazioni governative, dipendenti);

[9] Collard, A., "*Embracing digital transformation the HMRC way*", < https://www.iota-tax.org/sites/default/files/publications/public_files/impact-of-digitalisation-online-final.pdf>, (March 2020).
[10] Allen, B., Juillet, L., Paquet, G. and Roy, J., "*E-Governance & Government On-line in Canada: Partnerships, People & in Government Information Quarterly*", Vol. 30, No. 1. pp.36–47, (2001).
[11] World Bank, "e-Government", < https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government>, (May 2015).
[12] Nograšek, J., & Vintar, M., "E-government and organisational transformation of government: Black box revisited? Government Information Quarterly, XXXI, (pp. 108-118), 2014.
[13] Valentina (Dardha) Ndou, "E – government for developing countries: opportunities and challenges", EJISDC (2004) 18, 1, 1-24

3. Domini di applicazione dell'*eGovernment* (servizi elettronici, democrazia elettronica, amministrazione elettronica).

Come già affermava Tapscott, nel 1996, un'iniziativa di *eGovernment* "richiede un ripensamento radicale della natura e del funzionamento dell'organizzazione e delle relazioni tra le organizzazioni. Deve concentrarsi in una rete di relazioni che includa tutti i livelli e le funzioni aziendali, in cui i confini interni ed esterni siano permeabili e fluidi"[14]; infatti è possibile affermare che pensare all'*eGovernment* semplicemente come una riprogettazione dei processi aziendali, limita il potenziale che quest'ultimo può offrire. Bisogna innanzitutto tenere in considerazione le aree di trasformazione interna, esterna e relazionale.

Per quanto riguarda l'area di trasformazione interna, essa si riferisce all'uso di tecnologie per correlare diversi dipartimenti e agenzie in modo da far fluire più velocemente e facilmente le informazioni tra gli stessi, rendendo più efficaci ed efficienti le funzioni interne in modo da ridurre i tempi di elaborazione e delle procedure di approvazione lunghe, burocratiche e inefficienti. In questo modo si genereranno vantaggi per il sistema pubblico dovuti a una riduzione dei tempi di utilizzo e di gestione, dei costi di manodopera e all'archiviazione e raccolta dei dati, nonché la velocità e l'accuratezza dell'elaborazione delle attività.

La tecnologia inoltre, per quanto riguarda l'area di trasformazione esterna, rappresenta uno strumento per garantire la trasparenza delle informazioni ai cittadini e alle imprese, creando anche opportunità di partnership e collaborazione tra diverse istituzioni governative[15].

Infine, sul piano relazionale, è possibile individuare cambiamenti radicali nelle relazioni tra i cittadini e lo stato, e tra gli stati nazionali, realizzando per esempio integrazioni orizzontali e verticali di servizi e informazioni da varie agenzie governative, consentendo all'individuo la massima efficienza nello sfruttamento degli stessi. Fountain, utilizza il concetto di "stato virtuale" ovvero un'entità governativa organizzata con "agenzie virtuali, agenzie trasversali, reti pubblico-private le cui strutture e capacità dipendono da Internet e dal web"[16].

In base ai flussi di informazione interessati, è infatti possibile individuare quattro modelli di erogazione di *e-Government*[17]:

1. **Government to Citizens (G2C)**: si occupa del rapporto bilaterale tra governo e cittadini, che avviene attraverso piattaforme online. Queste consentono di apportare vantaggi per i cittadini abilitandoli ad accedere facilmente alle informazioni e ai servizi di cui hanno bisogno, come la richiesta di determinati certificati, e per il governo che può accedere agli stessi servizi.

[14] Valentina (Dardha) Ndou, "*E – government for developing countries: opportunities and challenges*", EJISDC (2004) 18, 1, 1-24
[15] Allen, B., Juillet, L., Paquet, G. and Roy, J., "*E-Governance & Government On-line in Canada: Partnerships, People & in Government Information Quarterly*", Vol. 30, No. 1. pp.36–47, (2001).
[16] Fountain, J. (2001). Building the Virtual State: Information Technology and Institutional Change. Brookings Institution Press.
[17] Bwalya, K., & Mutula, S, "*E-government: Implementation, Adoption and Synthesis in Developing Countries. De Gruyter/Saur*", (2014).

2. **Government to Business (G2B)**: consiste nelle interazioni elettroniche tra agenzie governative e aziende private per ridurre la burocrazia e semplificare i processi normativi. In questo ambito l'ICT permette alle aziende di ridurre i costi e migliorare il controllo dell'inventario, facendo aumentare la loro competitività sul mercato.
3. **Government to government (G2G)**: si occupa di favorire la collaborazione e la cooperazione tra le varie organizzazioni governative, realizzando un unico punto di accesso attraverso la condivisione di database, risorse, competenze e capacità.

   Secondo gli autori (Bwalya & Mutula, 2014) il G2G facilita le relazioni internazionali favorendo la diffusione di piattaforme ICT che consentano ai governi di diversi paesi di collaborare e scambiare idee su questioni relative allo sviluppo.
4. **Government to Employees (G2E)**: si riferisce al rapporto tra il governo e i suoi dipendenti, fornendo loro l'accesso a informazioni rilevanti riguardanti per esempio politiche di compensazione e benefici, opportunità di formazione e apprendimento, leggi sui diritti civili, ecc.. Il G2E fa riferimento anche alla possibilità di migliorare la formazione delle risorse attraverso piattaforme digitali, in modalità *e-Learning*, promuovendo la collaborazione e la competitività dei servizi offerti.

   Come afferma anche Richard Heeks, il pieno sfruttamento e implementazione di queste complesse reti di interrelazioni richiede tre principali domini applicativi per l'*eGovernment*[18]:
   - *e-Administration*: per l'informatizzazione dei ruoli amministrativi e per la realizzazione di interrelazioni tra dipartimenti e funzioni;
   - *e-Citizens* e *e-Services*: per la realizzazione di servizi digitali che favoriscano i collegamenti tra governi e cittadini;
   - *e-Society*: per realizzare collegamenti *inter-society* tra enti pubblici, settore privato e comunità civile in generale.

1.2 eGovernment: opportunità e prospettive

Un articolo del *The Economist* del 2000[19] individuò nell'*e-Government* come una promettente rivoluzione al pari dell'e-Commerce e dell'e-Business per i diversi benefici economici. Avendo esplicitato gli ambiti coinvolti nel processo di implementazione delle iniziative di *e-Government*, è opportuno ora analizzare le principali opportunità che questo può generare[20].

1. **Riduzione dei costi e guadagni di efficienza**: attraverso l'ICT è possibile ridurre il numero di inefficienze processuali attraverso la condivisione di file e dati tra i dipartimenti governativi,

[18] Richard Heeks, "*Implementing and Managing e-Government: An International Text*" (Sage, 2006).
[19] The Economist, "*A survey of government and the Internet, June 22nd, 2000*", <https://www.economist.com/special-report/2000/06/22/the-next-revolution>
[20] Valentina (Dardha) Ndou, "*E – government for developing countries: opportunities and challenges*", EJISDC (2004)

contribuendo così all'eliminazione degli errori dalle procedure manuali e riducendo il tempo necessario per le transazioni. Infatti, la messa in linea dei servizi riduce notevolmente i costi di elaborazione di molte attività rispetto alla modalità manuale di gestione delle operazioni;

2. **Qualità della fornitura del servizio ad aziende e clienti**: mettere in rete i servizi governativi, permette di migliorare la qualità dei servizi, in termini di tempo, contenuti e accessibilità. Infatti, sarà possibile ridurre la burocrazia, offrire accessibilità a tempo pieno ai cittadini, nonché transazioni veloci e convenienti;
3. **Trasparenza, anticorruzione, responsabilità**: la disponibilità di una varietà di pubblicazioni online riguardanti l'attività della pubblica amministrazione, nonché gli aspetti economici e legislativi, aumenta anche la trasparenza.
4. **Aumentare la capacità del governo**: attraverso le intranet è possibile condividere tra diversi reparti database di clienti comuni e di mettere in comune le competenze e le capacità dei loro membri per la risoluzione dei problemi. Le informazioni scambiate fluiranno molto più velocemente garantendo una fornitura più rapida ed economica di beni e servizi.
5. **Creazione di reti e comunità**: attraverso un approccio di rete, le interrelazioni tra governo, clienti, aziende, dipendenti e altre agenzie governative saranno agevolate grazie alla messa insieme di competenze, tecnologie, informazioni e conoscenze. Come affermano Mansell e Wehn, "l'uso e la diffusione di successo dell'ICT nel settore pubblico implica un processo di apprendimento collettivo, multidisciplinare e dinamico". Inoltre, un'iniziativa di *eGovernment* consente la creazione di comunità, dando ai cittadini e alle imprese la possibilità di partecipare a forum e processi decisionali, contribuendo attivamente a diverse discussioni politiche e governative.
6. **Migliorare la qualità del processo decisionale**: attraverso un paradigma di *open innovation*, favorito dalla creazione di comunità, di forum, dall'interazione continua tra governo e cittadini, il processo decisionale sarà implementato dalla contribuzione dei cittadini con le loro idee e informazioni. Infatti, porre al centro il cittadino considerandolo come cliente governativo, ascoltando e comprendendo i suoi bisogni è fondamentale per la qualità del servizio offerto.
7. **Promuovere l'uso dell'ICT in altri settori della società**: affinché una strategia di *eGovernment* funzioni, è necessario che le stesse parti interessate a partecipare, avviino un processo di digitalizzazione. È in questo senso che un'iniziativa di *eGovernment* favorisce la promozione dell'uso della tecnologia in altri settori. Per esempio, affinché si verifichi una transazione elettronica da governo a impresa, l'azienda stessa deve utilizzare apparecchiature elettroniche. D'altra parte, le istituzioni finanziarie devono creare metodi sicuri e affidabili per le transazioni elettroniche.

Sebbene sia evidente che ormai la tecnologia e lo stesso *eGovernment* sono potenti motori per la creazione di valore, rimangono ancora aperto molte sfide alle quali si sta cercando di porre un rimedio attraverso regolamentazioni europee. Le sfide da fronteggiare riguardano principalmente i seguenti aspetti:

1. **Infrastrutture ICT** (disponibilità in linea, alfabetizzazione informatica, apparecchiature per le telecomunicazioni): per una transizione al governo elettronico, è necessaria un'architettura, cioè un insieme guida di principi, modelli e standard e diversi metodi di accesso (come l'accesso remoto). A tal proposito risulta cruciale l'alfabetizzazione del capitale umano, il quale dovrà essere re-indirizzato verso un processo di re-skilling;
2. **Questioni politiche (legislazione)**: le funzioni dell'*eGovernment* richiedono di essere regolate da politiche e leggi per le attività elettroniche, come ad esempio le firme elettroniche, l'archiviazione elettronica, la libertà di informazione, la protezione dei dati, la criminalità informatica, i diritti di proprietà intellettuale e le questioni di copyright;
3. **Sviluppo del capitale umano e apprendimento lungo tutto l'arco della vita (abilità, capacità, istruzione, apprendimento)**: un governo tecnologico richiede capacità umane ibride: tecnologiche, commerciali e gestionali. Al giorno d'oggi diventa sempre più necessario investire nella formazione del personale in quanto ci sono ancora delle lacune riguardanti la mancanza di competenze ICT nel settore pubblico;
4. **Gestione del cambiamento (cultura, resistenza al cambiamento)**: la gestione del cambiamento può essere suddivisa in due sotto concetti: approccio alla gestione del cambiamento e gestione della resistenza al cambiamento. L'approccio di gestione del cambiamento si riferisce alle procedure di gestione del cambiamento stabilite all'interno delle organizzazioni, con particolare riguardo alla cultura, gerarchia, le intranet, la condivisione delle informazioni. La resistenza dei dipendenti al cambiamento è ancora il più grande ostacolo al cambiamento di successo in quanto temono che le macchine, in particolare i robot, prenderanno il loro posto;
5. **Partenariato e collaborazione (partenariato pubblico / privato, comunità e rete creazione)**: affinché si realizzi la collaborazione e la cooperazione a livello locale, regionale e nazionale, nonché tra organizzazioni pubbliche e private, è necessario incoraggiare un sistema di fiducia nel governo da parte dei cittadini e del settore privato. Quest'ultimo assume un'importanza fondamentale nel suo ruolo da collaboratore, in quanto potrebbe essere in grado di supportare il governo con competenze tecniche e infrastrutture. Anche le università forniranno il personale richiesto, corsi di apprendimento e formazione per personale governativo e cittadini, e altri dipartimenti possono contribuire al flusso di dati e informazioni e alla condivisione delle conoscenze per la risoluzione di problemi di attività o processi simili e così via;
6. **Strategia (visione, missione)**: la strategia deve essere orientata al raggiungimento di obiettivi di lungo termine, pertanto dovrà essere molto attenta, chiara, analitica e dinamica. Un governo che punta

all'efficacia non dovrebbe limitarsi a trasferire le informazioni digitalmente e a fornire servizi online, quanto piuttosto investire nel processo di reingegnerizzazione necessario per coglierne tutti i benefici;

7. **Ruolo di leadership (motivare, coinvolgere, influenzare, supportare)**: a differenza del settore privato, quello pubblico risulta più restio al cambiamento perché il processo di eGovernment richiede costi, rischi e sfide elevati. Il ruolo della leadership assume un ruolo chiave nella gestione di questo, dalla fase iniziale, a quella di sviluppo, a quella finale, in quanto deve essere in grado di comprendere i costi e i benefici reali del progetto, di motivare, influenzare, includere e supportare altre organizzazioni e istituzioni. Un buon leader, che sia un soggetto, un'organizzazione o un'istituzione, farà in modo che si abbandoni quella resistenza tipica di un governo o di un'organizzazione pubblica.

1.3 eGovernment: il nuovo contesto normativo

Capire la ricca normativa che caratterizza gli Enti della Pubblica Amministrazione ci permette di avere un quadro ancora più chiaro sul sistema burocratico che viene ad essa associato.
A tal proposito è opportuno illustrare il contesto sulle normative che caratterizzano in maniera diretta o indiretta l'oggetto della tesi, ovvero il processo di dematerializzazione.
La produzione normativa nazionale degli ultimi anni presenta un processo evolutivo complesso, ma decisamente orientato ad una sempre maggiore applicabilità, coerentemente con le disposizioni emanate dalla UE, verso la direzione dell'ampliamento dell'adozione delle tecnologie informatiche all'interno delle amministrazioni pubbliche, in particolare in materia di documento informatico e di riorganizzazione dei processi.

1.3.1 Il Codice dell'Amministrazione Digitale

Tra queste, in Italia, la prima risposta organica all'esigenza di riorganizzazione della PA alla luce delle trasformazioni imposte dalle nuove tecnologie è costituita dal Codice dell'Amministrazione Digitale.
"Il Codice dell'Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese"[21] e rappresenta ormai la norma centrale e di riferimento per la digitalizzazione della nostra pubblica amministrazione.
L'origine del Codice dell'Amministrazione Digitale (CAD) risale al decreto legislativo 7 marzo 2005 n. 82, ed ha subito un percorso piuttosto travagliato in quanto è stato oggetto di numerose modifiche. È stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179[22] e poi con il

[21] Agenzia per l'Italia Digitale
[22] Modifiche e 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.

decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale. Ad oggi è giunto alla sua sesta edizione.

Nasce come "Codice della Digitalizzazione della Pubblica Amministrazione" con novantasei articoli e una suddivisione in tredici Capi. In ordine crescente, dal Capo I al Capo XIII, il Codice sancisce i principi generali, la disponibilità dei dati, la gestione delle informazioni, la conservazione dei documenti, la trasmissione, l'accesso, la fruibilità, le infrastrutture nazionali di servizi telematici, i principi di attuazione, la sicurezza, le regole tecniche, lo sviluppo e l'utilizzazione dei programmi informatici nelle pubbliche amministrazioni e infine le norme transitorie. Successivamente approfondiremo il Capo III relativo alla gestione delle informazioni, in particolare trattando il documento informatico, la firma, il protocollo, i procedimenti amministrativi gestiti con modalità digitali e il sistema documentale.

L'ultimo intervento normativo ha voluto deregolamentare maggiormente il contenuto del CAD, attraverso un'azione di semplificazione terminologica e testuale, e di sostituzione delle precedenti regole tecniche con linee guida a cura di AgID.

Il CAD trova la sua ragione d'esistenza nel fatto che la regolazione dei rapporti tra soggetti è sempre fatta attraverso leggi stabili nel tempo[23]. Nel caso dei rapporti tra cittadini, imprese e amministrazione, l'avvento delle tecnologie, ha imposto un cambiamento notevole nelle modalità di rapporto tra cittadini e amministrazione, che non erano presenti negli attuali modelli e così si è pensato di abilitare la modalità digitale di dialogo. L'avvento di strumenti come il documento informatico, la firma elettronica, non erano presenti in nessuna parte dell'ordinamento e quindi si è pensato, per favorirne e obbligarne l'uso, che fosse necessario inserirli in una norma, ovvero il Codice dell'Amministrazione Digitale. Inoltre, contribuisce all'alfabetizzazione informatica dei cittadini e alla formazione dei dipendenti pubblici, favorendo lo scambio di dati e informazioni attraverso i diversi comparti della Pubblica Amministrazione, e con modalità prettamente digitali basate sulle regole del Sistema Pubblico di Connettività (SPC) e della Rete Internazionale della Pubblica Amministrazioni.

La riforma più importante del CAD è stata operata dal D.lsl. 179/2016 (nell'ambito della cosiddetta "Riforma Madia"), che ha modificato sostanzialmente le disposizioni le Codice precedente, seppure mantenendo inalterati i principi iniziali di questo, come l'informatizzazione dei servizi, dei pagamenti e delle relazioni tra PA e i suoi stakeholder.

Nel nostro caso, la Riforma Madia assume un rilievo particolare in quanto ha trattato un tema caldo per il nostro elaborato, ovvero la *firma digitale*, intesa come uno strumento che consente di scambiare documenti in rete con piena validità legale poiché garantisce l'autenticità e la piena integrità della documentazione "virtualmente" sottoscritta. Inoltre, sempre a sottolineare l'importanza riconosciuta al settore informatico come sviluppo e crescita dell'UE, ha proposto uno strumento di riconoscimento informatizzato che consente

[23] Giovanni Manca, "*Breve storia della PA digitale: la genesi e l'evoluzione del Codice dell'Amministrazione Digitale*", (06/07/2020)

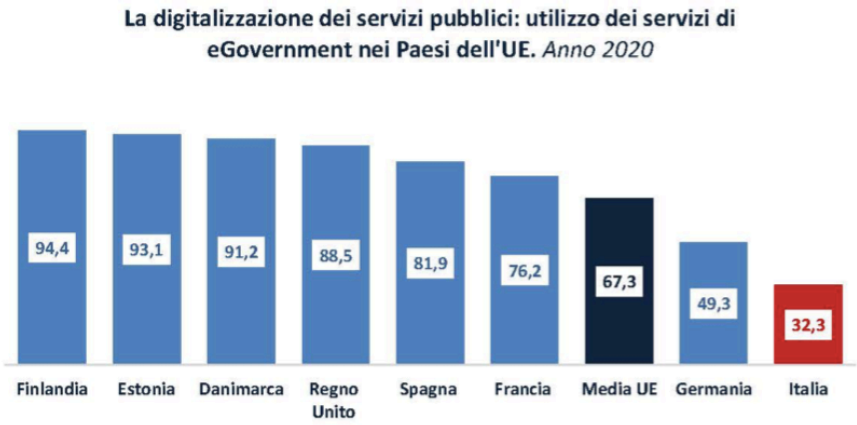
agli utenti, pubblici o privati, di accedere a tutti i servizi della PA, con un'identità digitale valida per tutti i servizi online, il cosiddetto *Sistema Pubblico di Identità Digitale (Spid)*.

Anche su scala sovrannazionale sono stati avanzati programmi e strategie volte a favorire la digitalizzazione dell'amministrazione pubblica. Nel 2010 la Commissione ha realizzato un documento confluito nell'Agenda Digitale Europea, che si proponeva il raggiungimento di determinati obiettivi entro il 2020.
Nonostante la conversione al digitale sia stata inoltre accompagnata da ingenti risorse economiche, per un ammontare di oltre 27 miliardi[24], la trasformazione digitale non ha avuto la sua massima manifestazione, in quanto ancora oggi si fa riferimento a strumenti "tradizionali" accompagnati a strumenti "digitali", rendendo difficile un processo di totale conversione.
Secondo lo studio Uil-Eures, il mancato raggiungimento degli obiettivi prefissati entro la fine del 2020, è attribuibile prima di tutto al fatto che le procedure sono state implementate formalmente e non sostanzialmente, quindi mostrando criticità sul fronte applicativo. Inoltre, sono risultati inefficienti anche gli investimenti nel *re-skilling* del personale nell'utilizzare le nuove procedure e i nuovi *softwares*.
In particolar modo, dal monitoraggio sullo stato di avanzamento dei progetti di trasformazione digitale realizzato all'Agenzia Italiana delle Entrate risulta che le Pubbliche Amministrazioni che consentono l'accesso tramite Sistema Pubblico per l'Identità Digitale sono circa 4,4 mila (mentre i cittadini in possesso delle credenziali SPID che sono 8,5 milioni), a fronte dell'obiettivo che era stato prefissato entro la fine dell'anno precedente, che prevedeva 10 mila enti aderenti.
Anche il target che era stato prefissato per quanto riguarda le transazioni effettuate mediante il sistema PagoPA (la piattaforma digitale che consente ai cittadini di pagare in modo più naturale, veloce e moderno e che solleva le amministrazioni dai costi e dai ritardi dei metodi di incasso tradizionali[25]), non è stato raggiunto.
Miglioramenti evidenti invece ci sono stati nella pubblicazione degli *open data*, grazie agli obblighi legislativi; il DecretoLegge 170/2012 infatti, che ha modificato l'art.53 del Codice dell'Amministrazione Digitale, sancisce l'obbligo di aggiornare, divulgare e permettere la consultazione dei dati pubblici. Ad oggi le amministrazioni che pubblicano *open data* sono 507 a fronte di un obiettivo pari a 300, mentre i *dataset* pubblicati sono 33 mila a fronte di un obiettivo di 25 mila entro la fine dell'anno.
In termini numerici e metodologici, la Commissione Europea ha effettuato uno studio tramite la realizzazione dell'*Indice Sintetico di Digitalizzazione dell'Economia e della Società (DESI)*, ovvero uno strumento che permette di relazionare le differenti performance dei Paesi europei, tramite una gamma di elaboratori che associano a ciascun Paese un indice sintetico compreso tra 0 e 100, significante lo stato del livello di digitalizzazione del paese. In base ai risultati ottenuti sulla base di questo indice, dal rapporto della

[24] Fonte: Elaborazione Eures Ricerche Economiche e Sociali su dati Agenzia per l'Italia Digitale, Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021 *escluse le regioni
[25] https://www.pagopa.gov.it

Commissione Europea si evince che l'Italia si trova al venticinquesimo posto (su ventotto paesi) con un indice di digitalizzazione pari a 43,6, paragonato ad un punteggio medio di 52,6 ottenuto dagli altri paesi. Prendendo in considerazione esclusivamente un ramo dell'indice DESI, ovvero la digitalizzazione dei servizi pubblici, il nostro paese si colloca nella diciannovesima posizione con un punteggio di 67,5, su una media di 72 degli altri paesi[26].

Figure 1. Fonte: Elaborazioni Eures Ricerche Economiche e Sociali su dati Commissione Europea



Un altro fattore in cui l'Italia risulta carente è il coordinamento e la comunicazione tra le diverse amministrazioni pubbliche, infatti il Paese si trova al diciannovesimo posto con un punteggio di 48,3%, relazionato ad una media del 59,4% degli altri Paesi europei.

Decisamente migliore è il quadro internazionale. È possibile evincere da questo che il problema dell'Italia rispetto alla disponibilità dei servizi pubblici, sta proprio nel mancato completamento del ciclo, infatti il nostro Paese si trova dodicesimo in graduatoria con un valore leggermente superiore alla media, esattamente del 92,3% (rispetto alla media pari all'89,8%), per quanto riguarda la disponibilità del servizio digitale, il punto critico però risiede nella mancata traduzione dell'offerta nell'effettiva fruizione da parte dei cittadini.

Per quanto riguarda la percentuale di servizi di imprenditoria disponibili online e la quota di *opendata* accessibili dai portali delle Pubbliche Amministrazione, l'Italia si colloca al sesto posto con valori rispettivamente del 94,5% e 76,7%.

Recentemente, con l'approvazione della legge n. 120/2020, di conversione del Decreto Semplificazioni (DL 76/2020), ci sono state modifiche del Codice dell'amministrazione Digitale (d.lgs. 82/2005), inerenti sempre all'innovazione tecnologica del settore pubblico, e volte ad accelerare il passaggio dal cartaceo al digitale della pubblica amministrazione (PA).

Il focus del decreto è fondamentalmente su identità digitale, pagamenti elettronici nelle PA, notifiche telematiche, servizi online, e interoperabilità tra le banche dati della pubblica amministrazione.

[26] Claudio Gerino, "*E-government, Italia è agli ultimi posti in Europa*", (06/08/2020).

1.3.2 L'agenda digitale europea 2020 e le prospettive future

Il binomio cittadino-tecnologia risulta ormai inscindibile ed è da questo che bisogna partire per lo sviluppo della società e dell'economia.
Le azioni mirate a incrementare il processo di digitalizzazione, vedono gli albori in Europa già a partire dalla fine degli anni '80, quando è stato implementato il programma sulle tecnologie delle informazioni (ESPRIT), con la definizione dell'intervento comunitario nel settore delle telecomunicazioni.
Successivamente, negli anni 2000, è venuta sempre maggiore l'esigenza di stimolare gli investimenti e le innovazioni in ambito ICT, infatti l'Europa ha continuato a diffondere la cultura della tecnologia e in particolare dell'uso di internet, lo sviluppo di servizi per le imprese e la Pubblica Amministrazione in ottica digitale. Gli sforzi hanno avuto la loro piena manifestazione nel piano "Europa 2020 – Una strategia per una crescita intelligente, sostenibile e inclusiva" che pone tre pilastri su cui costruire la strategia europea in materia di trasformazione digitale:

- **Crescita intelligente**: strategia volta a sviluppare un'economia basata sulla conoscenza e sull'innovazione;
- **Crescita sostenibile**: strategia volta a sviluppare un'economia sostenibile e maggiormente efficiente nell'utilizzo delle risorse disponibili;
- **Crescita inclusiva**: strategia volta a sviluppare un'economia con un alto tasso di occupazione.

Questi pilastri hanno posto le basi per l'iniziativa "Agenda Digitale Europea", con lo scopo di creare un mercato digitale unico bastato su internet e applicazioni interoperabili, che permettano alla società di ottenere vantaggi economici sostenibili e al cittadino stesso di poter trarre il massimo beneficio dalle tecnologie digitali implementate. Sette sono le iniziative su cui è costruita è sviluppata Agenda Digitale Europea:

1. Mercato Unico Digitale
2. Interoperabilità e Standards
3. Fiducia e sicurezza
4. Accesso a Internet veloce e ultra-veloce
5. Ricerca e innovazione
6. Migliorare l'alfabetizzazione, le competenze e l'inclusione digitali
7. Vantaggi abilitati dalle ICT per la società dell'Unione Europea

Gli obiettivi che si pone il programma sono fondamentalmente tre:

- Rendere maggiormente fruibili i servizi online per privati e cittadini in tutta Europa;
- Creare infrastrutture e servizi protetti e affidabili che garantiscano un terreno fertile su cui sviluppare reti e servizi digitali;

- Aumentare gli investimenti in infrastrutture tecnologiche come le nuvole informatiche (*cloud computing*) e i megadati (*big data*), al fine di massimizzare il potenziale di crescita dell'economia digitale europea.

Riassumendo, possiamo dire che per l'attuazione degli obiettivi, assumono un'importanza fondamentale gli investimenti in ICT e nella comunicazione tra i sistemi e servizi delle PA; in particolare si cerca di favorire l'interoperabilità e lo sviluppo di standard comuni e uniformi per piattaforme aperte che possano orientare lo sviluppo di nuove tecnologie. Per sfruttare al meglio il potenziale delle tecnologie, favorendo progresso e innovazione, è stato creato un quadro normativo sostenuto dai rappresentanti dei capi di Stato e di Governo europei con la Dichiarazione di Tallin nel 2017 e ripresa dalla Commissione Europea in fase di avvio della definizione del quadro finanziario pluriennale post 2020 nella Comunicazione COM(2018) 987, che ha evidenziato uno scenario che prevede di raddoppiare gli investimenti nel settore digitale[27], e inoltre anche successivamente, la Commissione europea ha presentato una proposta di Regolamento per l'istituzione del Programma Europa Digitale, per gli anni 2021-2027, come elemento centrale nelle risposte della Commissione alla sfida della trasformazione digitale inserito nella proposta sul quadro finanziario pluriennale (QFP) 2021-2027. Il programma si sviluppa attorno agli utilizzi di tecnologie, come l'intelligenza artificiale o la cybersecurity, e lo sviluppo di competenze digitali avanzate che possano fornire ali servizi del settore pubblico maggiore interoperabilità ed efficienza e che possano contribuire a sviluppare un'economica dei dati, promuovere l'inclusione e garantire la creazione di valore.

L'Italia, per conseguire le finalità fissate dall'Agenda Digitale 2020, ha assegnato all'Agenzia per l'Italia Digitale (AgID) il ruolo di soggetto attuatore dell'Agenda e coordinatore e supervisore dei piani ICT nella Pubblica Amministrazione, anche attraverso la predisposizione di un Piano Triennale per l'informatica nella Pubblica Amministrazione, giunto alla sua seconda edizione per il triennio 2019-2021.

1.3.3 Il Piano triennale per l'informatica nella Pubblica amministrazione

L'Agenzia Italiana delle Entrate (AgID), ha pubblicato ad agosto il nuovo Piano Triennale per l'informatica nella Pubblica Amministrazione (2020-2022). Il Piano è lo strumento che viene utilizzato per orientare e stabilire le regole per promuovere la trasformazione digitale del Paese operando sulla Pubblica Amministrazione. Non è il primo tentativo di creare un'economia intelligente, sostenibile e solidale, già dal 2010 la Strategia Europa 2020 si pone ambiziosi obiettivi in tema di occupazione, innovazione, istruzione, integrazione sociale e clima/energia ed individua, all'interno di "un mercato digitale unico europeo" gli obiettivi per sviluppare l'economia e la cultura digitale in Europa, lasciando a tutti gli Stati membri il compito di definire le proprie priorità e strategie nazionali.

[27] COM(2018) 98: "Un quadro finanziario pluriennale nuovo e moderno per un'Unione europea in grado di realizzare efficientemente le sue priorità post-2020".

Le politiche dell'innovazione hanno tradizionalmente pensato a digitalizzare processi esistenti, mentre il digitale rappresenta una leva di trasformazione economica e sociale. A tal proposito, il Piano redatto dall'Agenzia per l'Italia Digitale è stato costruito facendo rifermento a quanto indicato nella Strategia per la crescita digitale, avendo come fine primario quello di indirizzare gli investimenti in ICT del settore pubblico secondo le linee guida del Governo e in coerenza con gli obiettivi e i programmi europei.
Si vanno a snellire i processi burocratici che hanno da sempre caratterizzato le amministrazioni pubbliche, garantendo una maggiore trasparenza dei processi amministrativi, una maggiore efficienza nell'erogazione dei servizi pubblici e la razionalizzazione della spesa informatica.

Il piano è suddiviso in tre parti: Piano triennale, componenti tecnologiche e la governance.
Come introduzione alla prima parte è stato posto un *executive summary*, utile a rilevare i principi guida che confermano la continuità con i Piani precedenti. In questa parte si ribadisce che la trasformazione digitale deve avvenire nel contesto di un mercato unico europeo di beni e servizi digitali. Per fare questo la strategia deve cercare di migliorare l'accesso online ai beni e servizi per i consumatori e le imprese, creando le condizioni per aumentare il potenziale di crescita dell'economia digitale europea. Per questo motivo gli obiettivi del Piano triennale sono basati sulle indicazioni che emergono dalla nuova programmazione europea 2021-2027, sui principi dell'eGovernment Action Plan 2016-2020 e sulle azioni previste dalla eGovernment Declaration di Tallinn (2017-2021), i cui indicatori misurano il livello di digitalizzazione in tutta l'UE e rilevano l'effettiva presenza e l'uso dei servizi digitali da parte dei cittadini e imprese.
Possiamo affermare che questa terza edizione del Piano, rappresenta il piano di attuazione, in quanto nella prima edizione (2017-2019) si soffermava sull'introduzione del modello strategico dell'informatica nella PA, mentre nella seconda edizione (2019-2021) si proponeva di dettagliare l'implementazione del modello. L'attuazione è responsabilità delle amministrazioni che anche quando si trovano di fronte obiettivi spesso ambiziosi li devono considerare sostenibili perché è con le stesse che ci si è confrontati nella redazione del Piano.
I requisiti strategici da soddisfare sono inquadrati nel documento *Strategia per la crescita digitale 2014-2020*, cui si deve fare riferimento anche per abilitare i progetti, le piattaforme e i programmi. I requisiti possono essere così sintetizzati[28]:

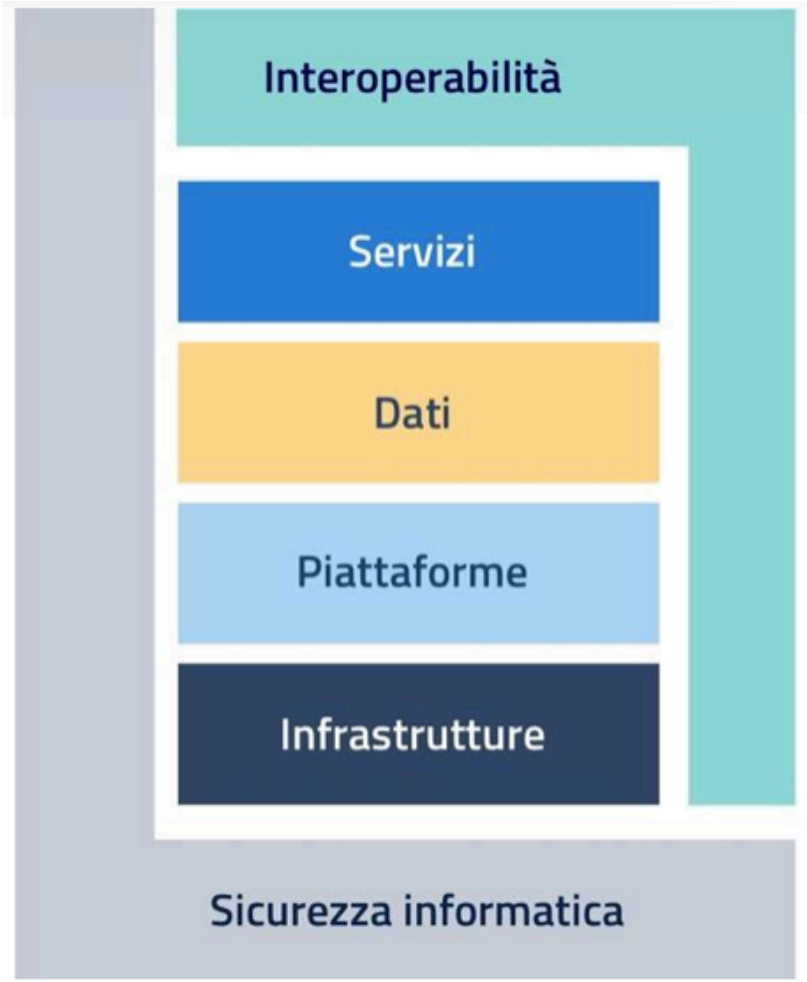
- Digital and mobile first (digitale e mobile come prima opzione): viene l'interesse primario delle pubbliche amministrazioni a realizzare servizi primariamente digitali;
- Digital Identity Only: le PA devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa;

[28] https://www.agid.gov.it/it/agenzia/piano-triennale

- Cloud first (cloud come prima opzione): le pubbliche amministrazioni devono adottare primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;
- Servizi inclusivi e accessibili: le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- 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;
- Interoperability by design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API (application programming interface);
- 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;

I piani precedenti si proponevano sempre come obiettivo il superamento dell'approccio storico adottato dalla Pubblica amministrazione, il cosiddetto approccio a "silos", favorendo un radicale ripensamento della strategia di progettazione, gestione ed erogazione dei servizi pubblici in rete, ponendo le basi sui principi che hanno determinato l'affermazione del modello di business della cosiddetta *API economy*. Questo avveniva attraverso la realizzazione di servizi digitali moderni, sempre disponibili sui dispositivi mobili, uniformando e razionalizzando le infrastrutture e i servizi informatici utilizzati dalla PA. Tali servizi dovevano poi essere costruiti con architetture sicure, scalabili, altamente affidabili e basate su interfacce applicative (API) chiaramente definite e che permettevano di creare interazioni favorendo il principio della sussidierietà.
Con l'attuazione del nuovo Piano, si rilevano almeno due concetti nuovi: il dato pubblico come bene comune e lo sviluppo di sistemi digitali in linea con le esigenze del lavoro agile.
Il Modello strategico può essere schematicamente rappresentato dalla mappa grafica illustrata in Figura sottostante (Fig.2). Tale rappresentazione è costituita da due livelli trasversali: l'interoperabilità e la sicurezza dei sistemi informativi e dei livelli verticali di servizi, dati, piattaforme ed infrastrutture.

Figure 2: Mappa del Modello strategico di evoluzione del sistema informativo della Pubblica Amministrazione[29]



In questa mappa sono raffigurate le macro-aree che richiamano gli elementi del Piano. È importante leggere la rappresentazione come un modello unico ed omogeneo e non disgregato come un modello architetturale a pila. Andiamo ad analizzare nel dettaglio le macro-aree identificate:

- **Servizi**: Con lo scopo di ottenere percorsi di innovazione omogenei, si è voluto mettere in comune le esperienze delle Pubblica Amministrazione, in particolare è stato previsto:
  - Incremento nell'utilizzo di soluzioni *Software as a Service* già esistenti;
  - Il riuso e la condivisione di software e competenze tra le diverse amministrazioni.
  - L'adozione di modelli e strumenti validati a disposizione di tutti;
  - Il costante monitoraggio da parte delle PA dei propri servizi on line.

  I servizi di digitalizzazioni si propongono di limitare l'afflusso di cittadini "a sportello" garantendo soluzioni remote almeno tramite SPID.
- **Dati**: come anche sottolineato dal Piano, il dato pubblico assume una rilevanza strategica nel nostro ambiente, caratterizzato dalla data economy. Infatti, il Piano evidenzia che: "*... è necessario ridefinire una nuova data governance coerente con la Strategia europea e con il quadro delineato dalla nuova*

[29] Agenzia Italiana delle Entrate

Direttiva europea sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico. È quindi opportuno individuare quanto prima le principali problematiche e sfide che l'attuale data governance del patrimonio informativo pubblico pone per delineare le motivazioni e gli obiettivi di una Strategia nazionale dati, anche in condivisione con i portatori di interesse pubblici e privati"[30].

Diviene di cruciale importanza il ruolo del dato e il suo utilizzo deve essere interscambiale tra le pubbliche amministrazioni stesse e tra pubbliche amministrazioni, cittadini e privati.

- **Piattaforme**: prima di tutto è utile interrogarsi su che cosa effettivamente è una piattaforma. Riprendendo la definizione di Parker et al., 2016, p. 5, "una piattaforma è un business basato sull'abilitazione di interazioni che creano valore tra produttori esterni e consumatori. La piattaforma fornisce una infrastruttura / architettura aperta e partecipativa per queste interazioni e ne definisce le condizioni di governance. Lo scopo della piattaforma è abbinare gli utenti e facilitare lo scambio di beni, servizi o valuta sociale, consentendo così la creazione di valore per tutti i partecipanti".

  Quindi bisogna pensare alla piattaforma come un'attività a più lati che interviene nel plasmare i mezzi e le possibilità di come due o più attori e risorse possono essere collegati e, naturalmente, trarne un profitto.

  Nel caso della pubblica amministrazione, lo scopo della piattaforma diventa quello di standardizzare i flussi operativi tra amministrazioni differenti. Esse dovrebbero essere abilitanti anche a livello territoriale ma anche favorire specifici servizi evolvendo specificamente verso di essi. Nel piano vengono identificate alcune piattaforme già esistenti (come SPID, pagoPA, ANPR, CIE, FSE, NoiPA ecc.) ed altre che sono una novità (come CUP integrati, Piattaforma IO, INAD, Piattaforma del Sistema Museale Nazionale). Per la gestione dei cosiddetti Big Data si riconferma la piattaforma digitale nazionale dati (PDND): che ha lo scopo di valorizzare il patrimonio informativo pubblico attraverso l'introduzione di tecniche moderne di analisi di grandi quantità di dati.
- **Infrastrutture**: le Infrastrutture sono una nota dolente per la PA, infatti alcune rilevazioni di AgID hanno evidenziato che molte infrastrutture risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo. Bisogna progettare le infrastrutture sul principio del cloud first, il cui utilizzo impone la disponibilità di capacità di rete adeguate ma anche la capacità delle pubbliche amministrazioni di gestire la migrazione applicativa dei data center e di garantire la protezione dei dati.
- **Interoperabilità**: l'interoperabilità è cruciale per l'attuazione del principio *once only*. Essa permette alle amministrazioni, cittadini e imprese di collaborare e interagire telematicamente. L'Italia ha recepito le indicazioni dell'*European Interoperability Framework*[31] che porta alla Linea guida sul

[30] COM/2020/66 final, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Una strategia europea per i dati", Bruxelles, 19.2.2020

[31] <https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf>.

Modello di Interoperabilità per la PA, che individua gli standard e le loro modalità di utilizzo per l'implementazione di interfacce software che favoriscono:

- l'aumento dell'interoperabilità tra PA e tra queste e cittadini e imprese;
- la qualità e la sicurezza delle soluzioni realizzate;
- la de-duplicazione e la co-creazione delle interfacce software.

- **Sicurezza informatica**: i servizi digitali della PA rappresentano un elemento cruciale per un corretto funzionamento di un Paese (si pensi per esempio alle manipolazioni a fini elettorali). In un contesto in cui il fenomeno della *data breach* (violazione dei dati) cresce sempre di più, la protezione del dato deve essere sempre garantita, ed infatti il Piano si focalizza sulla *Cyber Security Awareness*, poiché tale consapevolezza fa scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche.

La terza e ultima parte è dedicata alla governance, quindi assume una connotazione maggiormente politica. In particolare, si mette in luce il fine della trasformazione digitale, ovvero il miglioramento dell'efficienza e della qualità dei servizi pubblici.

1.4 Il cambiamento attraverso la dematerializzazione

La grande diffusione degli strumenti informatici e delle tecnologie ICT, nonché i benefici derivanti da questi, ha messo in crisi la gestione dei tradizionali documenti cartacei, facendo sorgere l'esigenza di digitalizzarli, ovvero di renderli documenti informatici. Infatti, grazie all'interconnessione dei computer, che consente uno scambio di dati veloce e fluido, è possibile trasferire qualsiasi documento da una parta all'altra del globo in pochissimi secondi. Sorgono inoltre vantaggi legati all'archiviazione, al reperimento e al trasferimento dei documenti.

A causa della loro caratteristica intrinseca e fondamentale dell'immaterialità, sono stati oggetti di numerosi dibatti circa il valore giuridico da attribuire al documento informatico e un possibile deterioramento. La paura più grande è relativa alla loro sicurezza. Il fatto che costituiscano entità immateriali, potenzialmente modificabili o eliminabili, farebbe pensare al cartaceo come la soluzione più sicura da adottare. Si potrebbe avere timore per esempio che questi vengano rubati da un pirata informatico o che il *database* dove questi sono collocati smetta di funzionare causando una perdita cospicua di dati. Altri dubbi sono legati alla certezza della provenienza dei documenti, e in particolare all'*accountability*, ovvero alla responsabilità, di chi li ha redatti. A tal proposito, è venuta a manifestarsi la necessità di stabilire nuove metodologie e strumenti che consentano la prova della manifestazione della volontà per via telematica.

Nonostante questi dubbi, la maggior parte della letteratura sostiene che il digitale sia la forma più sicura per conservare i documenti, superando le problematiche esposte precedentemente grazie alle moderne tecnologie

dell'informazione e della comunicazione, come ad esempio attraverso copie di sicurezza (c.d. copie di *backup*), utilizzo di *firewalls* e antivirus.

Giungiamo pertanto al punto cruciale del cambiamento della pubblica amministrazione, ovvero al raggiungimento della "dematerializzazione" dal documento cartaceo. La letteratura si è interrogata molto circa la definizione di "dematerializzazione", e riprendendo una definizione, possiamo affermare che con tale termine si "identifica la tendenza alla sostituzione della documentazione amministrativa solitamente cartacea in favore del documento informatico"[32].

Il problema è che la dematerializzazione è un processo articolato e complesso, che non si può ridurre alla semplice azione volta all'eliminazione dei supporti documentali cartacei. Bisogna infatti associare il concetto di dematerializzazione a quello di digitalizzazione, che nell'ambito documentale è intesa appunto come quel processo volto a ripensare processi e procedimenti dal cartaceo a un più efficiente contesto digitale. Seppur utilizzati l'uno come il sinonimo dell'altro, i due termini non hanno affatto lo stesso significato, basti pensare agli obiettivi di entrambi.

La dematerializzazione ha come fine ultimo la conversione di un documento cartaceo in un documento informatico (o elettronico), preservandone sia il relativo valore giuridico e probatorio, sia gli elementi afferenti al contesto archivistico di riferimento, ma anche la sostituzione e l'eliminazione dei documenti originali analogici dei quali si è prodotta una copia informatica avente il medesimo valore giuridico, probatorio e archivistico dei rispettivi originali.

I processi di digitalizzazione invece presuppongono alla base i documenti informatici, ma sono orientati alla "reingegnerizzazione" dei procedimenti e dei servizi offerti online, ovvero al ripensamento e alla riorganizzazione ti tali servizi.

Uno dei maggiori punti di criticità per l'attuazione di un effettivo processo di dematerializzazione e digitalizzazione della Pubblica Amministrazione, si riscontra nell'ingessante e complesso quadro normativo che disciplina tali processi. Infatti, il problema è che nonostante le numerose norme e modifiche, quella che manca è una strategia di lungo periodo che tenga conto non solo della componente legata agli aspetti tecnico-informatici delle soluzioni delineate, ma soprattutto dell'importanza e della complessità relativa agli aspetti giuridici e archivistici dei documenti e dei processi delle pubbliche amministrazioni.

In tema di dematerializzazione e digitalizzazione, il punto di riferimento è il Codice dell'Amministrazione digitale (D.Lgs. n. 82/2005), ingessato da norme e regole tecniche che necessitano di un ripensamento. Il Manifesto per l'innovazione digitale proposto all'interno del Gruppo di Lavoro per la Governance digitale delle associazioni ANORC e ANORC Professioni, ha evidenziato che "*occorre un testo recante pochi principi generali della materia, resi chiari e "autoconsistenti" di modo da fornire un saldo riferimento a cui attingere.*

[32] CNIPA (a cura del), *La dematerializzazione del documento amministrativo. Libro Bianco del Gruppo di Lavoro interministeriale per la dematerializzazione della documentazione tramite supporto digitale*, Roma, 2006, in http://www.cnipa.gov.it/site/_files/Libro%20BiancoDEM.pdf., .10.

Il Codice dell'Amministrazione Digitale nella sua attuale formulazione, appare martoriato da una sequenza di interventi normativi che non hanno fatto altro che rendere manifesta l'imperfezione del testo ab origine".
Tra le altre fonti da tenere in considerazione, ci sono il DPR 445/2000 (Testo Unico sulla documentazione amministrativa), e il Codice dei beni culturali, di cui al D.Lgs.n. 42/2004, senza contare tutte altre le norme che, in ogni caso devono essere applicate in prospettiva digitale nelle loro diverse finalità (ad esempio, la nota L. 241/90 sul procedimento amministrativo, il D.lgs. n. 196/2003 sulla protezione dei dati personali o il D.Lgs. n. 33/2013 sulla trasparenza, solo per citarne alcune).
Nonostante la complessità del quadro normativo, porre in essere un processo volto alla dematerializzazione dei documenti della pubblica amministrazione è possibile ed è stato già attuato da grandi realtà come per esempio dall'Automobile Club d'Italia. Il punto cruciale cui dedicare maggiore attenzione è appunto il cambiamento, del resto come affermava Nelson Mandela, "*il compito più difficile nella vita è quello di cambiare sé stessi*". Se si vuole operare una reale rivoluzione digitale bisogna partire da un cambiamento di consuetudini, di approcci e di metodi.

La spinta verso la dematerializzazione proviene dalla necessità di contenere i costi della spesa pubblica; in questo modo infatti, la Pubblica Amministrazione vedrebbe ridursi i costi relativi alla stampa, alla copia, all'invio e alla conservazione dei documenti, sia in termini di risorse umane che materiali.
Il nostro Paese è stato uno dei primi a provvedere alla regolamentazione del documento informatico, così come della firma digitale. Il 13 novembre 1999, la direttiva CE n. 93, ha complicato il quadro normativo facendo sorgere una distinzione tra "firma elettronica" e "firma elettronica avanzata". Successivamente è stato varato il "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (DPR 28 dicembre 2000, n. 445, noto anche come TUDA), poi modificato dal DLsl 23 gennaio 2002, n.10 ("Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche") e dal DPR 7 aprile 2003, n. 137 ("Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del DLgs 23 gennaio 2002, n.10").
In particolare, il ricorrere alle tecnologie più innovative per arrivare alla definitiva eliminazione della carta, ha trovato largo spazio con l'introduzione del CAD (Codice dell'amministrazione digitale) nel 2005 dove nell'art. 42 si fa esplicitamente riferimento al concetto di dematerializzazione. Art. 42: "*Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71."*[33]
Riassumendo quanto finora detto, possiamo affermare che gli obiettivi della dematerializzazione sono sostanzialmente due: si cerca di evitare lo spreco di carta, cercando di ridurre in maniera significativa la

[33] "Dematerializzazione, tutto su significato, normativa e obblighi per la PA", Agenda Digitale, (09/03/2018)

creazione di nuovi documenti cartacei e dall'altra parte si punta ad eliminare i documenti cartacei attualmente esistenti negli archivi, sostituendoli con opportune registrazioni informatiche.

Nel proseguo della tesi andremo ad approfondire il tema della dematerializzazione, andando a vedere come questa permetta alla rete di evolvere il proprio modo di operare per raggiungere i livelli di efficacia ed efficienza auspicati dalle strategie di *eGovernment*.

CAPITOLO SECONDO: DAL CARTACEO AL DIGITALE: LE SFIDE DEL CLOUD

2.1 La nascita del documento informatico

Siamo stati e siamo spettatori di una trasformazione rivoluzionaria che in poco più di un decennio ci ha permesso di transitare dal floppy disk al cd, e poi alla chiave USB e ad altri tipi di supporti portatili di memoria. L'esigenza di disporre di un supporto fisico per la produzione e conservazione di dati, documenti e informazioni, viene sempre meno grazie alla progressiva diffusione del cloud computing.

La frenetica evoluzione tecnologica è stata accompagnata dal proliferarsi di norme volte a regolamentare il nuovo modello informatizzato del "sistema impresa". Questo nuovo sistema sembrava però non essere accompagnato da una mentalità tale da supportarlo, in quanto il cittadino sembrava subire un'impostazione culturale consuetudinaria vincolata al supporto cartaceo, attribuendogli le caratteristiche di inalterabilità e autenticità.

Queste problematiche sono state affrontate nel corso degli anni grazie all'introduzione di leggi e normative volte a regolamentare il documento informatico. Infatti, con l'emanazione della legge n. 59 del 15 marzo 1997[34], il documento firmato con strumenti informatici e telematici inizia ad assumere rilevanza giuridica. Inoltre, le problematiche legate all'integrità e all'autenticazione dei documenti iniziano ad essere risolte dall'introduzione della firma digitale e dal riconoscimento giuridico del documento firmato elettronicamente. La norma ha subito diverse modifiche e integrazioni, soprattutto dopo il recepimento della disciplina europea, che seppur confermando il valore giuridico del documento informatico, ammette, in alcuni contesti, il valore e la veridicità di questo nonostante la sottoscrizione mediante la firma digitale. Infatti, il recepimento dell'impostazione comunitaria nella normativa nazionale, ha prodotto una disciplina che riconosce gradi diversi di validità ed efficacia probatoria del documento informatico a seconda che si ricorra alla sua sottoscrizione mediante firma elettronica o firma elettronica avanzata, di cui la firma elettronica e la firma elettronica qualificata è un esempio.

È necessario sviluppare sistemi multicanale per gestire la conservazione di documenti digitali ed è fondamentale tener conto delle caratteristiche peculiari di questi flussi informativi. Risultano essere in questo modo, più facilmente modificabili e più difficilmente riconducibili al loro autore e facilmente conservabili nel tempo. Bisogna pertanto adottare metodologie che siano a "norma" che consentano di garantire l'attribuibilità, l'integrità, l'autenticità, la sicurezza e la corretta archiviazione dei documenti elettronici.

2.2 Dematerializzazione e digitalizzazione

[34] Legge n. 59 del 15 marzo 1997, "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa".

Spesso i termini dematerializzazione e digitalizzazione sono due termini che vengono affiancati e confusi. Un documento digitale può nascere digitale o può diventare tale in fase di realizzazione o può essere frutto di un processo di dematerializzazione.

Il fine ultimo di entrambi i termini è certamente lo stesso, ovvero quello di ridurre sprechi di carta e agevolare le procedure amministrative, ma il significato è diverso.

In particolare, con il termine "dematerializzazione" si vuole intendere il "progressivo incremento della gestione documentale digitale, la conseguente sostituzione dei supporti tradizionali della documentazione amministrativa (sistema cartaceo) a favore del documento informatico in tutti gli ambiti aziendali"[35]. Questo implica un processo di trasformazione vero e proprio. Il documento cartaceo viene trasformato in documento digitale, utilizzando tecnologie e strumenti in grado di catturare immagini, come scanner, macchine fotografiche ma anche semplici smartphone.

Con "digitalizzazione" invece si intendono quei documenti già prodotti in formato digitale. Entrambi sono documenti informatici con la differenza che risiede nell'origine dei documenti, uno nasce cartaceo e uno ha bisogno di una trasformazione.

Se inizialmente la digitalizzazione dei documenti poteva rappresentare un vantaggio competitivo per istituzioni e aziende, al giorno d'oggi, è diventata un imperativo, nell'ottica di rendere un modello organizzativo più sostenibile e rispettoso dell'ambiente.

Una gestione aziendale più sostenibile inizia con la riduzione dell'utilizzo della carta dai processi lavorativi, per giungere a un processo irreversibile facendo si che i costi legati alla gestione dei documenti cartacei, possa invece essere destinata ad altri investimenti con un'adeguata gestione documenti in archivio cloud, per esempio.

Un approccio *paperless document*, seppure richieda di abbandonare le abitudini e le prassi che hanno accompagnato da sempre il processo aziendale, a lungo termine produrrà vantaggi notevoli, che vanno oltre a quelli che si ottengono in termini di costo. I più immediati possono essere identificati per esempio nei seguenti:

- **Accesso facilitato e da remoto**: l'accesso al documento digitale diviene più rapido e facilmente accessibile via web, da qualsiasi device e in qualsiasi momento.
- **Testo ricercabile**: attraverso la ricerca di una semplice parola è possibile giungere a documenti che riguardano un cliente in particolare o progetto. Questa semplificazione procura un vantaggio anche nella gestione del marketing, del controllo e della gestione del cliente in quanto la ricerca può trasformare file ordinari in potenziali database di informazioni.
- **Gestione più competitiva**: con la digitalizzazione dei documenti cartacei si ottiene una gestione più competitiva e dinamica che riduce l'errore umano e favorisce la condivisione dei file con annesse modifiche in tempo reale, soprattutto grazie a tecnologie cloud.

[35] "Dematerializzazione", < http://qualitapa.gov.it/sitoarcheologico/relazioni-con-i-cittadini/open-government/strumenti-della-pa-digitale/dematerializzazione/index.html>

- **Tracciabilità e rintracciabilità**: se la dematerializzazione favorisce la tracciabilità e la rintracciabilità costante dei dati, d'altra parte garantisce anche la riservatezza, la sicurezza e il valore giuridico dei file e delle informazioni archiviate.

Sia che il documento nasca digitale o lo diventi nel tempo, la gestione deve avvenire obbligatoriamente attraverso un archivio elettronico, che a sua volta richiede l'informatizzazione dei processi di caricamento, classificazione, archiviazione, interrogazione, consultazione, condivisione e riproduzione.
Esistono in tale ambito sistemi di archiviazione digitale on site e soluzioni in Cloud come ASP o SAAS, che consentono di memorizzare, archiviare, protocollare e conservare, organizzare, consultare ed esibire il documento.

2.3 IL CLOUD COMPUTING

2.3.1 Il Cloud Computing: definizione e caratteristiche

Il Cloud computing può essere interpretato non solo come una piattaforma abilitante per la trasformazione digitale, ma anche come un ecosistema che crea valore per l'impresa grazie alle numerose possibilità di interconnessione di strumenti.
Sono due le prospettive da cui è possibile trarre una definizione di Cloud: una tecnologica e una più commerciale.
Da un punto di vista tecnologico, il NIST (*National Institute for Standards and Technology*), definisce tale tecnologia come "*un modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi. Questo modello cloud è composto da cinque caratteristiche essenziali, tre modalità di servizio e quattro modelli di distribuzione*".
Da un punto di vista commerciale invece, si guarda al Cloud computing come artefice della minimizzazione complessiva dei costi della tecnologia: integrando diversi profili di domanda su risorse condivise, consente il raggiungimento di importanti economie di scala e l'erogazione agevole e flessibile dei servizi. Conseguenza diretta di questa flessibilità, è la riduzione del time-to-market della digitalizzazione, infatti il servizio Cloud permette di accedere ai servizi attraverso la rete, pagandoli direttamente al consumo.
È possibile identificare, per qualsiasi realtà, pubblica o privata, quattro principali vantaggi del Cloud Computing:

1. **Agilità e flessibilità**: il Cloud permette all'azienda di cogliere le future opportunità di business, rendendola aperta a qualsiasi tipo di cambiamento;

2. **Riduzione del time to market**: la costante evoluzione del Cloud e la possibilità di non occuparsi della gestione infrastrutturale, consente di stare al passo con il progresso tecnologico;
3. **Riduzione dei costi**: adottare servizi Cloud, in un'ottica di lungo termine, contribuisce alla riduzione dei costi di gestione delle infrastrutture, del personale dedicato e di eventuali problemi tecnologici relativi alla gestione delle attività.
4. **Sicurezza e affidabilità**: il Cloud presenta un modello più snello basato sul servizio e riduce il rischio di sovra-allocazione delle risorse.

Nell'ambito delle caratteristiche principali che contraddistinguono un cloud computing, se ne possono identificare cinque essenziali[36]:

1. *On-demand self-service*: in questo caso non vi è nessuna interazione tra il consumatore e il fornitore del servizio, il quale può essere direttamente richiesto e sfruttato dal cloud dal ciente, in base alle proprie necessità e in maniera automatica;
2. *A broad network access*: le funzionalità, i servizi e le applicazioni sono disponibili in rete e il cliente può accedervi da diverse piattaforme come telefoni cellulari, tablet, computer portatili o workstation;
3. *Resource pooling*: le risorse sono condivise per servire diversi clienti utilizzando il modello multi-tenant. C'è un senso di indipendenza dal luogo, in cui il cliente non ha alcun controllo o conoscenza sulla posizione esatta delle risorse assegnate ma può essere in grado di specificare la posizione ad un livello più elevato di astrazione (ad esempio, paese, stato o datacenter). Esempi di risorse includono conservazione e elaborazione di dati, memoria e larghezza di banda.
4. *Rapid elasticity*: le risorse vengono ridimensionate e aumentate in base alle esigenze, vi è la possibilità di scalare rapidamente verso l'alto e verso il basso in maniera commisurata alla domanda. Le funzionalità cloud possono essere fornite al cliente in modo rapido ed elastico, consentendo di aumentare o diminuire i servizi, in qualsiasi quantità e in qualsiasi momento.
5. *Measured service*: così come la scalabilità verso l'alto e verso il basso, anche il controllo dell'utilizzo delle risorse viene eseguito automaticamente e ottimizzando l'utilizzo delle risorse. In particolare, i sistemi cloud, sfruttano una misurazione della capability ad un certo livello di astrazione appropriato per il tipo di servizio (ad esempio, la conservazione, l'elaborazione, la larghezza di banda, e gli account utente attivi). L'utilizzo delle risorse può essere monitorato, controllato e segnalato, fornendo trasparenza sia lato fornitore che consumatore del servizio utilizzato.

Dal punto di vista dell'utente finale, le tre componenti principali del cloud computing sono:

[36] N. Dowlin, R. Gilad-Bachrach, and K. Laine, "*Manual for using homomorphic encryption for bioinformatics*" Proceedings of the IEEE, (2017)

1. *End-user*: è un software o un dispositivo che permette al consumatore di accedere ai servizi cloud forniti dal provider;
2. *Cloud Network*: è una rete che relaziona diversi dispositivi per connettere i clienti a un provider di cloud computing.
3. *Cloud Application Programming Interface (API)*: sono set di definizioni, istruzioni e protocolli con i quali vengono realizzati e integrati software applicativi.

2.3.2 L'architettura del Cloud Computing

Il sistema di cloud computing è caratterizzato da un'architettura contenente una rete (come raffigurato successivamente nella figura 6) che collega l'utente al fornitore di servizi. Questi ultimi differiscono per le caratteristiche degli elementi tecnologici che li compongono.
I tre principali modelli di fornitura di servizi cloud[37] sono:

1. **SaaS (Software as a Service)**: questo modello, è uno dei modelli di distribuzione più diffuso. Prevede un'offerta di applicazioni da parte del provider, gestite su un'infrastruttura cloud. Il cliente accede al servizio in modalità on-demand tramite tecnologie Internet, pagando una licenza in abbonamento con pagamento rispetto al consumo. Infatti, uno dei principali vantaggi di questo software, è che il cliente non deve preoccuparsi dei costi e della gestione associata all'installazione, gestione, supporto e licenza, ma può fruire del software in modalità trasparente rispetto all' infrastruttura sottostante e dispone solo di limitate possibilità di personalizzazione.
   Il modello delle applicazioni basate su SaaS rappresenta un'evoluzione dei tradizionali servizi ASP (*Application Service Provider*), in quanto è caratterizzato da un architettura software di tipo "multitenant", ovvero in grado di supportare più utenti contemporaneamente.
   Dal punto di vista infrastrutturale, il SaaS non richiede necessariamente l'utilizzo di un'infrastruttura Cloud, in quanto è possibile accedere alle applicazioni tramite Web. Viene da sé che anche per questo software la sicurezza del browser Web è fondamentale, infatti spesso si ricorre a alla sicurezza dei servizi Web (WS), crittografia XML (Extendable Markup Language), Secure Socket Layer (SSL) e opzioni disponibili utilizzate per applicare la protezione dei dati trasmessi su Internet.

[37] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "*What's Inside the Cloud? An Architectural Map of the Cloud Landscape*" IEEE Xplore, pp 23-31, Jun. 2009

Figure 3

2. **PaaS (Platform as a Service)**: Platform-as-a-Service (PaaS) è un modello a piattaforma in cui il provider offre all'utente, piattaforme pre-configurate ottimizzate per lo sviluppo di applicazioni custom. Il cliente quindi può gestire, eseguire e sviluppare nuove applicazioni o servizi senza venire a contatto con l'infrastruttura sottostante, che viene gestita in modo trasparente dal service provider. Non è necessario acquistare alcun software ma è necessario pagare solo per il tempo che utilizza.
   Le soluzioni PaaS vincolano il cliente alle tecnologie e alla piattaforma predisposta dal fornitore, a sua volta costituita da soluzioni proprietarie che limitano la possibilità di migrazione ad altri fornitori.
   In questo servizio, è necessario porre un'attenzione maggiore alle macchine virtuali, che fungono da catalizzatore. Queste devono essere periodicamente sottoposte a controllo per evitare che vengano attaccate da virus, come il malware cloud.

Figure 4

3. **IaaS (Infrastrucutre as a Service)**: con questo servizio il provider offre all'utente risorse di calcolo sulle quali installare e gestire autonomamente le proprie applicazioni. È la categoria di servizi più essenziali in quanto le risorse vengono condivise solo con i clienti a contratto a una tariffa *pay-per-use*. In altre parole, con questa soluzione, il cliente affitta l'infrastruttura IT, come server, sistemi operativi o macchine virtuali con pagamento in base alle esigenze.

   È un servizio che permette di ridurre un ingente investimento in infrastrutture IT e di avere una flessibilità finanziaria e funzionale maggiore rispetto a un data center interno o con un servizio di collocazione, in quanto le risorse potranno essere aggiunte o rilasciate più economicamente e rapidamente. Inoltre, IaaS permette all'utente di utilizzare l'infrastruttura senza preoccuparsi dei problemi sottostanti.

   Questo tipo di servizio, dati i vantaggi enunciati, se da un lato potrebbe rappresentare un valore vincente per una realtà aziendale, dall'altro fornisce solo un livello di sicurezza di base.

Figure 5

Come illustrato dalla figura 6, la rete, la piattaforma, l'archiviazione e i software sono forniti come servizi che aumentano o diminuiscono a seconda della domanda. In particolare, il modello di cloud computing ha tre modelli di distribuzione principali che sono:

1. **Cloud Privato**: in questo tipo di modello, l'infrastruttura rimane di proprietà esclusiva dell'organizzazione. Spesso viene disposto all'interno del data center dell'impresa stessa e quindi gestito dal personale interno. Dal punto di vista gestionale, è anche possibile identificare due tipi di Private Cloud: il Managed Private Cloud, quando la gestione viene affidata a un fornitore esterno e gli asset fisici rimangono di proprietà dell'azienda, e l'Hosted Private Cloud, in cui sia le infrastrutture che la gestione vengono affidate al fornitore terzo[38].

   A differenza di un Cloud pubblico, il livello di sicurezza garantito dal Cloud Privato è maggiore, in quanto solo l'organizzazione e le parti interessate designate possono avere l'accesso per operare.
2. **Cloud Pubblico**: L'infrastruttura è di proprietà del service provider che eroga servizi disponibili al pubblico attraverso Internet su risorse condivise da più utenti.

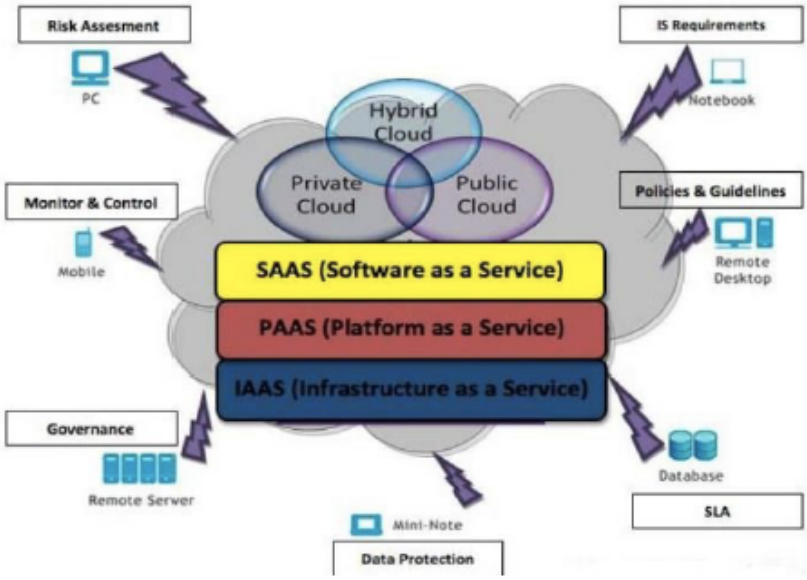
   Gli investimenti infrastrutturali sono interamente sostenuti dal fornitore, mentre il cliente paga a consumo solamente per i servizi effettivamente fruiti[39].
3. **Community Cloud**: è un modello che prevede la condivisione e la gestione dell'infrastruttura tra diverse organizzazioni, che assumono la forma di un consorzio. Sono le stesse organizzazioni a gestire i costi legati agli investimenti per l'implementazione del modello, mentre per quanto riguarda la gestione, come nel Cloud Privato, questa può essere interna, Hosted o Managed.

[38] S. Arnold, "*Cloud computing and the issue of privacy*", KM World, pp14-22, (2009, Jul.)
[39] A Platform Computing Whitepaper. "*Enterprise Cloud Computing: Transforming IT*", Platform Computing, pp6, (2010)

Il vantaggio principale di questo modello è che i costi possono essere ripartiti, infatti più di un'organizzazione può accedere a infrastrutture, risorse, strutture e servizi cloud, ma perché questo avvenga è necessario che il consorzio condivida la stessa mission[40].

4. **Cloud Ibrido**: Il cloud ibrido, così come preannuncia il nome, combina due e più tipi di cloud. In particolare, ci si riferisce a un Cloud privato collegato a uno o più servizi cloud esterni. Questo tipo di modulo è una combinazione di cloud privato, pubblico e comunitario e garantisce una sicurezza maggiore sul controllo dei dati e delle applicazioni, questo perché varie parti possono accedere alle informazioni detenute. Ha anche un'architettura aperta che consente interfacce con altri sistemi di gestione.

Figure 6



2.3.3 Il Cloud Computing: la sfida della sicurezza

Come abbiamo potuto notare, il Cloud Computing ha costituito una vera e propria trasformazione digitale per la maggior parte dell'attività delle imprese, in particolar modo agevolando la gestione dell'accesso alle applicazioni software online, l'archiviazione dei dati e la potenza di elaborazione.

I modelli di distribuzione dei servizi analizzati, hanno messo in luce come un'organizzazione, pubblica o privata che sia, possa aumentare i propri livelli di efficienza in modo dinamico, senza investire in nuove infrastrutture, formare nuovo personale o concedere in licenza un nuovo software.

Nonostante sia in continua evoluzione, il Cloud computing desta diverse preoccupazioni. Basti pensare a quante informazioni, risorse e dati relative a individui circolano nel cloud aziendale e a come la sicurezza diventi un tema di fondamentale importanza. Infatti, se da un lato la sicurezza potrebbe raggiungere un livello

[40] Global Netoptex Incorporated. "*Demystifying the cloud. Important opportunities, crucial choices*", pp4-14

superiore grazie alla centralizzazione dei dati e alle maggiori risorse usate, d'altra parte la perdita di controllo su dati sensibili desta diverse preoccupazioni nell'adottare tale tecnologia.
I problemi di sicurezza nel cloud computing hanno svolto un ruolo importante nel rallentarne l'accettazione, infatti la sicurezza si è classificata al primo posto come la più grande sfida del cloud computing, come illustrato nella figura sottostante.

Figure 7: Fonte: IDC Survey Ranking Security Challenge

In generale, possiamo concentrare il tema della sicurezza informativa su sette requisiti fondamentali:

1. **Disponibilità**: l'accessibilità degli utenti deve avvenire in qualsiasi momento e da qualsiasi luogo. Ci sono tre principali minacce alla disponibilità: la disponibilità del provider di servizi cloud, l'attacco basato sulla rete e backup dei dati salvati da parte del provider di servizi cloud;
2. **Riservatezza**: le informazioni devono essere accessibili solo ed esclusivamente agli utenti autorizzati ad accedervi;
3. **Integrità dei dati**: esclusivamente gli utenti autorizzati possono eseguire la modifica dei dati, le informazioni devono essere corrette e non manipolabili da chi non è autorizzato a farlo, né modificate in modo inaspettato a causa di errori o problemi nel software;
4. **Rimanenza dei dati**: nel caso di rimozione dei dati, è necessaria una particolare attenzione per evitare di divulgare le informazioni a una terza parte non autorizzata a recepirle;
5. **Gestione degli accessi**: bisogna verificare costantemente chi può accedere ai sistemi contenenti dati e informazioni strategiche;
6. **Audit**: il sistema richiede un sistema di controllo efficace per la protezione dei dati;
7. **Controllo**: il provider di cloud computing imposta strategie e regolamenti per organizzare l'utilizzo di applicazioni, servizi, risorse e così via.

Per comprendere al meglio il tema della sicurezza, in particolar modo i problemi e le sfide che da essa derivano, un aspetto su cui è opportuno focalizzare l'attenzione, è la relazione e la dipendenza tra i tre principali modelli di fornitura di servizi cloud citati precedentemente (SaaS, IaaS e Paas).

Questi tre servizi sono caratterizzati dalla cumulabilità, ovvero un virus o un attacco sullo strato Iaas, avrà un'influenza anche sui due livelli precedenti (SaaS e Paas)[41].

Per ogni modello, la sfida della sicurezza è diversa.

Il modello Saas è quello di cui il cliente si fida di meno, in quanto il controllo sulla sicurezza è nettamente inferiore rispetto agli altri due modelli. In questo modello, infatti, la responsabilità di renderlo sicuro spetta al fornitore del servizio.

Nel modello Paas, come detto precedentemente, entra in gioco sia la figura del provider, che offre il servizio, sia quella del cliente, che ha la possibilità di progettare la sua applicazione sulla piattaforma offerta. Di conseguenza, il livello di sicurezza su questo modello è duplice, riguardante entrambe la sicurezza dell'applicazione generata dal cliente e quella della piattaforma stessa. Ci sono delle questioni che rimangono irrisolte con questo modello, come ad esempio la sicurezza dei dati e quella dell'infrastruttura e dei servizi di parti terze.

Un livello di sicurezza maggiore può essere raggiunto con il modello Iaas, dove l'autonomia del cliente è tale da assumere il totale controllo sulla sicurezza come la configurazione dell'organizzazione, l'infrastruttura di controllo e la sicurezza della policy.

L'affidabilità dei modelli può essere aumentata anche grazie ad alcune tecniche di rete che diminuiscono la probabilità di ricevere attacchi che vadano a minare la sicurezza. Specificatamente, è possibile classificare[42]:

- ***Hyper Visor Attack***: consente a due o più sistemi operativi di utilizzare lo stesso hardware della piattaforma. Il rischio sistemico aumenta in quanto minacce che si verificano sul sistema operativo guest potrebbero manifestarsi anche per il sistema operativo host;
- ***Denial of Services***: questo sistema non permette ai clienti autorizzati di accedere ai propri dati e alle proprie informazioni online. Inoltre, a fronte di un numero alto di richieste da parte dell'attaccante, il sistema di blocca impedendo l'accesso anche a coloro che sono autorizzati;
- ***Sniffer Attacks***: gli *sniffer* sono programmi o dispositivi hardware in grado di spiare l'utente e tutte le sue attività in Internet. Gli hacker possono eseguire lo "sniffing" del traffico, registrando e analizzando ogni attività e dati sensibili come nome utente, password, dettagli delle carte di credito e altre informazioni private. È fondamentale in questo caso trasferire dati attraverso pacchetti crittografati.
- ***Reused IP addresses***: L'Internet Protocol Address, o "indirizzo IP", rappresenta l'indirizzo chiaramente unico e identificabile di un dispositivo (ad esempio computer, server web, stampanti) in

[41] E. Mathisen, "*Security challenges and solutions in cloud computing*", in 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011).

[42] V. Ashktorab, and R. T. Seyed, "*Security threats and countermeasures in cloud computing*", International Journal of Application or Innovation in Engineering & Management (IJAIEM) vol. 1, (2012)

una rete interna o esterna. Ogni indirizzo IP, appartenendo ad un unico utente, rappresenta la base per una trasmissione corretta delle informazioni dal mittente al destinatario. Gli indirizzi sono costituiti da una parte di rete (per l'individuazione del percorso nel routing IP) e una parte dell'host (per l'inoltro a un computer specifico). Quando un dispositivo invia un pacchetto di dati o informazioni, affinché vi sia uno scambio, necessariamente il router corrispondente deve orientarsi sul cosiddetto *header IP* e confrontare l'IP di origine con l'IP di destinazione. Nel caso di mancato abbinamento, il router (il servizio postale di Internet) contatta il *Domain Name System* (DNS), che ha la possibilità di risalire al nome apparente a quell'indirizzo IP e viceversa.

Il rischio di questo sistema deriva dal fatto che se un utente esce dalla rete, il suo indirizzo IP verrà ceduto a un altro utente, ma poiché spesso di verificano ritardi tra la modifica di un indirizzo IP in DNS e la cancellazione di quell'indirizzo nelle cache DNS, il vecchio indirizzo IP può ancora accedere ai dati, violando così la privacy dell'utente precedente.

- ***Google Hacking Attack***: alcuni motori di ricerca, come "Google", vengono utilizzati dagli hacker per scovare i punti deboli di un sistema che vogliono hackerare. Esistono due tipi di vulnerabilità riscontrate su Internet: configurazioni mancanti e vulnerabilità del software.

Anche l'ambiente in cui sono conservati i sistemi cloud influisce sulla loro sicurezza, per tre motivi principali:

1. Trasferire i dati attraverso i confini dei paesi;
2. Varie località e fornitori di servizi;
3. Raccolta dati e miscelazione.

2.3.4 Metodi e algoritmi per la sicurezza del cloud

Esistono diversi metodi e algoritmi studiati per incrementare la sicurezza nell'ambiente cloud. Alcuni dei quali sono gli Strumenti di Sicurezza Cloud, l'uso di un codice telefonico monouso (OTP), la Sicurezza del Software e la Sicurezza fisica. Vediamoli nel dettaglio uno ad uno.

- **Strumenti di Sicurezza Cloud**: gli strumenti che vengono utilizzati dal Cloud per impedire l'accesso non autorizzato ai dati del cliente, possono essere i seguenti[43]:
  - *Silver Sky*: è una soluzione che mette in sicurezza la posta elettronica e la rete, fornendo il controllo e il monitoraggio di questa;
  - *DocTracker*: garantisce la sicurezza del trasferimento dei documenti sul cloud grazie alla possibilità di tracciare, seguire e controllare un documento inviato.

[43] S. Kuila, S. Shruthi, P. Chandan, and N. Ch SN Iyengar, "*Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management*", Journal of Computer and Mathematical Sciences vol. 7, (2016)

- *Proof point*: consente di rilevare in tempi rapidi la presenza di spam tramite e-mail, permettendo di bloccarli in modo da garantireo la protezione di dati in entrata e in uscita.
- *Qualys*: offre sicurezza delle applicazioni Web, gestione delle vulnerabilità, gestione della sicurezza delle app, gestione dell'accesso al Web.
- *White Hat*: offre un alto livello di protezione del sito Web durante il processo di codifica.
- *Valuation*: tutti i dati trasferiti dalla rete devono essere crittografati; questo strumento fornisce la crittografia dei dati con il metodo AES.

- **Utilizzo della password mobile one-time (OTP)**[44]: il codice OTP è una password usa e getta composta un codice alfanumerico, generato automaticamente da un algoritmo e inviata all'utente tramite canali come e-mail, SMS, app su smartphone etc. Il vantaggio del codice rispetto a una password tradizionale, è che quest'ultima è molto più vulnerabile e facilmente hackerabile. Una password usa e getta invece, non può essere riutilizzata né per l'accesso al servizio, né per un'eventuale transazione.

  L'accesso e l'identificazione dell'utente tramite OTP è molto diffuso nei processi di registrazione e autenticazione, nei processi di firma digitale, nei processi di acquisto on line, nei siti web che prevedono l'accesso a dati sensibili e privati. Tre tecniche più popolari per generare un codice OTP si ricordano le seguenti:
  - Sincronizzazione dell'ora: affinché il codice OTP sia generato, il server e l'utente devono essere sincronizzati utilizzando orologi sincroni;
  - Sincronizzazione degli eventi: con questa tecnica, gli OTP sono caratterizzati da un pulsante da premere quando si desidera ricevere una nuova password. Una volta visualizzata la nuova password, il valore del contatore interno al token viene aumentato di uno, e lo stesso per il server: ogni volta che un'autenticazione avviene con successo, incrementa il proprio valore del contatore, sempre di un'unità. Tale sincronizzazione permette di generare la stessa password.
  - Tecnica di risposta alla sfida asincrona: con questa tecnica, il server fornirà una sfida al cliente, che sarà unica ogni volta in modo da impedire azioni di hacking.
- **Sicurezza del software**: la sicurezza di un software open-source, al quale possono accedere tutti, sia persone che sviluppatori, aumenta il rischio di hackeraggio. Pertanto, esistono a tal proposito tecniche come[45]:
  - Virtualizzazione: utilizzando questa tecnica, è possibile astrarre componenti hardware e software, creando un ambiente di elaborazione virtuale rispetto a un ambiente fisico;

[44] S. Kuila, S. Shruthi, P. Chandan, and N. Ch SN Iyengar, "*Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management*", Journal of Computer and Mathematical Sciences vol. 7., (2016)
[45] K. K. Chauhan, A. Sanger, and A. Verma, "*Homomorphic Encryption for Data Security in Cloud*", IEEE, pp. 206-209, (2015)

- Sistema operativo host: questo sistema deve essere sicuro, facile da aggiornare e costantemente monitorato, in quanto l'accesso a questo sistema operativo da parte di un agente non autorizzato, permette di accedere anche a tutti gli altri sistemi operativi sul computer.
- Sistema operativo ospite: alcuni sistemi operativi permettono al cliente di modificare, creare, aggiornare o eliminare il proprio server virtuale. Il cliente quindi, deve essere necessariamente responsabile di aggiornare l'ultima versione del sistema operativo, dei servizi e dei prodotti.
- Crittografia dei dati: si utilizza per tenere al sicuro i dati.

2.3.5 Il valore del mercato Cloud in Italia

Il mercato Cloud sta raggiungendo una fase di maturità anche in Italia, diventando una scelta strategica e dominante per una grande parte delle imprese, ancora però poco consapevoli delle implicazioni strategiche e organizzative che la stessa adozione del Cloud può innestare.

Analizzando il trend evolutivo degli ultimi tre anni, dal 2018 fino ad oggi, è possibile affermare che il tasso di crescita dell'adozione di servizi Cloud da parte delle imprese è in costante crescita. Nel 2018 il mercato Cloud italiano valeva 2,34 Miliardi, fino a crescere del 18% a 2,77 miliardi nel 2019. La pandemia Covid-19 è stato il fattore scatenante per implementare nuove strategie online, portando al 42% l'adozione del Cloud nelle PMI.

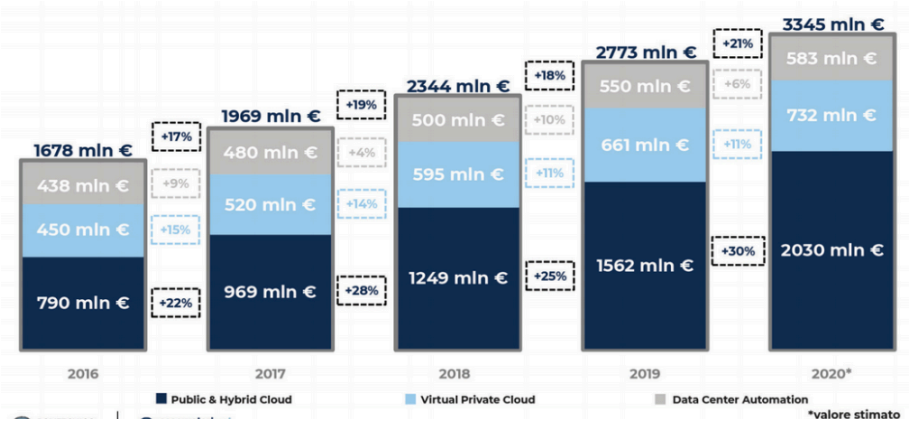
A guidare l'adozione del Cloud in Italia, sono stati soprattutto i servizi Saas, che nel 2020 hanno costituito la metà del volume di spesa complessivo nel Cloud Privato e Ibrido (oltre 1 Miliardo di Euro di spesa complessiva, +46% rispetto al 2019)[46].

Come quanto dichiarato da Alessandro Piva, direttore dell'Osservatorio Cloud Transformation, "*L'emergenza sanitaria ha creato una situazione senza precedenti, che ha richiesto un cambio di passo: le imprese sono state all'improvviso costrette a lavorare in modo agile, rendendo il Cloud il miglior alleato per rispondere rapidamente alle esigenze di collaborazione, gestione progettuale e valutazione delle performance"*. Da quella che è stata un'esigenza per la sopravvivenza del business, oggi rappresenta una vera e propria strategia. La sfida per le imprese è quella di seguire un percorso effettivo di trasformazione.

Il Cloud privato e quello pubblico, rispetto a un valore di 1,56 miliardi e a un tasso di crescita del 25% dell'anno precedente, raggiunge un valore di 2 miliardi di euro con un tasso di crescita del 30%; un'accelerazione chiaramente più rapida rispetto alla media internazionale, che segnale un +8% per un mercato che vale 198 Miliardi di dollari a livello globale[47].

[46] "*Cloud Transformation: gli ingredienti mancanti*", Osservatorio Cloud Transformation (Ottobre 2019)
[47] Fonte: Gartner, (Luglio 2020).

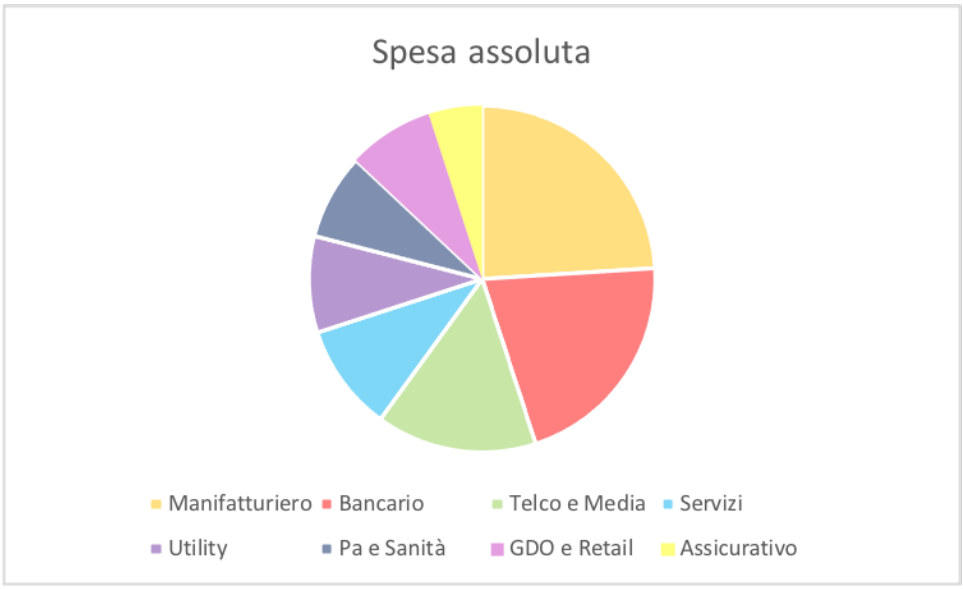
Figure 8: Fonte: Osservatori.net



Il *Virtual & Hosted Private Cloud*, ovvero le infrastrutture presso fornitori esterni, aumenta nel 2020 fino a 732 Milioni di euro, con una dinamica del +11%.
Contrariamente, l'automazione e la modernizzazione dei datacenter, rallenta con un tasso del 6% fino ad arrivare a 583 Milioni di Euro, rispetto al 2019 in cui si era registrato un tasso del 10% con un valore di 550 milioni di Euro.

Come possiamo notare dal grafico sottostante, il settore manifatturiero si conferma al primo posto nel mix di spesa con il 24% del mercato complessivo, seguito dal settore Bancario (21%), Telco e Media (15%), i Servizi (10%), Utility (9%), PA e Sanità (8%), GDO e Retail (8%) e Assicurativo (5%).

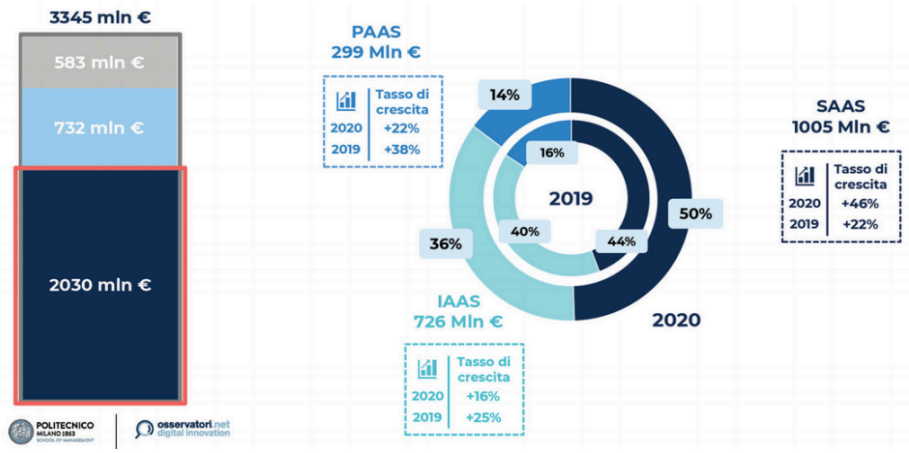
Figure 9: Fonte di rielaborazione propria



A seguire, anche l'infrastruttura dei servizi Iaas cresce del 16% rappresentando il 36% della spesa complessiva, con un forte impulso delle Virtual Machine per ambienti di produzione e del Container Management.; infine, il trend dell'aumento delle attività online, e quindi dei dati generati e della necessità di

trasferirli tra unità di business diverse, nonché tra aziende diverse, ha fatto crescere anche l'adozione de i servizi Paas, con un tasso di crescita del 22%, raggiungendo il 14% del mix.

Figure 10: Fonte: Osservatori.net



A tal proposito, la ricerca dell'Osservatorio ha messo in luce come rispetto al 2019, ci sono stati due trend in costante evoluzione: quello dell'intelligenze del dato, ovvero tutti i servizi IaaS, PaaS e SaaS dedicati alla gestione, alla manipolazione e all'analisi dei dati, che conta un valore di circa 352 Milioni di Euro (una crescita del +24% rispetto all'anno precedente) e quello dell'Edge computing & Orchestration, che seppur subendo un rallentamento, sono rimasti in costante crescita raggiungendo un valore di 45 Milioni di Euro.

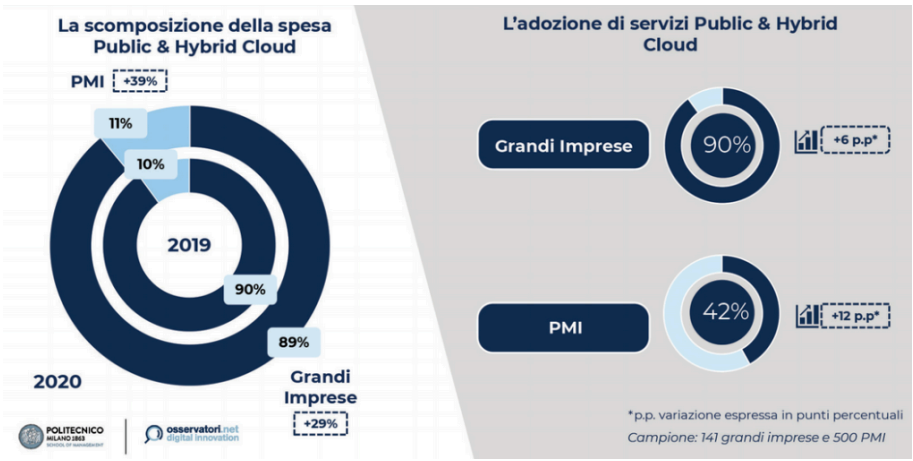
In un momento in cui le tematiche ambientali diventano centrali e urgenti anche nelle agende dell'ONU e dell'Unione Europea, il Cloud si rivela tecnologia abilitante per lo sviluppo della sostenibilità ambientale. Infatti, il Cloud ha determinato un impatto molto rilevante nel 93% dei casi, insieme anche alla Cybersecuirty e ai Big Data Analytics e con percentuali inferiori anche con il 5G (41%) e l'Edge Computing (34%).
Seppur la risposta all'emergenza COVID-19 ha fatto sì che le aziende incrementassero i servizi online, dalla ricerca dell'Osservatorio Cloud Transformation emerge come il fattore umano sia indispensabile nell'abilitazione della tecnologia. Si richiede un cambiamento organizzativo che, partendo dalle basi e dalle innovazioni del comparto IT delle aziende, si estende a tutto il resto dell'organizzazione. Il personale deve essere educato ad una nuova metodologia e rendere un concetto che per anni è sembrato teorico e astratto, un qualcosa di concreto ed effettivamente efficace a lungo termine, per evitare che il paese faccia un passo indietro rispetto a quanto conseguito nel 2020. Le competenze sul Cloud dei lavoratori sono assai scarse, e questo alimenta all'interno delle PMI un tendenziale timore nell'adozione di servizi Cloud, a causa di un gap culturale e infrastrutturale. Infatti, nonostante il 55% delle PMI utilizzi sistemi Cloud, preferisce la gestione internalizzata delle tecnologie, anche per il fattore sicurezza legato all'importanza dei dati e delle informazioni sensibili.

Come raffigurato nella figura 11, l'evoluzione della gestione dei sistemi informativi aziendali, si affaccia a un bivio. Nel 43% delle grandi imprese, i nuovi progetti nascono nel Cloud come una scelta obbligata nel 13% dei casi e preferenziale nel 30%. La maggior parte delle aziende, circa il 48%, è orientata ad un approccio selettivo, scegliendo il modello di sourcing a seconda delle circostanze e del contesto. Solo una piccola parte (il 9%) delle imprese sceglie di conservare tutti i loro dati e avere il pieno controllo di ciò che accade loro, attuando una strategia cosiddetta "*on-premises*".

D'altra parte, la migrazione verso i modelli Cloud è sempre più forte e in costante evoluzione. L'11% delle grandi imprese detiene i propri datacenter in Cloud privati o pubblici, e un ulteriore 27% prevede di adottare questa strategia nei prossimi anni.

Sostanzialmente, il sistema informativo verso il quale si sta dirigendo la maggior parte delle imprese è una configurazione ibrida, ovvero che prevede l'integrazione di servizi esterni Iaas, PaaS e SaaS a servizi interni, quindi una parte del legacy migrerà in Cloud e la restante resterà on-premises. Infatti, il 50% delle imprese è in procinto di adottare un sistema ibrido, e solo il 12% attuerà invece una strategia completamente on-premises.

Figure 11: Fonte: Osservatori.net



Guardando alcuni numeri, la scelta dell'Hybrid Cloud, nel 54% dei casi deriva da una visione strategica di lungo periodo volta a massimizzare i benefici delle due modalità di erogazione delle tecnologie; per il 46% restante invece, risulta da decisioni prese nel passare degli anni per cause contingenti.

Nelle aziende taliane, in media, si registra la presenza di circa quattro Cloud provider attivi, in linea con quanto registrato a livello internazionale[48]. Si contano generalmente tre provider Saas, anche se, oltre a sistemi ibridi, in Italia si registrano anche casi di Multi Cloud, che prevedono la presenza del deployment di più cloud dello stesso tipo (pubblico o privato) offerti da diversi fornitori, per i servizi IaaS e Paas.

[48] Fonte: Flexera, State of the Cloud Report, (2020)

Il freno principale all'adozione di strategie Multi Cloud è legato alle sfide circa la complessità che genera. Infatti, questo implica gestire diversi set di strumenti, piattaforme, approcci alla sicurezza, silos operativi e carichi di lavoro/applicazioni con scarsa mobilità. Inoltre, per pianificare, progettare, configurare, erogare e gestire le risorse IT nel cloud è necessario sviluppare competenze verticali su tecnologie diverse. Molte organizzazioni hanno difficoltà a trovare o mantenere tali competenze, causando problemi che a loro volta influiscono negativamente sulle prestazioni e causano interruzioni.

2.3.6 Il Cloud nella PA italiana: stato dell'arte e prospettive

Il Cloud, come abbiamo potuto finora constatare, permette di semplificare la gestione dei sistemi informativi trasformando le infrastrutture fisiche in servizi virtuali. Nel campo della Pubblica Amministrazione italiana, l'introduzione di tale paradigma consente di ottenere diversi vantaggi, tra cui un'elevata sicurezza informatica ad un costo nettamente inferiore rispetto alle infrastrutture fisiche, aumentando notevolmente l'affidabilità delle infrastrutture IT e facilitando così il rinnovamento complessivo dei servizi IT.
Clayton Christensen e Joseph Bower, nel 1995, con la pubblicazione del loro articolo sull'Harvard Business Review, "*Disruptive technologies: catching the wave*" hanno definito per la prima volta il concetto di "*disruptive innovation*", facendo riferimento a tutte quelle innovazioni in grado di stravolgere modello di business preesistente ridefinendo i confini dell'arena competitiva e stravolgendo il modo in cui i consumatori sono abituati a utilizzare prodotti e servizi.
Nell'ambito di questa rivoluzione digitale, il Cloud favorisce un cambiamento notevole volto a eliminare il sistema burocratico tipico delle Pubbliche Amministrazioni. In particolare, in termini di:

- Elasticità reale
- Facilità degli aggiornamenti
- Riduzione delle attività manuali a basso valore aggiunto
- Riduzione complessità del supporto
- Riduzione dei costi

Questi benefici vengono considerati se la strategia di implementazione segue sei regole definite:

1. Capire perché il Cloud è differente e può svolgere un ruolo positivo;
2. Progettare il processo di migrazione a servizi IT rendendo partecipi le persone interne;
3. Individuare il "*cloud deployment model*" più adeguato[49];
4. Sviluppare la concezione di Sicurezza come una responsabilità condivisa;
5. Definire un piano di policy per la "Cloud governance"[50];
6. Individuare requisiti per i fornitori orientati a sfruttare al massimo il modello Cloud adottato.

[49] ISO 17788 – clausola 6.5
[50] ISO 17888 – clausola 6.6

La Pubblica Amministrazione (PA) ha deciso in particolare di definire ed adottare un modello cloud ad hoc denominato per l'appunto "Cloud della PA"[51].

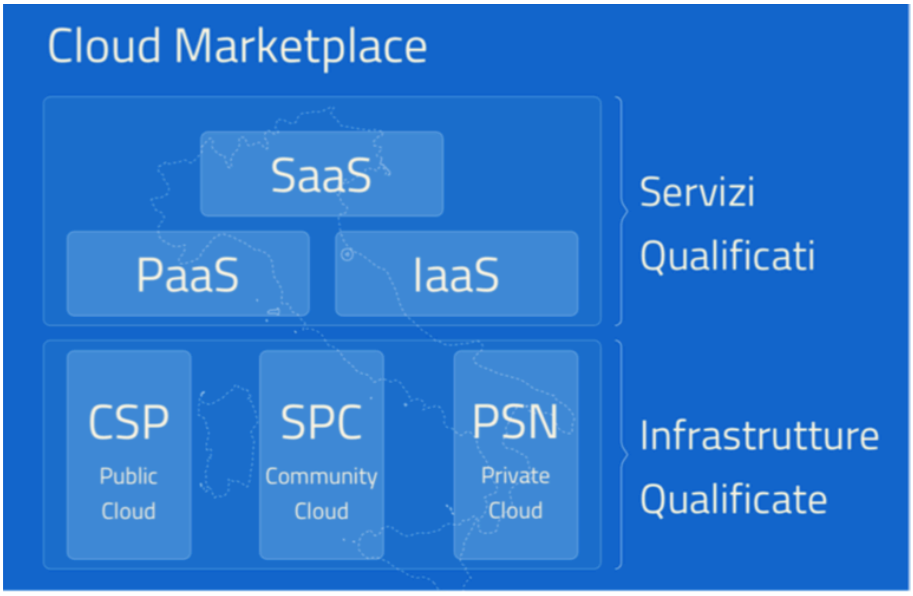
Tale modello, permette di ridurre il rischio di sicurezza e affidabilità dei server dei cloud provider, qualificando i servizi e le infrastrutture Cloud secondo specifici parametri di sicurezza ed affidabilità idonei per le esigenze della PA, coerentemente con i seguenti principi:

- Migliorare dei livelli di servizio, accessibilità, usabilità e sicurezza;
- Interoperabilità dei servizi nell'ambito del modello Cloud della PA;
- Ridurre il rischio di creare un link di dipendenza con il provider del servizio (*lock-in*);
- Riqualificare l'offerta, ampliare e modificare la rete dei fornitori;
- Resilienza, scalabilità, "reversibilità" e protezione dei dati;
- Aprire il mercato alle Piccole e Medie Imprese (PMI).

Il Cloud della PA è composto da infrastrutture e servizi qualificati dall'Agenzia delle Entrate, sulla base di requisiti minimi secondo il modello "Cloud Marketplace".

È un modello misto che nasce con l'intento di soddisfare le diverse e complesse esigenze del settore pubblico. Come possiamo notare dalla figura 12, si compone di servizi qualificati (SaaS, IaaS e PaaS) e infrastrutture qualificate (Cloud service provider, Cloud SPC Lotto 1 e Poli strategici nazionali).

Figure 12: Le componenti del modello del Cloud della PA



I Cloud Service Provider o CSP sono tutte le infrastrutture e i servizi di Public Cloud offerti dai fornitori di servizi cloud qualificati da AgID. Gli SPC Cloud sono i servizi cloud infrastrutturali erogati nell'ambito del

[51] "Cloud della PA", Agenzia per l'Italia digitale (AGID)

contratto quadro Consip - Cloud SPC Lotto. Mentre i Poli strategici nazionali o PSN si riferiscono alle infrastrutture digitali, di cui lo Stato è proprietario, elette a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri e che erogano servizi cloud ad altre amministrazioni.

Il consolidamento della digitalizzazione nella Pubblica Amministrazione richiede una definita *road map* di migrazioni di servizi erogati in modo tradizionale verso un ambiente digitale, caratterizzato dal cloud. Il processo di abilitazione, elaborato da AgID e Team Digitale, ha preso il nome di "*Cloud Enablement*", e nasce appunto con lo scopo di creare, operare e mantenere le proprie infrastrutture IT attraverso l'utilizzo di servizi cloud.
Sono stati individuati tre elementi principali che caratterizzano la trasformazione digitale[52]:

- **Il principio Cloud First**: come indicato nel nome, bisogna adottare il paradigma cloud per l'erogazione di nuovi servizi e la definizione di un nuovo progetto.
- **La strategia di Cloud Enablement**: per la migrazione delle infrastrutture e delle applicazioni esistenti verso il modello Cloud della PA sono state definite due vie possibili:
    - Il **programma di Cloud Enablement nazionale**, ovvero l'insieme dei progetti specifici che consentiranno alle PA di migrare le applicazioni in ambiente cloud;
    - Il **framework di lavoro del Cloud Enablement** che delinea l'insieme delle strategie, risorse, metodologie e strumenti necessari per abilitare la transizione. Tale framework è costituito da due elementi caratteristici: un'unità di controllo, che aggiorna, gestisce e monitora l'ambiente, e diverse unità di esecuzione, che sono i soggetti responsabili della progettazione e dell'esecuzione di uno specifico progetto di migrazione cloud.
- **Centri di competenza**: servono per acquisire le conoscenze e l'esperienza relativa alla gestione dei servizi cloud nella PA.

2.4 Conclusioni del capitolo

Dalla letteratura proposta e dai numeri analizzati, è possibile concludere che certamente il Cloud Computing migliora l'utilizzo delle risorse in termini di efficacia ed efficienza e rappresenta solo l'inizio di un'evoluzione nell'ambito dell'Information Technology che interesserà l'economia nel corso dei prossimi decenni.
Sebbene sia vero che questa tecnologia abiliti l'utilizzo di molte infrastrutture, flessibilità e disponibilità, le sfide che deve superare, soprattutto nel campo della sicurezza della privacy dati, sono molteplici.
Infatti, si può correre il rischio che i dati vengano diffusi all'esterno e raggiungano parti non interessate, specialmente quando i data centers contenenti dati pubblici sono di natura privata o sono localizzati in stati

[52] "Programma di abilitazione al cloud", Agenzia per l'Italia digitale (AGID), < https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/cloud-enablement.html>

diversi. Oppure, utilizzando piattaforme o sistemi esterni, potrebbero verificarsi delle interruzioni di servizio che comportano una paralisi totale delle attività.

Anche nella Pubblica Amministrazione il Cloud ha un impatto positivo. Oltre a produrre benefici diretti per gli enti amministrativi, impatta indirettamente anche sulle performance delle imprese italiane che riscontrano minori difficoltà nel trattare con la PA, costi e commissioni ridotte ed una maggiore efficienza comunicativa ed operativa.

Inoltre, nonostante l'adozione del Cloud in Italia sia già in costante crescita, il Piano Triennale 2020-2022, di cui abbiamo parlato nel capitolo precedente (capitolo 1), detta le linee guida e i requisiti fondamentali per l'adozione del Cloud della Pubblica Amministrazione, in modo da conferire a questa tutte le caratteristiche per poter essere equiparata alle più efficienti PA europee.

CAPITOLO TERZO: LA FIRMA DIGITALE COME STRUMENTO DI DEMATERIALIZZAZIONE

Abbiamo visto come la sicurezza sia un aspetto fondamentale in tema di Cloud Computing e di documento informatico, infatti, un tema di rilevante importanza a tal proposito è la possibilità di determinare l'autenticità del documento in caso di contestazione. Il metodo più efficace è sostanzialmente la presenza di una firma elettronica (avanzata o digitale) che possa attestare l'effettiva autenticità e riconducibilità del firmatario.
Per la gestione informatica della documentazione amministrativa, la firma digitale si pone come pilastro per il processo di *e-government* (di cui si rimanda al capitolo primo), in quanto strumento studiato per contribuire significativamente al processo di digitalizzazione dei processi amministrativi, nella gestione digitale dei documenti e procedure e soprattutto nell'eliminazione del documento cartaceo (oggetto della tesi).
All'interno del capitolo andremo ad analizzare il ruolo della crittografia nella "*new digital economy*", soffermandoci sulle caratteristiche delle diverse tipologie di firme elettroniche e in particolare della firma grafometrica, pensata come strumento per contribuire al passaggio dal cartaceo al digitale, e analizzando possibili vantaggi e rischi che essa comporta.

Il ruolo della crittografia nell'era digitale

Partendo dall'etimologia della parola, Kryptós (nascosto) e graphía (scrittura), è possibile definire la "crittografia" come un sistema capace di codificare un messaggio e renderlo illeggibile a chi non è autorizzato a decodificarlo.
La crittografia è uno dei pilastri più importanti che ha reso possibile la creazione delle criptovalute e blockchain moderne. Nonostante questo, il significato di questo termine ha origini piuttosto antiche. Gli studiosi lo fanno risalire addirittura al V secolo a.C., quando Plutarco nella vita di Lisandro, si riferisce all'utilizzo della cosiddetta "scitala lacedemonica" da parte degli spartani. La scitala non era nient'altro che un bastone avvolto da un nastro di cuoio sul quale si scriveva per colonne parallele all'asse del bastone lettera dopo lettera. In questo modo, dopo aver sciolto il nastro, le parole scritte erano trasposte e difficilmente leggibili se non con un bastone di misura identica a quello originale.
Anche i romani utilizzavano tecniche di crittografia, come il cifrario di Cesare, che consisteva nel sostituire le lettere di un messaggio criptato facendole scorrere di un certo numero di posizioni nell'alfabeto latino. Solo con la conoscenza di questo sistema e del numero delle posizioni dello scorrimento, il messaggio diventava leggibile al ricevente.
Successivamente, nel Medioevo, sono stati poi sviluppati metodi matematici per decifrare messaggi criptati, come l'analisi di frequenza sviluppata dal matematico Al-Kindi o il sistema di cifratura polialfabetica di Leone Alberti. Il secondo non era nient'altro che un'integrazione del cifrario a sostituzione, volto ad aumentare la

sicurezza delle informazioni criptate, infatti, in un cifrario alfabetico, il testo veniva codificato attraverso l'alfabeto in cui era stato scritto il messaggio originale e un secondo alfabeto usato dal testo criptato. La sicurezza del testo era garantita dal fatto che se il ricevente non conosceva l'alfabeto del messaggio originale, non poteva di certo decifrarlo.
La scienza della crittografia è progredita durante gli anni, anche durante la Seconda Guerra Mondiale, furono inventati sistemi più complessi, come il sistema Enigma, basato sul concetto di crittografia analogica. Era un dispositivo che utilizzava ruote mobili per cifrare un messaggio, rendendo impossibile la lettura senza l'uso di un altro Enigma[53].

Oggi, il significato della crittografia si colloca nell'ambito della sicurezza informatica e della tutela di dati e informazioni che sono in circolazione sulla rete, essendo in grado di fornire la maggior parte dei servizi contemplati nell'architettura di sicurezza stabilita dall'ISO (*International Organization for Standardization*). Per questo è necessario sviluppare sistemi sofisticati che possano garantire un livello alto di confidenzialità e sicurezza, come per esempio la crittografia quantistica che eleva ancora di più il livello di protezione della crittografia moderna.
Secondo l'ISO, un documento affidabile deve mantenere determinate caratteristiche[54]:

- **Confidenzialità**: riguarda la capacità di proteggere i dati da entità non autorizzate;
- **Integrità dei dati**: tale caratteristica vuole che i dati siano protetti da modifiche indesiderate e non autorizzate, ma anche da cancellazioni o cambiamento nell'ordine dei dati;
- **Autenticazione**: i servizi di autenticazione accertano l'identità di un soggetto e si suddividono in:
  - Servizi di autenticazione dell'entità: è il caso in cui si accerta l'identità di un soggetto remoto che vuole prendere parte a un servizio online;
  - Servizi di autenticazione dell'origine dei dati: è il caso in cui si autentica l'identità di chi invia o crea un messaggio o un documento;
- **Controllo degli accessi**: è possibile svolgerlo solo dopo la fase precedente dell'autenticazione in modo da accertare l'accesso solo ai servizi autorizzati;
- **Non ripudio**: questa caratteristica va oltre le problematiche di integrità e autenticazione, serve principalmente per dimostrare l'inizio di una transazione o comunicazione tra due parti, in modo tale da vietare il rinnego e da garantire la paternità in caso di contenzioso. Lo strumento per garantire il non ripudio nei documenti cartacei, come i contratti o i bonifici, è la firma autografa, invece, per i documenti elettronici e digitali si ricorre a tecniche di crittografia asimmetrica, come la firma digitale.

[53] Alessandro Languasco, Alessandro Zaccagnini, "*Manuale di crittografia: Teoria, algoritmi e protocolli*", Hoepli Editore, (2015)
[54] ISO 27001 e conservazione sostitutiva, <https://www.csqa.it/Sicurezza-ICT/Focus/ISO-27001-e-Conservazione-sostitutiva>

Più recentemente, le tecniche crittografiche sono state anche sviluppate per rendere possibili le criptovalute, che utilizzando strumenti avanzati, come le funzioni *hash*, crittografia a chiave pubblica e firme digitali. Queste funzioni infatti vengono usate per garantire la sicurezza dei dati archiviati sulle blockchain e per autenticare le transazioni.
La trasformazione dei caratteri tramite l'utilizzo di algoritmi matematici, si basa sul valore di una chiave segreta, ovvero il parametro dell'algoritmo cifratufura/decifratura. In base al tipo di chiave utilizzato, la crittografia informatica può essere simmetrica o asimmetrica.
In particolare, ci si riferisce al numero di chiavi: quando la chiave è unica la crittografia è simmetrica o a chiave segreta (ciò significa che la chiave del mittente coincide con quella del destinatario), quando invece le chiavi sono due, si parla di crittografia a chiave asimmetrica o a chiave pubblica (la chiave di cifratura è pubblica e condivisa da tutti i corrispondenti, mentre la chiave di decifratura è privata e segreta per il proprietario stesso). In questo ultimo tipo di crittografia le chiavi sono interdipendenti, ovvero una chiave è utilizzata per cifrare e la seconda per decifrare[55].

La **crittografia simmetrica** pertanto è costituita da un'unica chiave, condivisa tra due o più utenti, utilizzata per cifrare e decifrare l'informazione codificata. Infatti, il processo di cifratura prevede un input, ovvero il testo semplice, e un output, il testo cifrato, reso tale dall'algoritmo di cifratura chiamato "cifrario". La chiave per accedere alle informazioni e decifrare il messaggio è la stessa, pertanto occorrerà creare un canale sicuro per scambiare la chiave tra le parti interessate, rendendola sconosciuta a terzi. Possiamo averne una rappresentazione nella figura riportata successivamente.

Figure 13: raffigurazione crittografia simmetrica

L'esempio portante della crittografia simmetrica è l'algoritmo *Advanced Encryption Standard* (AES), sviluppato nel secolo scorso da Joan Daemen e Vincent Rijmen[56], su richiesta del *National Institute of Standards and Technology*. Alla base dell'algoritmo ci sono dei blocchi di dati da 16 byte, sui quali sono eseguite diverse operazioni chiamate round. È composto inoltre da tre algoritmi di cifrature a blocchi di 128

[55] Alessandro Languasco, Alessandro Zaccagnini, "*Manuale di crittografia: Teoria, algoritmi e protocolli*", Hoepli Editore, (2015).
[56] Joan Daemen e Vincent Rijmen, "*The Design of Rijndael: Aes-The Advanced Encryption Standard*", Springer, (2002).

bit. Se la chiave ha 128 bit, l'algoritmo ha 10 round, che aumentano di due con chiave a 192 bit e ancora di due nel caso di chiave a 256 bit.

Nella **crittografia pubblica o asimmetrica** invece, come precedentemente accennato, si utilizzano due chiavi, una delle quali è condivisa pubblicamente, mentre l'altra rimane segreta. Di conseguenza, si cifra il testo con una chiave differente da quella per decifrarlo, le due chiavi sono generate con la stessa procedura e correlate univocamente e infine, non c'è nessuna possibilità di risalire ad una chiave seppur conoscendo l'altra. Per avere una rappresentazione visuale dell'invio di un messaggio con sistema asimmetrico, dalla figura sottostante è possibile notare che per la cifratura è necessaria la chiave pubblica del destinatario, il quale è anche l'unico utente in grado di decifrare l'informazione, grazie alla sua chiave privata correlata alla chiave pubblica usata dal mittente.

Figure 14: raffigurazione crittografia asimmetrica

L'algoritmo più utilizzato in questa tecnica crittografica, è il *Rivest, Shamir, Adleman (RSA)* creato nel 1977 appunto dai ricercatori di cui porta il nome. La sicurezza che questo algoritmo offre, è dovuta alla lunghezza delle chiavi ma presentando lo svantaggio della lentezza rispetto a un algoritmo per la crittografia simmetrica, generalmente si decifrano i dati con un algoritmo simmetrico, e si crittografa la chiave simmetrica, sicuramente più breve, tramite l'RSA[57].

Sebbene gli algoritmi simmetrici offrano un livello di sicurezza elevato, come per esempio nel caso dell'algoritmo *Advanced Encryption Standard* (AES), che è stato adottato dalla National Security Agency per proteggere le informazioni governative e per i documenti top secret, presentano lo svantaggio principale per le parti interessate di doversi scambiare la chiave utilizzata prima di potere avere accesso ai dati. Infatti, quando le chiavi passano per vie non protette, possono essere facilmente intercettate da terze parti. Per questo motivo, sempre per gestire le chiavi in modo sicuro e affidabile, si ricorre anche ad altri algoritmi di cifratura basati su un modello ibrido, ovvero una combinazione di cifratura asimmetrica e simmetrica, come nel caso del protocollo crittografico *Transport Layer Security* (TLS).

[57] Ben-Zion Chor (1986), "*Two issues in public key cryptography: RSA bit security and a new knapsack type system*", MIT Press55 Hayward St.CambridgeMAUnited States.

Le diverse tipologie di firme elettroniche e la firma digitale

Gli algoritmi di cifratura di crittografia asimmetrica vengono impiegati, tra l'altro, nella firma digitale.
La nascita della firma digitale risale all'introduzione, nell'ordinamento italiano, della Legge Bassanini[58] (legge 59/97), che ha riconosciuto il valore giuridico del documento elettronico affermando che "gli atti, dati e documenti firmati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge". Sempre nella stessa legge, si rimanda ad un regolamento specifico, approvato con DPR 513/97, per dare prova della validità attraverso la firma digitale.
Con il corso degli anni ci sono state diverse modifiche e integrazioni per adeguare la legge italiana alla disciplina europea. Quest'ultima, infatti, continua ad attestare il valore giuridico del documento informatico tramite la firma digitale, riconoscendone la validità in determinati contesti anche senza la rigidità tecnica delle regole per l'apposizione della firma digitale. Inoltre, si ritiene che per limitare la discrezionalità del legislatore nel condizionare in modo eccessivo il mercato, tale firma debba essere accompagnata anche da altre tecnologie esistenti[59].
A seguito dell'introduzione di questa disciplina, e del recepimento nella normativa nazionale, il documento informatico è sottoposto a diversi gradi di validità ed efficacia probatoria, a seconda che l'autografo avvenga tramite firma elettronica o firma elettronica avanzata, di cui la firma elettronica qualificata e quella digitale ne costituiscono il massimo esempio.
Spesso si tende a utilizzare la firma digitale e quella elettronica come sinonimi, non comprendendo in realtà che esiste una differenza relativamente al valore probatorio. Il Codice dell'Amministrazione Digitale chiarisce queste differenze proponendo una definizione per ciascuna categoria:

- **Firma elettronica**: "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica".
  Un esempio può essere dato dalle credenziali di accesso a un sito o dai codici digitali, come il PIN delle carte magnetiche;
- **Firma elettronica avanzata**: è una firma elettronica maggiorata di determinate caratteristiche, o meglio "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".

[58] Legge 15 marzo 1997, n. 59, "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"
[59] Intervista a Giovanni Manca, "*Breve excursus sulla firma digitale*"

- **Firma digitale**: è definita come "un particolare tipo di Firma Elettronica Avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici". Questa tipologia di firma si basa sulla crittografia a chiavi asimmetriche e si appone tramite diversi strumenti, i più diffusi sono il token e la smart card.
- **Firma elettronica qualificata**: così come la firma digitale, anche la firma elettronica avanzata viene apposta tramite dispositivi come token e smart card, ma si basa su un certificato qualificato. È possibile identificare il titolare della firma attraverso i mezzi messi a disposizione del firmatario, di cui lo stesso ne detiene il controllo.

Il documento cartaceo possiede determinati requisiti, dai quali il legislatore non poteva esimersi riconoscendo al documento informatico valore analogo a quello citato. I requisiti sono tre: l'integrità, ovvero che il supporto cartaceo deve essere tale che una qualsiasi modifica sia evidente, la provenienza, in cui la sottoscrizione in calce al documento comporta l'assunzione che il documento provenga da chi l'ha sottoscritto o che quest'ultimo ne conosca il contenuto e lo faccia proprio e infine la paternità, che prevede l'attribuibilità della firma autografa a una sola persona identificabile mediante tecniche individuate dall'ordinamento giuridico.
Riconoscendo valore giuridico al documento informatico si dovevano creare le condizioni affinché questo verificasse i principi sopra elencati, ovvero:

- Fosse impedita la modifica dello stesso
- Fosse assicurata la provenienza del documento
- Fosse possibile identificare il sottoscrittore

Con l'approvazione alla firma digitale da parte del legislatore, il documento informatico ha potuto ottenere tali requisiti.
La firma digitale ha dato validità a questo documento sia sul lato tecnologico che amministrativo. Sul fronte tecnologico ricorre a tecniche di crittografia asimmetrica per garantire l'identificazione della provenienza del documento, su quello organizzativo assicura la verifica dell'identità del sottoscrittore attraverso registri affidati ad autorità esterne, le c.d. autorità di certificazione[60].
Il sistema crittografico è anche utile per verificare l'integrità di un messaggio, informazione o documento informatico, caratteristica fondamentale perché attesta l'autenticità, la completezza e l'assenza di modifiche dell'oggetto considerato.

[60] Redolfi, Daniela,"*Firma digitale, posta elettronica certificata e dematerializzazione*", p. 53-71, Marsilio. Ricerche (Marsilio), (2011).

La firma digitale, seppur poggiando sul sistema di crittografia asimmetrica, deve garantire l'integrità del documento. Infatti, in questo contesto è spesso utilizzata la funzione crittografia di *hash*, ovvero un algoritmo matematico unidirezionale utilizzato per trasformare dati, come un messaggio qualsiasi lunghezza su una stringa di bit di una dimensione fissa, chiamata anche *hash value* o *message digest*[61].

In modo specifico, dalla funzione di *hash* si ricava l'impronta digitale del documento, un file di controllo relativamente piccolo che contiene una sorta di codice di controllo relativo al documento stesso. La funzione di *hash* ha una funzione di garanzia in quanto riduce la possibilità che da testi diversi si possa ottenere lo stesso valore dell'impronta e rende impossibile ottenere dall'impronta il testo originario. È possibile in questo modo verificare ogni alterazione e modifica del documento in quanto una volta prodotta l'impronta digitale da un determinato documento, se questo viene modificato, produrrà un'impronta diversa dalla prima.

Successivamente, per far si che la provenienza del documento sia accertata, l'impronta viene decrittata dal sottoscrittore con la propria chiave privata, in questo modo la firma appartiene all'impronta digitale cifrata con la chiave privata di chi firma.

Con i software attualmente in commercio, questi passaggi sono evitati agli utenti e le operazioni di sottoscrizione, verifica e firma vengono effettuate in modo automatico.

Il processo di sottoscrizione mediante firma digitale quindi prevede i seguenti passaggi:

1. Documento da sottoscrivere
2. Produzione dell'impronta
3. Applicazione della chiave segreta dell'impronta del documento
4. Documento sottoscritto

Successivamente avrà luogo il processo di verifica della sottoscrizione attraverso il quale si controllerà che l'impronta appartenga al documento in modo tale da accertare che esso non sia stato modificato e si applicherà la chiave pubblica del sottoscrittore in modo da verificare che il documento sia stato firmato da lui in prima persona.

La firma grafometrica a supporto della dematerializzazione

Il legislatore, nell' ottica di semplificare i processi burocratici e assicurare un livello di sicurezza adeguato per impedire eventuali contraffazioni, ha reso possibile l'utilizzo di una firma che può essere apposta con strumenti tecnologici. Questa tipologia è la firma elettronica avanzata, definita dal regolamento eIDAS come "*firma elettronica che soddisfi i seguenti requisiti: 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*

[61] <http://siba-ese.unisalento.it/index.php/quadmat/article/viewFile/21267/17971>, pp.207

elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati"[62].

Tra le firme elettroniche avanzate, nell'ottica di garantire una maggiore sicurezza e una limitata contraffazione, assume un particolare rilevo la firma grafometrica, che si basa su un sistema di biometria, ovvero è in grado di rilevare una serie di parametri biometrici legati al comportamento dell'utente, che vengono poi cifrati e associati al documento firmato[63].

Tale firma, attraverso un processo informatico, è in grado di rilevare alcuni dati biometrici del firmatario. Nel momento in cui l'utente appone la firma tramite un tablet, riesce a cogliere i movimenti naturali associati alla mano nell'atto di firmare, associandoli in maniera univoca al documento firmato.

Per il raggiungimento di questo risultato viene impiegato un software che interagisce con il tablet utilizzato dal firmatario, che è installato in una postazione di lavoro che permette al cliente di accertarsi del documento online e solo in un secondo momento di apporre la firma. È prevista la possibilità di ripetere l'operazione, modificando o annullando quella precedente.

Questa facilità nell'utilizzo ha comportato il successo della firma grafometrica a discapito di altre firme elettroniche, per il fatto che in un contesto generazionale, dove le tecnologie sono sempre all'avanguardia e in continua evoluzione, l'adozione di strumenti come codici, carte magnetiche e token o dispositivi personali, come smart card e lettori, potrebbe risultare poco agevoli nell'utilizzo. Così, anche la firma elettronica avanzata implementata tramite l'utilizzo di codici segreti (PIN) o "*One Time Password*" (OTP) può destare ambiguità nell'utilizzo da parte del cliente.

È possibile acquisire la firma grafometrica attraverso specifici software incorporati in dispositivi esterni come tablet o signature pad, che riescono a generare il documento informatico registrando informazioni dinamiche, come la velocità di scrittura, la pressione esercitata su tavoletta o altro device, l'angolo di inclinazione della penna, l'accelerazione del movimento e il numero di volte che la penna viene sollevata, e movimenti statici, come l'immagine e le caratteristiche della firma.

La prima considerazione che può essere fatta riguarda appunto la sicurezza offerta dai dispositivi hardware e software utilizzati, in quanto, se l'immagine della firma è visibile anche al cliente, i dati biometrici crittografati non lo sono, e rimangono nascosti nella componente informatica del documento.

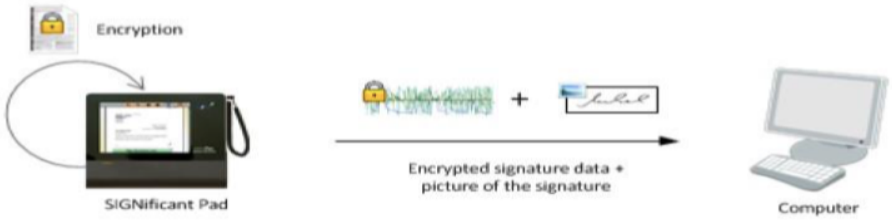
Volendo avere una rappresentazione grafica del processo di trasmissione, possiamo prendere in considerazione la figura qui rappresentata[64].

[62] Regolamento UE n° 910/2014 – eIDAS

[63] Daniel Riccio, Clemente Galdi, Luigi Catuogno, "*Sistemi Biometrici e Sicurezza*"

[64] "La soluzione di Firma Elettronica Avanzata (FEA) grafometrica. Le caratteristiche del sistema e le tecnologie utilizzate", < https://www.sanfelice1893.it/sites/default/files/2020-09/firma_elettronica_avanzata.pdf>

Figure 15



La firma grafometrica quindi, si configura come uno strumento in grado di assecondare le esigenze del cliente, non dovendo più essere vincolato a dispositivi appositi scomodi per apporla, ma ci sono delle considerazioni da fare circa il tema della sicurezza che permettono allo stesso firmatario di agire in modo sicuro.

Per garantire la sicurezza, i dati biometrici del firmatario acquisiti tramite tablet vengono protetti attraverso una chiave di cifratura e legati all'impronta (*hash*) del documento. Per far sì che le informazioni transitino in modo sicuro tra tablet al computer, i dati biometrici e l'impronta del documento, vengono uniti e cifrati insieme in modo da avviare una procedura, chiamata "*document binding*", che in caso di contestazione, correla inequivocabilmente il documento alla firma apposta. Una volta che il viaggio di transizione è giunto a termine, i dati biometrici acquisiti vengono cancellati.

Da questa considerazione ne deriva una seconda legata alla gestione delle chiavi di cifratura. Come abbiamo detto precedentemente, nella crittografia pubblica o asimmetrica, si utilizzano due chiavi, una pubblica e una privata. I dati vengono cifrati con una chiave pubblica, mentre la chiave privata deve essere conservata accuratamente da un soggetto esterno, in modo tale da poter dimostrare la veridicità del documento in caso di contenzioso. Per questo esistono le autorità di certificazione che hanno il compito di garantire l'associazione tra la chiave pubblica e un determinato soggetto detentore della coppia di chiavi. A tale scopo i certificatori identificano i titolari della coppia di chiavi, tengono il registro con gli identificativi dei titolari e la chiave pubblica a loro attribuita ed emettono un certificato digitale che attesta che la chiave pubblica è assegnata a quel determinato titolare.

Nel certificato digitale sono riportare le informazioni riguardanti[65]:

- L'autorità di certificazione che l'ha emesso
- Il periodo di validità
- Gli identificativi del soggetto a cui è stata attribuita la coppia di chiavi
- La chiave pubblica

[65] Redolfi, Daniela, "*Firma digitale, posta elettronica certificata e dematerializzazione*", p. 53-71, Marsilio. Ricerche (Marsilio), (2011).

Il certificato digitale con annesse informazioni, è posto in allegato alla firma in modo da garantire la verifica dell'identità del sottoscrittore, infatti, se il certificato è sospeso o revocato, la firma apposta non è considerata validante.

Processo di riconoscimento biometrico

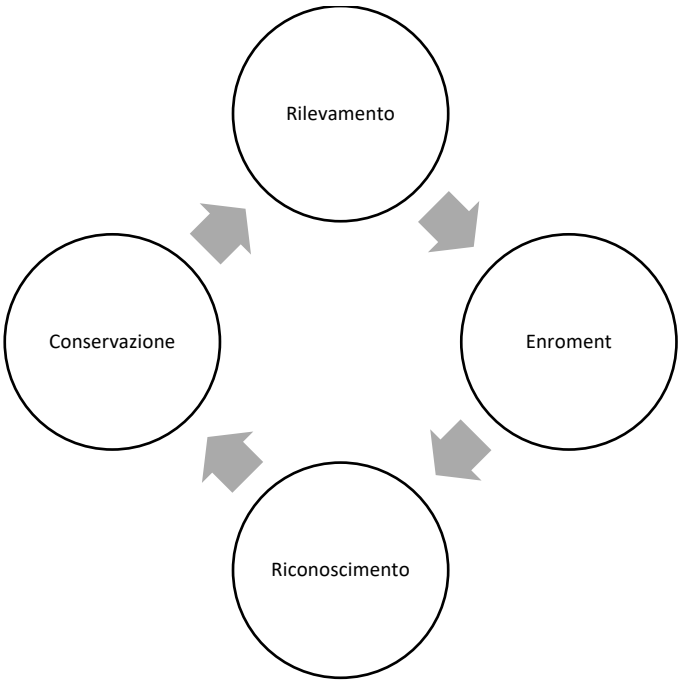
Per "riconoscimento biometrico" si intende un processo informatico volto a identificare e a verificare l'identità di una persona, attraverso l'analisi di caratteristiche fisico-biologiche, come impronte digitali, fisionomica del viso, il colore e la forma dell'iride o la retina eccetera, e comportamentali, come il timbro della voce e le caratteristiche della scrittura.
Alla base di questo sistema informatico ci sono algoritmi progettati per confrontare ogni accesso che avviene con i dati e gli input acquisiti precedentemente.
La verifica e l'identificazione di un soggetto sono due fasi distinte e consecutive, in quanto in un processo di verifica i dati acquisiti sono confrontati con i dati precedentemente rilasciati da quell'utente, mentre nel processo di identificazione, i dati vengono comparati con altri dati biometrici rilasciati da altri utenti e che sono conservati in un archivio. La verifica biometrica, non è nient'altro che un processo informatico che permette di autenticare un soggetto similmente ad altri strumenti, come password, PIN, PUK ecc..
Nel caso di verifica dell'identità dell'utente, si effettua un riconoscimento "*one to one*", ovvero un confronto tra il modello biometrico associato all'input dell'identità dichiarata dall'utente nella fase di accesso, tramite un codice d'utente per esempio, e il modello biometrico che viene creato nella richiesta di riconoscimento. Se i due modelli corrispondono si procederà all'abilitazione a un sistema informatico.
Nel caso invece dell'identificazione biometrica, si effettua un riconoscimento "*one to many*", in quanto il modello biometrico ricavato, servirà come campione da confrontarsi con altri modelli biometrici conservati in un archivio informatico. Viene da se che la complessità di questa seconda operazione è di gran lunga maggiore, potendo essere conservati dati numerosi e non trattati e altrettanti algoritmi di ricerca utilizzati.
La firma grafometrica viene utilizzata per una sicurezza maggiore rispetto agli ordinari sistemi di autenticazione informatica come *password, user ID, badge* o *token*, in quanto tali credenziali possono essere smarrite, dimenticate o intercettate. La tecnica di riconoscimento biometrico risulta anche essere più efficace di altri sistemi basati su tessere di diversa tecnologia (magnetica, ottica, a contatto, a radiofrequenza) o su sistemi di autenticazione come OTP (*one-time password*), in quanto, seppur conferendo un livello di sicurezza più elevato rispetto alle tecniche appena citate, possono anche questi essere oggetto di smarrimento o furto portando alla violazione dei dati personali (*data breach*).
Proprio perché garantisce un livello di sicurezza elevato, la firma grafometrica è utilizzata spesso nella sottoscrizione di documenti informatici, in cui i dati biometrici dell'individuo sono conservati all'interno dello stesso documento per realizzare soluzioni di firma elettronica avanzata, oppure per incorporare nel documento

le informazioni e i dati legati all'individuo e al fascicolo in modo da poterne verificare l'autenticità, l'integrità e la non ripudiabilità.
Attraverso un sistema efficace di crittografia, ogni singola firma, viene acquisita e incorporata nel documento informatico archiviato in modalità cloud in un sistema di gestione documentale[66].

Il ciclo di vita dei dati biometrici

I dati biometrici seguono un circolo virtuoso di produzione che conta 4 fasi consecutive, a partire dal rilevamento fino a concludersi con la conservazione. Iansiti e Lakhani lo definiscono un circolo virtuoso, ma può anche essere un circolo vizioso se uno qualsiasi dei passaggi contiene pregiudizi, errori o presupposti sbagliati. Ogni fase deve essere accuratamente eseguita e controllata, in quanto se si sbaglia un singolo passaggio si avranno ripercussioni su tutta la catena[67].
Il ciclo di vita dei dati biometrici inizia con il rilevamento e l'acquisizione biometrica, a cui seguono un processo di enrolment e creazione del dato biometrico, che viene poi riconosciuto e conservato[68].

Figure 16: Fonte di rielaborazione propria: "Ciclo di vita dei dati biometrici"



1. Rilevamento e acquisizione biometrica

[66] Maria Rosaria Lenti, "*Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security*", (2017)
[67] Iansiti, M., & Lakhani, K. R., "Rearchitecting the firm", Competing in the Age of AI. Harvard Business Press Chapter 4, pp. 79-97, (2020)
[68] Hayat Khaloufia, Karim Abouelmehdi, Abderrahim Beni-Hssane, Mostafa Saadi, "*Security model for Big Healthcare Data Lifecycle*", (2018),

Il rilevamento dei dati biometrici inizia con l'acquisizione di ogni caratteristica biometrica, biologica o comportamentale di un individuo, attraverso sensori o dispositivi appositi, e si conclude con la creazione di un campione, ovvero di un file dalle dimensioni dipendenti dal tipo di sistema biometrico e sensore utilizzato. I sensori utilizzati, infatti, possono essere specializzati, come nel caso di scanner, dispositivi per il rilevamento della topografia della mano e tavolette grafometriche, o non specializzati, come videocamere, webcam, microfoni, tablet o simili.

Un aspetto fondamentale da considerare è appunto la dimensione del file ricavato, che non deve eccedere verso una dimensione minima o massima ma che sia strettamente legata alla finalità e all'utilizzo del modello; infatti, la dimensione deve essere abbastanza estesa per assicurare un livello di accuratezza adeguato nel riconoscimento biometrico, ma non troppo per evitare che il campione rilevato possa essere facilmente ricostruito.

2. Enrolment e creazione del modello biometrico

La registrazione biometrica, detta anche "*biometric enrolment*", permette di acquisire una determinata caratteristica per effettuare poi il riconoscimento biometrico. I dati registrati possono essere poi conservati in due modalità: sotto forma di campione biometrico o sotto forma di modello biometrico, ovvero un modello matematico che sintetizza e raccoglie gli aspetti salienti del campione. Da quest'ultimo poi è possibile estrarre tratti caratteristici di un individuo e conservarli per riutilizzarli al posto del campione stesso. Le rilevazioni successive, fatte per confrontare i diversi tratti, devono seguire la stessa procedura scongiurando il rischio che i modelli da confrontare siano decrittografati e passino per reti insicure.

3. Riconoscimento biometrico

I campioni biometrici devono essere necessariamente conservati in banche dati centralizzate per confrontare le identità degli accessi. Se vi è un match tra l'identità da verificare e il modello biometrico allora il firmatario può essere identificato. Per quanto riguarda il sistema di verifica invece, è possibile ricorrere a entrambi i tipi di conservazione, centralizzata o decentralizzata; nel caso della prima i modelli biometrici saranno conservati in una singola banca dati, mentre nella soluzione decentralizzata saranno apposti direttamente sui dispositivi di rilevazione o affidati all'interessato.

4. Conservazione dei dati biometrici

La sfida dei dati raccolti è mantenerli e gestirli. Le informazioni acquisite attraverso tecniche biometriche, possono essere conservate in forma di *Hardware Security Module* (HSM) in una banca dati centralizzata, in ambienti informatici o negli stessi dispositivi che le hanno rilevate. Possono essere utilizzati anche dispositivi come token o smart card di proprietà del firmatario, ma bisogna tenere in considerazione la possibilità di

smarrimento e la conseguente impossibilità di accesso dell'interessato, o addirittura ricorrere a soluzioni cloud, tenendo comunque presente le implicazioni trattate nel capitolo precedente.

3.3.3 Analisi dei rischi della biometria

Le tecniche di identificazione biometrica, come abbiamo potuto vedere, offrono una semplicità, sicurezza e univocità al processo di gestione delle credenziali, ma i rischi che sono loro connessi sono molteplici, relativamente alla violazione del trattamento dei dati personali degli interessati. In particolare, il rischio maggiore consiste nella vulnerabilità di un particolare set di informazioni che può causare un furto d'identità o un trattamento illecito dei dati personali del firmatario.

È possibile analizzare i rischi principali[69] dei sistemi biometrici partendo dal controllo sociale e dagli usi discriminatori che ne possono derivare. Alcuni dati biometrici sono considerati unici nella popolazione, tanto da risultare un efficace parametro di identificazione universale. Il punto critico e controverso è che tali caratteristiche, come per esempio l'etnia, la forma fisica, i tratti somatici, la salute di un soggetto, possono essere acquisite da soggetti privati o istituzioni, ed essere collegate e intrecciate con altri dati provenienti da banche dati differenti, con finalità differenti diverse da quelle per cui sono state captate in origine, giovando del fatto che al giorno d'oggi stiamo assistendo a un diluvio di dati. Non sappiamo spesso come vengono prodotti, la condizione alla base della loro produzione e scambio, quindi la loro qualità. Ci sono, come abbiamo visto, devices che pensano a tutto e vengono prodotti in maniera nuova e inconsapevole. Inoltre, ci sembra di dimenticare che i dati sono sempre il risultato di processi decisionali organizzativi e processi tecnologici e istituzionali complessi e possono presentare pregiudizi e limitazioni che devono essere prese in considerazione, in particolare quando riutilizzati (o usati per prendere decisioni).
Infatti, i dati biometrici possono essere riutilizzati senza la consapevolezza di un individuo, nel tracciare i suoi spostamenti attraverso tecnologie automatizzate che comportano un'invasione della sfera privata, tanto da rendere la biometria non più una misura di sicurezza e facilitazione, bensì uno strumento di controllo generalizzato. Queste caratteristiche biometriche possono per esempio essere l'input per trattamenti discriminatori.
Spesso sentiamo che più le tecnologie sono avanzate meno rischi ci sono nell'avere dei dati oggettivi aderenti alla realtà. Questo non è sempre vero, nonostante le tecnologie più avanzate di oggi sono più precise nella restituzione dei fatti, è pur vero però che essendo molto complesso produrre i dati, c'è sempre uno spazio che rimane fra quello che si misura e come questa misurazione è riportata anche nei dati digitali nonostante la

[69] "*Linee-guida in materia di riconoscimento biometrico e firma grafometrica*", <https://www.garanteprivacy.it/documents/10160/0/All+A+al+Provv.+513+del+12+novembre+2014+-+Linee-guida+biometria.pdf/9d80ff69-31e3-4b9d-b8f5-a255096bfe96?version=1.3 >

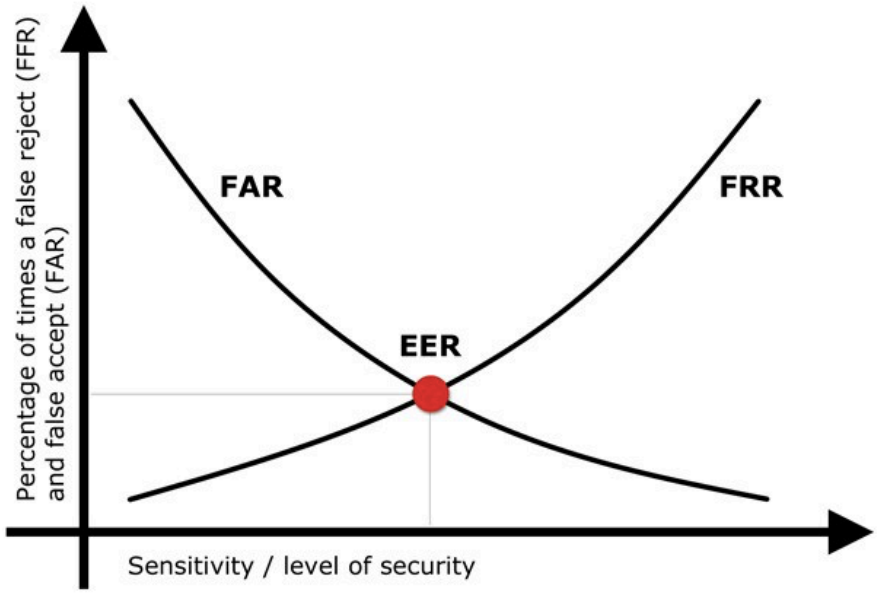
tecnologia possa essere sofisticata. Per questo motivo l'utilizzo di sistemi di riconoscimento biometrici implica l'adozione di misure di sicurezza speciali per garantire la conservazione e la privacy dei dati personali, conservati appunto per le finalità acconsentite e nella consapevolezza del trattamento degli stessi.

Un altro rischio che è opportuno tenere in considerazione è quello di un possibile furto dell'identità biometrica. Il furto d'identità digitale risulta essere un fenomeno lesivo nei confronti degli utenti, in quanto il dato biometrico è univocamente correlato ad un'unica identità, per cui nel caso in cui si verificasse un furto di questa, non potrà essere ricostituita una nuova identità biometrica connessa allo stesso dato iniziale. Infatti, le caratteristiche biometriche fungono da credenziali di autenticazione che non possono essere revocabili o sostituibili. Il furto dell'identità biometrica avviene generalmente appropriandosi di determinate caratteristiche che lasciano il segno, come l'impronta digitale, o che possono essere rilevate senza che l'interessato ne sia complice, come ad esempio la registrazione della voce, il riconoscimento facciale o la scansione dei tratti somatici del volto.
Per scongiurare tali rischi e per tutelare l'identità digitale, si dovrebbero utilizzare tecniche biometriche in combinazione con sistemi *multi-factor*, ovvero utilizzando un sistema ibrido, che preveda l'utilizzo di biometria, *password* o *token* e ricorrere a sistemi di sicurezza informatica che impediscano l'accesso a informazioni riservata. Inoltre, sotto il profilo dell'identità personale dell'utente, dovranno intervenire normative e regole per per gli operatori per garantire la liceità del trattamento.

Sebbene l'utilizzo di credenziali e password sia maggiormente dimenticabile, è anche vero che ci porta davanti a due opzioni (corretta o errata). Il sistema di autenticazione e identificazione biometrica invece, basandosi su basi probabilistiche e non deterministiche, possono generare tassi di falsi positivi (*false acceptance rate – FAR*), che indicano una misura di quanti estranei non autorizzati riescono ad accedere al sistema, e di falsi negativi (*false rejection rate – FRR*), che stabilisce quanti utenti legittimi vengono respinti. I due valori sono tra loro correlati, per questo è giusto trovare il giusto compromesso tra il numero di falsi positivi e quello di falsi negativi, sulla base delle specifiche esigenze di sicurezza, come possiamo notare nella figura qui sotto riportata[70].

[70] Fonte: recotech.com

Figure 17



Un altro rischio è legato alla possibilità di ricreare un campione biometrico a partire dal modello stesso. La falsificazione biometrica genera dei timori per gli esperti della sicurezza per quanto riguarda il futuro delle tecniche biometriche. Infatti, la creazione del modello dovrebbe essere un processo unico e irreversibile, ma ci sono dei casi in cui questo possa essere facilmente manomesso. Si pensi per esempio alle impronte digitali. Secondo alcuni ricercatori della New York University e della Michigan University, sarebbe possibile "hackerare" le impronte digitali di un individuo attraverso un sistema, chiamato DeepMasterPrints, che riesce a emulare il 20% o più delle impronte digitali presenti su un qualsiasi sistema biometrico.

Il sistema è basato su un algoritmo generativo, noto come *Generative Adversial Networks* (*GANs*)[71], in grado di generare un nuovo campione biometrico a partire dal modello biometrico, ovvero a partire dalle impronte registrate precedentemente.

Per esempio, recentemente, si è potuto constatare come la creazione di un campione biometrico dattiloscopico "artificiale" di elevata qualità e accuratezza, sia piuttosto semplice estrapolando minuzie parziali fino all'assemblaggio dell'immagine finale del campione originale. In questo caso si otterrebbe un modello biometrico analogo a quello originario, tanto da produrre un risultato positivo.

Nonostante questo, attraverso gli occhi di un esperto, si ritiene sia possibile cogliere le differenze con il campione inziale, in quanto, seppur simili, non sono del tutto uguali, ma i rischi che può comportare sono di particolare importanza e possono essere mitigati solo dai sistemi in rapida evoluzione.

Ultimo ma non di minore considerazione, è l'aumento del rischio nel contesto mobile e BYOD (*Bring Your Own Device*)**,** la pratica per cui i dipendenti possono utilizzare i propri dispositivi personali per scopi

[71] Wafa Njima, Marwa Chafii, Raed Shubair, (2021), "*GAN Based Data Augmentation for Indoor Localization Using Labeled and Unlabeled Data*"

lavorativi. Questo implica la scelta di strumenti adeguati per garantire la sicurezza dei dati. Infatti, in questo caso, qualsiasi lavoratore può connettersi a risorse aziendali attraverso il proprio dispositivo, accedendo a dati o informazioni rilevanti attraverso applicazioni appositamente installate. Per questo motivo bisogna adottare delle accuratezze nei confronti della protezione dei dati informatici, come il tenere traccia dei dispositivi utilizzati e degli utenti, la personalizzazione del dispositivo, una chiara politica sugli utilizzi concessi, l'investimento nella formazione e nella consapevolezza dei lavorati, il blocco da remoto e memorie criptate, regole particolari per gli accessi alla rete e l'attenzione alla privacy degli impiegati.

3.3.4 I vantaggi della firma elettronica

Come anticipato precedentemente, la firma grafometrica è uno degli strumenti maggiormente utilizzato per snellire i processi burocratici favorendo la dematerializzazione della modulistica delle operazioni.
Nonostante i rischi che possono verificarsi e che abbiamo appena analizzato, nel contesto della *digital business transformation*, la firma grafometrica, si pone come soluzione abilitante per la digitalizzazione dei processi documentali cartacei assicurando piena *compliance* e validità legale, dando luogo a processi di digitalizzazione che permettono di dematerializzare il cartaceo, creando efficienza e contenimento dei costi di gestione.
Secondo alcuni dati rilevati attraverso una *survey* condotta da Aruba a Luglio 2020, come possiamo notare nella figura sottostante, gli utilizzatori della firma digitale sono per il 70% liberi professionisti, per il 20% le persone fisiche e per il 10% le aziende[72].

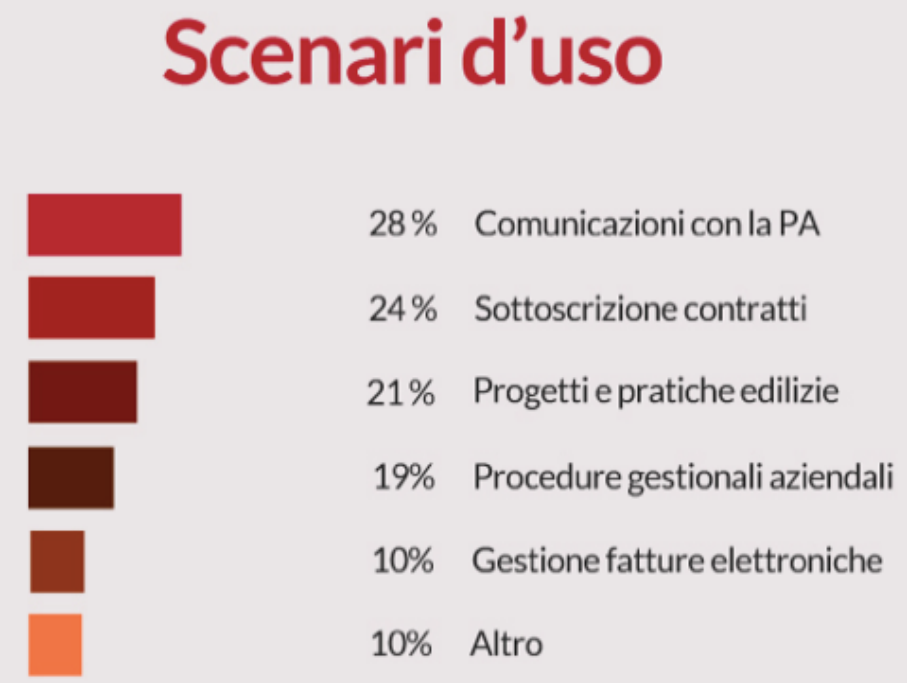
[72] Dati rilevati attraverso una Survey condotta da Aruba – Luglio 2020

Figure 18

Inoltre, gli scenari d'uso più comuni sono per il 28% nelle comunicazioni con la Pubblica Amministrazione, per il 24% nella sottoscrizione dei contratti, per il 21% nei progetti e nelle pratiche edilizie, per il 19% nelle procedure gestionali aziendali, per il 10% nella gestione delle fatture elettroniche e per il 10% altri scenari[73].

[73] Dati rilevati attraverso una Survey condotta da Aruba – Luglio 2020

Figure 19



Nell'ambito della Pubblica Amministrazione in particolare, crea un impatto di gran lunga positivo. Si pensi per esempio al cambiamento che si è dovuto fronteggiare nell'ultimo anno, a seguito della pandemia COVID-19, per quanto riguarda il settore terziario. Si è manifestata la necessità di gestire processi e documenti informatici in modalità del tutto digitale garantendo alti livelli di integrità e riservatezza. Non si tratta più di dotare le Pubbliche Amministrazioni di computer e accessori digitali per realizzare una trasformazione digitale, ma si deve focalizzare l'attenzione sul patrimonio dei dati industriali e posseduti dalla PA, la cui gestione sicura e la cui economia è la sfida del futuro per il Paese.

Digitalizzare le attività organizzative non vuol dire semplicemente sostituire il documento cartaceo con quello digitale, bensì progettare e gestire tutti i processi organizzativi in modo integrato e collaborativo modificando i modelli di business, i processi operativi e le *customer experience*. L'introduzione di tecnologie specifiche come la firma digitale fa parte della radicale trasformazione all'interno della PA italiana, permettendo anche un nuovo modo di lavorare, significativi vantaggi in termini di costi, tempi e gestione delle risorse umane[74].

Tra i principali vantaggi apportati dalla dematerializzazione dei documenti infatti, vi è il contenimento dei costi di gestione dei documenti cartacei: è possibile creare direttamente un documento elettronico legale con firma autografa, eliminando il passaggio dal cartaceo al digitale, in modo da rendere nulli i costi legati alla gestione della carta, del toner e dell'usura delle stampanti e riducendo i costi di scansione e archiviazione.

La firma digitale comporta anche un aumento della peformance dei processi che diventano più efficienti, snelli e veloci, infatti i documenti firmati in modalità elettronica sono subito disponibili al Sistema Informativo aziendale e condivisibili, così da eliminare fraudolente duplicazioni.

[74] Vincenzo Pensa, responsabile in ACI (Automobile Club d'Italia) di transazione digitale

CAPITOLO QUARTO: INTERVISTA A VINCENZO PENSA DELL'AUTOMOBILE CLUB D'ITALIA: UN CASO DI SUCCESSO DELLA DIGITALIZZAZIONE DELLA PUBBLICA AMMINISTRAZIONE

Introduzione

Nei precedenti capitoli è stata analizzata ed approfondita l'evoluzione in atto del settore della pubblica amministrazione, con i relativi programmi di Amministrazione Digitale e E-Government. Ci si è soffermati sull'utilizzo delle tecniche di Cloud Computing e l'utilizzo di tecnologie a supporto, come la firma digitale, per implementare processi di dematerializzazione e adottando una strategia digitale volta ad abbandonare l'utilizzo di documenti cartacei. Si è voluto dimostrare come ad oggi la digitalizzazione, in particolare dei documenti, rappresenti la leva trainante di ogni business e anche per la PA nel rapporto col cittadino.
Sono state numerose le realtà pubbliche italiane che hanno intrapreso ormai da tempo un percorso digitale per garantire i servizi pubblici ai cittadini e durante l'emergenza COVID-19 è emersa ancor più chiaramente a tutti, cittadini e dipendenti pubblici, l'importanza di rendere i processi interamente digitali per evitare la diffusione del virus a seguito dell'affluenza presso gli sportelli pubblici.
È stato proposto il caso studio di ACI (Automobile Club d'Italia) in quanto è stata una delle prime Pubbliche Amministrazioni a passare a servizi e tecnologie ICT, anche se da sempre la tecnologia è stata interpretata come elemento competitivo di sviluppo e di trasformazione, anche in epoche in cui era meno evidente l'impatto che la digitalizzazione avrebbe avuto sulle attività e sul mondo. Al giorno d'oggi stiamo assistendo a come la PA sta cambiando e ci sono dei programmi rivolti appunto all'innovazione e alla trasformazione digitale di questa (vediamo per esempio il Piano Triennale 2020-2022).

Per condurre il caso studio, sono state utilizzate diverse fonti, tra le quali un maggiore contributo è derivato dalle interviste al personale di ACI e in particolare al Responsabile di Transizione Digitale dell'ACI, Vincenzo Pensa. Le interviste condotte sono state tre, ognuna delle quali basata su un tema specifico. Nella prima si è chiesto di illustrare la storia evolutiva dell'ente in questione, contestualizzando il cambio della *mission* in concomitanza con l'era della "*digital transformation*". Nella seconda, si è chiesto di raccontare come ACI ha risposto alle misure adottate dal governo per intraprendere la trasformazione digitale della Pubblica Amministrazione, in particolare quale *road map* ha seguito e quali sono stati i filoni di attività prevalenti nonché il cambiamento del modello di business e operativo. Infine, nella terza e ultima intervista, ci si è soffermati sull'utilizzo delle tecnologie a supporto della digitalizzazione, ovvero sistemi *cloud based* e la firma digitale, ed è in quest'ultima parte che si è potuto evincere il forte contributo della firma digitale. Questa, è stata la tecnologia abilitate la dematerializzazione dei documenti che ha potuto poi costituire l'impalcatura su cui implementare la vera trasformazione digitale dell'ente.

Un'ulteriore intervista, circa il funzionamento tecnico della firma digitale e come questa possa garantire sicurezza e integrità ai documenti, è stata condotta a Federico Berti, Marketing Manager di ItAgile, società specializzata nella fornitura di soluzioni informatiche per il documento digitale, e che rappresenta la punta di diamante per i servizi di firma digitale remota in Italia.
Ai fini della stesura del caso in questione, sono stati raccolti anche dati di archivio, consultato il bilancio sociale e video esplicativi sulla base della letteratura e degli approfondimenti riportati nell'elaborato.
Per la raccolta delle diverse fonti si è impiegato un tempo di circa sei mesi.
Nel presente capitolo verrà quindi illustrato come la società ACI ha ormai adottato una strategia interamente digitale, basata su infrastrutture come SPid, PagoPA, fatturazione elettronica, il passaggio al cloud, IO App, iniziata primariamente dall'introduzione della firma digitale per firmare documenti online e adottare un approccio "*paperless*", favorendo la digitalizzazione e la dematerializzazione dei documenti informatici.

La storia dell'ACI e l'evoluzione tecnologica

Prima di analizzare la società con i relativi progetti innovativi, è opportuno descriverla menzionando la sua storia, i suoi obiettivi, la sua vision e mission.
ACI è un ente pubblico ed è anche la più grande associazione nazionale esistente, libera associazione di automobilisti, che coniuga di fatto questa sua particolare condizione di essere un'associazione libera di persone, automobilisti in questo caso, e una pubblica amministrazione a cui lo stato affida dei compiti attraverso la legge. Questa è la peculiarità di ACI, che spazia in diversi settori, da quello della mobilità, che è quello che la contraddistingue, a quello dello sport, infatti ACI è anche la federazione sportiva del CONI per gli sport automobilistici, a quello della Pubblica Amministrazione, per la gestione del Pubblico Registro Automobilistico, e altri compiti che riguardano la gestione amministrativa e fiscale dei veicoli, conosciuti soprattutto per il pagamento del bollo auto. Si occupa inoltre di assistenze tecniche e sanitarie.
La mission è mutata nel corso degli anni, infatti, quando è stato costituito l'ACI verso la fine dell'800, la mission era quella di promuovere la motorizzazione di un paese che chiaramente veniva da una tradizione diversa basata per lo più sull'agricoltura. Questo obiettivo primario nel corso degli anni è andato via via trasformandosi e adeguandosi ai tempi, per cui oggi la mission dell'ACI "è diventata quella di presidiare i molteplici versanti della mobilità, declinata in tutte le sue forme, e quindi il compito istituzionale, il compito legato all'innovazione, legato all'ambiente, alle dinamiche sociali ed economiche basate su una forma di tutela legata all'esperienza e alla professionalità dell'ACI nella difesa dei diritti alla mobilità […] Questa è una mission coerente con l'organizzazione ti tipo federativo dell'ACI ed è un ente presente su tutto il territorio nazionale, su tutte le province e che ha un'articolazione particolarmente ramificata attraverso i 1600 punti di servizi sul territorio" (Vincenzo Pensa).

È stato chiesto allo stesso Vincenzo Pensa, Responsabile di Transizione Digitale dell'ACI, quale *road map* abbia seguito l'ACI per quanto riguarda la digitalizzazione, e quali sono stati i filoni di attività prevalenti, il cambiamento del modello di business e operativo. Non è facile individuare i driver su cui impostare il percorso di trasformazione digitale in quanto i driver sono molteplici, il percorso sulla scia del digitale è stato intrapreso da ACI molto tempo fa e continua oggi; riportando le parole del Dr. Pensa "in ACI da sempre la tecnologia, l'innovazione e il cambiamento hanno sempre rappresentato un punto di riferimento e sono stati interpretati come elemento competitivo di sviluppo e di trasformazione, anche in epoche in cui era meno evidente l'impatto che la digitalizzazione avrebbe avuto sulle attività e sul mondo. Questo è importante perché la trasformazione deve trovare all'interno di un'organizzazione un terreno fertile, altrimenti le resistenze sono un elemento di criticità non indifferente. Noi abbiamo puntato molto sulla digitalizzazione dei processi, questo sicuramente è un elemento che consente di abilitare tutta un'altra serie di attività e sviluppi, altrimenti è difficile immaginare una transizione digitale se i processi non sono progettati e pensati in un'ottica digitale. Dico questo perché spesso si confonde la mera trasposizione di un processo attraverso l'impiego di tecnologie dell'informazione. Questo non fa altro che replicare, migliorando probabilmente in termini di efficienza il processo, ma non cogliendo tutte quelle che sono le opportunità che la digitalizzazione offre nel momento in cui il processo viene integralmente ripensato".
Nella reingegnerizzazione dei processi di servizio al pubblico, ACI ha sempre avuto come punto di riferimento il cittadino e un aspetto sul quale si è investito molto è stato quello della formazione del personale perché "per calare una cultura nuova e un modo nuovo di rapportarsi con le attività usuali, il fattore umano è determinante sotto molteplici punti di vista: il corretto utilizzo degli strumenti, delle procedure ma anche l'interpretazione del ruolo cambia, perché parte delle attività vengono in qualche modo assorbite dal processo tecnologico e quindi viene riservato al fattore umano un elemento di maggior livello e maggiore qualità, quindi c'è una spinta verso l'alto delle competenze e per fare questo occorre passare attraverso un processo di promozione, di addestramento, che non è banale e quindi anche questo tipo di percorso va avviato per tempo" (Vincenzo Pensa).

Nel corso dell'elaborato, si è voluto mettere in luce come nell'era della *digital transformation*, la digitalizzazione dei documenti assume un valore importante nel rapporto con l'utenza e di conseguenza come questa rappresenti un vantaggio competitivo per ogni amministrazione pubblica. Da sempre ACI è stata protagonista di grandi progetti di digitalizzazione e informatizzazione nell'ambito della Pubblica Amministrazione. Intorno agli anni 90, attraverso la microfilmatura, sono stati digitalizzati volumi cartacei su cui erano annotati atti e provvedimenti, un processo che ha permesso ad ACI di arricchire il proprio patrimonio informativo all'interno di un perimetro di trattamento delle informazioni automatizzate, quindi trasformando la carta in BIT. Successivamente la carta è stata abbandonata anche come input e l'input è avvenuto direttamente in digitale.

In particolar modo, si fa risalire una particolare accelerazione di questi processi, a partire dal 2015 con l'introduzione del Certificato di Proprietà digitale, volto a semplificare la mobilità dell'autista italiano.
Il 5 ottobre 2015, è stata una data cruciale per l'organizzazione in quanto ha dato inizio a tutti i processi di digitalizzazione nel mondo automobilistico favorendo e incrementando la semplificazione dei servizi, alleggerendo la burocrazia della PA, rendendola meno invasiva. Infatti, tale digitalizzazione costituiva l'asse portante del progetto "Semplific@uto", una strategia nazionale di semplificazione e digitalizzazione della documentazione relativa ai veicoli.
A livello di ecosistema, questo ha avuto un grande impatto per tutti i soggetti coinvolti, cittadini, ente stesso e altre Pubbliche Amministrazioni, e ha comportato l'introduzione di procedure informatiche per consentire la gestione del documento in modo digitale. Sempre in linea con quanto riportato dalle disposizioni del Codice dell'Amministrazione Digitale (D.lgs n.82/2005 e s.m), il vantaggio immediato generato per il cittadino è stato l'impossibilità di smarrire tale certificato, evitando una nuova richiesta del duplicato al Pubblico Registro Automobilistico (PRA), così da limitare sprechi di tempo e risorse economiche. Il certificato di proprietà, infatti, non viene più rilasciato all'utente, il quale riceve in cambio una ricevuta disponibile anche online. La ricevuta contiene anche un codice per visionare il certificato e che testimonia la certezza dell'autenticità del documento. La consultazione può avvenire mediante smartphone o altro dispositivo idoneo con lettura del QR-code, direttamente sul sito web indicato nella ricevuta stessa oppure collegandosi al sito web ufficiale ACI.
A contribuire alla dematerializzazione del certificato è stato il dispositivo HSM (*hardware security module*) di firma remota CoSign. Con questa soluzione si è potuta garantire la protezione e la conservazione di migliaia di certificati digitali e se precedentemente, in caso di smarrimento era necessaria la denuncia alle Autorità, i nuovi certificati non possono più essere contraffatti o smarriti e non comportano ulteriori costi.
Il primo bilancio dei certificati di proprietà digitali dei veicoli presentato a sei mesi dal lancio ha potuto subito contare circa 6 milioni di certificati di proprietà.
Questo ha sicuramente apportato vantaggi all'intero ecosistema dell'auto, dagli operatori professionali, all'Agenzia delle Entrate, agli utenti e anche alla Pubblica Amministrazione in termini di risparmi economici, snellimento delle procedure e sicurezza dei documenti. Inoltre, questo cambiamento di digitalizzazione del PRA, ha avuto anche dei ritorni economici per la stessa associazione, in quanto i certificati digitali non devono più necessariamente subire un processo di trasformazione ma possono essere direttamente emessi digitalmente, evitando sprechi inutili di carta.

ACI al giorno d'oggi si ha sviluppato progetti interamente digitali per quanto riguarda il mondo sportivo, il mondo associativo, il mondo dei servizi all'automobile con la piena digitalizzazione del supporto di servizio al soccorso stradale, per cui oggi il cittadino, utilizzando un'applicazione, può tranquillamente fare richiesta di assistenza, seguire lo stato di avanzamento del soccorso fino a quando non lo vengono a prendere e lo

portano a destinazione. Può essere considerata un caso studio europeo di ammodernamento della Pubblica Amministrazione per la gestione dei procedimenti amministrativi, dematerializzazione e conservazione dei documenti, adempiendo alle linee guida individuate nel Codice dell'Amministrazione Digitale (CAD), dall'Agenzia per l'Italia Digitale, dal Decreto Semplificazione e Sviluppo e dalle iniziative sulla Cittadinanza Digitale.

È stato chiesto, a tal proposito, allo stesso Vincenzo Pensa, in che modo ACI ha risposto alle misure messe in atto dal governo a seguito del *lockdown* al fine di garantire continua operatività e servizio.

"Il governo ha adottato una serie di provvedimenti nel corso degli anni che dovrebbero aiutare il nostro paese alla digitalizzazione dei servizi, per esempio, nell'ultimo periodo sono state abbozzate linee di sviluppo per quanto riguarda infrastrutture, piattaforme (come Spid, PagoPA, fatturazione elettronica, il passaggio al Cloud, l'abbozzo dei poli strategici nazionali). Sono linee sulle quali occorre che il governo e il parlamento puntino ad una maggiore risolutezza perché se c'è un fatto che il *lockdown* ha dimostrato è che esistono delle possibilità di avere un altro tipo di amministrazione pubblica, un altro tipo di impresa, un altro tipo di rapporto lavorativo. Ora bisogna percorrere con coraggio questa strada perché io credo che la digitalizzazione potrà arrecare dei grossi benefici in termini di competitività, di benefici ambientali e anche dal punto di vista del vantaggio dei lavoratori".

Verso un'amministrazione interamente digitale: il progetto "PagoBollo"

A partire dalla dematerializzazione del certificato digitale e dall'adozione della firma digitale, negli anni a seguire ACI ha intrapreso una strategia basata sulla generazione di processi totalmente digitale come il processo di compravendita di un'auto, che può avvenire tramite strumenti e tecnologie che consentono di gestire la firma digitale e l'autenticazione degli operatori abilitati ad espletare le formalità in ambito del Pubblico Registro Automobilistico (PRA).

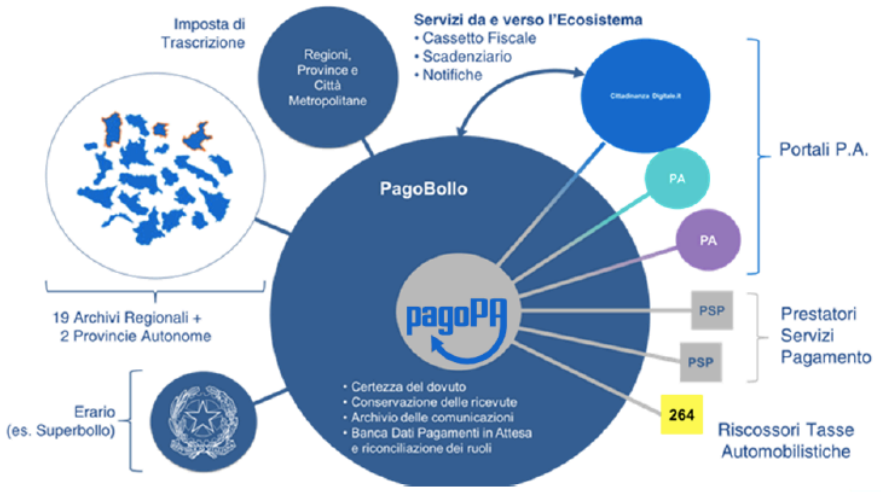
Inoltre, per evitare l'affluenza delle persone fisiche sul luogo, è stato sviluppato internamente un applicativo WEB, "PrenotACI", che consente ai cittadini e agli operatori professionali di prenotare gli appuntamenti dal sito WEB ACI e dai siti web degli Uffici Territoriali del PRA, tramite accesso SPID.

In particolare, un progetto che ha contribuito a realizzare un cambio di paradigma dell'ACI, facendone una Pubblica Amministrazione interamente digitale connessa al Sistema Pubblico del Paese, è stato il progetto "PagoBollo", realizzato in collaborazione ACI Informatica, partner tecnologico dell'Automobile Club d'Italia (ACI), con AGID e il Team per la trasformazione Digitale per dare la possibilità ai cittadini di aderire agli obblighi di pagamento online con pagoPA in modo agevole, direttamente da casa o dai dispositivi mobili.

Gli obiettivi del progetto sono stati tre:

- Estendere l'incasso del pagamento del tributo a tutte le reti dei Prestatori di Servizi di Pagamento (PSP) collegate al nodo dei pagamenti pagoBollo e pagoPA;

- Creare un servizio comune per favorire il monitoraggio e il controllo dei versamenti a tutte le Amministrazioni;
- Dotare l'ACI e la propria rete fisica di delegazioni di un collegamento diretto con PagoPA facendo sì che gli incassi dei tributi dovuti alla Pubblica Amministrazione fossero possibili anche attraverso la propria rete.

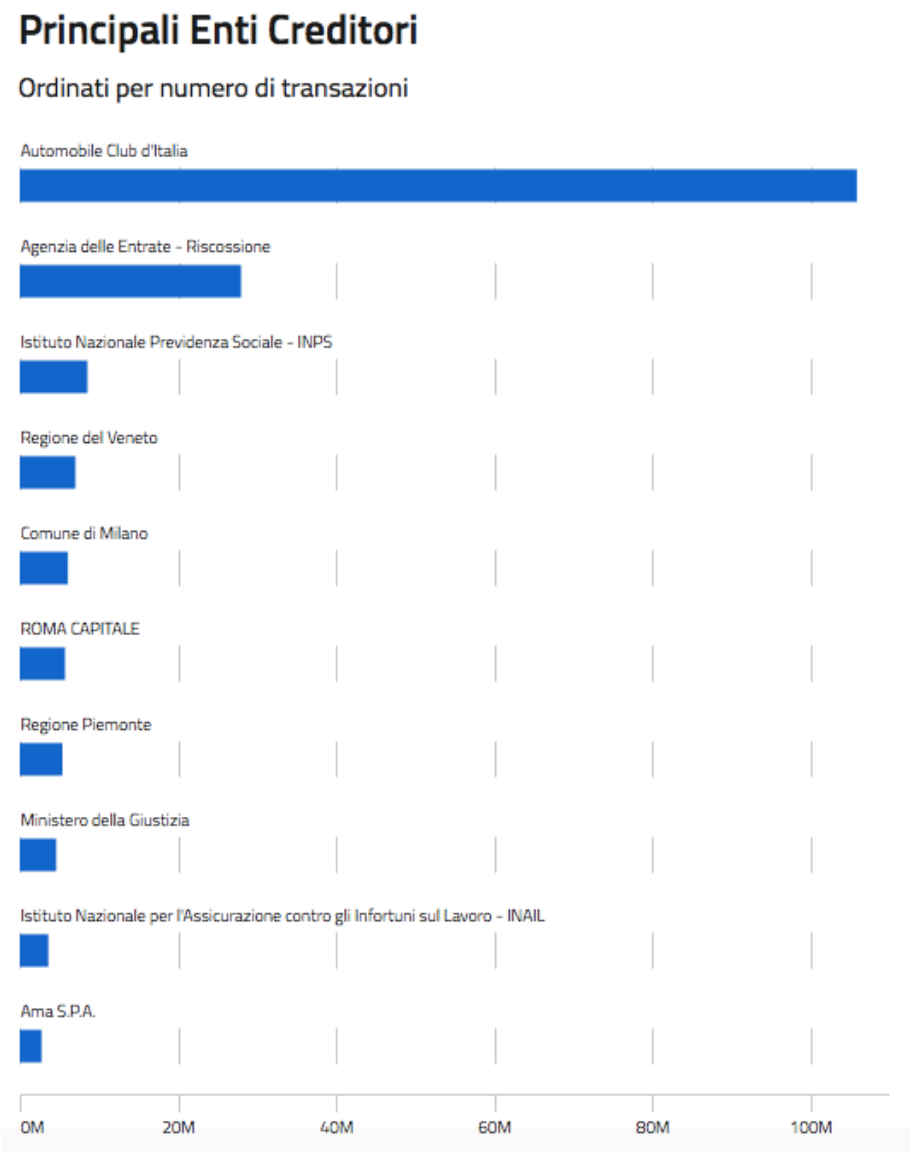


Questo progetto ha avuto benefici sia per i soggetti interni che esterni:

- Si sono potuti limitare i costi di gestione della riscossione dei tributi generati dalle commissioni bancarie, necessari per garantire i pagamenti online;
- Si è dato vita alla digitalizzazione e alla conservazione delle ricevute online risparmiando in termini di carta;
- Benefici legati all'introduzione del sistema innovativo di orchestrazione dei vari archivi che ha consentito ad ACI di aumentare la propria capillarità (ha convertito la propria rete fisica di Delegazioni, circa 1500, in PSP) e di razionalizzare alcune funzioni di controllo consentendo risparmi significativi e una riduzione dei contenziosi tra regioni e cittadini.

Successivamente, anche i pagamenti PRA sono confluiti sul sistema PagoPA e da subito si è potuto prendere atto del forte contributo generato da ACI alla digitalizzazione della Pubblica Amministrazione Italiana.
Di seguito infatti sono riportate le transazioni generate su pagoPA, nonché il valore economico generato, negli ultimi tre anni, dal 2019 al 2021, con previsioni future per la fine dell'anno.
Subito di seguito è riportato un grafico dei principali Enti Creditori ordinati per numero di transazioni dal 2019 al 2021.

Anno	Transazioni	Valore economico generato	Totale transazioni	Totale valore economico generato
2019	51.784.408	€8.341.588.984	244.222.514	€ 46.322.390.605
2020	101.053.996	€19.780.706.406		
2021[75]	91.384.110	€18.200.095.215		
Previsioni fine 2021	177.772.420	€35.110.082.607	**Tasso di crescita** +65%	



[75] Numeri aggiornati in data 24/08/2021

La roadmap dell'applicazione IO

Il sistema di autenticazione digitale (SPID), introdotto da ACI Informatica già con nel 2015 con la digitalizzazione dei certificati di proprietà e in linea con le direttive del Codice dell'Amministrazione Digitale, ha permesso all'ente pubblico di abilitare altri processi per semplificare la vita del cittadino.
ACI infatti, è stata tra le prime Pubbliche Amministrazioni italiane a prendere parte, nel 2019, alla sperimentazione dell'applicazione IO, il progetto ideato dal Governo italiano che permette di creare una sinergia tra le diverse Pubbliche Amministrazioni, fornendo al cittadino un portale per interagire con le PPAA per informazioni, scadenze e pagamenti. In particolare, si è permesso ai cittadini di tenere traccia delle comunicazioni, pagamenti e documenti in un'unica applicazione, in modo sicuro e sempre a portata di mano.
Il progetto aderisce al rispetto dell'art. 64 bis del nuovo CAD, che prevede un singolo canale di accesso digitale per i servizi erogati dalla PA e che mette in evidenza un cambio di paradigma nei rapporti con il cittadino volto a rendere questi ultimi più semplici, rapidi e trasparenti.
Per iniziare a utilizzare l'applicazione IO, bisogna registrarsi con le credenziali SPID o, in alternativa, con la Carta d'Identità Elettronica (CIE). In seguito alla prima registrazione, è possibile accedere più facilmente digitando un PIN personale o tramite riconoscimento biometrico (impronta digitale o riconoscimento del volto) per rendere IO un canale sicuro; infatti, utilizzare l'identità digitale per accedere ai servizi significa garantirla come certa e inequivocabile agli Enti che sono chiamati ad esaminarla. Anche il PIN e i dati biometrici utilizzati per accedere all'app vengono conservati criptati solo nel tuo smarphone.
ACI, nel Luglio 2019, sbarca su IO con i certificati di proprietà dei veicoli e la possibilità di pagare online il bollo auto, mettendo a disposizione sull'applicazione i dati relativi al pagamento della tassa automobilistica e ai certificati di proprietà digitale. Attraverso l'integrazione con le piattaforme pagoPA, ANPR e SPID, l'app IO consente ai soci ACI di essere avvisati quindici giorni prima della scadenza del bollo auto, di ricevere un avviso di bollo scaduto se non pagato, con annessa possibilità di pagamento attraverso la piattaforma PagoPA e la visualizzazione del certificato di proprietà digitale del veicolo. Infatti, le funzionalità dell'applicazione IO sono riconducibili a tre aree:

1. **Messaggistica**: gli enti pubblici possono inviare messaggi ai cittadini relativamente a scadenze e comunicazioni personali;
2. **Pagamenti**: attraverso l'integrazione nell'app di PagoPA, è possibile pagare direttamente dall'applicazione utilizzando un QR code e archiviare sul Cloud le operazioni effettuate per consultarle quando si voglia;
3. **Documenti**: in un'ottica sempre più digitale, la dematerializzazione dei documenti ha permesso di ricercare, consultare, richiedere e condividere sul proprio smartphone i documenti personali, i certificati e le ricevute.

Queste funzionalità sono state rese possibili dall'integrazione di alcune piattaforme abilitanti come l'identificazione tramite SPID, l'anagrafe unica ANPR, per raccogliere i dati dei cittadini da tutte le anagrafi e il sistema dei pagamenti PagoPA.
I servizi attivi resi da ACI sull'applicazione sono quattro:

1. **Certificazioni e Attestazioni di Proprietà**: il servizio è valido per tutte le certificazioni e attestazioni dei veicoli registrate al PRA dal 5 ottobre 2015, in modalità interamente digitale. Permette all'utente di visualizzare il suo certificato di proprietà digitale in caso di acquisto di un nuovo veicolo o di visualizzare i veicoli a lui intestati con i relativi certificati digitali;

2. **AvvisACI**: il servizio "AvvisACI" invia all'utente, intestatario di un veicolo, una notifica relativa alla trascrizione al PRA dello stesso veicolo in caso di pratiche a questo allegate, come per esempio l'iscrizione o la cancellazione del fermo amministrativo da parte di un Agente della riscossione, la redazione per la demolizione, il passaggio di proprietà al nuovo acquirente o la perdita/rientro in possesso del veicolo;

3. **Bollo Auto**: attraverso l'applicazione sarà possibile ricevere una notifica per ricordare all'utente della scadenza del pagamento del Bollo Auto e pagare lo stesso online, tenendo traccia dell'importo versato.

4. **Comunicazione Istituzionale**: il servizio sarà annesso all'introduzione della versione open-beta dell'app IO, ancora in fase di sviluppo, e farà si che l'utente possa ricevere messaggi informativi a carattere istituzionale ed essere aggiornato nel caso in cui vengano introdotti servizi differenti.

Per avere un'idea dei numeri, nel corso del 2020, ACI ha erogato 4 servizi di messaggistica per il cittadino:

- Circa 2.980.000 messaggi di benvenuto inviati nell'anno
- Circa 232.000 messaggi inerenti la scadenza della Tassa Automobilistica
- Circa 2.108.000 messaggi di riepilogo CDP/AdpD
- Circa 111.000 messaggi AvvisACI

CONCLUSIONI

Abbiamo visto come nell'epoca della *digital transformation*, la digitalizzazione della Pubblica Amministrazione rappresenti una delle principali innovazioni che ha inciso fortemente nella gestione dei rapporti con gli utenti per quanto riguarda la fruizione dei servizi amministrativi.

L'innovazione, intesa come forza trasformatrice volta a modificare e a provocare uno svecchiamento di antiche tecniche e metodologie, è stato un aspetto cruciale per la Pubblica Amministrazione e su cui si sta cercando continuamente di fare leva per determinare un cambiamento strutturale per l'ecosistema che la circonda. La sfida consiste nel diventare un tipo diverso di organizzazione, meno ingessata, meno rigida e abituata a una trasformazione continua che possa supportare i cittadini attraverso l'erogazione dei servizi digitale, che devono essere semplici da usare.

In questo caso, l'implementazione di tali servizi attraverso nuove tecnologie, è stata una delle maggiori innovazioni che ha alimentato la nuova organizzazione delle attività, del lavoro dei dipendenti e delle procedure della Pubblica Amministrazione. In questo contesto, la normativa nazionale degli ultimi anni, ha voluto regolamentare l'ampliamento delle tecnologie informatiche all'interno delle amministrazioni pubbliche, a partire proprio dalla regolamentazione dei documenti informatici e dei dati sensibili che contengono. Per promuovere la trasformazione digitale del Paese e degli enti pubblici infatti, l'Agenzia Italiana delle Entrate (AgID), ha pubblicato il nuovo Piano Triennale per l'informatica nella Pubblica Amministrazione (2020-2022), avendo come fine primario quello di indirizzare gli investimenti in ICT del settore pubblico, in modo da eliminare i processi burocratici che da sempre lo caratterizzano.

Si è dimostrato come il processo di trasformazione e l'allineamento tra modelli operativi e di business, tecnologia, cultura organizzativa richieda tempo e sforzi enormi, infatti, deve essere un processo che viene implementato attraverso una *road map* chiara e concisa. Non è possibile pensare di adoperare tecnologie e sistemi digitali, cambiando il modo di operare, senza aver definito una strategia che gradualmente porti ad adottarli.

Abbiamo potuto vedere come la dematerializzazione e la digitalizzazione dei documenti cartacei sia stato il punto da cui partire per poi abilitare tutta un'altra serie di servizi a supporto del cittadino che hanno fatto della Pubblica Amministrazione una realtà completamente digitale. È possibile traferire, consultare o inviare un documento nel giro di pochi istanti tra amministrazioni diverse, operando in un'ottica interoperabile. È necessario infatti sviluppare sistemi multicanale per gestire la conservazione di documenti digitali e in modalità interamente *paperless*.

Come piattaforma abilitante per la trasformazione digitale si è parlato del Cloud computing, in quanto, a seconda del modello adottato (Saas, Paas o IaaS), consente di abilitare una serie di economia di scala volte a ridurre i costi della tecnologia, a rendere più agile e flessibile l'azienda, a ridurre il time to market e i costi e a garantire sicurezza e affidabilità. Infatti, il punto su cui ci si è soffermati maggiormente è stato quello relativo

alla sicurezza di tali documenti, tema che, secondo l'*IDC Survery Ranking Security Challenge*, si è classificato al primo posto come la più grande sfida del cloud computing, dal momento che i documenti digitali conservati potrebbero costituire oggetto di furto da parte di pirati informatici o essere perduti a causa di un guasto nel *database* dell'azienda.

Nonostante questo, sono stati studiati diversi metodi e algoritmi per incrementare la sicurezza nell'ambiente Coud, come l'uso di un codice telefonico monouso (OTP), la Sicurezza del Software, la Sicurezza fisica e l'approccio algoritmico per la messa in sicurezza del Cloud. Sistemi che hanno riscontrato una forte adozione soprattutto nell'ultimo anno a seguito della pandemia COVID-19, in quanto le imprese e le pubbliche amministrazioni sono state costrette a lavorare in modo agile, rendendo il Cloud il miglior alleato per rispondere rapidamente alle esigenze pervenute. Nell'ambito della Pubblica Amministrazione è stato infatti dimostrato come l'approccio burocratico che la caratterizza possa essere eliminato, o quanto meno ridotto grazie all'elasticità dei servizi, alla facilità degli aggiornamenti, alla riduzione delle attività manuali, della complessità del supporto e ovviamente dei costi. La Pubblica Amministrazione infatti ha adottato un modello Cloud ad hoc, il "Cloud della PA", nato come modello ibrido per soddisfare le diverse esigenze del settore pubblico.

Per ovviare alla sicurezza dei documenti informatici, garantendo la loro autenticità e riconducibilità del firmatario, si è parlato dell'utilizzo della firma elettronica (avanzata o digitale) e in particolare della firma grafometrica, che, basandosi su un sistema biometrico, è in grado di rilevare una serie di parametri legati al comportamento dell'utente, che vengono poi cifrati e associati al documento firmato rendendo tale tecnica più efficace di altri sistemi basati su altri sistemi tecnologici, come quelli precedentemente citati. Tale strumento, soprattutto in risposta all'emergenza COVID-19, ha permesso alle aziende e alla Pubblica Amministrazione di gestire processi e documenti informatici in modalità del tutto digitale garantendo alti livelli di integrità e riservatezza. Dalla digitalizzazione dei documenti si è potuto dare il via alla digitalizzazione di altre attività modificando modelli operativi e di business e andando a creare un valore diverso per l'utente finale.

Se ancora ci sono dei ritardi nel processo di digitalizzazione della Pubblica Amministrazione, è stato dimostrato come il caso dell'Automobile Club d'Italia abbia fronteggiato con risolutezza e successo un'era tecnologicamente avanzata e la pandemia che stiamo vivendo al giorno d'oggi. Il successo dell'organizzazione è stato garantito dalla flessibilità con cui si è potuta sempre adattare al contesto, essendo stata una delle prime tra le Pubbliche Amministrazioni ad adottare servizi e tecnologie ICT anche quando l'impatto che queste avrebbero avuto sui servizi era ancora sottovalutato.

Infatti, a partire dalla dematerializzazione dei documenti (si è parlato in particolare del Certificato di Proprietà Digitale), grazie all'introduzione della firma digitale e a tecniche di microfilmatura, l'ACI ha dato vita a una *road map* di digitalizzazione basata su infrastrutture come SPid, PagoPA, fatturazione elettronica, il passaggio al Cloud e come ultimo progetto IO App, adempiendo completamente alle linee guida individuate nel Codice

dell'Amministrazione Digitale (CAD), dall'Agenzia per l'Italia Digitale, dal Decreto Semplificazione e Sviluppo e dalle iniziative sulla Cittadinanza Digitale.

Se all'interno del quadro illustrato nell'elaborato ci si è chiesti se le aziende e in particolare la Pubblica Amministrazione, riusciranno a sfruttare il potere del digitale, è possibile concludere che la velocità del progresso digitale, che ha messo a disposizione un ritmo di innovazione crescente, ha anche richiesto l'esodo dalla cultura precedente e l'ingresso nella nuova. Questo necessita di tempo, si tratta di un lungo cammino che richiede di uscire da sé stessi, dai propri schemi mentali, dalle norme di comportamento sociale per adattarsi alla costante per eccellenza della nuova epoca digitale. Quello di ACI ha rappresentato un caso di successo di efficienza digitale della Pubblica Amministrazione, dando vita a un vero e proprio cambio di paradigma che si traduce in risparmio di costi associati alla carta, alla semplificazione delle procedure, al massimo controllo e sicurezza dei documenti e che attesta l'Italia tra i precursori in questo cambiamento.

Bibliografia

A Platform Computing Whitepaper. “Enterprise Cloud Computing: Transforming IT”, Platform Computing, pp6, (2010).

Alaimo, C & Giustiniano, L., Il pendolo del digitale tra innovazione e continuità, in Nunziata, E. (ed) Strategia e azione per la trasformazione digitale, LUP, (2020, forthcoming)

Allen, B., Juillet, L., Paquet, G. and Roy, J., “E-Governance & Government On-line in Canada: Partnerships, People & in Government Information Quarterly”, Vol. 30, No. 1. pp.36–47, (2001)

Agenzia per l’Italia Digitale, “La spesa ICT nella PA italiana” (2019)

Agenzia per l’Italia Digitale, “Piano Triennale 2020-2022”, (2021)

Alessandro Languasco, Alessandro Zaccagnini, “Manuale di crittografia: Teoria, algoritmi e protocolli”, Hoepli Editore, (2015)

Antonino Salvaggio, “Codice OTP: cos’è e come funziona” (2020)

Aruba, Survey interna ai clienti relativamente all’utilizzo della firma digitale (2020)

Bwalya, K., & Mutula, S, “E-government: Implementation, Adoption and Synthesis in Developing Countries. De Gruyter/Saur”, (2014).

Bellini, M., *Internet 4 Things*. Retrieved from Network Digital 360: https://www.Internet4things.it/iot-library/Internet-of-things-gli-ambiti-applicativi- in-italia/, (2020, May 6)

Ben-Zion Chor, “Two issues in public key cryptography: RSA bit security and a new knapsack type system”, MIT Press55 Hayward St.Cambridge MA United States, (1986)

Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective - Sune Dueholm Müller (2015)

Bilancio Sociale 2020 ACI Informatica S.p.a, <http://www.informatica.aci.it/il-nostro-valore/bilancio-sociale.html>

Caterina Ingrosso, “Lean Thinking: Il “pensiero snello” nella Pubblica Amministrazione. Che cos’è? È possibile?”, (2018)

Clayton Christensen, Michael Raynor e Rory McDonald – “What Is Disruptive Innovation?2” (HBR, dicembre 2015)

Chesbrough, H., “Managing open innovation - Research in Technology Management”, 47(1), 23-26, (2004)

Chesborough, H., “The era of Open Innovation”, MIT Sloan Management Review, (2003)

Claudio Gerino “E-government, Italia è agli ultimi posti in Europa”, (2020)

“Cloud computing in Italia, quanto è diffuso?”, https://www.zerounoweb.it/cloud-computing/cloud-computing-in-italia-quanto-e-diffuso/>, (2020)

“Cloud della PA”, <https://www.agid.gov.it/it/infrastrutture/cloud-pa> (2020)

“Cloud Security based on the Homomorphic Encryption”, Article Published in International Journal of Advanced Computer Science and Applications (IJACSA), Volume 10 Issue 8, 2019.

Codice dell’Amministrazione Digitale

Collard, A., “Embracing digital transformation the HMRC way”, https://www.iota-tax.org/sites/default/files/publications/public_files/impact-of-digitalisation-online-final.pdf, (March 2020).

COM/2020/66 final, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni “Una strategia europea per i dati”, Bruxelles, 19.2.2020.

Daniel Riccio, Clemente Galdi, Luigi Catuogno, “Sistemi Biometrici e Sicurezza”

Drucker, P.F., “Innovation and Entrepreneurship”, (1986)

Ernesto Bellisario, “La nuova pubblica amministrazione digitale”, cap. IV, pp. 55-57 , (2019)

E. Mathisen, “Security challenges and solutions in cloud computing”, in 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011).

Fang, Z.Y., “*E-Government in Digital Era: Concept, Practice and Development*”. International Journal of the Computer, the Internet and Management, (2002)

Faraj, S., Pachidi, S., & Sayegh, K., “Working and organizing in the age of the learning algorithm. Information and Organization”, 28(1), 62-70, (2018).

Fountain, J.,“Building the Virtual State: Information Technology and Institutional Change”. Brookings Institution Press, (2001)

Gianluca Bellomo, “Biometria e digitalizzazione della Pubblica Amministrazione”, in “A 150 anni dall’unificazione amministrativa italiana: La tecnificazione”, pp.59/64, (2017).

Giovanni Manca “Breve storia della PA digitale: la genesi e l’evoluzione del Codice dell’Amministrazione Digitale”, (2020)

Giovanni Manca, “Piano triennale Agid 2020-2022 analizzato punto per punto: attuare la PA digitale”, (2020)

Giusella Finocchiaro, “Diritto di Internet”, 3. ed. Zanichelli, (2020)

Global Netoptex Incorporated, “Demystifying the cloud. Important opportunities, crucial choices” pp4-14, (2011)

Hayat Khaloufia, Karim Abouelmehdi, Abderrahim Beni-Hssane, Mostafa Saadi, “Security model for Big Healthcare Data Lifecycle”, (2018)

“I vantaggi delle interfacce di programmazione delle applicazioni”, <https://www.redhat.com/it/topics/api/what-are-application-programming-interfaces>

“Il modello di Cloud della PA”, <https://docs.italia.it/media/pdf/cloud-docs/2019.1/cloud-docs.pdf>, (2020)

Iansiti, M., & Lakhani, K. R., “Rearchitecting the firm”, Competing in the Age of AI. Harvard Business Press Chapter 4, pp. 79-97, (2020)

Intervista a Giovanni Manca, “Breve excursus sulla firma digitale”.

ISO 17888 – clausola 6.6

ISO 17788 – clausola 6.5

ISO 27001 e conservazione sostitutiva, <https://www.csqa.it/Sicurezza-ICT/Focus/ISO-27001-e-Conservazione-sostitutiva>

James P. Womack, Daniel, T. Jones, “Lean Thinking”, Somon & Schuster (1996)

Joan Daemen e Vincent Rijmen, “The Design of Rijndael: Aes-The Advanced Encryption Standard”, Springer, (2002)

Johnson, M., Christensen, C., & Kagermann, H., “Reinventing Your Business Model. In M. W. Johnson, C. M. Christensen, & H. Kagermann, HBR’s 10 Must Read on Business Model Innovation”. Boston, Massachussets: Harvard Busiess Review Press, (2019).

K. K. Chauhan, A. Sanger, and A. Verma, “Homomorphic Encryption for Data Security in Cloud”, IEEE, pp. 206-209, (2015)

Know How, “Indirizzi IP: tutto quello che c'è da sapere”, (2020)

Kuyoro S. O., Ibikunle F. & Awodele O., “Cloud Computing Security Issues and Challenges” (2011)

Legge n. 59 del 15 marzo 1997, “Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa”.

Lips, M., “*Digital Government: Managing Public Sector Reform in the Digital Era*”, Routledge, (2020).

Lundvall e Johnson, “The Learning Economy”, pp. 23-42 (1994)

M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai., “What’s Inside the Cloud? An Architectural Map of the Cloud Landscape.” IEEE Xplore, pp 23-31, (Jun. 2009)

Maria Rosaria Lenti “Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security”, (2017)

Massimiliano Pucciarelli, “Il Cloud nella PA italiana: stato dell’arte e prospettive evolutive” (2020)

Massimo Giussani, “Il riconoscimento biometrico”, (2006)
Mauro Domenici, “Il furto dell’identità digitale e l’illecito utilizzo dei dati raccolti”, (2021)

N. Dowlin, R. Gilad-Bachrach, and K. Laine, “Manual for using homomorphic encryption for bioinformatics” Proceedings of the IEEE, (2017)

Nograšek & Vintar, “E-government and organisational transformation of government: Black box revisited?”, (2014)

Osservatorio Cloud Transformation, “Cloud computing. Cos'è e quali vantaggi porta in azienda”, (2019)

Osservatorio Cloud Transformation, “Cloud in Italia: mercato da 3,34 miliardi, cresce l'adozione anche nelle PMI”, (2020)

Osservatorio Cloud Transformation, “Cloud Transformation: gli ingredienti mancanti” (2019)

Pierguido Iezzi, “Biometria, la terza dimensione della cyber security: soluzioni e problematiche di sicurezza” (2019)

Redolfi, Daniela, “Firma digitale, posta elettronica certificata e dematerializzazione”, p. 53-71, Marsilio, 2011. Ricerche (Marsilio), (2011)

Regolamento UE n° 910/2014 – eIDAS

Riccardo Berti, “Biometria per la sicurezza di computer e cellulare: rischi e limiti”, (2019)

Richard Heeks, “Implementing and Managing e-Government: An International Text”, Sage, (2006).

S. Arnold, “Cloud computing and the issue of privacy”, KM World, pp14-22, (Luglio 2009)

S. Kuila, S. Shruthi, P. Chandan, and N. Ch SN Iyengar, “Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management”, Journal of Computer and Mathematical Sciences vol. 7, (2016)

Sanfelice 1893 Banca Popolare, “La soluzione di Firma Elettronica Avanzata (FEA) grafometrica”
Sarah Ungaro & Andrea Lisi “Che c’è da sapere sulla battaglia per passare dalla carta al digitale nella pubblica amministrazione. I punti fondamentali, le resistenze della PA, le norme e che fare per una svolta”, (2018)

Tapscott, D. and Caston, “*A. Paradigm Shift: The New Promise of Information Technology*”, McGraw-Hill: New York, (1993).

Tat-Kei Ho, A. J., “Reinventing Local Governments and the E-Government Initiative”, (2002)

The Economist, “A survey of government and the Internet”, https://www.economist.com/special-report/2000/06/22/the-next-revolution, (2000)

V. Ashktorab, and R. T. Seyed, “Security threats and countermeasures in cloud computing”, International Journal of Application or Innovation in Engineering & Management (IJAIEM) vol. 1, (2012)

Valentina (Dardha) Ndou, “E – government for developing countries: opportunities and challenges” (2004) p.1-24

Wafa Njima, Marwa Chafii, Raed Shubair, “GAN Based Data Augmentation for Indoor Localization Using Labeled and Unlabeled Data”, (2021),

World Bank, “e-Government”, https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government, (May 2015).

Sitografia

www.aci.it

www.agendadigitale.eu

www.agid.gov.it

www.altalex.com

www.cybersecurity360.it

www.corrierecomunicazioni.it

www.digital4.biz

www.ec.europa.eu

www.eurostat.it

www.forbes.com

www.forumpa.it

www.gartner.com

www.innovationpost.it

www.internet4things.it

www.istat.it

www.mise.gov.it

www.osservatori.net

www.recotech.com

www.sanfelice1893.it

www.zerounoweb.it

Summary

Quando parliamo di innovazione, ci riferiamo a "l'atto, l'opera di innovare, cioè di introdurre nuovi sistemi, nuovi ordinamenti, nuovi metodi di produzione. (…) In senso concreto, ogni novità, mutamento, trasformazione che modifichi radicalmente o provochi comunque un efficace svecchiamento in un ordinamento politico o sociale, in un metodo di produzione, in una tecnica"[76].

Se inventare quindi significa creare qualcosa di nuovo, l'innovazione si sviluppa in questo senso fondendo tecnologie e idee, andando a determinare un cambiamento radicale nella vita delle persone o delle aziende.

Questo ci permette di definire il concetto di "*digital disruption*", il cui fondatore fu Clayton Christensen, ideatore della teoria "*job to be done*", in base alla quale si individua un processo mediante il quale un prodotto o servizio attecchisce inizialmente in semplici applicazioni nella parte inferiore di un mercato e poi si muove inesorabilmente verso l'alto, sostituendo infine i concorrenti affermati. Quindi, l'innovazione dirompente si focalizza non sul prodotto, ma sul bisogno, ancora non soddisfatto, che il prodotto è chiamato a soddisfare. Al centro del processo c'è l'individuo, è possibile affermare che la caratteristica principale della "*disruptive innovation"* è quella di essere legata non tanto a mutamenti tecnologici complessi, quanto alla capacità di definire e cogliere i bisogni di un individuo[77].

Nel campo della Pubblica Amministrazione, è possibile applicare lo stesso concetto andando ad esaminare nuovi modi, ideati sulla base di strategie a lungo termine, di certo meno costosi e più efficaci, quindi anche misurabili, per erogare i servizi pubblici e che giovino all'ecosistema che circonda questi enti, identificando lo sviluppo come una mentalità diffusa.

Nella Pubblica Amministrazione si stanno facendo pressanti due necessità, la prima è il recupero di risorse, dovuta alla necessità di contenere i costi a fronte di esigenze di qualità e livello di servizi crescenti, la seconda è la crescente istanza di semplificazione e de-burocratizzazione che ispira anche i più recenti provvedimenti legislativi.

Già a partire dagli anni Novanta, ci si è iniziati a interrogare su modelli che permettessero alle realtà pubbliche di essere più efficienti ("*Lean Thinking*"[78]), e che oggi sono ripresi con un'inclinazione diversa, andando a identificare l'efficacia di tale modello nella centralità dell'utente e delle sue aspettative, nell'efficienza e nell'efficacia dell'azione amministrativa, nello sviluppo e nel coinvolgimento dei dipendenti pubblici[79]. Ci si chiede infatti le aziende, e in particolare la Pubblica Amministrazione, riusciranno a sfruttare il potere del digitale, la cui sfida risiede nel far convivere l'aspetto teorico e tecnologico dell'innovazione, con quello

[76] Treccani, il portale del sapere, https://www.treccani.it
[77] Clayton Christensen, Michael Raynor e Rory McDonald in "*What Is Disruptive Innovation?*" (HBR, dicembre 2015)
[78] James P. Womack, Daniel, T. Jones, "*Lean Thinking*", Somon & Schuster (1996)
[79] Caterina Ingrosso, "*Lean Thinking: Il "pensiero snello" nella Pubblica Amministrazione. Che cos'è? È possibile?*", (2018)

pratico della sua effettiva applicazione nel tessuto sociale ed economico, e delle relative implicazioni, anche in termini di valore pubblico[80].

Nel corso degli anni ci sono stati diversi cambiamenti finalizzati a creare strutture improntate verso la cultura dell'efficienza e dell'efficacia, a partire da leggi nazionali ed internazionali, intente a modificare in modo "formale la pubblica amministrazione", partendo dalla nuova cultura che si sviluppa di pari passo con la diffusione delle tecnologie ICT. Queste norme mirano a snellire il modello burocratico delle realtà pubbliche, in particolare in materia di documento informatico e di riorganizzazione dei processi, per favorire una corretta gestione dei documenti, andando a sostituire il documento cartaceo con quello informatico, pur mantenendo gli stessi standard di sicurezza. È in questo ambito che viene considerato necessario identificare una *road map* che permetta agli Enti di orientarsi al processo di dematerializzazione con un'ottica di lungo termine, che sia effettivamente praticabile, funzionale e coerente con una strategia di *e-government*.

La connettività digitale ha dato inizio a un nuovo tipo di competizione tra le organizzazioni, basata su informazione e tecnologia, che attiva un ordine di innovazioni dirompenti e cambiamenti bruschi e sediziosi e che vede l'innovazione come un requisito fondamentale per le organizzazioni pubbliche e private che vogliano raggiungere un vantaggio competitivo[81]. Mentre le organizzazioni private si erano già mosse sulla strada del digitale, nel settore pubblico si riscontravano ancora dei ritardi, ma con l'esplosione dell'epoca della *digital transformation*, è stato dato avvio al processo di *e-government*, che ha previsto una serie di azioni e strategie volte a innovare e reinventare il governo attraverso la tecnologia, provocando un "cambio di paradigma", che da burocratico e tradizionale, diventa più flessibile, imprenditoriale e competitivo. Si è visto nella tecnologia uno dei fattori abilitanti la qualità e la reattività dei servizi che forniscono ai propri cittadini, ampliando la portata e l'accessibilità dei propri servizi e delle infrastrutture pubbliche e consentendo ai cittadini di sperimentare una forma più rapida e trasparente di accesso ai servizi governativi, che potrebbero condurre a forme innovative di consultazione pubblica e ad altre forme di partecipazione democratica (Lips 2020[82]). Questa *disruptive innovation* nel settore pubblico ha introdotto "l'era dell'intelligenza di rete", reinventando aziende, governi e individui[83]. Tuttavia, non si tratta semplicemente di adottare tecnologie volte a implementare un servizio già offerto, infatti, definendo l'*eGovernment* come un mero processo verso la transazione digitale o come l'adozione di tecnologie volte a implementare un servizio offerto, non si coglie l'effettiva portata, bisogna piuttosto considerare la tecnologia come una variabile che possa agire pari passo e in maniera co-dipendente ad altri elementi organizzativi come le persone, le infrastrutture e i processi.[84]

[80] Nino Lo Bianco, "*È il momento di osare. Riusciranno le aziende a sfruttare il potere del digitale*?", OpenLab, (2020)
[81] Lundvall e Johnson, "*The Learning Economy*", pp. 23-42 (1994).
[82] Lips, M., "*Digital Government: Managing Public Sector Reform in the Digital Era*", Routledge, (2020)
[83] Collard, A., "Embracing digital transformation the HMRC way", < https://www.iota-tax.org/sites/default/files/publications/public_files/impact-of-digitalisation-online-final.pdf>, (March 2020).
[84] Nograšek, J., & Vintar, M., "E-government and organisational transformation of government: Black box revisited? Government Information Quarterly, XXXI, (pp. 108-118), 2014.

In particolare, ci sono tre aree critiche di trasformazione dell'*eGovernment*[85]:

4. Aree di trasformazione: a seconda dell'uso che si fa della tecnologia, l'area di trasformazione può essere interna, quando la tecnologa è utilizzata per correlare diversi dipartimenti, esterna, quando la si pone al centro per garantire la trasparenza delle informazioni ai cittadini e alle imprese e relazionale, quando crea degli "stati virtuali" (Fountain (2001)) tra le reti pubbliche e private;
5. Utenti, clienti, attori e loro interrelazioni (cittadini, imprese, organizzazioni governative, dipendenti): si vanno a definire in questo ambito quattro blocchi principali: Government to Citizens (G2C), Government to Business (G2B), Government to government (G2G), Government to Employees (G2E)
6. Domini di applicazione dell'*eGovernment* (servizi elettronici, democrazia elettronica, amministrazione elettronica).

L'obiettivo dell'*eGovernment* in relazione è quello di agire su queste aree di trasformazione per generare vantaggi in termini di riduzione dei costi e guadagni di efficienza, qualità della fornitura del servizio ad aziende e clienti, trasparenza, anticorruzione e responsabilità, aumento della capacità del governo, creazione di reti e comunità, miglioramento della qualità del processo decisionale, promozione dell'uso dell'ICT in altri settori della società. Nonostante i vantaggi che la tecnologia possa generare per creare delle amministrazioni digitali, ci sono ancora diverse sfide irrisolte in termini di: infrastrutture ICT (disponibilità in linea, alfabetizzazione informatica, apparecchiature per le telecomunicazioni), mancanza di leggi volte a regolamentare le attività elettroniche, sviluppo delle competenze tecnologiche nel capitale umano, resistenza al cambiamento per problematiche culturali, partenariato e collaborazione, strategia, e ruolo di leadership.

La produzione normativa nazionale degli ultimi anni presenta un processo evolutivo complesso, ma decisamente orientato ad una sempre maggiore applicabilità, coerentemente con le disposizioni emanate dalla UE, verso la direzione dell'ampliamento dell'adozione delle tecnologie informatiche all'interno delle amministrazioni pubbliche, in particolare in materia di documento informatico e di riorganizzazione dei processi. Tra queste, in Italia, la prima risposta organica all'esigenza di riorganizzazione della PA, alla luce delle trasformazioni imposte dalle nuove tecnologie e che rappresenta ormai la norma centrale e di riferimento per la digitalizzazione della nostra pubblica amministrazione, è costituita dal Codice dell'Amministrazione Digitale (introdotto per la prima volta con il D.lsl. n. 82/2005), che regolamenta strumenti informatici, un esempio ne è la firma digitale.

Anche su scala sovrannazionale sono stati avanzati programmi e strategie volti a favorire la digitalizzazione dell'amministrazione pubblica. Nel 2010 la Commissione ha realizzato un documento confluito nell'Agenda Digitale Europea, che si proponeva il raggiungimento di determinati obiettivi entro il 2020, come l'utilizzo dello Spid (Sistema Pubblico per l'Identità Digitale) per l'accesso ai portali, o l'utilizzo della piattaforma

[85] Valentina (Dardha) Ndou, "E – government for developing countries: opportunities and challenges", EJISDC (2004) 18, 1, 1-24

PagoPA per la gestione delle transazioni. Secondo lo studio Uil-Eures[86], questi obiettivi ancora non sono stati realizzati del tutto a causa di un'implementazione delle procedure sul piano formale ma non sostanziale e applicativo, e a causa della scarsità di investimenti nel *re-skilling* del personale nell'utilizzare le nuove procedure e i nuovi *softwares*.

Secondo l'*Indice Sintetico di Digitalizzazione dell'Economia e della Società (DESI)*, l'Italia si trova al venticinquesimo posto (su ventotto paesi) con un indice di digitalizzazione pari a 43,6, paragonato ad un punteggio medio di 52,6 ottenuto dagli altri paesi[87]. Per colmare a questo gap, l'AgID ha pubblicato il nuovo Piano Triennale per l'informatica nella Pubblica Amministrazione (2020-2022)[88], col fine primario quello di indirizzare gli investimenti in ICT del settore pubblico soddisfacendo i seguenti requisiti: "digital and mobile first, digital identity only, cloud first, servizi inclusivi e accessibili, dati pubblici un bene comune, interoperability by design, sicurezza e privacy by design, user-centric, data driven e agile"[89].

Uno dei maggiori punti di criticità per l'attuazione di un effettivo processo di dematerializzazione e digitalizzazione della Pubblica Amministrazione, si riscontra nell'ingessante e complesso quadro normativo che disciplina i processi di gestione documentale. Negli ultimi anni, si è vista la necessità di ripensare alla gestione tradizionale dei documenti cartacei, con l'esigenza di digitalizzarli, al fine di contenerne i costi relativi alla stampa, alla copia, all'invio e alla conservazione.

Siamo stati e siamo spettatori di una trasformazione rivoluzionaria che in poco più di un decennio ci ha permesso di transitare dal floppy disk al cd, e poi alla chiave USB e ad altri tipi di supporti portatili di memoria. L'esigenza di disporre di un supporto fisico per la produzione e conservazione di dati, documenti e informazioni, è venuta sempre meno grazie alla progressiva diffusione del *cloud computing*. Se inizialmente il cittadino rimaneva comunque vincolato al supporto cartaceo, ritenendolo inalterabile e autentico, con l'introduzione della firma digitale e del riconoscimento giuridico del documento firmato elettronicamente, questo inizia ad avere diversi gradi di validità ed efficacia[90].

Sia che il documento nasca informatico o che lo diventi nel tempo, il fine ultimo è quello di ridurre sprechi di carta e agevolare le procedure amministrative. Infatti, un approccio *paperless document*, oltre a realizzare questo ultimo obiettivo, agevola le procedure amministrative (accesso facilitato da remoto, testo ricercabile, gestione più competitiva, tracciabilità e rintracciabilità) e al giorno d'oggi rappresenta un imperativo nell'ottica di ridurre i costi di gestione per indirizzarli in investimenti cloud.

---

[86] Fonte: Elaborazione Eures Ricerche Economiche e Sociali su dati Agenzia per l'Italia Digitale, Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021 *escluse le regioni

[87] Claudio Gerino, "E-government, Italia è agli ultimi posti in Europa", (06/08/2020).

[88] COM(2018) 98: "Un quadro finanziario pluriennale nuovo e moderno per un'Unione europea in grado di realizzare efficientemente le sue priorità post-2020".

[89] https://www.agid.gov.it/it/agenzia/piano-triennale

[90] Legge n. 59 del 15 marzo 1997, "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa".

Il cloud computing può essere interpretato non solo come una piattaforma abilitante per la trasformazione digitale, ma anche come un ecosistema che crea valore per l'impresa grazie alle numerose possibilità di interconnessione di strumenti, permettendo alle aziende di essere maggiormente agili e flessibili, di ridurre il time to market e i costi, e garantendo sicurezza e affidabilità. Infatti, è possibile identificare due definizioni, una sul lato tecnologico, intendendo il cloud come "*un modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi"*[91], e l'altra da un punto di vista commerciale, guardando al cloud computing come l'artefice della minimizzazione complessiva dei costi della tecnologia: integrando diversi profili di domanda su risorse condivise, consente il raggiungimento di importanti economie di scala e l'erogazione agevole e flessibile dei servizi.

In particolare, il sistema di cloud computing è caratterizzato da un'architettura contenente una rete che collega l'utente al fornitore di servizi, che può offrire tre principali *cloud service model*[92]: Saas, Paas e Iaas. Il primo, prevede un'offerta di applicazioni da parte del provider, gestite su un'infrastruttura cloud, in modo tale che il cliente possa accedere al servizio in modalità on-demand tramite tecnologie Internet, pagando una licenza in abbonamento con pagamento rispetto al consumo.

Il modello PaaS è un modello a piattaforma in cui il provider offre all'utente, piattaforme pre-configurate ottimizzate per lo sviluppo di applicazioni custom. Il cliente quindi può gestire, eseguire e sviluppare nuove applicazioni o servizi senza venire a contatto con l'infrastruttura sottostante, che viene gestita in modo trasparente dal service provider.

Infine, con il modello IaaS il provider offre all'utente risorse di calcolo sulle quali installare e gestire autonomamente le proprie applicazioni. È la categoria di servizi più essenziali in quanto le risorse vengono condivise solo con i clienti a contratto a una tariffa *pay-per-use*.

Nonostante i vantaggi che questa tecnologia possa apportare in tema di archiviazione, un tema caldo che ne ha impedito un pieno sviluppo, è ancorato alla sicurezza, al primo posto come la più grande sfida del cloud computing, con particolare rilievo in tema di accessibilità da remoto, riservatezza delle informazioni, integrità e controllo dei dati. Il punto è che i servizi cloud sono caratterizzati dalla cumulabilità, ovvero un attacco sullo strato Iaas, avrà un'influenza anche sui due livelli precedenti (SaaS e Paas). Per ovviare a questi incovenienti, sono state sviluppate anche diverse tecniche di rete[93] come l'*Hyper Visor Attack*, il *Denial of Services*, lo *Sniffer Attack*, il *Reused IP addresses*, il *Google Hacking Attack* e metodi e algoritmi

[91] "La definizione di Cloud Computing del NIST", < http://www.akite.net/Media/Default/files/nist-traduzione.pdf>

[92] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, (Jun. 2009)

[93] E. Mathisen, "*Security challenges and solutions in cloud computing*", in 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011).

come strumenti di sicurezza Cloud, utilizzo della password mobile (OTP)[94], strumenti di sicurezza del software[95] (come la virtualizzazione, il sistema operativo host e ospite e la crittografia dei dati).
Nel 2018 il mercato Cloud italiano valeva 2,34 Miliardi, fino a crescere del 18% a 2,77 miliardi nel 2019[96]. La pandemia Covid-19 è stato il fattore scatenante per implementare nuove strategie online, portando al 42% l'adozione del Cloud nelle PMI, in particolare rispetto al 2019, ci sono stati due trend in costante evoluzione: quello dell'intelligenze del dato, ovvero tutti i servizi IaaS, PaaS e SaaS dedicati alla gestione, alla manipolazione e all'analisi dei dati, che conta un valore di circa 352 Milioni di Euro (una crescita del +24% rispetto all'anno precedente) e quello dell'Edge computing & Orchestration, che seppur subendo un rallentamento, sono rimasti in costante crescita raggiungendo un valore di 45 Milioni di Euro.
Nell'ambito della Pubblica Amministrazione, il Cloud ha permesso di effettuare un vero cambio di paradigma, una "*disruptive innovation*", definita per la prima volta da Clayton Christensen e Joseph Bower, con la pubblicazione del loro articolo sull'Harvard Business Review, "*Disruptive technologies: catching the wave*"[97], facendo riferimento a tutte quelle innovazioni in grado di stravolgere modello di business preesistente riallocando i confini dell'arena competitiva e stravolgendo il modo in cui i consumatori sono abituati a utilizzare prodotti e servizi. Infatti, il cloud può contribuire allo snellimento del sistema burocratico che caratterizzava questi enti e ridefinire il modo in cui i consumatori sono abituati a utilizzare prodotti e servizi. Oltre a produrre benefici diretti per gli enti amministrativi, impatta indirettamente anche sulle performance delle imprese italiane che riscontrano minori difficoltà nel trattare con la PA, costi e commissioni ridotte ed una maggiore efficienza comunicativa ed operativa. La Pubblica Amministrazione (PA) ha deciso in particolare di definire ed adottare un modello cloud ad hoc denominato per l'appunto "Cloud della PA"[98], per ridurre il rischio di sicurezza e affidabilità dei server dei cloud provider, qualificando i servizi e le infrastrutture cloud secondo specifici parametri di sicurezza ed affidabilità idonei per le esigenze della PA.

Un tema rilevante nella dematerializzazione del documento cartaceo è la possibilità di determinare l'autenticità del documento in caso di contestazione. Il metodo più efficace è sostanzialmente la presenza di una firma elettronica (avanzata o digitale) che possa attestare l'effettiva autenticità e riconducibilità del firmatario e che si basa su specifici algoritmi di cifratura di crittografia, il cui significato si colloca nell'ambito della sicurezza informatica e della tutela di dati e informazioni che sono in circolazione sulla rete, essendo in grado di fornire la maggior parte dei servizi contemplati nell'architettura di sicurezza stabilita dall'ISO (*International Organization for Standardization*).

[94] S. Kuila, S. Shruthi, P. Chandan, and N. Ch SN Iyengar, "*Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management*", Journal of Computer and Mathematical Sciences vol. 7., (2016)
[95] K. K. Chauhan, A. Sanger, and A. Verma, "Homomorphic Encryption for Data Security in Cloud", IEEE, pp. 206-209, (2015).
[96] "Cloud Transformation: gli ingredienti mancanti", Osservatorio Cloud Transformation (Ottobre 2019)
[97] Clayton Christensen e Joseph Bower, "*Disruptive technologies: catching the wave*", Harvard Business Review (1995)
[98] "Cloud della PA", Agenzia per l'Italia digitale (AGID)

In base al tipo di chiave utilizzato, la crittografia informatica può essere simmetrica o asimmetrica. In particolare, ci si riferisce al numero di chiavi utilizzate: quando la chiave è unica la crittografia è simmetrica o a chiave segreta (ciò significa che la chiave del mittente coincide con quella del destinatario), quando invece le chiavi sono due, si parla di crittografia a chiave asimmetrica o a chiave pubblica (la chiave di cifratura è pubblica e condivisa da tutti i corrispondenti, mentre la chiave di decifratura è privata e segreta per il proprietario stesso)[99]. Gli algoritmi di cifratura di crittografia asimmetrica vengono impiegati, tra l'altro, nella firma digitale. Con l'approvazione alla firma digitale da parte del legislatore, il documento informatico ha potuto ottenere gli stessi requisiti del documento cartaceo, rendendoli equiparabili.

Tra le firme elettroniche avanzate, nell'ottica di garantire una maggiore sicurezza e una limitata contraffazione, assume un particolare rilevo la firma grafometrica, che si basa su un sistema di biometria, ovvero è in grado di rilevare una serie di parametri biometrici legati al comportamento dell'utente, che vengono poi cifrati e associati al documento firmato[100]. Nel momento in cui l'utente appone la firma tramite un tablet, si riesce a cogliere i movimenti naturali associati alla mano nell'atto di firmare, associandoli in maniera univoca al documento firmato.

È possibile acquisire la firma grafometrica attraverso specifici software incorporati in dispositivi esterni come tablet o signature pad, che riescono a generare il documento informatico registrando informazioni dinamiche, come la velocità di scrittura, la pressione esercitata su tavoletta o altro device, l'angolo di inclinazione della penna, l'accelerazione del movimento e il numero di volte che la penna viene sollevata, e movimenti statici, come l'immagine e le caratteristiche della firma. Infatti, per "riconoscimento biometrico" si intende un processo informatico volto a identificare e a verificare l'identità di una persona, attraverso l'analisi di caratteristiche fisico-biologiche, come impronte digitali, fisionomica del viso, il colore e la forma dell'iride o la retina eccetera, e comportamentali, come il timbro della voce e le caratteristiche della scrittura. Iansiti e Lakhani lo definiscono un circolo virtuoso, ma può anche essere un circolo vizioso se uno qualsiasi dei passaggi contiene pregiudizi, errori o presupposti sbagliati. Ogni fase deve essere accuratamente eseguita e controllata, in quanto se si sbaglia un singolo passaggio si avranno ripercussioni su tutta la catena[101].

Si possono correre diversi rischi durante l'acquisizione e il mantenimento dei dati, come il controllo sociale e gli usi discriminatori che ne possono derivare, un possibile furto dell'identità biometrica, la generazione di falsi positivi e falsi negativi, la falsificazione biometrica (ovvero la possibilità di ricreare un campione biometrico a partire dal modello stesso) e l'aumento del rischio nel contesto mobile e BYOD (*Bring Your Own Device*). Proprio per questo, anche qui la gestione della sicurezza è un tema caldo e la firma grafometrica è uno degli strumenti maggiormente utilizzato per snellire i processi burocratici favorendo la

[99] Alessandro Languasco, Alessandro Zaccagnini, "*Manuale di crittografia: Teoria, algoritmi e protocolli*", Hoepli Editore, (2015).
[100] Daniel Riccio, Clemente Galdi, Luigi Catuogno, "*Sistemi Biometrici e Sicurezza*"
[101] Iansiti, M., & Lakhani, K. R., "Rearchitecting the firm", Competing in the Age of AI. Harvard Business Press Chapter 4, pp. 79-97, (2020)

dematerializzazione della modulistica delle operazioni. Nell'ambito della Pubblica Amministrazione in particolare, crea un impatto di gran lunga positivo, soprattutto a seguito pandemia COVID-19, quando è venuta sempre maggiore l'esigenza di gestire processi e documenti informatici in modalità del tutto digitale garantendo alti livelli di integrità e riservatezza. L'introduzione di tecnologie specifiche come la firma digitale fa parte della radicale trasformazione all'interno della PA italiana, permettendo anche un nuovo modo di lavorare, significativi vantaggi in termini di costi, tempi e gestione delle risorse umane[102].
Tra i principali vantaggi apportati dalla dematerializzazione dei documenti infatti, vi è il contenimento dei costi di gestione dei documenti cartacei: è possibile creare direttamente un documento elettronico legale con firma autografa, eliminando il passaggio dal cartaceo al digitale, in modo da rendere nulli i costi legati alla gestione della carta, del toner e dell'usura delle stampanti e riducendo i costi di scansione e archiviazione.
La firma digitale comporta anche un aumento della peformance dei processi che diventano più efficienti, snelli e veloci, infatti i documenti firmati in modalità elettronica sono subito disponibili al Sistema Informativo aziendale e condivisibili, così da eliminare fraudolente duplicazioni.

A seguito dell'evoluzione in atto del settore della pubblica amministrazione, con i relativi programmi di Amministrazione Digitale e E-Government, tecniche di Cloud Computing e l'utilizzo di tecnologie a supporto, si è voluto dimostrare come ad oggi la digitalizzazione, in particolare dei documenti, rappresenti la leva trainante di ogni business e anche per la PA nel rapporto col cittadino. In particolare, è stato proposto il caso studio di ACI (Automobile Club d'Italia) in quanto è stata una delle prime Pubbliche Amministrazioni a passare a servizi e tecnologie ICT, anche se da sempre la tecnologia è stata interpretata come elemento competitivo di sviluppo e di trasformazione, anche in epoche in cui era meno evidente l'impatto che la digitalizzazione avrebbe avuto sulle attività e sul mondo.
Sulla base di interviste al personale di ACI e in particolare al Responsabile di Transizione Digitale dell'ACI, Vincenzo Pensa, dati di archivio, il bilancio sociale e video esplicativi sulla base della letteratura e degli approfondimenti riportati nella tesi proposta, si è illustrato il percorso di digitalizzazione intrapreso dalla società a partire proprio dall'introduzione della firma digitale per firmare documenti online e adottare un approccio "*paperless*", favorendo la digitalizzazione e la dematerializzazione dei documenti informatici.
Nonostante le funzionalità dell'ACI, spazino in diversi settori, da quello della mobilità, a quello dello sport, nell'ambito della pubblica amministrazione, gestisce il Pubblico Registro Automobilistico, e altri compiti che riguardano la gestione amministrativa e fiscale dei veicoli, conosciuti soprattutto per il pagamento del bollo auto.
Come riportato da Vincenzo Pensa, la tecnologia, l'innovazione e il cambiamento hanno sempre rappresentato un punto di riferimento e sono stati interpretati come elemento competitivo di sviluppo e di trasformazione, anche in epoche in cui era meno evidente l'impatto che la digitalizzazione avrebbe avuto sulle attività e sul

[102] Vincenzo Pensa, responsabile in ACI (Automobile Club d'Italia) di transazione digitale

mondo. L'ACI ha puntato molto sulla digitalizzazione dei processi per abilitare tutta un'altra serie di attività e sviluppi, tenendo sempre come punto di riferimento il cittadino e la formazione del fattore umano, considerato la vera liquidità aziendale. Infatti, intorno agli anni 90, attraverso la microfilmatura, sono stati digitalizzati volumi cartacei su cui erano annotati atti e provvedimenti, un processo che ha permesso ad ACI di arricchire il proprio patrimonio informativo all'interno di un perimetro di trattamento delle informazioni automatizzate, quindi trasformando la carta in BIT. Successivamente la carta è stata abbandonata anche come input e l'input è avvenuto direttamente in digitale.

In particolar modo, si fa risalire una particolare accelerazione di questi processi, a partire dal 2015 con l'introduzione del Certificato di Proprietà digitale, volto a semplificare la mobilità dell'autista italiano e a comportare l'introduzione di procedure informatiche per consentire la gestione del documento in modo digitale, creando valore per tutto l'ecosistema. A contribuire alla dematerializzazione del certificato è stato il dispositivo HSM (*hardware security module*) di firma remota CoSign. Con questa soluzione si è potuta garantire la protezione e la conservazione di migliaia di certificati digitali apportando vantaggi in termini di risparmi economici, snellimento delle procedure e sicurezza dei documenti.

L'ACI al giorno d'oggi si ha sviluppato progetti interamente digitali per quanto riguarda il mondo sportivo, il mondo associativo, il mondo dei servizi all'automobile con la piena digitalizzazione del supporto di servizio al soccorso stradale, per cui oggi il cittadino, utilizzando un'applicazione, può tranquillamente fare richiesta di assistenza, seguire lo stato di avanzamento del soccorso fino a quando non lo vengono a prendere e lo portano a destinazione.

A partire dalla dematerializzazione del certificato digitale e dall'adozione della firma digitale, negli anni a seguire l'ACI ha intrapreso una strategia basata sulla generazione di processi totalmente digitale come il processo di compravendita di un'auto, che può avvenire tramite strumenti e tecnologie che consentono di gestire la firma digitale e l'autenticazione degli operatori abilitati ad espletare le formalità in ambito del Pubblico Registro Automobilistico (PRA).

Inoltre, per evitare l'affluenza delle persone fisiche sul luogo, è stato sviluppato internamente un applicativo WEB, "PrenotACI", che consente ai cittadini e agli operatori professionali di prenotare gli appuntamenti dal sito WEB ACI e dai siti web degli Uffici Territoriali del PRA, tramite accesso SPID.

Un progetto che ha contribuito a realizzare un vero cambio di paradigma, facendo dell'ACI una Pubblica Amministrazione interamente digitale connessa al Sistema Pubblico del Paese, è stato il progetto "PagoBollo", realizzato in collaborazione ACI Informatica, partner tecnologico dell'Automobile Club d'Italia (ACI), con AGID e il Team per la trasformazione Digitale per dare la possibilità ai cittadini di aderire agli obblighi di pagamento online con pagoPA in modo agevole, direttamente da casa o dai dispositivi mobili.

Questo progetto ha avuto benefici sia per i soggetti interni che esterni, poiché si sono potuti limitare i costi di gestione della riscossione dei tributi generati dalle commissioni bancarie, necessari per garantire i pagamenti online, si è dato vita alla digitalizzazione e alla conservazione delle ricevute online risparmiando in termini di

carta; ci sono stati dei benefici legati all'introduzione del sistema innovativo di orchestrazione dei vari archivi che ha consentito alla società di aumentare la propria capillarità e di razionalizzare alcune funzioni di controllo consentendo risparmi significativi e una riduzione dei contenziosi tra regioni e cittadini.
Successivamente, anche i pagamenti PRA sono confluiti sul sistema PagoPA e da subito si è potuto prendere atto del forte contributo generato dall'ACI alla digitalizzazione della Pubblica Amministrazione Italiana.
Il sistema di autenticazione digitale (SPID), introdotto da ACI Informatica già con nel 2015 con la digitalizzazione dei certificati di proprietà, ha permesso all'ente pubblico di abilitare altri processi per semplificare la vita del cittadino, facendo dell'ACI, una tra le prime Pubbliche Amministrazioni italiane a prendere parte, nel 2019, alla sperimentazione dell' "applicazione IO", il progetto ideato dal Governo italiano che permette di creare una sinergia tra le diverse Pubbliche Amministrazioni, fornendo al cittadino un portale per interagire con le PPAA per informazioni, scadenze e pagamenti. In particolare, si è permesso ai cittadini di tenere traccia delle comunicazioni, pagamenti e documenti in un'unica applicazione, in modo sicuro e sempre a portata di mano, integrando alcune piattaforme abilitanti come l'identificazione tramite SPID, l'anagrafe unica ANPR, per raccogliere i dati dei cittadini da tutte le anagrafi e il sistema dei pagamenti PagoPA. I servizi attivi resi da ACI sull'applicazione le certificazioni e le attestazioni di proprietà, il servizio "AvvisACI", il pagamento del Bollo Auto e la comunicazione istituzionale.

Nel corso dell'elaborato, abbiamo visto come nell'epoca della *digital transformation*, la digitalizzazione della Pubblica Amministrazione rappresenti una delle principali innovazioni che ha inciso fortemente nella gestione dei rapporti con gli utenti per quanto riguarda la fruizione dei servizi amministrativi, e sulla quale si sta cercando continuamente di fare leva per determinare un cambiamento strutturale per l'ecosistema che la circonda. A partire dalla dematerializzazione e dalla digitalizzazione dei documenti cartacei, l'implementazione dei servizi attraverso nuove tecnologie, sulla base di una *road map* chiara e concisa, è stata una delle maggiori innovazioni che ha alimentato la nuova organizzazione delle attività, del lavoro dei dipendenti e delle procedure della Pubblica Amministrazione. Abbiamo visto come il cloud computing possa essere considerata la piattaforma abilitante per la trasformazione digitale, nonostante i rischi che ne comporta, infatti, è stato dimostrato come l'approccio burocratico che la caratterizza possa essere eliminato, o quanto meno ridotto grazie all'elasticità dei servizi, alla facilità degli aggiornamenti, alla riduzione delle attività manuali, della complessità del supporto e ovviamente dei costi.
Se ancora è possibile riscontrare ritardi nel processo di digitalizzazione della Pubblica Amministrazione, è stato dimostrato come il caso dell'Automobile Club d'Italia abbia fronteggiato con risolutezza e successo un'era tecnologicamente avanzata e la pandemia che stiamo vivendo al giorno d'oggi. Il successo dell'organizzazione è stato garantito dalla flessibilità con cui si è potuta sempre adattare al contesto, essendo stata una delle prime tra le Pubbliche Amministrazioni ad adottare servizi e tecnologie ICT anche quando l'impatto che queste avrebbero avuto sui servizi era ancora sottovalutato.

Se all'interno del quadro illustrato nell'elaborato ci si è chiesti se le aziende e in particolare la Pubblica Amministrazione, riusciranno a sfruttare il potere del digitale, è possibile concludere che la velocità del progresso digitale, che ha messo a disposizione un ritmo di innovazione crescente, ha anche richiesto l'esodo dalla cultura precedente e l'ingresso nella nuova. Questo necessita di tempo, si tratta di un lungo cammino che richiede di uscire da sé stessi, dai propri schemi mentali, dalle norme di comportamento sociale per adattarsi alla costante per eccellenza della nuova epoca digitale. Quello di ACI ha rappresentato un caso di successo di efficienza digitale della Pubblica Amministrazione, dando vita a un vero e proprio cambio di paradigma che si traduce in risparmio di costi associati alla carta, alla semplificazione delle procedure, al massimo controllo e sicurezza dei documenti e che attesta l'Italia tra i precursori in questo cambiamento.