UNIVERSITÀ DEL PIEMONTE ORIENTALE

DIPARTIMENTO DI GIURISPRUDENZA E SCIENZE POLITICHE, ECONOMICHE E SOCIALI

CORSO DI LAUREA MAGISTRALE IN SOCIETA' E SVILUPPO LOCALE

TESI DI LAUREA

DIGITALIZZAZIONE E CYBERSECURITY NELLA PA

Relatore:

Chiar.mo Prof. Domenico Carbone

Correlatore:

Chiar.mo Prof. Bruno Cattero

Candidato:

Matteo Michele Deserventi

ANNO ACCADEMICO 2022/2023

Indice

INTRODUZIONE

L’idea di una ricerca sulla digitalizzazione ed in particolare sulla Cybersecurity deriva dal fatto che lavoro nell’ambito delle Aziende Sanitarie del Piemonte da molti anni e il tema della Sicurezza Informatica è diventato estremamente importante. Ormai è all’ordine del giorno parlare di attacchi informatici rivolti soprattutto alle Aziende Sanitarie. Questo perché costituiscono la maggior fonte di dati “sensibili” che possono essere utilizzati per vari scopi.

I cosiddetti “Hackers” hanno creato vere e proprie imprese[1] diventando di fatto degli imprenditori, iniziando ad utilizzare per i propri scopi lo schema SaaS (Software as a Service) chiamato in questi casi anche RaaS (Ransomware as a Service).

Viene utilizzato questo schema perché ha il vantaggio di essere più economico e semplice da utilizzare per i cosiddetti “clienti”.

Il primo capitolo introduce l’argomento principale che è la digitalizzazione.

Vengono illustrate le normative, si parla di organizzazione nella pubblica amministrazione e di investimenti tra cui il PNRR (Piano Nazionale di Ripresa e Resilienza).

Di fatto il passaggio dall'analogico al digitale implica una trasformazione radicale delle pratiche industriali e commerciali, definendo una nuova era nella quale la tecnologia digitale è al centro di molteplici settori.

In campo informatico, la digitalizzazione comporta la conversione di immagini, suoni e documenti in un formato interpretabile dai “computer” attraverso il linguaggio binario composto da zero e uno. Ad esempio, l'ascolto di una canzone da un vinile rappresenta un'espressione analogica del suono, mentre la sua riproduzione tramite un computer si manifesta nel formato digitale.[2]

Nel settore delle telecomunicazioni, la digitalizzazione evidenzia il passaggio da tecnologie a trasmissione analogica a quelle a trasmissione digitale, segnando un avanzamento significativo nelle comunicazioni.

Nel contesto della Pubblica Amministrazione (PA), la digitalizzazione riveste un ruolo centrale nelle politiche di innovazione, come la Transizione Digitale, che include il ruolo del Responsabile per la Transizione Digitale (RTD), il Piano Triennale e il quadro normativo.

[1] https://www.pandasecurity.com/it/mediacenter/hacker-diventati-imprenditori/
[2] https://www.transizionedigitale.it/2022/07/14/digitalizzazione-pa-significato-normativa-e-piano-triennale/

Le parole chiave della Missione 1 del Piano Nazionale di Ripresa e Resilienza (PNRR) sono Digitalizzazione, Innovazione e Sicurezza, con l'obiettivo di modernizzare l'Italia dal punto di vista produttivo e amministrativo.[3]

Il Governo italiano ha attivamente promosso una vera Transizione Digitale, investendo non solo nelle infrastrutture ma anche nelle competenze digitali.

Nella PA, questa trasformazione comporta la ridefinizione di procedure, ruoli e processi per migliorare l'erogazione dei servizi ai cittadini.

Nonostante la complessità apparente, la comprensione della digitalizzazione nella PA è cruciale, soprattutto per i dipendenti pubblici. Questo processo, avviato nel 2005 con l'implementazione del Codice dell'Amministrazione Digitale (CAD), comprende l'ammodernamento dell'intera struttura. Si pone enfasi sulla creazione di nuove infrastrutture e strategie per semplificare l'accesso, la gestione e la sicurezza delle informazioni, a vantaggio dei cittadini e delle istituzioni pubbliche.

Questo ha creato importanti passaggi, tra cui la creazione di “AgID” nel 2012, agenzia incaricata di raggiungere gli obiettivi dell'Agenda Digitale europea e l'adozione della "Strategia per la crescita digitale 2014-2020" nel 2015.

Nel 2017 è stato introdotto il "Piano Triennale per l’Informatica nella Pubblica Amministrazione," in linea con la Missione 1 del PNRR.

Una parte significativa degli investimenti è stata indirizzata verso la Cybersecurity, aspetto che approfondiremo in questa ricerca, soprattutto nel secondo capitolo, per esaminarne l'impatto sulla gestione e sugli investimenti della PA. La sicurezza informatica rappresenta una componente essenziale della digitalizzazione, garantendo la protezione delle informazioni sensibili e la continuità dei servizi pubblici in un ambiente sempre più interconnesso e tecnologicamente avanzato.

Nel terzo capitolo si parla ancora di Cybersecurity ma collegata ai conflitti armati e soprattutto al conflitto RUSSIA ed UCRAINA. Ci si concentra sulle conseguenze in Italia soprattutto nella Pubblica Amministrazione e vengono fatti alcuni esempi reali.

L’ultimo capitolo è quello basato sul questionario. Per avere un quadro più reale possibile sull’argomento oggetto della ricerca è stato creato un vero e proprio questionario che è stato proposto e compilato dai dipendenti pubblici di alcune Aziende Sanitarie del Piemonte. In questo modo sono emerse le percezioni degli operatori delle Aziende Sanitarie sia come

[3]https://www.weclapp.it/glossario/digitalizzazione/

“Lavoratori” che come “Cittadini”. Questo perché la digitalizzazione e la Cybersecurity sono argomenti che interessano tanto la sfera privata che quella lavorativa: è dimostrato che molti attacchi o esfiltrazione di dati hanno origine proprio con l’attacco agli account e pc privati del personale delle Aziende.

Il questionario è stato creato registrando un nuovo dominio questionari.eu ed installando un software dal nome “Limesurvey”.

I risultati sono stati analizzati attraverso il famoso software “STATA” utilizzato in vari corsi nella mia carriera universitaria.

1. CAPITOLO 1 – La Digitalizzazione nella PA

1.1 Cenni normativi

Con la comparsa dei primi computer negli anni Cinquanta si può dire che sia iniziato realmente il processo di digitalizzazione il quale diventa formale nel 2002. Alcuni studiosi considerano il 2002 il momento in cui l'umanità è stata in grado di immagazzinare una maggiore quantità di informazione in una forma digitale, piuttosto che analogica. Il cosiddetto inizio dell'Era Digitale[4].

Il decreto legislativo del 7 marzo 2005, n.82 (successivamente modificato ed integrato dai decreti, 22 agosto 2016 n.179, 13 dicembre 2017 n.217) istituisce il primo vero pilastro della digitalizzazione nella pubblica amministrazione e cioè il Codice dell'Amministrazione Digitale (CAD)[5].

Il CAD riunisce ed organizza le norme sull'informatizzazione della Pubblica Amministrazione. Esso sin dall'inizio ha cercato di garantire la sicurezza dei dati informatici ed i diritti di cittadinanza digitale.

Un aspetto critico della digitalizzazione è la gestione sicura dei dati. Normative sulla protezione dei dati, come il GDPR nell'Unione Europea, stabiliscono regole chiare sulla raccolta, l'elaborazione e la conservazione dei dati personali, garantendo la sicurezza e la privacy delle informazioni.

Le normative incoraggiano spesso l'adozione di standard tecnologici comuni e la promozione dell'interoperabilità tra sistemi informatici. Ciò facilita il funzionamento armonioso di diversi sistemi, agevolando lo scambio di informazioni tra le diverse entità della pubblica amministrazione.

La digitalizzazione include anche l'accessibilità informatica, con leggi che stabiliscono i requisiti per garantire che i servizi digitali siano accessibili a tutti gli individui, indipendentemente dalle loro abilità o disabilità. Le linee guida sull'accessibilità assicurano che siti web, applicazioni e servizi siano progettati per soddisfare le esigenze di tutti gli utenti.

Alcune normative promuovono la partecipazione pubblica e la consultazione durante il processo di digitalizzazione. Ciò può coinvolgere la pubblicazione online di documenti e progetti, nonché la raccolta di feedback da parte dei cittadini, garantendo un approccio inclusivo e trasparente.

[4]https://www.wolterskluwer.com/it-it/expert-insights/genya-digitalizzazione-lavoro
[5]https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale

Le normative possono prevedere iniziative di formazione per i dipendenti della pubblica amministrazione, assicurando che siano adeguatamente preparati per gestire e utilizzare le nuove tecnologie. Ad esempio, in Italia, l'AgID svolge un ruolo chiave nella promozione della digitalizzazione, fornendo linee guida e supporto tecnico.

L'ANAC invece fornisce disposizioni per lo sviluppo e l'interoperabilità di tutta la gestione appalti della Pubblica Amministrazione. L'obbligo di qualificazione delle stazioni appaltanti pubbliche prevede il dovere di formare il dipendente sulla digitalizzazione.

È cruciale sottolineare che questo è un processo in costante evoluzione, e le normative vengono periodicamente aggiornate per affrontare sfide emergenti e sfruttare opportunità offerte dalle nuove tecnologie. La collaborazione tra settori pubblici e privati è spesso promossa per garantire il successo della trasformazione digitale nella pubblica amministrazione.

Importanti nell'ultimo periodo sono gli investimenti PNRR che permetteranno alle aziende di evolversi proprio su questo tema.

1.2 Investimenti previsti dal PNRR

Il PNRR dedica il 20,7% delle risorse totali alla Missione 1, corrispondente a 46,3 miliardi di euro. Gli investimenti riguardano diverse aree, come i servizi digitali, migrazione al Cloud, infrastrutture digitali, "task force" per la digitalizzazione, dati e interoperabilità, Cybersecurity, digitalizzazione delle grandi amministrazioni centrali, competenze e capacità amministrativa, e competenze digitali di base [6]:

- Investimento in capitale umano per rafforzare l'Ufficio del Processo e superare le disparità tra tribunali – € 2.268.050.000
- Servizi digitali e cittadinanza digitale – € 2.013.000.000
- Abilitazione e facilitazione migrazione al Cloud – € 1.000.000.000
- Infrastrutture digitali – € 900.000.000
- Task Force digitalizzazione, monitoraggio e performance – € 734.200.000
- Dati e interoperabilità – € 646.000.000
- Cybersecurity – € 623.000.000
- Digitalizzazione delle grandi amministrazioni centrali – € 611.200.000
- Competenze: Competenze e capacità amministrativa – € 489.900.000

[6]https://www.transizionedigitale.it/2022/07/14/digitalizzazione-pa-significato-normativa-e-piano-triennale/

- Competenze digitali di base – € 195.000.000

A gennaio 2022, il Piano Nazionale di Ripresa e Resilienza (PNRR) è stato proposto dal Governo italiano come risposta alla crisi economica derivante dalla pandemia di COVID-19. Il PNRR rappresenta un quadro strategico che prevede investimenti significativi in diversi settori, compresa la digitalizzazione nella pubblica amministrazione.

Gli investimenti del Piano Nazionale di Ripresa e Resilienza (PNRR) mirano a promuovere la digitalizzazione nella pubblica amministrazione italiana, con diversi punti chiave che delineano la sua strategia. In primo luogo, il PNRR si propone di modernizzare la pubblica amministrazione, rendendola più efficiente, trasparente e centrata sul cittadino. Questo implica la trasformazione dei processi interni, l'implementazione di servizi online e lo sviluppo di infrastrutture digitali robuste.

Il piano identifica progetti specifici legati alla digitalizzazione della pubblica amministrazione, che possono includere lo sviluppo di piattaforme digitali per semplificare le procedure burocratiche, l'implementazione di sistemi di gestione elettronica dei documenti e la promozione di servizi online. Inoltre, gli investimenti potrebbero essere destinati allo sviluppo delle competenze digitali del personale pubblico, garantendo che siano in grado di utilizzare efficacemente le nuove tecnologie.

La creazione di infrastrutture digitali robuste è un elemento critico del PNRR, comprendendo la costruzione di reti ad alta velocità, l'implementazione di “data center” e misure di sicurezza informatica per proteggere i dati sensibili. L'approccio del PNRR prevede anche “partenariati” pubblico-privato per accelerare la realizzazione di progetti di digitalizzazione, sfruttando la collaborazione con aziende tecnologiche per soluzioni innovative.

Un aspetto cruciale è il monitoraggio e la valutazione dei progressi raggiunti in questo processo, garantendo che gli obiettivi vengano raggiunti e che gli investimenti siano impiegati in modo efficace e coerente con gli obiettivi più ampi dell'Unione Europea in materia di trasformazione digitale, garantendo un allineamento con le strategie europee.

1.2.1. Cosa prevede il Piano Triennale nel dettaglio

Il Piano Triennale per la digitalizzazione della Pubblica Amministrazione (PA) rappresenta uno strumento cruciale nell'impulso della trasformazione digitale in Italia.

Attualmente noto come "Aggiornamento 2021-2023", questo piano mantiene sostanzialmente lo stesso schema della versione precedente (2020-2022). Esso è strutturato in tre parti fondamentali, ognuna delle quali gioca un ruolo chiave nella guida e implementazione della digitalizzazione.

La Prima Parte, denominata "Il Piano Triennale", comprende un Executive Summary che richiama esplicitamente il Piano Nazionale di Ripresa e Resilienza (PNRR), la strategia Italia Digitale 2026 e l'articolo 18-bis del Codice dell'Amministrazione Digitale (CAD). Inoltre, contiene il progetto nazionale e i principi guida del piano stesso, delineando così l'orientamento strategico e i principi chiave che guidano la trasformazione digitale della PA.

La Seconda Parte, intitolata "Le Componenti Tecnologiche", approfondisce dettagliatamente le componenti tecnologiche nei primi sei capitoli del piano. Questa sezione si focalizza sulla comprensione approfondita delle tecnologie coinvolte, delineando gli strumenti e le soluzioni che saranno implementati per raggiungere gli obiettivi di digitalizzazione.

La Terza Parte, "La Governance", è suddivisa in tre capitoli che descrivono la governance necessaria per attuare questa trasformazione a livello nazionale. Questa sezione specifica le azioni che devono essere intraprese dalle amministrazioni coinvolte, fornendo una guida chiara su come implementare e gestire la digitalizzazione in modo efficace.

A partire da gennaio 2022, il "Piano Triennale per l'Informatica nella Pubblica Amministrazione" (PTIPA) è stato un elemento chiave nell'orientare la digitalizzazione della PA in Italia. Questo piano triennale non solo definisce obiettivi strategici chiari per promuovere la digitalizzazione, ma comprende anche una serie di iniziative specifiche per raggiungere tali obiettivi.

Tra gli aspetti fondamentali del PTIPA vi sono gli obiettivi strategici che solitamente apportano miglioramenti nell'erogazione dei servizi pubblici, nell'efficienza operativa, nella trasparenza e nella partecipazione dei cittadini. Inoltre, il piano delinea iniziative specifiche di digitalizzazione, come lo sviluppo di piattaforme digitali, la creazione di servizi online accessibili e l'adozione di tecnologie innovative per migliorare i processi interni.

Il PTIPA prevede anche investimenti nelle infrastrutture tecnologiche necessarie per sostenere la digitalizzazione, quali la modernizzazione delle reti e l'implementazione di soluzioni avanzate come intelligenza artificiale e analisi dei dati. La sicurezza informatica è un aspetto cruciale, con misure specifiche per garantire la protezione dei dati sensibili attraverso l'implementazione di protocolli e soluzioni avanzate.

La promozione dell'interoperabilità tra sistemi informatici, la formazione e lo sviluppo delle competenze del personale pubblico, attraverso strumenti digitali e il monitoraggio regolare delle iniziative di digitalizzazione sono altrettanti elementi inclusi nel PTIPA. Questo piano stabilisce anche meccanismi di valutazione per misurare il progresso e apportare eventuali correzioni di rotta in corso d'opera, assicurando così la coerenza e l'efficacia dell'implementazione nella PA.

1.3 Il ruolo del Responsabile per la Transizione Digitale (RTD)

Il Responsabile per la Transizione Digitale (RTD) rappresenta una figura di estrema importanza all'interno di organizzazioni o strutture pubbliche, assumendo il ruolo chiave di guida e coordinamento del complesso processo di transizione verso la digitalizzazione. Nel contesto della pubblica amministrazione, l’RTD assume un ruolo cruciale per migliorare l'efficienza, la trasparenza e la qualità dei servizi pubblici.

Il primo pilastro del suo ruolo consiste nella definizione di una strategia digitale chiara e mirata. Questa strategia deve essere attentamente allineata agli obiettivi più ampi dell'organizzazione o della pubblica amministrazione, identificando in modo preciso le iniziative chiave necessarie per la trasformazione digitale.

Un secondo aspetto rilevante è il coordinamento e la supervisione di tutte le iniziative digitali all'interno dell'organizzazione. Questo compito abbraccia progetti specifici: lo sviluppo di piattaforme digitali, l'implementazione di servizi online e la digitalizzazione dei processi interni.

Inoltre, l'RTD è chiamato a collaborare con una varietà di stakeholder, sia interni che esterni. Questa collaborazione può coinvolgere dipartimenti interni, fornitori di servizi digitali, organizzazioni partner e, in alcuni casi, anche cittadini e imprese.

La promozione dello sviluppo delle competenze digitali all'interno dell'organizzazione costituisce un altro aspetto chiave del ruolo dell'RTD. Questo implica la progettazione e l'implementazione di programmi di formazione del personale, assicurando che siano in grado di utilizzare in modo efficace le nuove tecnologie e di adottare nuovi approcci digitali.

Affrontare e gestire la resistenza al cambiamento all'interno dell'organizzazione è un compito delicato, in quanto la trasformazione digitale spesso comporta cambiamenti significativi nei processi di lavoro e nella cultura organizzativa. L'RTD è chiamato a gestire questo processo in modo efficace.

La sicurezza e la conformità rappresentano un aspetto critico del ruolo dell'RTD, che si impegna a garantire che le iniziative digitali rispettino le normative sulla sicurezza informatica e sulla protezione dei dati, implementando misure di sicurezza adeguate per proteggere le informazioni sensibili.

Un ulteriore compito è rappresentato dal monitoraggio e valutazione delle prestazioni delle iniziative digitali. Ciò include la raccolta e analisi dei dati per valutare l'efficacia delle soluzioni utilizzate e apportare eventuali miglioramenti.

L'RTD favorisce la partecipazione pubblica attraverso l'implementazione di soluzioni digitali che semplificano l'interazione con la pubblica amministrazione. Inoltre, è responsabile di comunicare in modo trasparente sugli sviluppi digitali e sugli impatti attesi.

Mantenere un'attenzione costante alle nuove tecnologie e alle tendenze digitali emergenti costituisce una parte integrante del ruolo dell'RTD. Questo coinvolge il suo impegno nella ricerca e nell'adozione di innovazioni che possano ulteriormente migliorare la digitalizzazione dell'organizzazione.

Infine, l'RTD si impegna a garantire che i rimedi digitali siano sostenibili a lungo termine e scalabili per adattarsi alle future esigenze. Ciò può comportare la scelta di tecnologie flessibili e l'implementazione di soluzioni che possano evolversi con il tempo.

In sintesi, il Responsabile per la Transizione Digitale svolge un compito fondamentale nell'orientare un'organizzazione attraverso il processo di trasformazione digitale. La sua leadership e competenze sono fondamentali per garantire che la digitalizzazione avvenga in modo coerente, efficace e in linea con gli obiettivi strategici prefissati.

1.4 Differenze con altri paesi

La digitalizzazione della pubblica amministrazione presenta differenze significative tra i vari paesi, e tali disparità sono influenzate da una molteplicità di fattori. I contesti culturali giocano un ruolo fondamentale.

La predisposizione della popolazione all'utilizzo di servizi digitali può variare considerevolmente da nazione a nazione, con alcune più propense a questa innovazione rispetto ad altre, dove potrebbe esserci una maggiore resistenza al cambiamento.

Le normative e la legislazione rappresentano un altro elemento chiave, con paesi che adottano approcci diversi per affrontare questioni cruciali come la privacy dei dati e la

sicurezza informatica. Tale diversità può portare a cambiamenti significativi nelle politiche di protezione dei dati personali.

Le infrastrutture tecnologiche disponibili e la loro qualità costituiscono un altro fattore determinante. Paesi con reti ad alta velocità più sviluppate e ampio accesso a Internet possono beneficiare di una maggiore facilità nella digitalizzazione, mentre altri potrebbero affrontare sfide logistiche.

Il livello di sviluppo economico di una nazione è strettamente correlato alla sua capacità di investire nll'informatizzazione. Paesi più avanzati economicamente possono godere di risorse finanziarie e umane più abbondanti, accelerando l'adozione di tecnologie avanzate.

Il coinvolgimento del settore privato può variare considerevolmente. In alcuni paesi, il settore privato svolge un ruolo attivo nello sviluppo di soluzioni digitali per la pubblica amministrazione, mentre in altri la collaborazione potrebbe essere meno marcata.

Gli approcci alla partecipazione pubblica differiscono anch'essi. Mentre alcuni paesi incoraggiano attivamente la partecipazione dei cittadini attraverso piattaforme digitali, altri mantengono metodi più tradizionali.

La struttura della pubblica amministrazione è un elemento che non può essere trascurato. Paesi con una struttura più decentralizzata potrebbero affrontare sfide e opportunità diverse rispetto a quelli con una struttura più centralizzata.

La cittadinanza e l'alfabetizzazione digitale rappresentano ulteriori variabili. La familiarità dei cittadini con l'uso di servizi digitali può variare notevolmente, richiedendo sforzi diversificati per sensibilizzare e formare la popolazione.

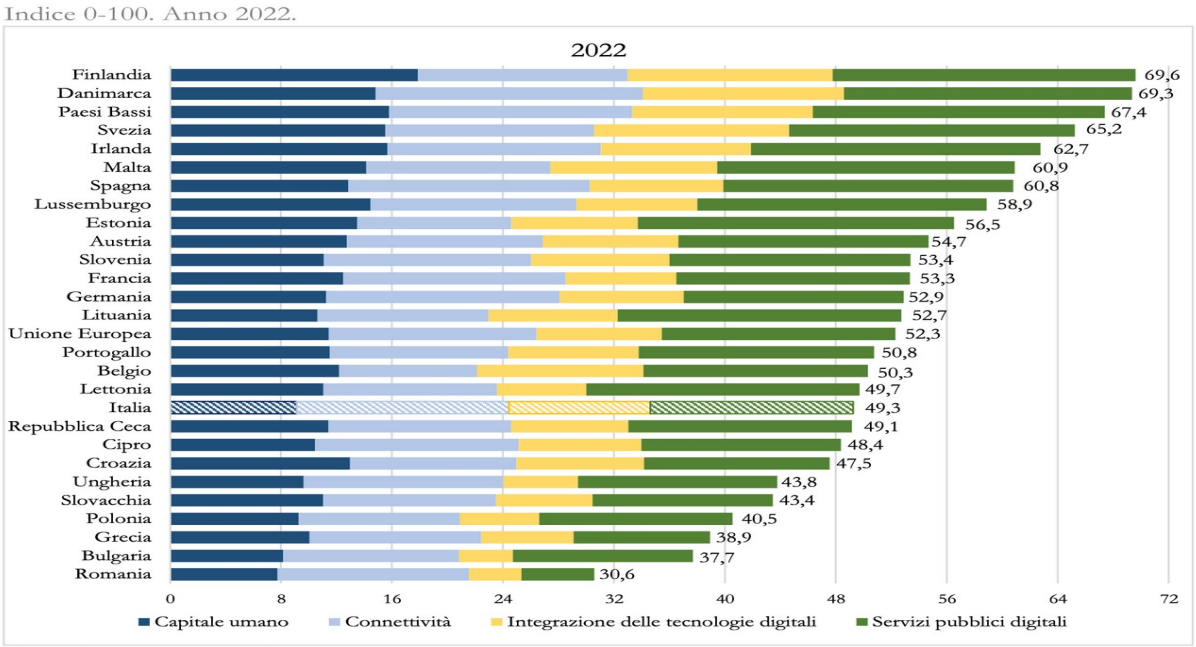
Gli obiettivi strategici nazionali sono un fattore cruciale: mentre alcuni paesi si concentrano sulla semplificazione burocratica, altri pongono un'enfasi maggiore su trasparenza, efficienza operativa o partecipazione dei cittadini.

La cooperazione internazionale e l'interoperabilità tra paesi possono svolgere un ruolo chiave nell'armonizzare soluzioni digitali. Iniziative collaborative possono facilitare lo scambio di best practice e lo sviluppo di standard condivisi, contribuendo così a ridurre le differenze e promuovere una digitalizzazione più uniforme e integrata a livello globale.

È importante considerare che queste differenze possono evolversi nel tempo e che l'adozione della digitalizzazione nella pubblica amministrazione è spesso un processo dinamico influenzato da una serie di fattori interconnessi.

Per evidenziare le differenze con altri paesi, abbiamo analizzato il DESI, che sintetizza gli indicatori sulle prestazioni digitali in Europa. Nell'edizione 2022, l'Italia si posiziona al diciottesimo posto tra i 27 Stati membri dell'Unione Europea, con una migliorata performance rispetto al 2017, ma con possibilità di ulteriore miglioramento nel contesto del DESI. (Figura 2).

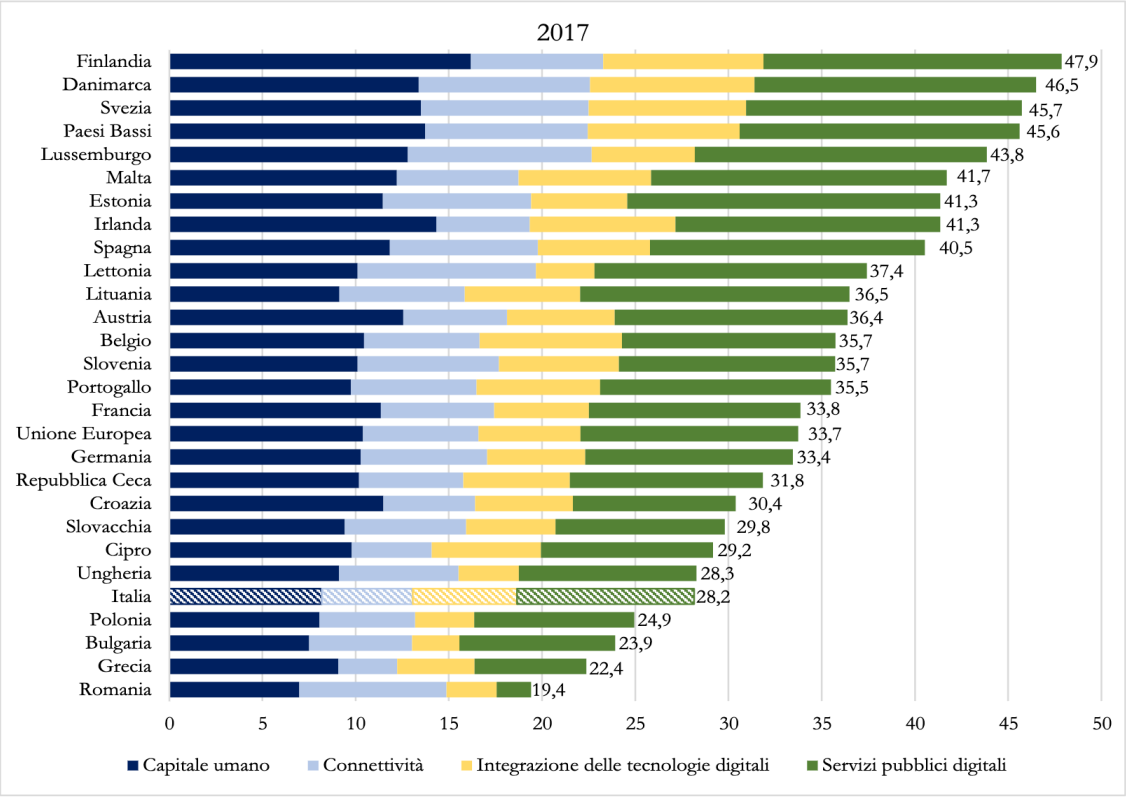
Figura 1: Scomposizione dell'indice DESI anno 2022 nelle sue componenti, divisione per paesi dell'UE (27 paesi)



Fonte: elaborazioni Osservatorio delle libere professioni su dati European Commision

Figura 2: Scomposizione dell'indice DESI anno 2017 nelle sue componenti, divisione per paesi dell'UE (27 paesi)

Indice 0-100. Anno 2017.



1.5 Gli strumenti

La digitalizzazione nella pubblica amministrazione si configura come un approccio rivoluzionario che si avvale di diversi strumenti e tecnologie per potenziare l'efficienza operativa, accrescere la trasparenza e migliorare la qualità dei servizi pubblici. Questo processo di trasformazione coinvolge una serie di strumenti e soluzioni, ciascuno pensato per rispondere a specifiche esigenze e contribuire all'evoluzione del settore pubblico.

Tra i pilastri fondamentali di questa trasformazione, si individuano i Portali Governativi, veri e propri siti web centralizzati, che non solo offrono accesso a una vasta gamma di servizi pubblici, ma fungono anche da hub informativo per i cittadini, fornendo dettagli e risorse.

Le Piattaforme di Servizi Online rappresentano un altro tassello cruciale, semplificando la vita quotidiana dei cittadini attraverso servizi come richieste di documenti, pagamenti delle tasse e prenotazioni di appuntamenti. Il tutto accessibile con pochi clic.

Gli Archivi Digitali sono progettati per gestire, archiviare e garantire l'accesso sicuro ed efficiente a documenti e dati digitali. Questo aspetto non solo elimina il bisogno di ingombranti archivi cartacei ma permette anche una ricerca e un recupero dei dati molto più efficienti.

Le Firme Digitali rivoluzionano la sicurezza delle transazioni, offrendo una soluzione rapida e sicura. Nel contesto della pubblica amministrazione, questo strumento si traduce in una semplificazione delle procedure e in una riduzione dei tempi burocratici.

I Workflow Digitali e la Robotic Process Automation (RPA) vanno a braccetto per automatizzare compiti ripetitivi, liberando il personale da attività manuali e consentendo un utilizzo più efficiente delle risorse umane.

Le Tecnologie e le piattorme Cloud sono fondamentali per archiviare e gestire dati in modo sicuro e flessibile, senza la necessità di infrastrutture locali complesse.

Gli Strumenti di Analisi dei Dati e le Dashboard Interattive forniscono informazioni approfondite sulle performance, aiutando nella valutazione e nell'adattamento delle strategie.

L'Intelligenza Artificiale e l'Automazione Cognitiva, incluse Chatbot e Assistenza Virtuale, rappresentano la frontiera dell'interazione automatizzata con i cittadini, offrendo supporto immediato e rispondendo alle domande in modo intelligente.

L'Elaborazione del Linguaggio Naturale (NLP) migliora ulteriormente l'interazione tra cittadino e amministrazione, permettendo la comprensione e la risposta a richieste scritte in linguaggio naturale.

L'Internet delle Cose (IoT), con i suoi Sensori Intelligenti, permette la raccolta di dati da vari dispositivi e ambienti, fornendo una base solida per decisioni informate.

Le Smart City Solutions utilizzano l'IoT per ottimizzare i servizi urbani, rendendo le città più efficienti e sostenibili.

In aggiunta agli strumenti menzionati, vi sono implementazioni specifiche come l'Albo Pretorio Online, la Carta d'Identità Elettronica, la Carta Nazionale dei Servizi, la Dematerializzazione, l'Open Data, la Posta Elettronica Certificata, il Protocollo Informatico e la Firma Digitale. Questi strumenti specifici contribuiscono in modo significativo alla modernizzazione dei servizi pubblici e alla semplificazione dei processi amministrativi.

L'efficacia di questo processo di digitalizzazione dipende dalla corretta integrazione e dall'utilizzo sinergico di questi strumenti, considerando le esigenze specifiche e le sfide di ciascun contesto. Inoltre, la sicurezza informatica, attraverso l’utilizzo di Firewall e Sistemi di

Protezione, insieme all'uso di Software Antivirus, è essenziale per garantire la protezione delle reti e dei sistemi informativi da minacce esterne, garantendo la sicurezza dei dati sensibili gestiti dalla pubblica amministrazione.

1.5.1. Albo Pretorio[7]

L'Albo Pretorio, elemento chiave della pubblica amministrazione italiana, rappresenta uno strumento fondamentale di trasparenza e pubblicità. Si configura come una sezione dedicata, spesso online, in cui trovano posto atti, documenti e comunicazioni ufficiali dell'ente pubblico. La sua funzione primaria è quella di assicurare l'accesso pubblico alle informazioni amministrative, contribuendo a rendere più trasparente l'operato delle istituzioni.

Questo strumento si distingue per diversi aspetti fondamentali. In primo luogo, il suo contenuto è variegato e di interesse pubblico. Esso spazia dagli avvisi alle ordinanze, dalle determinazioni alle delibere, fino ai bandi, ai concorsi ed altri atti ufficiali. L'Albo Pretorio copre un'ampia gamma di settori, tra cui urbanistica, lavori pubblici, appalti, personale e altro ancora.

L'accessibilità rappresenta un tratto distintivo di questa piattaforma. Solitamente reso disponibile attraverso il sito web dell'ente pubblico, l'Albo Pretorio assicura ai cittadini un facile accesso agli atti in pubblicazione, permettendo loro di rimanere informati sulle decisioni e le attività in corso dell'amministrazione.

Il termine stesso, "Albo Pretorio", trae origine dal latino "albus praetorium", che si traduce in "tavola bianca" o "registro ufficiale". Tale denominazione sottolinea l'obbligo di pubblicità e trasparenza associato agli atti ufficiali.

Un aspetto rilevante è la pubblicazione temporanea degli atti nell'Albo Pretorio. Questi documenti sono generalmente visibili per un periodo limitato, variabile in base alla natura dell'atto e alle disposizioni normative locali.

La normativa di riferimento gioca un ruolo cruciale. In Italia, il Decreto Legislativo n. 33 del 14 marzo 2013, noto come "Codice dell'Amministrazione Digitale", definisce le regole per la pubblicazione online degli atti amministrativi, compresi quelli presenti nell'Albo Pretorio.

[7]http://qualitapa.gov.it/sitoarcheologico/relazioni-con-i-cittadini/open-government/strumenti-della-pa-digitale/albo-pretorio-on-line/index.html

L'Albo Pretorio non è solo uno strumento di consultazione per i cittadini, ma anche per gli operatori economici come imprese e professionisti. Questi possono trovare informazioni cruciali su bandi di gara e opportunità di appalto, facilitando la partecipazione a procedure concorsuali.

La presenza dell'Albo Pretorio promuove la trasparenza e l'accountability nell'azione amministrativa. Facilita un maggiore controllo sull'operato della pubblica amministrazione, incoraggiando la partecipazione attiva dei cittadini e contribuendo a rendere il processo decisionale più aperto e responsabile. L'implementazione e la gestione di tale strumento possono variare leggermente da un ente pubblico all'altro, ma l'obiettivo comune è quello di garantire la massima trasparenza possibile nell'ambito della pubblica amministrazione italiana.

1.5.2. Carta d'identità elettronica[8]

La Carta d'Identità Elettronica (CIE) costituisce un documento di identificazione avanzato, incorporando funzionalità digitali che contribuiscono a migliorare la sicurezza e l'efficienza nei servizi pubblici, semplificando al contempo l'interazione con i cittadini.

Nell'ambito della pubblica amministrazione, l'introduzione della CIE ha generato significativi vantaggi.

Innanzitutto, la CIE si distingue per le sue misure di sicurezza avanzate e anticontraffazione, che ne garantiscono l'autenticità. L'utilizzo di elementi di sicurezza sia elettronici che fisici la rende un documento altamente sicuro. Inoltre, può incorporare dati biometrici, come impronte digitali o foto digitali, migliorando la precisione dell'identificazione.

La firma digitale rappresenta un'applicazione chiave della CIE, consentendo la generazione di firme legalmente valide. Ciò semplifica la gestione di processi digitali e la sottoscrizione di documenti online. La carta può anche essere impiegata per autenticarsi online, semplificando l'accesso ai servizi pubblici digitali e riducendo la necessità di diverse credenziali.

La progettazione della CIE mira all'interoperabilità, facilitando l'integrazione con diverse piattaforme e sistemi utilizzati dalla pubblica amministrazione. La sua adozione

[8]http://qualitapa.gov.it/sitoarcheologico/relazioni-con-i-cittadini/open-government/strumenti-della-pa-digitale/carta-didentita-elettronica/index.html

contribuisce alla riduzione della burocrazia, semplificando la gestione di pratiche amministrative e transazioni.

La privacy e la protezione dei dati sono considerate con attenzione. L'accesso ai dati contenuti nella CIE è limitato e controllato per garantire la privacy degli individui. Questo documento può essere integrato con altri documenti elettronici, come la Patente di Guida Elettronica, formando un ecosistema di identificazione digitale e documentazione elettronica.

La CIE non è solo uno strumento tecnologico, ma è parte di un più ampio sforzo di digitalizzazione della pubblica amministrazione, promuovendo l'adozione di tecnologie avanzate per migliorare i servizi e semplificare le interazioni con i cittadini. In questo contesto, la CIE agevola la partecipazione dei cittadini ai servizi online, migliorando l'accesso a informazioni e agevolando la partecipazione a consultazioni pubbliche o sondaggi.

È fondamentale notare che l'implementazione e l'utilizzo specifico della Carta d'Identità Elettronica possono variare da paese a paese, influenzati dalle normative locali e dalle decisioni governative. Inoltre, le tecnologie e le funzionalità integrate nella CIE possono evolversi nel tempo per rispondere alle esigenze emergenti della società digitale.

1.5.3. Carta nazionale dei servizi[9]

La Carta Nazionale dei Servizi (CNS) emerge come un elemento fondamentale nel contesto della digitalizzazione della pubblica amministrazione in Italia. Questo dispositivo elettronico si pone come strumento multifunzionale, integrando dati digitali dell'individuo per offrire soluzioni avanzate in termini di autenticazione e firma digitale.

Una delle sue principali funzionalità risiede nell'autenticazione sicura per consentire agli individui di accedere in modo affidabile ai servizi online forniti dalla pubblica amministrazione. Questo non solo semplifica il processo di accesso, ma contribuisce significativamente alla sicurezza delle transazioni online, riducendo il rischio di accessi non autorizzati.

La CNS si distingue anche per la capacità di fornire una firma digitale valida legalmente, consentendo agli utenti di apporre la propria firma su documenti digitali come contratti e moduli. Questo passo innovativo semplifica la gestione di numerosi documenti online, eliminando la necessità di procedure cartacee e accelerando i tempi delle transazioni.

[9]http://qualitapa.gov.it/sitoarcheologico/relazioni-con-i-cittadini/open-government/strumenti-della-pa-digitale/carta-nazionale-dei-servizi/index.html

L'interoperabilità della CNS con la Carta d'Identità Elettronica (CIE) rappresenta un passo avanti significativo. Questi due strumenti collaborano per creare un solido ecosistema di identificazione digitale e autenticazione, fornendo un sistema integrato che amplifica l'efficacia delle transazioni online.

Oltre a ciò, la CNS agisce come uno strumento concreto per la semplificazione burocratica. L'obiettivo è quello di ridurre la necessità di interazioni fisiche negli uffici pubblici, favorendo la digitalizzazione delle procedure e rendendo più agevoli le interazioni tra cittadini e amministrazione.

Tutto ciò è regolamentato da specifiche normative, incluse quelle relative alla firma digitale e all'accesso ai servizi online. Questo quadro normativo, insieme alla sicurezza avanzata incorporata nella CNS, contribuisce a garantire la protezione dei dati personali e la validità legale delle transazioni online.

In conclusione, la Carta Nazionale dei Servizi rappresenta un importante passo avanti nell'ambito della digitalizzazione dei servizi pubblici in Italia, promuovendo l'efficienza, la sicurezza e la semplificazione delle interazioni tra cittadini e amministrazione.

1.5.4. Dematerializzazione

La dematerializzazione nella pubblica amministrazione rappresenta una trasformazione fondamentale, mirata a spostare l'intero processo gestionale dei documenti dal tradizionale formato cartaceo al formato digitale. Questo processo ambizioso è motivato da diversi obiettivi chiave, ognuno finalizzato a migliorare l'efficienza, ridurre la burocrazia e promuovere la trasparenza all'interno del contesto amministrativo.

La fase iniziale della dematerializzazione coinvolge la digitalizzazione dei documenti cartacei, mediante la scansione di tali documenti per crearne una copia informatica o computerizzata. Questo passo è essenziale per avviare la transizione verso un ambiente digitale e garantire l'accessibilità rapida e efficiente alle informazioni.

L'adozione di sistemi di Gestione Documentale Elettronica (GED) costituisce una tappa cruciale in questo processo. Tali sistemi consentono la catalogazione, l'archiviazione e la gestione efficiente dei documenti digitali, semplificando notevolmente la ricerca, la condivisione e la conservazione rispetto ai tradizionali archivi cartacei.

La dematerializzazione incorpora anche l'uso di firme digitali e approvazioni elettroniche, fornendo una validità legale ai documenti digitali. Queste soluzioni non solo eliminano la necessità di procedure basate su carta ma accelerano anche i processi decisionali.

La pubblica amministrazione, attraverso la dematerializzazione, può offrire portali e servizi online per cittadini e imprese, facilitando l'accesso a informazioni, la presentazione di documenti e l'interazione digitale con gli enti pubblici. Questa trasformazione mira anche all'eliminazione del supporto cartaceo nei processi amministrativi, riducendo i costi associati alla stampa, all'archiviazione e alla distribuzione.

La dematerializzazione consente inoltre l'accesso remoto ai documenti, permettendo al personale della pubblica amministrazione di lavorare in modo flessibile e di rispondere rapidamente alle esigenze dei cittadini. Parallelamente, essa favorisce la trasparenza e l'Open Data, permettendo la pubblicazione di dati aperti e semplificando l'accesso alle informazioni pubbliche.

La sicurezza e la protezione dei dati rappresentano elementi cruciali di questo processo. Protocolli di sicurezza attenti sono implementati per garantire la confidenzialità, l'integrità e la disponibilità dei documenti digitali.

Infine, è essenziale la formazione del personale, che gioca un ruolo chiave nell'adozione efficace di questi nuovi strumenti e processi digitali.

In definitiva, l'implementazione della dematerializzazione nella pubblica amministrazione è parte di un più ampio sforzo di modernizzazione dei servizi, semplificazione delle procedure e miglioramento complessivo dell'esperienza di cittadini e imprese.

1.5.5. Open data

Nella pubblica amministrazione, il concetto di Open Data si traduce nell'atto di rendere disponibili al pubblico insiemi di dati prodotti e gestiti dagli enti governativi. L'obiettivo primario di questa pratica è stimolare la trasparenza, coinvolgere attivamente i cittadini, promuovere l'innovazione e creare valore attraverso la condivisione di informazioni pubbliche.

Iniziamo con la definizione di Open Data. Si tratta di dati liberamente accessibili, riutilizzabili e redistribuibili da chiunque, solitamente resi disponibili attraverso licenze aperte che consentono l'utilizzo senza restrizioni e promuovono la condivisione.

Gli Open Data possono abbracciare una vasta gamma di informazioni, inclusi dati statistici, geografici, economici, amministrativi, ambientali e sociali, a seconda delle attività specifiche di ciascuna pubblica amministrazione.

Le istituzioni gestiscono spesso portali dedicati per la pubblicazione e distribuzione di dati aperti, offrendo un punto centrale per il download, l'accesso e strumenti per la visualizzazione e l'analisi.

L'aspetto della trasparenza e dell'accountability è cruciale. La pubblicazione di dati aperti contribuisce a rendere trasparenti le attività delle istituzioni, permettendo ai cittadini di monitorare le prestazioni e partecipare attivamente al processo decisionale.

Gli Open Data rappresentano anche una risorsa chiave per l'innovazione e lo sviluppo economico. Sviluppatori, imprese e ricercatori possono utilizzare tali dati per creare nuove applicazioni, servizi e soluzioni, generando valore aggiunto per la società.

La partecipazione civica è favorita dagli Open Data, consentendo ai cittadini di analizzare dati governativi, esprimere opinioni informate e partecipare ai processi decisionali, rafforzando il coinvolgimento della comunità e la fiducia nel governo.

L'adozione di standard per la pubblicazione di Open Data favorisce l'interoperabilità tra diverse fonti di dati, semplificando l'integrazione e l'analisi di informazioni provenienti da diverse fonti.

Gli Open Data trovano applicazione in vari settori, come trasporti, ambiente, sanità, istruzione ed economia, portando a miglioramenti nei servizi pubblici e alla risoluzione di problemi sociali.

La pubblicazione di dati aperti deve avvenire in conformità alle normative sulla protezione della privacy e la sicurezza dei dati, adottando misure per anonimizzare i dati sensibili e prevenire rischi per la privacy.

Infine, il ciclo di feedback e iterazione gioca un ruolo fondamentale. Gli utenti possono fornire feedback, consentendo alle pubbliche amministrazioni di migliorare la qualità dei dati pubblicati e ampliare l'offerta di informazioni utili.

L'adozione di politiche di Open Data rappresenta un passo significativo verso una pubblica amministrazione più aperta, responsabile e orientata alla partecipazione, promuovendo una cultura che sfrutta il potenziale informativo a beneficio della società nel suo complesso.

1.5.6. La posta elettronica certificata

La Posta Elettronica Certificata (PEC) emerge come uno strumento fondamentale nella sfera della comunicazione elettronica, rivestendo particolare importanza quando si tratta di documenti ufficiali e comunicazioni legalmente rilevanti, soprattutto nel contesto della pubblica amministrazione italiana. Questo strumento è disciplinato da normative specifiche che mirano a garantire sicurezza, tracciabilità e validità legale delle comunicazioni elettroniche. Alcuni aspetti chiave della posta elettronica certificata nella pubblica amministrazione includono:

che sia definita come un servizio di posta elettronica che assicura l'invio e la ricezione di messaggi con valore legale equiparabile a quelli delle tradizionali raccomandate con ricevuta di ritorno. Ogni messaggio inviato tramite PEC è dotato di una firma digitale che ne certifica l'autenticità.

La normativa di riferimento in Italia per l'utilizzo della stessa è il Decreto Legislativo n. 82 del 2005, che stabilisce le caratteristiche tecniche e gli standard di sicurezza che le caselle PEC devono rispettare per garantire la validità legale delle comunicazioni.

Essa conferisce ai messaggi un'autenticità giuridica, garantendo la validità legale delle comunicazioni elettroniche. Questo aspetto assume rilevanza per documenti ufficiali, notifiche, atti giudiziari e altri scambi di informazioni legalmente vincolanti.

Un elemento distintivo della PEC è la tracciabilità e la certificazione temporale. Ogni messaggio inviato o ricevuto è dotato di un timestamp che ne attesta l'orario e la data di invio, contribuendo a stabilire la sequenza cronologica degli eventi.

Le pubbliche amministrazioni in Italia hanno l’obbligo dell’utilizzo della posta certificata per le comunicazioni ufficiali, incluso l'invio di atti, provvedimenti, determinazioni e altri documenti aventi valore legale.

La registrazione delle caselle PEC presso l'Autorità di Regolamentazione delle Comunicazioni (AgID) è un requisito, attraverso normative tecniche e di sicurezza specifiche da rispettare.

Nella pubblica amministrazione mira a semplificare le procedure, accelerare gli scambi di informazioni e ridurre la dipendenza dalla carta stampata.

La PEC è spesso integrata con altri servizi digitali della PA, facilitando l'invio e la ricezione di documenti in ambienti digitali.

L'adozione della PEC contribuisce a ridurre i costi legati alle comunicazioni cartacee e all'archiviazione fisica dei documenti, comportando un impatto ambientale ridotto grazie alla diminuzione dell'uso di carta.

La sicurezza delle comunicazioni è garantita attraverso l'utilizzo di firme digitali e crittografia, proteggendo i documenti inviati da manipolazioni e assicurando la riservatezza delle informazioni.

In sintesi, la posta certificata gioca un ruolo cruciale nella modernizzazione delle comunicazioni nella pubblica amministrazione italiana, promuovendo l'efficienza, la trasparenza e la sicurezza nelle interazioni elettroniche.

1.5.7. Protocollo informatico

Il protocollo informatico, cuore pulsante della gestione documentale nella pubblica amministrazione, rivela la sua complessità e importanza nel passaggio verso un mondo digitale. Si tratta di un sistema elettronico sapientemente progettato per orchestrare il flusso dei documenti digitali, garantendo un'elevata tracciabilità e sicurezza delle informazioni.

La sua definizione sottolinea la sua natura multifunzionale, abbracciando la registrazione, l'assegnazione di numeri progressivi e la conservazione dei documenti all'interno dell'organizzazione. È concepito come un garante della tracciabilità e della gestione efficiente di documenti che, in formato elettronico, sono l'anima delle attività amministrative.

Le normative di riferimento, tra cui il Decreto Legislativo n. 82 del 2005 in Italia, fungono da bussola, plasmando un contesto regolamentare che ne garantisce la coerenza e la validità giuridica. Queste norme forniscono le linee guida per l'adozione e l'implementazione del protocollo informatico nell'ambito della pubblica amministrazione.

Il Registro Generale dei Documenti, sorvegliato dal protocollo informatico, assume il ruolo di custode digitale, assegnando a ciascun documento un numero univoco e progressivo. Tale registro costituisce un elenco completo, vivace e in continua evoluzione, di tutti i documenti che varcano la soglia dell'ente pubblico.

L'aspetto della classificazione e categorizzazione riflette la sua capacità di organizzare documenti secondo criteri prefissati, consentendo una gestione efficiente e facilitando il rapido reperimento delle informazioni. Inoltre, l'integrazione della firma digitale emerge come un tassello essenziale per garantire la validità legale dei documenti digitali, autenticandone origine e integrità.

Il protocollo informatico non si limita alla gestione statica dei documenti, bensì s'integra dinamicamente con flussi di lavoro documentali. Questi delineano il percorso di ogni documento attraverso diverse fasi di approvazione e revisione, contribuendo a strutturare un processo documentale che è sia solido che tracciabile.

La gestione dell'archiviazione, uno dei compiti chiave del protocollo informatico, offre un rifugio digitale sicuro per i documenti, garantendo l'accesso sicuro e la conservazione a lungo termine. Ciò rappresenta un passo significativo verso la riduzione dell'uso di documenti cartacei, promuovendo un ambiente più sostenibile.

La facilità della trasmissione e dello scambio di documenti, sia all'interno dell'organizzazione che con altre entità, sottolinea la sua funzione di catalizzatore delle comunicazioni digitali. Tale facilitazione avviene in un contesto sicuro e tracciabile, conferendo affidabilità al processo.

Il controllo dell'accesso a documenti sensibili è un pilastro dell'architettura del protocollo informatico. L'accesso è strettamente controllato e limitato a utenti autorizzati, preservando la sicurezza delle informazioni e mitigando rischi potenziali.

Infine, l'audit e la tracciabilità registrati dal protocollo informatico forniscono un quadro dettagliato di ogni attività legata ai documenti. Questo non solo serve a fini di responsabilità interna, ma rappresenta un elemento fondamentale per garantire la conformità normativa.

In sintesi, l'implementazione efficace del protocollo informatico nella pubblica amministrazione non solo testimonia la transizione verso un'era digitale, ma rappresenta un passo significativo verso la trasparenza, l'efficienza operativa e la conformità normativa nella gestione dei documenti digitali.

1.5.8. La firma digitale

La firma digitale emerge come un pilastro cruciale nell'evoluzione dei processi amministrativi nella pubblica amministrazione, fornendo una robusta cornice di sicurezza e validità legale per i documenti elettronici. Questa trasformazione digitale, in linea con normative specifiche, costituisce un passo avanti significativo verso l'efficienza, la trasparenza e la sicurezza nei processi amministrativi.

La firma digitale, in termini chiari, si configura come un insieme di dati elettronici associati a un documento digitale. La sua funzione cardine risiede nella garanzia dell'autenticità dell'origine del documento, nell'incolumità del suo contenuto e, in alcuni

contesti, nella non repudiabilità da parte del firmatario. Un pilastro normativo come il Decreto Legislativo n. 82 del 2005 in Italia stabilisce le regole e i parametri per l'impiego della firma digitale e della firma digitale avanzata, fornendo un solido fondamento legale.

Diverse sfumature di firma digitale si delineano nel panorama normativo, spaziando dalla firma digitale semplice alla firma digitale avanzata. Quest'ultima, spesso sostenuta da dispositivi di firma sicura come smart card o token USB, emerge come la scelta preminente per garantire un livello superiore di sicurezza nei processi di firma.

La validità legale conferita dalla firma digitale è un punto di svolta. I documenti firmati con questo sistema godono di parità di validità giuridica rispetto a quelli sottoscritti manualmente, spianando la strada per una dematerializzazione più ampia degli atti amministrativi.

La Firma Elettronica Avanzata (FEA), in conformità con le normative europee e italiane, si erge come una tipologia di firma digitale che va oltre, collegando in modo inequivocabile il firmatario al documento, garantendo la sua identificazione e preservando l'integrità del documento.

Il processo di firma digitale non si limita a un mero apporre di sigilli elettronici; si integra sinergicamente in flussi di lavoro digitali, snellendo (alleggerendo) la gestione dei documenti e agevolando la collaborazione tra diverse unità amministrative. Questa integrazione facilita una transizione fluida verso un ambiente digitale, riducendo la dipendenza dalla documentazione cartacea.

Nella pubblica amministrazione, la firma digitale imprime la sua firma su una vasta gamma di documenti: dai contratti agli accordi, dalle determinazioni ai verbali e ad altri atti amministrativi. Questa pratica, oltre a accelerare i processi, contribuisce a emancipare gli uffici dalla necessità di affrontare volumi ingenti di documentazione cartacea.

Il suo impatto si estende alla sicurezza dell'accesso ai documenti, garantendo che solo coloro che sono autorizzati possano attingere ai documenti firmati, preservando così la riservatezza e la sicurezza delle informazioni sensibili. La tracciabilità delle firme digitali, ancorate a timestamp, offre un quadro dettagliato delle attività legate ai documenti, facilitando audit accurati e assicurando la conformità normativa.

In sintesi, l'adozione della firma digitale nella pubblica amministrazione è una tessera essenziale nella partita della digitalizzazione, apportando benefici tangibili in termini di efficienza, trasparenza e sicurezza nei processi amministrativi.

1.6 E-Government e Street-level Bureaucracy ed Europa nei processi di digitalizzazione

Nel contesto dell'analisi della digitalizzazione nel settore pubblico, emerge il concetto di governo elettronico (e-government)[10]. Questa terminologia, introdotta dal politologo Michael Lipsky, si collega intimamente alla street-level bureaucracy, che focalizza l'attenzione sul livello operativo dei servizi pubblici e sugli operatori che interagiscono direttamente con i cittadini.

L' e-government funge da ponte tra la PA e le nuove tecnologie, sfumandone i confini attuando la digitalizzazione dei processi amministrativi, come sottolineato da Giritli Nygren (2012, 616). Esso viene definito in molteplici modi nella letteratura: secondo Bovaird (2003, 37), rappresenta l'abilitazione elettronica di tutti i servizi pubblici, mentre Lau et al. (2008, 89) ampliano la prospettiva includendo gli utenti, concependo l'e-government come il processo che connette digitalmente i cittadini al governo centrale delle amministrazioni

In Europa, è la Dichiarazione di Malmo sulle politiche di e-Government del 2009 ad annunciare un percorso di apertura delle amministrazioni europee attraverso le potenzialità dell'ICT. L' Open declaration on European public services individua tre capisaldi Trasparenza, Partecipazione, Empowerment; la trasparenza nell'ambito della PA è da intendersi come pubblicazione non discrezionale dei dati in formato riusabile che ha tra le altre finalità quella di aumentare la partecipazione e l'empowerment dei cittadini.

Il libero accesso alle informazioni pubbliche, reso possibile da questa iniziativa, contribuisce a creare un ambiente di trasparenza che migliora la qualità del dibattito sulle politiche pubbliche e rende più efficiente l'amministrazione pubblica. In questo contesto, si parla di "Open data per l'Accountability".

Il governo digitale è quindi strettamente intrecciato alla street-level bureaucracy, in quanto si occupa della fornitura di informazioni e servizi attraverso Internet o altri dispositivi digitali, proprio come gli operatori di base, come assistenti sociali e insegnanti, si trovano in prima linea nell'affrontare le esigenze concrete della comunità. Homburg (2018, 348) sottolinea che il governo digitale è intrinsecamente legato alla trasformazione e alla riforma dei governi, in sintonia con la street-level bureaucracy che richiede una gestione più efficiente ed efficace delle politiche pubbliche.

[10]La digitalizzazione del settore pubblico: una revisione sistematica della letteratura (doi: 10.1483/100372)

Ma cos’è realmente la "street-level bureaucracy"? È un concetto coniato, anch’esso, dal politologo Michael Lipsky nel 1980 per evidenziare l'importanza della discrezionalità che gli operatori della Pubblica Amministrazione hanno nel tradurre in pratica leggi, regolamenti, standard e linee guida. Questi operatori, come poliziotti, assistenti sociali e insegnanti, godono spesso di un margine di discrezionalità nell'applicare le politiche e si trovano in prima linea nell'affrontare le esigenze specifiche della comunità.

L'avanzare della digitalizzazione ha profondamente influenzato la street-level bureaucracy, modificando il modo in cui gli operatori erogano servizi e interagiscono con i cittadini.

Nell’ambito della digitalizzazione anche gli operatori informatici sono impegnati nell’implementazione delle linee guida AGID senza dimenticare l’operatività dell’utente finale. Le linee guida sul cloud ed i data center sono state trasformate in direttive per riuscire ad erogare correttamente i servizi, i data center che dovevano essere smantellati sono diventati dei centri ove vengono erogati i servizi vitali del mondo medicale.

I servizi di autenticazione sono stati adattati in modo da essere il più vicino possibile alle linee guida e le misure minime di sicurezza ma senza ostacolare troppo l’accesso dell’utente.

I servizi di video sorveglianza che hanno regolamenti digitali rigidi vengono gestiti da operatori che cercano di risolvere soprattutto il problema principale e cioè dare i dati che servono alle autorità per poter capire chi abbia effettuato un furto oppure un atto vandalico. Quindi gli operatori trovano degli accordi a volte solo verbale in modo da poter comunque dare quanto richiesto nonostante restrizioni sul tempo di conservazione o altro.

L’autenticazione a due fattori viene configurata in modo da poter far accedere tutti, in alcuni casi viene esclusa ma vengono implementate policy di sicurezza che permettano comunque l’accesso sicuro alle risorse.

Tutto questo viene fatto in autonomia dagli operatori per cercare di creare meno disparità possibili e per far sì che i dipendenti della pubblica amministrazione possano lavorare agevolmente e che i cittadini possano comunque accedere ai servizi in sicurezza.

In tutti i settori come forze dell’ordine, scuole, servizi sociali la digitalizzazione e le linee guida e disposizioni in materia devono, tutti i giorni, essere messe in atto non pensando solo al rispetto delle normative ma soprattutto all’operatività e l’effettiva erogazione dei servizi.

Cosa ha fatto l'Unione Europea? L'Unione Europea (UE) ha esercitato una considerevole spinta verso la digitalizzazione nell'ambito delle pubbliche amministrazioni dei suoi Stati membri. Questo impulso è stato guidato da una serie di iniziative e politiche che mirano a migliorare l'efficienza, la trasparenza e l'accessibilità dei servizi pubblici attraverso l'adozione delle tecnologie digitali.

Anche in questo contesto, la street-level bureaucracy, gioca un ruolo cruciale. Le politiche europee di digitalizzazione, come l'Agenda Digitale per l'Europa, hanno incoraggiato gli Stati membri a modernizzare le loro pubbliche amministrazioni attraverso l'implementazione di soluzioni digitali. Ciò include lo sviluppo di servizi online, la digitalizzazione dei processi decisionali e l'adozione di tecnologie avanzate per migliorare l'efficacia delle istituzioni pubbliche.

Un esempio tangibile di questa spinta è la creazione di portali digitali e piattaforme online che facilitano l'accesso ai servizi pubblici. Tali strumenti non solo semplificano le procedure per i cittadini, ma anche per gli operatori a livello di street-level bureaucracy, fornendo loro strumenti digitali per gestire in modo più efficiente le richieste e le esigenze della comunità.

L'Unione Europea, attraverso programmi di finanziamento e incentivi, ha sostenuto gli Stati membri nel potenziamento delle loro capacità digitali. Ciò ha comportato la formazione degli operatori della street-level bureaucracy sull'uso di nuove tecnologie e la promozione di una cultura digitale all'interno delle pubbliche amministrazioni.

In sintesi, l'UE ha esercitato una spinta notevole verso la digitalizzazione nelle pubbliche amministrazioni, influenzando direttamente il modo in cui la street-level bureaucracy eroga i servizi pubblici. Il bilanciamento tra l'impulso europeo per l'innovazione digitale e le dinamiche concrete a livello locale rappresenta una sfida chiave per garantire che la digitalizzazione abbia un impatto positivo sulla vita quotidiana dei cittadini.

1.7 Vantaggi e criticità[11] [12]

La digitalizzazione della pubblica amministrazione italiana rappresenta una trasformazione significativa che genera diversi benefici. Esaminiamo da vicino sia gli aspetti positivi che le difficoltà associate a questo processo.

[11]https://www.sogei.it/it/sogei-homepage/azienda/sala-stampa/Articolieinterviste/articoli-e-interviste-2023/i-vantaggi-di-una-pubblica-amministrazione-digitale.html
[12]http://focus.formez.it/sites/all/files/competenze_digitali_report_focus_group_dicembre_2021_.pdf

Parlando dei vantaggi, l'adozione di processi digitali si traduce in un flusso di lavoro più rapido ed efficiente, migliorando notevolmente la gestione dei dati e riducendo i tempi di elaborazione. Questo si riflette in un accesso semplificato ai servizi pubblici, consentendo ai cittadini e alle imprese di interagire in modo più diretto attraverso canali online, riducendo la necessità di spostamenti fisici.

La dematerializzazione dei documenti gioca un ruolo chiave nella riduzione della burocrazia, facilitando la gestione e la condivisione delle informazioni tra le diverse unità amministrative. Inoltre, la trasparenza viene favorita attraverso la pubblicazione di dati aperti, promuovendo così la partecipazione civica e permettendo ai cittadini di essere attivamente coinvolti nella vita pubblica.

La riduzione della dipendenza dalla documentazione cartacea non solo comporta un risparmio significativo di costi a lungo termine ma contribuisce anche a un minore impatto ambientale, sostenendo gli sforzi di sostenibilità. L'innovazione e lo sviluppo tecnologico sono ulteriormente stimolati, portando alla creazione di nuove soluzioni e servizi che migliorano la qualità complessiva dell'offerta pubblica.

Tuttavia, quest'ampia digitalizzazione non è priva di sfide. Il divario tecnologico tra diverse Organizzazioni e Regioni può rappresentare un ostacolo, con alcuni enti che potrebbero faticare ad adottare soluzioni digitali avanzate. L'aumento delle attività digitali espone la pubblica amministrazione a nuovi rischi di sicurezza informatica, come attacchi informatici e violazioni dei dati.

L'analfabetismo digitale o divario digitale (Digital Divide), specialmente tra cittadini di età avanzata o con limitate competenze digitali, potrebbe comportare difficoltà nell'interagire con i servizi digitali mentre l'accesso ai servizi digitali potrebbe essere difficoltoso per alcuni cittadini con disabilità o senza accesso affidabile a Internet.

La resistenza al cambiamento da parte del personale e degli utenti abituati a procedure tradizionali è un'altra sfida da affrontare. Le preoccupazioni sulla privacy e sulla protezione dei dati, specialmente in gestione di informazioni sensibili, richiedono un approccio attento e sicuro.

L'implementazione di soluzioni digitali richiede investimenti significativi in tecnologia e formazione del personale, presentando sfide in termini di risorse finanziarie e umane. La

presenza di sistemi disconnessi o scarsamente interoperabili può ostacolare la fluidità dell'informazione tra diverse entità amministrative.

In sintesi, la digitalizzazione in corso nella pubblica amministrazione italiana è un processo complesso e in divenire che richiede una gestione attenta e bilanciata. Affrontare queste criticità in modo efficace è fondamentale per sfruttare appieno i vantaggi offerti dalla trasformazione digitale.

1.8 Introduzione alla Cybersecurity

Anche la sicurezza riveste un ruolo cruciale nel processo di digitalizzazione della PA, al fine di garantire ai cittadini la possibilità di accedere ai servizi da remoto, gestendo dati spesso critici o sensibili. Oltre il 79%[13] delle PA mette a disposizione dei propri utenti sia credenziali proprietarie sia sistemi di identità digitale nazionali (come SPID e CIE) per garantire l'accesso sicuro ai propri servizi online. Nel 18% dei casi è sufficiente l'utilizzo di credenziali proprietarie, mentre nel restante 3% l'accesso può avvenire unicamente attraverso identità digitali nazionali. Questa rilevazione evidenzia un generale ritardo rispetto a quanto previsto dalla normativa vigente: secondo quanto stabilito dal Decreto Semplificazioni, tutte le amministrazioni locali e centrali avrebbero dovuto integrare SPID e CIE come sistemi di autenticazione e accesso ai servizi pubblici digitali a partire da febbraio 2021.

All'interno della pubblica amministrazione, inoltre, si osserva un livello di attenzione spesso insufficiente per l'individuazione di potenziali vulnerabilità di sicurezza che possono coinvolgere le applicazioni e le infrastrutture basate su Cloud. Queste vulnerabilità sono sfruttabili dai criminali informatici come punto di ingresso per attuare azioni malevole nei sistemi aziendali. Il 37% delle organizzazioni sembra non aver ancora definito una strategia chiara per riconoscere le vulnerabilità presenti nelle applicazioni e nelle infrastrutture: tra queste, il 35% effettua solo occasionalmente attività di identificazione, mentre il restante 2% non svolge alcuna forma di valutazione della sicurezza.

Particolare attenzione merita il "Capitolo 6. Sicurezza informatica" del Piano Triennale in cui si evidenzia l'importanza dei servizi digitali erogati dalla Pubblica Amministrazione per il corretto funzionamento del Sistema Paese.2

[13]https://www.digitech.news/digital/14/08/2023/cloud-computing-e-cybersecurity-le-nuove-sfide-per-la-pa-italiana/

Il cuore del capitolo sono i temi relativi al Cyber Risk e alla Cyber Security che evidenziano la necessità di aumentare sia la consapevolezza della minaccia cibernetica nella PA, sia i livelli di sicurezza informatica nei portali della Pubblica Amministrazione allo scopo di contenere i rischi connessi alle potenziali minacce informatiche.

Contrastare tali minacce è fondamentale poiché assicura la disponibilità, l'integrità, la riservatezza e la protezione delle informazioni e ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla Pubblica Amministrazione.

2. CAPITOLO 2 – La Cybersecurity

2.1 Cenni normativi[14]

In Italia, la sicurezza informatica nella pubblica amministrazione è un tema di fondamentale importanza, e diverse normative sono state istituite per regolarne gli aspetti. Uno dei principali punti di riferimento è il Codice dell'Amministrazione Digitale (CAD), emanato attraverso il Decreto Legislativo n. 82/2005. Questo codice regola l'utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito della PA, fornendo disposizioni specifiche sulla sicurezza informatica e la tutela dei dati.

Le Linee Guida in materia di Sicurezza per la Pubblica Amministrazione per gli enti pubblici (LGS/PA), elaborate dall'Agenzia per l'Italia Digitale (AgID), costituiscono un altro pilastro normativo. Queste linee guida forniscono dettagliate indicazioni sulla sicurezza informatica per gli enti, garantendo un adattamento continuo alle nuove sfide emergenti nel campo della cybersecurity.

Parallelamente, le Regole Tecniche in materia di Sicurezza per la Pubblica Amministrazione (RTS/PA), anch'esse emanate da AgID, stabiliscono standard tecnici e specifiche per l'implementazione di misure di sicurezza informatica a livello tecnologico, assicurando una base solida per la protezione dei sistemi informatici governativi.

Un altro importante contributo alla sicurezza dei dati è rappresentato dal Regolamento Europeo sulla Protezione dei Dati Personali (GDPR). Benché non sia specifico per l'Italia, il GDPR si applica a tutte le organizzazioni che trattano dati personali, inclusi gli enti

[14]https://www.forumpa.it/pa-digitale/sicurezza-digitale/la-cybersecurity-nella-pa-quali-sono-i-principali-rischi-e-come-affrontarli/

governativi. Questo regolamento impone rigorosi standard di protezione dei dati personali, accompagnati da sanzioni significative in caso di violazioni.

La normativa italiana sulla crittografia costituisce un ulteriore strumento di difesa, stabilendo l'utilizzo di tecniche crittografiche per preservare la riservatezza e l'integrità delle informazioni. La regolamentazione in questo settore guida l'impiego di chiavi crittografiche e firme digitali, garantendo un elevato livello di sicurezza nelle comunicazioni elettroniche.

Gli enti pubblici sono tenuti a redigere e adottare Documenti Operativi di Sicurezza (DOS) e Documenti Programmatici di Sicurezza (DPS). Questi costituiscono strumenti operativi e strategici che permettono di condurre al meglio la gestione della sicurezza informatica all'interno delle organizzazioni governative.

Inoltre, il Piano Triennale per l'Informatica nella PA rappresenta uno strumento strategico che definisce gli obiettivi e le priorità per l'evoluzione tecnologica della pubblica amministrazione, includendo aspetti cruciali legati alla sicurezza informatica.

Infine, il Provvedimento del Garante per la Protezione dei Dati Personali n. 311/2019 fornisce indicazioni specifiche sulle misure minime di sicurezza per il trattamento dei dati personali da parte degli enti, consolidando ulteriormente gli sforzi per garantire standard elevati di sicurezza informatica e proteggere l'integrità, la riservatezza e la disponibilità delle informazioni gestite dagli enti governativi italiani.

2.2 Differenze con altri paesi[15]

Le politiche e le normative sulla sicurezza informatica nella pubblica amministrazione nell’amministrazione pubblica mostrano notevoli variazioni tra i diversi paesi, a causa di leggi specifiche, tradizioni giuridiche, infrastrutture digitali e minacce cibernetiche uniche a ciascuna regione. Queste differenze si manifestano in vari aspetti:

In primo luogo, la regolamentazione e le normative variano anche se gli Stati europei, inclusa l'Italia, sono soggetti a normative comuni come il GDPR. Alcuni paesi, come il Regno Unito, possono avere normative più specifiche che dettano requisiti dettagliati per la sicurezza informatica.

[15]https://www.cybersecitalia.it/la-cybersecurity-in-italia-francia-e-germania-sistemi-a-confronto/20469/

L'adozione di standard e framework per la sicurezza informatica può differire notevolmente tra i paesi. Mentre alcuni seguono normative internazionali come ISO/IEC 27001, altri sviluppano standard nazionali su misura.

Alcuni paesi avanzati, tra cui il Regno Unito e la Germania, hanno elaborato strategie nazionali di cybersecurity con obiettivi specifici e linee guida dettagliate per proteggere le amministrazioni dalle minacce cibernetiche. Tuttavia, le priorità e i dettagli di queste strategie possono variare.

Il coordinamento tra agenzie governative è un aspetto critico che differisce notevolmente. Alcuni paesi presentano una stretta collaborazione per garantire una risposta unificata alle minacce, mentre in altri casi, le iniziative possono essere più frammentate.

Il livello di consapevolezza e formazione sulla sicurezza informatica nella PA può variare considerevolmente, con paesi come i Paesi Bassi che potrebbero avere programmi avanzati e maggiore consapevolezza tra il personale pubblico.

Gli investimenti e le risorse dedicati alla sicurezza informatica variano notevolmente tra i paesi, con alcune nazioni che dispongono di strutture più avanzate, mentre altre affrontano sfide legate alle risorse.

Le minacce cibernetiche specifiche di un paese possono influenzare le priorità e le strategie di sicurezza informatica. Ad esempio, contesti geopolitici o economici specifici possono rendere un paese più suscettibile a determinati tipi di attacchi.

La protezione delle infrastrutture critiche, come l'energia, le telecomunicazioni e i trasporti, varia notevolmente tra i paesi ed è spesso una componente chiave delle strategie di sicurezza informatica nazionali.

La collaborazione internazionale sulla sicurezza informatica può variare, con alcuni paesi coinvolti in iniziative di condivisione di informazioni e collaborazione, mentre altri seguono una strategia più nazionalista.

L'infrastruttura di sicurezza cibernetica, come Centri Nazionali di Cyber Security e meccanismi di coordinamento, può essere più sviluppata in paesi come la Germania, ma la disponibilità e l'uso di tali strutture differiscono.

Iniziative di collaborazione a livello europeo, come quelle promosse dall'ENISA, evidenziano la varietà di approcci adottati dai paesi europei per affrontare le minacce cibernetiche.

L'approccio alla gestione delle vulnerabilità, alla risposta agli incidenti e all'innovazione tecnologica può variare notevolmente tra i paesi, con alcuni più avanzati nell'adozione di soluzioni innovative.

In conclusione, la diversità nella sicurezza informatica nella pubblica amministrazione è plasmata da una combinazione di fattori normativi, culturali, economici e geopolitici. Mentre alcuni principi sono universali, la loro implementazione pratica varia significativamente su scala globale.

2.3 Investimenti sulla Cybersecurity nella PA Italiana

La sicurezza informatica nella pubblica amministrazione italiana rappresenta un elemento cruciale per proteggere i dati e i servizi digitali gestiti dalle istituzioni governative. Gli investimenti in questa area sono finalizzati a preservare l'integrità dei sistemi informativi, prevenire violazioni della sicurezza e assicurare la continuità dei servizi pubblici.

Un primo aspetto da considerare riguarda i finanziamenti previsti nel Piano Triennale per l'Informatica delle PA, che include disposizioni specifiche per gli investimenti nella sicurezza informatica. Questo piano stabilisce le priorità e gli obiettivi di investimento, orientati al potenziamento delle infrastrutture digitali e alla sicurezza dei dati.

Inoltre, l'Italia può beneficiare di programmi di finanziamento europei dedicati alla sicurezza cibernetica. Un esempio tangibile è rappresentato dal Quadro Finanziario Pluriennale (QFP) dell'Unione Europea, che potrebbe includere risorse destinate alle iniziative di sicurezza informatica nei paesi membri, tra cui l'Italia.

Il Centro di Competenza Nazionale Cybersecurity (CNC) svolge un ruolo chiave, fornendo competenze avanzate e consulenza sulla sicurezza cibernetica agli enti pubblici. Gli investimenti possono essere diretti a potenziare le risorse e le capacità del CNC, contribuendo così alla sicurezza generale.

È inoltre importante sottolineare che gli investimenti in sicurezza informatica spesso si integrano nei progetti più ampi di modernizzazione e digitalizzazione. Ciò implica l'adozione di tecnologie avanzate, come sistemi di rilevamento delle minacce e soluzioni di sicurezza avanzate, all'interno di iniziative più ampie.

Parte degli investimenti è destinata a programmi di formazione per il personale dipendente, al fine di migliorare la consapevolezza sulla sicurezza informatica e sviluppare competenze specializzate per affrontare le crescenti minacce cibernetiche.

La ricerca e lo sviluppo rappresentano un ulteriore ambito di investimento, con l'obiettivo di sviluppare soluzioni innovative e tecnologie avanzate per migliorare la sicurezza informatica degli enti amministrativi.

L'acquisizione di tecnologie e servizi di sicurezza informatica, come soluzioni di crittografia e sistemi di autenticazione avanzati, è un ulteriore passo per rafforzare la sicurezza digitale.

Infine, parte degli investimenti potrebbe essere dedicata alla collaborazione internazionale sulla sicurezza informatica, consentendo lo scambio di informazioni e l'adozione delle migliori pratiche a livello globale. In definitiva, il continuo impegno e gli investimenti in cybersecurity sono fondamentali per affrontare le minacce sempre più sofisticate nel panorama digitale, garantendo la sicurezza dei dati e la fiducia dei cittadini nella gestione digitale della pubblica amministrazione.

2.4 Gli strumenti

La sicurezza informatica si basa sull'utilizzo di una serie di strumenti e tecnologie avanzate, mirate a garantire la protezione dei sistemi informativi e dei dati sensibili, nonché a assicurare la continuità dei servizi digitali.

Uno degli strumenti chiave impiegati è il “firewall”, un dispositivo o software progettato per monitorare, filtrare e controllare il traffico di rete. Questo strumento è ampiamente adottato per proteggere i confini della rete e prevenire l'accesso non autorizzato, fornendo un primo scudo difensivo contro potenziali minacce.

Altro elemento cruciale è rappresentato dai Sistemi di Rilevamento delle Intrusioni (IDS) e di Prevenzione delle Intrusioni (IPS). Gli IDS monitorano attivamente il traffico di rete, identificando attività sospette o possibili violazioni della sicurezza. Gli IPS, a differenza, vanno oltre, intraprendendo azioni preventive in tempo reale per bloccare gli attacchi.

La sicurezza delle applicazioni è garantita attraverso l'utilizzo di strumenti specializzati come i Web Application Firewalls (WAF), che proteggono le applicazioni web da vulnerabilità e attacchi comuni come SQL injection e cross-site scripting (XSS).

Software antivirus e antimalware sono elementi fondamentali per la rilevazione e la rimozione di malware, virus e altre minacce informatiche. Questi strumenti assicurano la protezione dei dispositivi e dei sistemi da infezioni dannose.

La crittografia è impiegata per preservare la confidenzialità dei dati, offrendo una barriera crittografica per proteggere le comunicazioni, i dati archiviati e altri asset critici della pubblica amministrazione.

La sicurezza della posta elettronica è gestita attraverso soluzioni dedicate come filtri antispam e antiphishing, che contribuiscono a proteggere la pubblica amministrazione da e-mail dannose e tentativi di ingegneria sociale.

L'autenticazione multifattore (MFA) rappresenta un'ulteriore strato di sicurezza, richiedendo più di un metodo di verifica per accedere ai sistemi. Ciò può includere l'utilizzo di password, token, biometria o altri metodi.

I sistemi di Gestione delle Identità e degli Accessi (IAM) consentono di dirigere e controllare le identità degli utenti e i relativi accessi alle risorse digitali, assicurando che solo utenti autorizzati possano accedere a determinati dati e servizi.

La Gestione delle Vulnerabilità è effettuata tramite strumenti dedicati che identificano e affrontano potenziali debolezze nei sistemi, eseguendo scansioni alla ricerca di vulnerabilità e facilitando l'applicazione di patch correttive.

Per il monitoraggio delle minacce ci si avvale di sistemi specializzati rilevando attività sospette o comportamenti anomali all'interno della rete e consentendo una risposta tempestiva agli incidenti di sicurezza.

In caso di incidenti, gli strumenti di Analisi Forense Digitale vengono impiegati per investigare sull'origine e sulla portata dell'attacco, raccogliendo prove digitali cruciali per comprendere e risolvere la situazione.

Infine, la sicurezza dei dispositivi endpoint è assicurata attraverso soluzioni specifiche che proteggono computer, laptop e dispositivi mobili all'interno della rete della pubblica amministrazione.

L'integrazione di questi strumenti crea un ambiente di sicurezza completo e resiliente contro le minacce cibernetiche, con la scelta e la configurazione degli stessi guidate dalle specifiche esigenze della della PA e dalla natura dei dati e dei servizi gestiti.

2.5 Gli enti governativi in materia di Cybersecurity e la loro evoluzione[16]

Nel contesto della sicurezza informatica, gli enti governativi assumono un ruolo di rilievo nella formulazione di politiche, normative e strategie volte a garantire la sicurezza dei sistemi informativi e dei dati sensibili. La loro evoluzione è strettamente connessa alla necessità di adattarsi alle veloci e complesse sfide nel campo cibernetico.

Le Agenzie Nazionali di Cybersecurity, noto in Italia come ACN, svolgono un ruolo chiave nel coordinare gli sforzi a livello nazionale, contribuendo allo sviluppo di politiche e standard e offrendo supporto tecnico sia alle istituzioni pubbliche che al settore privato.

L'Evoluzione Normativa è guidata dagli enti governativi, che contribuiscono alla definizione di normative specifiche sulla sicurezza informatica. Questo processo di evoluzione normativa rappresenta un adattamento costante alle nuove minacce e alle tecnologie emergenti, spesso realizzato attraverso la promulgazione di leggi atte a stabilire standard di sicurezza.

Le Strategie Nazionali di Cybersecurity sono un altro elemento fondamentale, con molti paesi che sviluppano e aggiornano regolarmente queste strategie per affrontare le minacce cibernetiche e migliorare la resilienza a livello nazionale, delineando obiettivi a lungo termine, priorità e iniziative.

La Collaborazione Internazionale rappresenta un aspetto chiave, coinvolgendo gli enti governativi in collaborazioni su scala internazionale per affrontare minacce cibernetiche che superano i confini nazionali. La partecipazione a iniziative regionali e globali è fondamentale per la condivisione di informazioni, lo sviluppo di standard e la cooperazione contro le minacce transfrontaliere.

Alcuni paesi istituiscono Centri di Competenza e Ricerca specializzati in cybersecurity, che svolgono un ruolo fondamentale nella ricerca, nell'innovazione e nell'offerta di formazione avanzata nel campo della sicurezza informatica.

Il Monitoraggio Continuo e l'Analisi delle Minacce sono attività a cui gli enti governativi dedicano impegno costante per identificare e rispondere tempestivamente alle nuove minacce, coinvolgendo spesso la raccolta di intelligence cibernetica.

Il Supporto Tecnico alle Istituzioni Pubbliche è un'altra componente essenziale, con gli enti governativi che forniscono consulenza sulla configurazione di sicurezza e rispondono agli

[16]https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza

incidenti per migliorare la postura di sicurezza cibernetica di istituzioni pubbliche, aziende e altri attori critici.

Inoltre, gli enti governativi hanno un ruolo significativo nella Formazione e Sensibilizzazione sulla sicurezza informatica, contribuendo a migliorare la consapevolezza degli utenti e a promuovere comportamenti sicuri online.

Le Esercitazioni e Simulazioni di incidenti cibernetici rappresentano un ulteriore passo verso la preparazione in caso di situazioni di emergenza, consentendo di testare la capacità di risposta e identificare eventuali aree di miglioramento.

L'Adattamento alle Nuove Tecnologie è una sfida costante per gli enti governativi, che devono tener conto delle implicazioni sulla sicurezza cibernetica derivanti dall'emergere di nuove tecnologie come l'Internet delle cose (IoT), l'intelligenza artificiale e la blockchain.

In definitiva, l'evoluzione degli enti governativi nel campo della cybersecurity è un processo continuo e dinamico, spinto dalla rapida evoluzione delle minacce e delle tecnologie. La capacità di adattarsi e innovare risulta fondamentale per mantenere un ambiente digitale sicuro e affidabile.

2.6 La Cybersecurity ed il PNRR

Il Piano Nazionale di Ripresa e Resilienza (PNRR) è uno strumento strategico adottato dal governo italiano per affrontare le sfide derivanti dalla pandemia e promuovere la crescita sostenibile. Nel contesto della sicurezza informatica, il PNRR prevede significativi investimenti nella digitalizzazione, con un forte focus sulla sicurezza informatica per migliorare l'efficienza dei servizi pubblici.

La resilienza digitale è uno degli assi tematici del PNRR, con investimenti specifici mirati a potenziare la sicurezza informatica. L'innovazione tecnologica è promossa, ma con un'attenzione particolare alla protezione dei dati e servizi digitali. Le infrastrutture critiche, digitali comprese, sono parte integrante della resilienza del paese, con il PNRR che potrebbe prevedere investimenti per garantirne la sicurezza ed integrità. La formazione e lo sviluppo di competenze digitali e di sicurezza informatica potrebbero essere ulteriori componenti dei progetti formativi sostenuti dal PNRR.

2.7 Come la Cybersecurity ha influito positivamente o negativamente nelle organizzazioni interne delle PA

La cybersecurity rappresenta un elemento di grande rilevanza all'interno delle organizzazioni delle Pubbliche Amministrazioni (PA), generando un impatto con conseguenze sia positive che sfidanti. Esaminiamo dettagliatamente gli effetti della cybersecurity sulle PA, distinguendo tra impatti positivi e negativi.

Tra gli impatti positivi della cybersecurity, si evidenziano diverse dimensioni cruciali. Innanzitutto, la protezione dei dati sensibili è uno degli aspetti principali. La cybersecurity svolge un ruolo fondamentale nel garantire la riservatezza, l'integrità e la disponibilità delle informazioni sensibili gestite dalle PA, preservandone la garanzia in modo completo. Inoltre, la implementazione di misure di sicurezza informatica contribuisce notevolmente alla continuità dei servizi offerti dalle PA, assicurando che tali servizi non siano compromessi anche in presenza di minacce o attacchi cibernetici.

La fiducia dei cittadini rappresenta un altro beneficio importante. Una postura solida in materia di sicurezza influisce positivamente sulla percezione che i cittadini hanno nei confronti delle PA, trasmettendo l'immagine di un'organizzazione responsabile e attenta alla protezione dei dati personali dei cittadini. Inoltre, la conformità normativa è garantita attraverso l'adozione di adeguate misure, riducendo così il rischio di sanzioni legali e assicurando la conformità alle normative e ai requisiti di sicurezza vigenti.

Altro elemento chiave è la gestione delle identità e degli accessi, che viene ottimizzata attraverso sistemi appositi. Essi migliorano la sicurezza, garantendo che solo utenti autorizzati abbiano accesso a risorse e dati specifici. Inoltre, la prevenzione delle frodi è un obiettivo raggiungibile grazie alle misure di sicurezza che proteggono le transazioni finanziarie e riducono il rischio di frodi all'interno delle PA.

La cybersecurity agevola anche la collaborazione protetta ra enti pubblici e privati, facilitando lo scambio di informazioni sensibili in modo protetto.

D'altra parte, gli impatti negativi della cybersecurity meritano attenzione. La continua evoluzione delle minacce cibernetiche rappresenta una sfida costante. Gli attori malevoli si adattano continuamente, presentando nuove minacce e mettendo a dura prova la capacità delle PA di difendersi.

I costi operativi associati all'implementazione e alla gestione delle soluzioni di sicurezza possono essere significativi. Questi includono investimenti in tecnologie, formazione del personale e monitoraggio continuo, aggiungendo un carico finanziario alle PA.

L'aumento della complessità operativa è un altro aspetto negativo, richiedendo una gestione e una manutenzione più attente delle infrastrutture e delle procedure di salvaguardia. Il rischio di incidenti di sicurezza, nonostante le misure preventive adottate, rimane una realtà. Gli attacchi riusciti possono causare interruzioni dei servizi e compromettere la reputazione delle PA.

Inoltre, la cybersecurity richiede un adattamento continuo per affrontare le nuove minacce. Questo adattamento può comportare la necessità di aggiornare regolarmente politiche, procedure e tecnologie.

La questione della privacy e del trattamento etico dei dati rappresenta un'altra sfida importante per le PA nel contesto digitale, richiedendo una gestione attenta e risposte efficaci alle preoccupazioni dei cittadini.

In conclusione, la cybersecurity gioca un ruolo cruciale nel garantire la sicurezza e l'affidabilità negli enti pubblici. Pur apportando benefici sostanziali, è essenziale riconoscere e affrontare le sfide emergenti per mantenere elevati standard di sicurezza e rispondere alle mutevoli minacce cibernetiche.

2.8 Come viene percepita la Cybersecurity dagli operatori della PA

La percezione della sicurezza informatica tra gli operatori della pubblica amministrazione italiana è soggetta a molteplici influenze. Diversi fattori giocano un ruolo significativo, modellando la visione dei professionisti nei confronti della cybersecurity.

Innanzitutto, la consapevolezza delle minacce cibernetiche e della necessità di proteggere le informazioni sensibili emerge come un elemento chiave. Gli operatori che comprendono appieno tali minacce tendono a sviluppare una percezione positiva della sicurezza informatica.

La formazione dedicata ad essa gioca un ruolo fondamentale nel plasmare la percezione degli operatori. Essa fornisce una comprensione approfondita delle best practices e delle minacce, contribuendo a posizionare la cybersecurity come una priorità.

La presenza di una cultura della sicurezza all'interno dell'organizzazione rappresenta un ulteriore elemento influente. Se le linee guida sono chiare e pratiche sicure sono adottate in

modo diffuso, gli operatori tendono a percepire la cybersecurity come un aspetto essenziale delle loro attività quotidiane.

Le esperienze precedenti con incidenti di sicurezza o attacchi cibernetici possono amplificare l'urgenza e la criticità della percezione della cybersecurity. Gli operatori che hanno vissuto direttamente tali situazioni sono più propensi a riconoscere l'importanza delle misure di sicurezza.

La disponibilità di supporto e risorse per affrontare questioni di sicurezza è un altro elemento determinante. Gli operatori sono più inclini a percepire la cybersecurity come gestibile se sono presenti risorse adeguate.

Il coinvolgimento del personale nelle decisioni relative alla sicurezza e nelle attività formative contribuisce a migliorare la comprensione e l'accettazione delle misure di cybersecurity.

Comunicazioni efficaci da parte delle autorità sulla sicurezza informatica possono avere un impatto positivo sulla percezione degli operatori.

L'impatto sulle attività lavorative è un aspetto rilevante: se le misure di sicurezza sono integrate senza eccessive interferenze, gli operatori sono più propensi a vederle positivamente.

Infine, il riconoscimento delle minacce emergenti gioca un ruolo fondamentale. La percezione della cybersecurity può migliorare se gli operatori riconoscono le nuove minacce cibernetiche e comprendono la necessità di adottare misure aggiuntive per affrontarle.

In conclusione, è essenziale sottolineare che la sicurezza informatica è una questione che va oltre la tecnologia, coinvolgendo aspetti culturali e comportamentali. La promozione della consapevolezza, la formazione continua e il coinvolgimento attivo degli operatori contribuiscono a una migliore percezione e attuazione della cybersecurity nella pubblica amministrazione italiana.

2.9 Vantaggi e criticità

La presenza di una solida infrastruttura di cybersecurity nella Pubblica Amministrazione Italiana comporta diversi vantaggi strategici.

In primo luogo, assicura la protezione dei dati sensibili, salvaguardando la loro integrità, riservatezza e disponibilità. Queste caratteristiche costituiscono una base fondamentale per la gestione affidabile delle informazioni confidenziali.

Le misure di sicurezza informatica contribuiscono alla continuità dei servizi pubblici, riducendo il rischio di interruzioni dovute a potenziali attacchi cibernetici. Questo impatto diretto sulla continuità delle operazioni favorisce un'efficace erogazione dei servizi pubblici.

Inoltre, la fiducia dei cittadini nelle istituzioni pubbliche è incrementata attraverso la presenza di un robusto sistema di sicurezza cibernetica. Tale impegno concreto per la protezione dei dati e della privacy dei cittadini favorisce un rapporto di fiducia reciproca.

La conformità alle normative e regolamenti sulla protezione dei dati costituisce un altro beneficio. La cybersecurity facilita l'aderenza alle leggi in vigore, evitando sanzioni legali e promuovendo la trasparenza nelle operazioni amministrative.

L'implementazione di soluzioni di gestione delle identità e degli accessi offre ulteriori vantaggi, consentendo alle Pubbliche Amministrazioni di controllare in modo efficace chi ha accesso a quali risorse. Questo non solo migliora la sicurezza, ma semplifica anche la gestione degli accessi alle informazioni sensibili.

La prevenzione delle frodi e manipolazioni di informazioni finanziarie costituisce un altro punto a favore. Le misure di sicurezza contribuiscono a garantire l'integrità delle transazioni e la protezione dei fondi pubblici.

La facilitazione della collaborazione sicura tra entità pubbliche e private è un risultato diretto di un ambiente cibernetico sicuro. Questo favorisce lo scambio di informazioni in modo protetto e contribuisce a sinergie più efficienti.

Tuttavia, è fondamentale considerare anche gli svantaggi connessi alla cybersecurity. I costi operativi significativi, inclusi investimenti in tecnologie, formazione del personale e monitoraggio continuo, rappresentano una sfida finanziaria.

L'introduzione di soluzioni di sicurezza può introdurre complessità operativa, richiedendo una gestione e manutenzione più attenta dei sistemi. Questo può comportare una curva di apprendimento significativa per il personale coinvolto.

La resistenza al cambiamento tra gli operatori è un altro ostacolo potenziale. Nuove procedure o tecnologie di sicurezza possono essere percepite come vincoli o ostacoli alle attività quotidiane, generando resistenza.

Alcune misure di sicurezza più stringenti possono avere un impatto sulle prestazioni dei sistemi, rallentando l'esecuzione di alcune operazioni critiche.

La necessità di adattamento continuo per affrontare nuove minacce rappresenta un altro svantaggio. Questo richiede aggiornamenti regolari delle politiche, procedure e tecnologie, implicando sforzi costanti.

Inoltre, la generazione di falsi positivi da sistemi di sicurezza avanzati può causare frustrazione tra gli operatori, indicando erroneamente attività legittime come minacce.

La complessità della formazione degli operatori sulla sicurezza informatica è un'altra sfida, richiedendo sforzi costanti per garantire che il personale sia adeguatamente informato e preparato.

Infine, alcune misure di sicurezza possono sollevare questioni sulla privacy, specialmente se coinvolgono la raccolta e l'analisi di dati personali.

In sintesi, mentre la cybersecurity offre notevoli vantaggi nella protezione dei dati e nella fiducia dei cittadini, è cruciale affrontare con attenzione gli svantaggi associati, bilanciando la sicurezza con l'efficacia delle operazioni quotidiane.

3. CAPITOLO 3 – La Cybersecurity ed i conflitti armati

3.1 Quanto influisce la Cybersecurity in un conflitto armato

La percezione del rischio digitale è fortemente radicato nella condizione sociale. Nel contesto attuale non si può non tener conto di quanto i conflitti armati abbiano influito sul sentire comune.

In un conflitto armato uno degli aspetti più evidenti è la guerra cibernetica, in cui le nazioni coinvolte nel conflitto cercano di compromettere i sistemi informatici, le reti di comunicazione e le infrastrutture critiche del nemico. Attacchi mirati possono interrompere servizi essenziali, danneggiare infrastrutture cruciali o sottrarre informazioni strategiche.

Il ruolo dello spionaggio e della raccolta di informazioni è altrettanto significativo. Le attività di spionaggio cibernetico vengono impiegate per ottenere informazioni sensibili sulle forze nemiche, le loro strategie e le vulnerabilità del sistema di difesa.

La manipolazione delle comunicazioni rappresenta un altro fronte, in cui gli attaccanti cercano di diffondere disinformazione, influenzare l'opinione pubblica o seminare confusione tra le forze nemiche. Questo può coinvolgere attacchi di disinformazione online o manipolazione delle comunicazioni tra le forze militari.

Le infrastrutture critiche sono sempre più digitalizzate, e attacchi cibernetici a reti energetiche, sistemi di approvvigionamento idrico e reti di trasporto possono causare danni significativi, influenzando direttamente la capacità di un paese di sostenere operazioni militari.

L'utilizzo di “malware” avanzato è un elemento importante in un conflitto cibernetico, in grado di danneggiare sistemi informatici, rubare informazioni sensibili o compromettere le operazioni militari.

La protezione delle informazioni sensibili è una priorità assoluta, con la crittografia, le misure di autenticazione e le reti sicure che diventano elementi cruciali per garantire riservatezza e integrità delle informazioni.

La difesa cibernetica è imperativa per le forze armate, che devono sviluppare capacità per contrastare attivamente gli attacchi avversari, sorvegliando costantemente le reti, rilevando precocemente attacchi e rispondendo tempestivamente agli incidenti di sicurezza.

Inoltre, la diplomazia e le norme internazionali giocano un ruolo essenziale. Le nazioni cercano di stabilire regole e accordi che regolamentino il comportamento nello spazio

cibernetico, mirando a mitigare il rischio di escalation durante i conflitti.

In sintesi, la cybersecurity assume un ruolo crescente e cruciale in contesti di conflitto armato, poiché le operazioni militari diventano sempre più dipendenti da tecnologie digitali. La capacità di proteggere informazioni e infrastrutture critiche, oltre a difendersi da attacchi avversari, è diventata una componente essenziale della preparazione militare e della sicurezza nazionale.

3.2 La Cybersecurity e la guerra tra RUSSIA ed UCRAINA[17]

Nel momento in cui la Russia ha invaso l'Ucraina il 24 febbraio 2022, il ruolo dei cyber attacchi nel contesto di un'invasione su vasta scala era incerto. La Russia aveva già condotto cyber attacchi contro l'Ucraina durante l'occupazione della Crimea nel 2014, rendendo probabile che avrebbe impiegato gli stessi strumenti in questa nuova situazione, specialmente dopo gli attacchi alla rete elettrica ucraina e la diffusione del worm NotPetya.

Il Servizio delle Comunicazioni Speciali e della Protezione dell'Informazione dello Stato Ucraino (SSSCIP) ha riferito che dall'inizio della guerra, il Paese è stato oggetto di 1.123 attacchi, di cui il 36,9% ha colpito enti associati al governo o alla difesa, il 23,7% ha comportato l'installazione di codice malevolo e il 27,2% ha coinvolto la raccolta di informazioni.

La componente "cyber" della guerra ha avuto inizio quasi 24 ore prima dell'invasione terrestre e può essere suddivisa in quattro categorie principali: attacchi distruttivi, disinformazione, hacktivismo e spionaggio.

Da gennaio 2022, attaccanti russi e pro-russi hanno diffuso malware mirato a cancellare i contenuti o impedire il funzionamento dei sistemi, con un focus su service provider, infrastrutture critiche ed enti pubblici in Ucraina. Tuttavia, il governo ucraino, spostando le sue funzioni online su un'infrastruttura cloud, è riuscito a mantenere operativi i servizi.

La Russia ha utilizzato la disinformazione come arma per raggiungere obiettivi politici, cercando di influenzare l'opinione pubblica in Ucraina e nel resto del mondo. Sono state tentate operazioni via SMS e sui social media, ma l'Ucraina, sempre più patriottica, ha

[17]https://www.cybersecurity360.it/cultura-cyber/sei-mesi-dopo-il-ruolo-dei-cyberattacchi-nella-guerra-ucraina/

resistito a tali tentativi. La Russia ha cercato di influenzare Paesi non allineati per ottenere supporto.

Dopo l'invasione, gli attacchi ransomware hanno registrato un calo.

Hacktivisti di entrambi i fronti hanno compiuto attacchi non sofisticati come il deturpamento di siti web e attacchi DDoS.

Attacchi spionistici, più nascosti e difficili da eccepire, sono stati diretti non solo contro l'Ucraina ma anche contro Stati Uniti, Unione Europea e membri della NATO.

In conclusione, la guerra in corso in Ucraina ha sottolineato l'importanza della cybersecurity e dei cyber attacchi. Le prime fasi del conflitto si sono concentrate su destabilizzazione, distruzione e disturbo, ma con la prolungata resistenza ucraina, il focus è passato allo spionaggio e alla disinformazione. Con l'evoluzione, soprattutto nel periodo invernale e il controllo russo sulle forniture energetiche europee, potrebbe portare a nuove sfide e cambiamenti nei cyber attacchi. Tuttavia, è improbabile che essi siano il fattore decisivo in questo conflitto, con una difesa solida che rimane una soluzione cruciale.

3.3 Le conseguenze in termini di cybersecurity in Italia soprattutto per le PA a causa della guerra RUSSIA/UCRAINA[18]

Roberto Baldoni, direttore generale dell'Agenzia per la Cybersicurezza nazionale, ha dichiarato durante un evento di 'Adnkronos Live' che la guerra cyber ha avuto inizio prima dell'invasione russa in Ucraina. Ha evidenziato tre significative ondate di attacchi cibernetici nel quadrante ucraino il 14 gennaio, il 14 febbraio e il 24 febbraio.

A metà febbraio, il CSIRT Italia ha già segnalato possibili impatti collaterali sulle infrastrutture ICT connesse al cyberspazio ucraino. Questi rischi derivano dalla natura interconnessa della rete Internet, che consente a azioni malevole dirette a una parte di essa di estendersi ad infrastrutture contigue. Il pericolo di attacchi cyber diretti all'Italia è cresciuto, con avvisi da parte del CSIRT riguardo ad attacchi informatici previsti dalla Russia e da Paesi orientali, con particolare attenzione anche all'Italia.

Il presidente degli Stati Uniti, Joe Biden, ha richiamato l'attenzione dei CEO delle principali aziende statunitensi sui potenziali attacchi informatici della Russia. Ha sottolineato

[18]https://www.agendadigitale.eu/sicurezza/conflitto-russo-ucraino-i-futuri-rischi-cyber-per-litalia-e-i-paesi-alleati/

il timore di attacchi in risposta alle ingenti sanzioni economiche inflitte alla Russia per la guerra in Ucraina.

Nonostante le offensive siano principalmente indirizzate all'Ucraina, inclusi quelli al governo ucraino e a un sistema satellitare chiamato Viasat, il Pentagono e le agenzie di intelligence statunitensi temono che le vulnerabilità esposte possano essere sfruttate per colpire le infrastrutture critiche americane, come società finanziarie, oleodotti e reti elettriche.

Il procuratore generale Merrick B. Garland ha dichiarato che l'FBI ha rimosso un malware dalle reti di computer globali, presumibilmente creato per formare una "botnet" controllata dalla GRU russa. Anche se il malware è stato interrotto prima di essere utilizzato, l'azione dimostra la volontà di disarmare potenziali minacce.

Le PA e le aziende statunitensi temono attacchi simili alle infrastrutture critiche, e la comunità elettrica cooperativa negli USA, per esempio, ha stimato necessari $50.000 per potenziare la sicurezza informatica.

Negli Stati Uniti, il senatore Gary Peters ha introdotto il Cybersecurity Act, richiedendo alle aziende coinvolte nelle infrastrutture critiche di segnalare ciberattacchi e pagamenti di ransomware entro 72 ore. La Casa Bianca ha presentato misure fondamentali per rafforzare la sicurezza informatica, sottolineando l'importanza dell'informazione e della formazione del personale.

In Italia, CLUSIT e CSIRT Italia hanno fornito linee guida per mitigare i rischi della cyberwar, tra cui la riduzione della superficie d'attacco, la revisione dei controlli di accesso e l'organizzazione di scenari di crisi. Baldoni, direttore dell'Agenzia per la Cybersicurezza Nazionale, anticipa una Strategia Nazionale di Cybersicurezza con 85 obiettivi entro il 2026.

In conclusione, mentre l'Italia recupera terreno in materia di cybersecurity, Baldoni sottolinea la necessità di una politica industriale comune nel digitale, puntando alla diversificazione delle aziende entro il suolo europeo per garantire la sovranità tecnologica.

3.4 Alcuni esempi di Cyber Attacchi durante il periodo del conflitto RUSSIA/UCRAINA[19]

Tra gli attacchi attribuiti a una matrice russa, si evidenziano le attività malevole che hanno preso di mira i siti governativi ucraini. A metà gennaio 2022, questi siti sono stati resi

[19]https://www.cybersecurity360.it/nuove-minacce/guerra-russia-ucraina-si-puo-parlare-di-cyberwar-il-punto-a-un-anno-dallinizio-del-conflitto/

inaccessibili per alcune ore, accompagnati da messaggi intimidatori indirizzati alla popolazione, invitando a "avere paura" e a "prepararsi al peggio".

Ulteriori esempi includono gli attacchi alle banche nazionali ucraine, che hanno ostacolato il prelievo di denaro da parte della popolazione, e quello a Viasat, l'azienda che fornisce servizi internet via satellite ai militari ucraini. Quest'ultimo è avvenuto nelle prime fasi dell'invasione russa il 24 febbraio 2022.

Dopo le fasi iniziali, gli strumenti cibernetici sono stati spesso utilizzati in concomitanza con gli attacchi tradizionali. I wipers, malware progettati per cancellare dati, sono stati ampiamente impiegati, come confermato anche nella Relazione annuale sulla politica dell'informazione per la sicurezza dei servizi segreti al Parlamento. Inoltre, gli attacchi DDoS (Distributed Denial of Services), che sovraccaricano un sito web rendendolo inaccessibile, sono stati utilizzati massicciamente. Questi trend non sono limitati all'Ucraina, ma si riflettono anche in nazioni alleate come l'Italia.

Analizzando le conseguenze della guerra ibrida in Italia, emerge che gli allarmi relativi ad attacchi cibernetici sono stati frequenti. Tuttavia, approfondendo le informazioni pubbliche disponibili, si nota che la maggior parte di essi è costituita da attacchi DDoS, come quelli ai siti web della Polizia, del Senato, e del Ministero della Difesa a maggio 2022. Attacchi più recenti hanno coinvolto i siti web dell'Arma dei Carabinieri e del Ministero degli Esteri, spesso correlati a prese di posizione pro-Ucraina da parte del governo italiano, come l'approvazione di pacchetti di aiuti.

Questi eventi dimostrano che, nonostante l'Italia sia stata coinvolta principalmente in attacchi di basso profilo, l'uso di strumenti cibernetici rimane una componente significativa delle operazioni ibride e delle risposte a eventi geopolitici.

4. CAPITOLO 4 – Survey/Questionario

L'obiettivo principale della mia ricerca consisteva nell'esaminare la percezione della digitalizzazione e della Cybersecurity, in particolare all'interno della Pubblica Amministrazione. Vivendo in prima persona questi temi in qualità di tecnico informatico, ho deciso di sviluppare un questionario specifico da distribuire principalmente tra i dipendenti dell'Azienda Ospedaliero Universitaria di Alessandria, dove sono impiegato. Il questionario è stato anche pubblicizzato esternamente all'AOU di Alessandria per coinvolgere membri esterni da analizzare.

La scelta di focalizzarsi sulla pubblica amministrazione e sul settore sanitario è motivata da una ragione precisa. Recentemente, le amministrazioni pubbliche nel campo della sanità sono state particolarmente colpite da attacchi informatici. Queste istituzioni hanno dovuto affrontare rapidamente tali emergenze sia a livello sanitario che amministrativo e organizzativo. Le Direzioni Sanitarie e Amministrative, insieme alle strutture coinvolte, hanno dovuto ristrutturarsi completamente per fornire un solido supporto ai dipendenti e, di conseguenza, ai cittadini.

Per proteggere un'azienda da attacchi esterni, è essenziale completare o quasi tutti i processi di digitalizzazione e informatizzazione. Fortunatamente, grazie alla collaborazione e alla comprensione di tutti, siamo riusciti a superare queste criticità acquisendo preziosa esperienza e spesso rafforzando il senso di appartenenza alla struttura.

Attraverso il questionario, ho ritenuto utile analizzare i risultati di questa situazione soprattutto all'interno dell'Azienda dove lavoro.

4.1 Le fasi della Survey

Ho iniziato con la fase di "Formulazione delle ipotesi di ricerca", dove ho elaborato diverse ipotesi riguardanti la digitalizzazione e la cybersecurity. Ho cercato di determinare se la terminologia ha avuto un impatto positivo o negativo, se ha causato danni o ha portato vantaggi, e se i dipendenti pubblici percepiscono positivamente la digitalizzazione e la cybersecurity.

Successivamente, ho proceduto con la "Definizione delle unità di analisi/casi studio (campionamento) - Definizione delle variabili da rilevare (operativizzazione)". Ho selezionato principalmente i dipendenti dell'Azienda Ospedaliero Universitaria di Alessandria come campione e ho identificato le variabili principali legate alla digitalizzazione e alla Cybersecurity da esaminare.

Inoltre mi sono concentrato sulla creazione del questionario. Ho condotto ricerche approfondite consultando diversi siti, articoli e studi correlati. Le domande sono state annotate su un foglio di calcolo per consentire una facile revisione, aggiunta, rimozione e correzione. Successivamente, le domande sono state trasferite su LimeSurvey, dove sono state inserite anche alcune condizioni logiche per migliorare l'esperienza degli intervistati. Infine, sono stati effettuati test con colleghi e il mio relatore per apportare le correzioni finali.

La fase di somministrazione è stata caratterizzata dalla creazione di un sito web dedicato www.questionari.eu, sul quale è stato ospitato il software LimeSurvey. Il link al questionario è stato pubblicato sulla intranet aziendale previa autorizzazione. Gli utenti hanno quindi potuto compilare il questionario utilizzando l'interfaccia di LimeSurvey. Durante questa fase, ho monitorato attentamente l'input dei dati per individuare eventuali problemi da parte degli utenti.

Una volta scaduto il periodo di compilazione del questionario, ho avviato le fasi di elaborazione, analisi ed interpretazione dei risultati. Utilizzando le funzionalità di esportazione di LimeSurvey, ho trasferito i dati in un formato compatibile con STATA per condurre un'analisi dettagliata. I risultati sono stati poi commentati e arricchiti con grafici generati utilizzando software di automazione per ufficio.

4.2 Prodotti utilizzati

Per la creazione del questionario, ho registrato un dominio dedicato "questionari.eu" tramite il service provider ARUBA. Successivamente, ho installato LimeSurvey, un software "Open Source" consolidato nel tempo e supportato dalla community, che consente di creare sondaggi con varie tipologie di domande, anche interdipendenti. Esse possono essere organizzate in gruppi e modificate facilmente tramite un'interfaccia grafica intuitiva. L'uso di template in HTML integrati consente un alto grado di personalizzazione grafica. Una volta creati, i sondaggi devono essere attivati e possono essere resi pubblici o accessibili tramite

password (token) uniche per ogni partecipante. I risultati raccolti possono essere anonimi o associati ai partecipanti, a seconda della configurazione del sondaggio.

Per garantire la privacy, ho optato per la creazione di un questionario anonimo senza registrare l'indirizzo IP o il timestamp di ogni compilazione.

L'utilizzo di LimeSurvey ha permesso anche di attivare un modulo per l'estrazione dei dati in un formato compatibile con il software STATA, facilitando così l'analisi dei dati. STATA è un pacchetto software statistico generico utilizzato per la manipolazione dei dati, la visualizzazione, le statistiche e l'automazione della segnalazione. È ampiamente utilizzato in vari campi di ricerca, tra cui economia, sociologia, scienze politiche, biomedicina ed epidemiologia.

STATA è stato sviluppato inizialmente dal Computing Resource Center in California, con la prima versione rilasciata nel 1985. Nel 1993, la società si è trasferita a College Station, TX, diventando Stata Corporation, ora nota come StataCorp. Negli anni successivi, sono state rilasciate nuove versioni con miglioramenti, inclusi un nuovo sistema grafico e finestre di dialogo per tutti i comandi. La versione più recente è Stata 17, rilasciata nell'aprile 2021.

In aggiunta a STATA, ho utilizzato software di automazione per ufficio soprattutto per la creazione delle tabelle.

4.3 Campione utilizzato

Come precedentemente spiegato, il campione utilizzato per l'analisi è stato ricavato dai risultati di un questionario specifico reso disponibile principalmente agli operatori della Città della Salute e della Scienza di Torino. I dati esportati dal software LimeSurvey sono stati importati in STATA per le elaborazioni successive.

Innanzitutto, è stata esaminata ogni singola variabile. Successivamente, sono state creati prospetti di contingenza apposite da analizzare e confrontare. Queste tabelle sono state costruite basandosi su quattro variabili indipendenti: genere, fasce d'età, aree funzionali, e sono state comparate con tutte le altre 27 variabili rimanenti. Le tabelle di contingenza sono

state analizzate per evidenziare i dati statistici rilevanti. Da questa analisi sono emerse e sono state riunite 27 tabelle, le quali evidenziano, nelle righe, tre variabili indipendenti cruciali. In ogni tabella, è indicato il valore di Chi2.

Cominciamo ora a discutere le variabili significative.

4.3.1. Rapporto con la digitalizzazione nella Pubblica Amministrazione in qualità di CITTADINO/UTENTE

Tab. 1: Ha familiarità con il concetto di digitalizzazione nella Pubblica Amministrazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere *	Maschi	14,88	39,67	45,45	100,00
	Femmine	17,32	55,84	26,84	100,00
Classi di età*	20-40 anni	17,89	43,16	38,95	100,00
	41-49 anni	15.12	44,19	40,70	100,00
	50-57 anni	12,62	60,19	27,18	100,00
	58-69 anni	26,25	52,50	21,25	100,00
Area Funzionale*	Area Tecnica	18,87	33,96	47,17	100,00
	Area Amministrativa	9,92	53,72	36,36	100,00
	Area Sanitaria	22,11	52,63	25,26	100,00

* P<=0,05

Nella tabella 1 notiamo che i più giovani hanno più familiarità con il concetto di digitalizzazione. La fascia più anziana ha correttamente meno familiarità con il 26,25%. I maschi superano di molto le femmine con 45,45% contro 26,84%. L'Area funzionale con meno familiarità è quella sanitaria.

Tab. 2: Quanto ritiene di essere informato/a riguardo ai processi di digitalizzazione attuati dalla Pubblica Amministrazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	33,06	44,63	22,31	100,00
	Femmine	32,90	50,22	16,88	100,00
Classi di età	20-40 anni	29,47	47,37	23,16	100,00
	41-49 anni	36,05	44,19	19,77	100,00
	50-57 anni	30,10	55,34	14,56	100,00
	58-69 anni	41,25	43,75	15,00	100,00
Area Funzionale*	Area Tecnica	33,96	37,74	28,30	100,00
	Area Amministrativa	23,14	57,85	19,01	100,00
	Area Sanitaria	40,53	44,74	14,74	100,00

* P<=0,05

Nella tabella 2 vediamo i maschi più informati di 6 punti circa, confronto alle femmine. Come fasce di età troviamo nuovamente le due fasce più giovani e poi quelle più anziane. Stessa cosa per le aree, l'area Sanitaria risulta la meno informata.

Tab. 3: Ritiene che la pandemia da Covid-19 abbia accelerato la digitalizzazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	11,57	33,88	54,55	100,00
	Femmine	9,52	26,84	63,64	100,00
Classi di età	20-40 anni	9,47	31,58	58,95	100,00
	41-49 anni	13,95	30,23	55,81	100,00
	50-57 anni	6,80	27,18	66,02	100,00
	58-69 anni	15,00	27,50	57,50	100,00
Area Funzionale	Area Tecnica	13,21	37,74	49,06	100,00
	Area Amministrativa	9,92	24,79	65,29	100,00
	Area Sanitaria	11,05	29,47	59,47	100,00

In tabella 3 troviamo le femmine con 63,64% che ritengono che il covid-19 abbia accelerato la digitalizzazione. Nelle fasce di età troviamo quella dai 50 ai 57 con il 66,02% e le altre tre molto vicine. L'area amministrativa è quella con la percentuale più alta confronto alle altre due.

Tab. 4: Quanto le sue aspettative, rispetto alla digitalizzazione nella Pubblica Amministrazione, sono state appagate?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	40,50	50,41	9,09	100,00
	Femmine	33,77	56,28	9,96	100,00
Classi di età	20-40 anni	40,00	45,26	14,74	100,00
	41-49 anni	39,53	52,33	8,14	100,00
	50-57 anni	32,04	62,14	5,83	100,00
	58-69 anni	37,50	52,50	10,00	100,00
Area Funzionale	Area Tecnica	45,28	50,94	3,77	100,00
	Area Amministrativa	36,36	56,20	7,44	100,00
	Area Sanitaria	35,26	52,11	12,63	100,00

In tabella 4 notiamo un po' di negatività soprattutto per i maschi più giovani dell'Area Tecnica. Negatività inaspettata soprattutto per quella fascia di età.

Tab. 5: Ritiene che la digitalizzazione abbia migliorato l'accessibilità della Pubblica Amministrazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere *	Maschi	27,27	38,02	34,71	100,00
	Femmine	23,38	50,65	25,97	100,00
Classi di età*	20-40 anni	17,89	41,05	41.05	100,00
	41-49 anni	33,72	41,86	24,42	100,00
	50-57 anni	24,27	52,43	23,30	100,00
	58-69 anni	28,75	45,60	28,57	100,00
Area Funzionale	Area Tecnica	20,75	47,17	32,08	100,00
	Area Amministrativa	29,75	47,11	23,14	100,00
	Area Sanitaria	24,74	44,21	31,05	100,00

* P<=0,05

In tabella 5 notiamo che i giovani maschi dell'Area Tecnica pensano che la digitalizzazione abbia migliorato l'accessibilità della Pubblica Amministrazione. Questa risposta è in linea con le aspettative tuttavia diventa un caso paragonando queste percentuali a quelle della domanda precedente in tabella 4.

Tab. 6: Ha riscontrato benefici personali nell'utilizzo dei servizi digitali rispetto a quelli tradizionali?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere *	Maschi	17,36	30,58	52,07	100,00
	Femmine	23,81	41,56	34,63	100,00
Classi di età*	20-40 anni	13,68	29,47	56,84	100,00
	41-49 anni	25,58	36,05	38,37	100,00
	50-57 anni	23,30	44,66	32,04	100,00
	58-69 anni	28,75	40,00	31,25	100,00
Area Funzionale*	Area Tecnica	15,09	37,74	47,17	100,00
	Area Amministrativa	22,31	46,28	31,40	100,00
	Area Sanitaria	24,74	32,11	43,16	100,00

* P<=0,05

Anche in tabella 6 notiamo che maschi più giovani dell'Area Tecnica hanno riscontrato benefici benefici personali nell'utilizzo dei servizi digitali rispetto a quelli tradizionali. Le femmine della fascia più anziana dell'Area Sanitaria hanno riscontrato meno benefici personali.

Tab. 7: Secondo lei, la digitalizzazione ha contribuito a ridurre la burocrazia nella Pubblica Amministrazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	50,41	29,75	19,83	100,00
	Femmine	49,35	36,36	14,29	100,00
Classi di età	20-40 anni	42,11	38,95	18,95	100,00
	41-49 anni	52,33	34,88	12,79	100,00
	50-57 anni	47,57	33,01	19,42	100,00
	58-69 anni	61,25	28,75	10,00	100,00
Area Funzionale	Area Tecnica	52,83	37,74	9,43	100,00
	Area Amministrativa	54,55	30,58	14,88	100,00
	Area Sanitaria	46,84	35,26	17,89	100,00

Sia i maschi che le femmine della fascia più anziana dell'area Amministrativa pensano che la digitalizzazione non abbia ridotto la burocrazia.

Tab. 8: Incontra spesso difficoltà nell'utilizzo dei servizi della Pubblica Amministrazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	48,76	28,10	23,14	100,00
	Femmine	36,80	46,75	16,45	100,00
Classi di età	20-40 anni	51,58	31,58	16,84	100,00
	41-49 anni	39,53	41,86	18,60	100,00
	50-57 anni	38,83	44,66	16,50	100,00
	58-69 anni	31,25	45,00	23,75	100,00
Area Funzionale	Area Tecnica	49,06	33,96	16,98	100,00
	Area Amministrativa	35,54	42,98	21,49	100,00
	Area Sanitaria	41,58	41,05	17,37	100,00

* P<=0,05

In tabella 8 notiamo che i maschi più anziani dell'Area Amministrativa ha incontrato più difficoltà. I maschi più giovani dell'Area Tecnica hanno incontrato meno difficoltà.

Tab. 9: Secondo lei, le informazioni in merito ai servizi di digitalizzazione della Pubblica Amministrazione sono state sufficienti?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	57,85	36,36	5,79	100,00
	Femmine	54,98	41,13	3,90	100,00
Classi di età	20-40 anni	54,74	37,89	7,37	100,00
	41-49 anni	53,49	43,02	3,49	100,00
	50-57 anni	55,34	39,81	4,85	100,00
	58-69 anni	63,75	35,00	1,25	100,00
Area Funzionale	Area Tecnica	58,49	33,96	7,55	100,00
	Area Amministrativa	57,85	37,19	4,96	100,00
	Area Sanitaria	55,26	41,58	3,16	100,00

In tabella 9 notiamo che i maschi più anziani dell'Area Tecnica pensano che le informazioni della Pubblica Amministrazione non siano state sufficienti. I maschi più giovani, sempre, dell'Area Tecnica hanno la percentuale più alta di molto+moltissimo anche se nel complesso è evidenziata una negatività in merito alle informazioni sui servizi di digitalizzazione.

Tab. 10: Pensa, che la digitalizzazione della Pubblica Amministrazione penalizzi gli anziani nell'accesso, soprattutto, ai servizi sanitari?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	17,36	23,14	59,50	100,00
	Femmine	10,39	15,58	74,03	100,00
Classi di età*	20-40 anni	20,00	26,32	53,68	100,00
	41-49 anni	12,79	19,77	67,44	100,00
	50-57 anni	11,65	15,53	72,82	100,00
	58-69 anni	6,25	11,25	82,50	100,00
Area Funzionale	Area Tecnica	22,64	24,53	52,83	100,00
	Area Amministrativa	9,92	16,53	73,55	100,00
	Area Sanitaria	12,11	17,89	70,00	100,00

* P<=0,05

In tabella 10 praticamente tutti pensano che gli anziani siano penalizzati. Quelle più negative sono le femmine più anziane dell'Area Amministrativa.

Tab. 11: Quanto si sente sicuro riguardo alla protezione dei suoi dati personali quando utilizza servizi online della Pubblica Amministrazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	27,27	48,76	23,97	100,00
	Femmine	24,24	55,41	20,35	100,00
Classi di età*	20-40 anni	16,84	61,05	22,11	100,00
	41-49 anni	25,58	45,35	29,07	100,00
	50-57 anni	29,13	54,37	16,50	100,00
	58-69 anni	37,50	46,25	16,25	100,00
Area Funzionale	Area Tecnica	32,08	50,94	16,98	100,00
	Area Amministrativa	28,93	57,02	14,05	100,00
	Area Sanitaria	24,21	49,47	26,32	100,00

* P<=0,05

In tabella 11 notiamo che i maschi anziani dell'Area Tecnica si sentono meno sicuri. La fascia di età dai 41-49 è quella che si sente più sicura.

Considerazione finali

Come ci si poteva aspettare dalla percezione comune, la survey conferma che i giovani hanno più familiarità con il concetto di digitalizzazione; nello specifico evidenzia che i maschi hanno molta più familiarità con la digitalizzazione delle femmine.

Seppur la normativa e le regolamentazioni europee abbiano spinto molto nella digitalizzazione in ambito sanitario si riscontra proprio nell'area funzionale sanitaria una minor sensibilità.

Sicuramente la pandemia ha agevolato la transizione al digitale, in particolare per le donne impiegate nell'area amministrativa che, probabilmente hanno trovato beneficio dall'utilizzo dei sistemi digitali.

Se è vero che le donne spesso si rivolgono positivamente al digitale per gestire meglio la conciliazione tra lavoro e altre responsabilità, come ad esempio la cura dei figli, tuttavia, l'impatto di approccio sul gender gap non è ancora del tutto chiaro dal momento che proprio le donne sono quelle che in molti casi hanno evidenziato dalle risposte di essere meno appagate dalle evoluzioni della digitalizzazione della PA.

Tuttavia le aspettative soprattutto fra i giovani sono sicuramente molto alte (Tab 5) e purtroppo dai dati raccolti (Tab 4) non sembrano soddisfatte. Potrebbe essere di futuro interesse analizzare in quali ambiti la distanza fra l'atteso e il percepito è più significativa.

Purtroppo in generale le persone meno giovani pensano che la digitalizzazione non abbia ridotto la burocrazia, indice di un fallimento generale dell'approccio sin ora perseguito e dell'incapacità delle amministrazioni di ridurre il digital divide.

Nell'analisi delle difficoltà emerge chiaramente che i maschi operanti in area amministrativa sono molto più in difficoltà di quelli giovani in area tecnica da cui si può dedurre una carente formazione che porti ad un buon livello di conoscenza le aree che più resistono ai cambiamenti e dove il personale è nelle fasce di età più elevate.

Altro aspetto rilevante è che purtroppo i cittadini non riconoscono nelle nuove tecnologie la possibilità di trovare soluzioni che possano agevolare l'accesso alla PA da parte degli anziani. Nonostante il PNRR abbia previsto diverse misure atte a sostenere la riforma dei servizi a favore degli anziani rendendone più agevole l'accesso attraverso le nuove tecnologie, non vi sono evidenze di un percepibile miglioramento delle condizioni nel tempo.

4.3.2. Rapporto con la digitalizzazione nella Pubblica Amministrazione in qualità di LAVORATORE/LAVORATRICE

Tab. 12: A seguito del lavoro su un computer/terminale ha riscontrato fastidi/problemi di salute che prima non manifestava?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere *	Maschi	76,03	1818	5,79	100,00
	Femmine	70,13	19,05	10,82	100,00
Classi di età*	20-40 anni	76,84	9,47	13,68	100,00
	41-49 anni	74,42	19,77	5,81	100,00
	50-57 anni	69,90	22,33	7,77	100,00
	58-69 anni	62,50	25,00	12,50	100,00
Area Funzionale	Area Tecnica	75,47	15,09	9,43	100,00
	Area Amministrativa	65,29	23,14	11,57	100,00
	Area Sanitaria	73,68	17,37	8,95	100,00

* P<=0,05

Da queste risposte notiamo che le percentuali di chi ha riscontrato molti problemi di salute, sono molto basse. Le percentuali di chi ha riscontrato molti problemi di salute sono quelle delle femmine più giovani dell'Area Amministrativa.

Tab. 13: Ha riscontrato benefici personali nell'utilizzo dei servizi digitali rispetto a quelli tradizionali?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	14,05	41,32	44,63	100,00
	Femmine	24,68	42,86	32,47	100,00
Classi di età	20-40 anni	12,63	40,00	47,37	100,00
	41-49 anni	27,91	40,70	31,40	100,00
	50-57 anni	25,24	40,78	33,98	100,00
	58-69 anni	21,25	50,00	28,75	100,00
Area Funzionale	Area Tecnica	16,98	49,06	33,96	100,00
	Area Amministrativa	25,62	43,80	30,58	100,00
	Area Sanitaria	20,53	40,00	39,47	100,00

* P<=0,05

Notiamo che in tabella 13 i maschi più giovani dell'Area Sanitaria hanno riscontrato maggiori benefici personali. Chi ne ha riscontrato meno sono le Femmine tra i 50-57 anni dell'Area Amministrativa.

Tab. 14: Ha riscontrato problemi muscolo-scheletrici usando un computer/terminale?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	68,60	24,79	6,61	100,00
	Femmine	58,87	23,81	17,32	100,00
Classi di età	20-40 anni	67,37	24,21	8,42	100,00
	41-49 anni	61,63	24,42	13,95	100,00
	50-57 anni	56,31	24,27	19,42	100,00
	58-69 anni	63,75	22,50	13,75	100,00
Area Funzionale*	Area Tecnica	60,38	22,64	16,98	100,00
	Area Amministrativa	53,72	23,97	22,31	100,00
	Area Sanitaria	67,89	24,21	7,89	100,00

* P<=0,05

In tabella 14 le Femmine tra i 50 e 57 anni dell'Area Amministrativa sono quelle ad aver riscontrato più problemi anche se le percentuali nel complesso sono basse.

Tab. 15: Ha riscontrato problemi di cefalea usando un computer/terminale?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	80,99	14,88	4,13	100,00
	Femmine	65,80	22,94	11,26	100,00
Classi di età	20-40 anni	70,53	21,05	8,42	100,00
	41-49 anni	65,12	25,58	9,30	100,00
	50-57 anni	72,82	18,45	8,74	100,00
	58-69 anni	71,25	16,25	12,50	100,00
Area Funzionale	Area Tecnica	73,58	16,98	9,43	100,00
	Area Amministrativa	66,94	21,49	11,57	100,00
	Area Sanitaria	71,05	20,53	8,42	100,00

* P<=0,05

Anche qui troviamo percentuali molto basse per chi ha riscontrato problemi di cefalea. Chi ne ha riscontrato meno sono i maschi (80,99%) della fascia dai 50 ai 57 anni dell'Area Tecnica.

Tab. 16: Ha riscontrato problemi visivi usando un computer/terminale?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	61,16	28,93	9,92	100,00
	Femmine	45,89	28,14	25,97	100,00
Classi di età	20-40 anni	61,05	22,11	16,84	100,00
	41-49 anni	47,67	26,74	25,58	100,00
	50-57 anni	49,51	31,07	19,42	100,00
	58-69 anni	43,75	36,25	20,00	100,00
Area Funzionale	Area Tecnica	47,17	33,96	18,87	100,00
	Area Amministrativa	42,15	31,40	26,45	100,00
	Area Sanitaria	57,37	25,79	16,84	100,00

* P<=0,05

Chi ha riscontrato più problemi visivi sono le Femmine tra i 41 e 49 anni dell'Area Amministrativa.

I maschi più giovani dell'Area Sanitaria sono quelli ad averne riscontrato di meno.

Tab. 17: A suo parere il lavoro sul computer può rappresentare forme di dipendenza da web?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	70,25	22,31	7,44	100,00
	Femmine	66,67	24,68	8,66	100,00
Classi di età*	20-40 anni	77,89	14,74	7,37	100,00
	41-49 anni	67,44	25,58	6,98	100,00
	50-57 anni	66,99	21,36	11,65	100,00
	58-69 anni	55,00	36,25	8,75	100,00
Area Funzionale	Area Tecnica	66,04	24,53	9,43	100,00
	Area Amministrativa	65,29	25,62	9,09	100,00
	Area Sanitaria	68,95	22,63	8,42	100,00

* P<=0,05

Le percentuali di chi pensa che il lavoro sul computer possa portare forme di dipendenza da web sono molto basse. Le femmine sono quelle con le percentuali più alte ma nel complesso moderate, solo 8,66%.

Tab. 18: Quante volte nell'ultimo anno, ha dovuto utilizzare una procedura manuale per malfunzionamento dei servizi informatici della sua azienda o nazionali?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	69,42	22,31	8,26	100,00
	Femmine	75,76	19,05	5,19	100,00
Classi di età	20-40 anni	69,47	23,16	7,37	100,00
	41-49 anni	69,77	19,77	10,47	100,00
	50-57 anni	75,73	18,45	5,83	100,00
	58-69 anni	76,25	18,75	5,00	100,00
Area Funzionale*	Area Tecnica	66,04	28,30	5,66	100,00
	Area Amministrativa	83,47	9,09	7,44	100,00
	Area Sanitaria	67,89	24,74	7,37	100,00

* P<=0,05

In tabella 18 si evidenzia il fatto che le procedure manuali siano state adottate pochissime volte. I maschi tra i 41-49 anni dell'Area Amministrativa raggiungono rispettivamente l'8,26%, il 10,47% ed il 7,44%.

Tab. 19: La digitalizzazione utilizzata in Smart Working, quanto ha migliorato il suo lavoro?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	53,72	23,14	23,14	100,00
	Femmine	65,80	17,32	16,88	100,00
Classi di età	20-40 anni	50,53	23,16	26,32	100,00
	41-49 anni	69,77	13,95	16,28	100,00
	50-57 anni	60,19	20,39	19,42	100,00
	58-69 anni	67,50	20,00	12,50	100,00
Area Funzionale*	Area Tecnica	45,28	18,87	35,85	100,00
	Area Amministrativa	53,72	21,49	24,79	100,00
	Area Sanitaria	71,05	18,42	10,53	100,00

* P<=0,05

I più scettici nei confronti dello smart working sono le Femmine tra i 40 e 49 anni dell'Area Sanitaria. L'Area Tecnica è quella che ritiene che il suo lavoro sia migliorato (35,85%).

Considerazioni finali

In generale non si riscontrano impatti negativi diretti riguardanti la salute degli operatori impiegati nella transizione digitale. Dal punto di vista fisico si rilevano percentuali molto basse di personale che evidenzia lievi disturbi che potrebbero anche essere generati da un generico stress nell'affrontare una nuova condizione lavorativa.

In particolare riguardo allo Smart Working, i dati confermano che la componente tecnica di età più giovane è quella che meglio ha saputo sfruttare la potenzialità di questa innovazione, sfruttandola per migliorare le proprie condizioni di lavoro.

4.3.3. Opinioni ed esperienze sulla CYBERSECURITY

Tab. 20: Ha partecipato a eventi o corsi sulla Cybersecurity nell'Azienda Pubblica ove lavora?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	54,55	19,83	25,62	100,00
	Femmine	58,01	15,58	26,41	100,00
Classi di età	20-40 anni	66,32	11,58	22,11	100,00
	41-49 anni	58,14	20,93	20,93	100,00
	50-57 anni	50,49	19,42	30,10	100,00
	58-69 anni	47,50	20,00	32,50	100,00
Area Funzionale*	Area Tecnica	52,83	24,53	22,64	100,00
	Area Amministrativa	36,36	23,14	40,50	100,00
	Area Sanitaria	68,95	12,63	18,42	100,00

* P<=0,05

Nella tabella 20 notiamo poche differenze tra maschi e femmine per chi ha risposto molto+moltissimo, invece è forte la differenza nelle aree ove quella amministrativa raggiunge il 40,50% confronto al 22,64% di quella Tecnica ed il 18,42% di quella Sanitaria.

Nella fasce di età più giovane troviamo un 66,32% di persone che non hanno partecipato ai corsi.

Tab. 21: I progetti si sicurezza informatica vedi MFA (Multi Factor Authentication/Autenticazione a più fattori) con OTP le danno maggiore tranquillità nell'utilizzo dei sistemi digitali?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	23,14	38,02	38,84	100,00
	Femmine	19,48	61,04	19,48	100,00
Classi di età	20-40 anni	18,95	46,32	34,74	100,00
	41-49 anni	23,26	61,63	15,12	100,00
	50-57 anni	20,39	54,37	25,24	100,00
	58-69 anni	25,00	46,25	28,75	100,00
Area Funzionale*	Area Tecnica	11,32	45,28	43,40	100,00
	Area Amministrativa	23,14	52,07	24,79	100,00
	Area Sanitaria	23,68	54,21	22,11	100,00

* P<=0,05

Per i maschi, giovani, dell'Area Tecnica i progetti di sicurezza informatica vedi MFA danno maggiore tranquillità. Le femmine giovani dell'area Tecnica invece pensano che questi progetti non diano tranquillità.

Tab. 22: Quanto ha sentito parlare di attacchi informatici o di Hackers?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	4,96	34,71	60,33	100,00
	Femmine	7,36	34,20	58,44	100,00
Classi di età*	20-40 anni	13,68	28,42	57,89	100,00
	41-49 anni	6,98	33,72	59,30	100,00
	50-57 anni	1,94	34,95	63,11	100,00
	58-69 anni	3,75	38,75	57,50	100,00
Area Funzionale	Area Tecnica	7,55	28,30	64,15	100,00
	Area Amministrativa	4,96	33,06	61,98	100,00
	Area Sanitaria	7,37	35,79	56,84	100,00

* P<=0,05

In generali tutti hanno sentito parlare di attacchi informatici. Quelli che ne hanno sentito parlare di meno sono le femmine giovani dell'Area Tecnica. I maschi della fascia di età dai 50 ai 57 e dell'Area Tecnica hanno sentito parlare molto di attacchi informatici o di Hackers.

Tab. 23: Pensa che l'implementazione di nuove misure di sicurezza siano utili per il suo lavoro ed i dati che inserisce/utilizza?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	14,88	33,88	51,24	100,00
	Femmine	10,39	41,99	47,62	100,00
Classi di età	20-40 anni	9,47	36,84	53,68	100,00
	41-49 anni	17,44	40,70	41,86	100,00
	50-57 anni	7,77	43,69	48,54	100,00
	58-69 anni	18,75	32,50	48,75	100,00
Area Funzionale	Area Tecnica	11,32	37,74	50,94	100,00
	Area Amministrativa	10,74	31,40	57,85	100,00
	Area Sanitaria	14,74	43,68	41,58	100,00

* P<=0,05

I maschi giovani dell'Area Amministrativa pensano molto che l'implementazione di nuove misure di sicurezza siano utili per il loro lavoro. Non sono d'accordo sempre i maschi anziani dell'Area Sanitaria.

Tab. 24: Crede che siano adottate adeguate misure di sicurezza Informatica?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	21,49	44,63	33,88	100,00
	Femmine	10,39	57,14	32,47	100,00
Classi di età	20-40 anni	23,16	45,26	31,58	100,00
	41-49 anni	16,28	52,33	31,40	100,00
	50-57 anni	9,71	55,34	34,95	100,00
	58-69 anni	12,50	56,25	31,25	100,00
Area Funzionale	Area Tecnica	26,42	47,17	26,42	100,00
	Area Amministrativa	14,88	48,76	36,36	100,00
	Area Sanitaria	12,63	55,79	31,58	100,00

* P<=0,05

Tutti pensano che siano state adottate adeguate misure di sicurezza informatica. I più scettici sono i maschi dai 20 ai 40 anni dell'Area Tecnica.

Tab. 25: Ritiene che la Cybersecurity sia un aspetto importante nella digitalizzazione dei sistemi?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere *	Maschi	5,79	25,62	68,60	100,00
	Femmine	0,87	31,17	67,97	100,00
Classi di età	20-40 anni	5,26	21,05	73,68	100,00
	41-49 anni	2,33	34,88	62,79	100,00
	50-57 anni	1,94	34,95	63,11	100,00
	58-69 anni	5,00	23,75	71,25	100,00
Area Funzionale*	Area Tecnica	9,43	26,42	64,15	100,00
	Area Amministrativa	0,83	23,97	75,21	100,00
	Area Sanitaria	3,68	32,63	63,98	100,00

* P<=0,05

Sia maschi che femmine della fascia di età più giovane e della fascia di età più anziana all'interno dell'Area Amministrativa pensano che la Cybersecurity sia un aspetto importante nella digitalizzazione dei sistemi.

Tab. 26: ritiene che l'introduzione di sistemi di Sicurezza Informatica abbiano rallentato e/o complicato l'accesso ai sistemi quali ad esempio la posta elettronica?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere	Maschi	56,20	22,31	21,49	100,00
	Femmine	57,58	27,71	14,72	100,00
Classi di età	20-40 anni	67,37	20,00	12,63	100,00
	41-49 anni	52,33	24,42	23,26	100,00
	50-57 anni	52,43	33,01	14,56	100,00
	58-69 anni	56,25	25,00	18,75	100,00
Area Funzionale*	Area Tecnica	54,72	35,85	9,43	100,00
	Area Amministrativa	64,46	22,31	13,22	100,00
	Area Sanitaria	53,16	25,26	21,58	100,00

* P<=0,05

Sia maschi che femmine della fascia più giovane e l'Area Amministrativa ritengono che l'introduzione di sistemi di Sicurezza Informatica abbiano rallentato e/o complicato l'accesso ai sistemi informatici quali ad esempio la posta elettronica. I maschi tra i 40 e 49 anni dell'Area Sanitaria invece la pensano al contrario.

Tab. 27: Quanto percepisce la Cybersecurity come necessità che cresce di pari passo con la digitalizzazione?

		Per nulla/Poco	Abbastanza	Molto/ Moltissimo	Totale
Genere*	Maschi	8,26	28,93	62,81	100,00
	Femmine	4,33	42,42	53,25	100,00
Classi di età	20-40 anni	6,32	36,84	56,84	100,00
	41-49 anni	9,30	40,70	50,00	100,00
	50-57 anni	2,91	39,81	57,28	100,00
	58-69 anni	7,50	31,25	61,25	100,00
Area Funzionale	Area Tecnica	9,43	32,08	58,49	100,00
	Area Amministrativa	3,31	35,54	61,16	100,00
	Area Sanitaria	7,37	40,00	52,63	100,00

* P<=0,05

I maschi della fascia più anziana e dell'Area Amministrativa percepiscono la Cybersecurity come necessità che cresce di pari passo con la digitalizzazione. In piccola percentuale sempre i maschi della fascia dai 41 ai 49 anni e dell'Area Tecnica pensano invece che non sia così.

Considerazioni finali

Nonostante la PA abbia fatto notevoli passi avanti investendo in progetti di formazione, primo fra tutti Syllabus, progetto sponsorizzato dal dipartimento della funzione pubblica, che ha permesso un'offerta formativa ampia e gratuita al fine di migliorare le competenze dei dipendenti pubblici e per supportare i processi di innovazione delle amministrazioni, si riscontra una bassissima partecipazione alla formazione.

In generale la maggior parte degli operatori ha letto notizie circa gli attacchi informatici. Sia maschi che femmine sia della fascia di età più giovane che della fascia di età più anziana all'interno dell'Area Amministrativa, pensano che la Cybersecurity sia un aspetto importante nella digitalizzazione dei sistemi.

È importante coinvolgere attivamente gli operatori nel processo di digitalizzazione rendendoli parte consapevole del sistema di prevenzione: se gli operatori non seguono strettamente i protocolli di sicurezza qualunque intervento sistemistico rischia di diventare inefficace. Bisogna quindi agire sui comportamenti degli utenti rendendo tutti consapevoli del pericolo e del contributo che ognuno può dare per rendere l'azienda più sicura in ambito informatico. Dalle rilevazioni si può concludere che permane ancora forte la percezione che alcune scelte tecniche che aumentano i livelli di sicurezza siano di ostacolo al rapido svolgimento delle proprie attività quotidiane e che non si percepisca ancora l'importanza di certi interventi dal punto di vista della sicurezza.

Indipendentemente dal genere e dalla fascia di età tuttavia pare che all'interno dell'Area Amministrativa cresca la percezione che la Cybersecurity sia un aspetto importante della digitalizzazione dei sistemi.

5. Conclusioni

In conclusione, dalle analisi effettuate durante lo svolgimento della tesi, è emerso che la digitalizzazione, e nello specifico la Cybersecurity, fanno ormai parte della vita dei cittadini e dei dipendenti pubblici lavoratori.

Nei vari capitoli abbiamo visto l'evoluzione delle normative, i finanziamenti della digitalizzazione e della Cybersecurity.

Negli anni la pubblica amministrazione ha lavorato moltissimo sul tema della digitalizzazione. Dai ministeri sono arrivate molteplici comunicazioni e progetti. Le singole PA hanno recepito queste direttive ed hanno realizzato al meglio i vari progetti. Ora abbiamo un'autenticazione unica per accedere ai servizi della PA, "SPID", abbiamo il portale dell'INPS che racchiude molti dati e ci aiuta molto con la dichiarazione dei redditi, ad esempio i famosi scontrini della farmacia che tutti buttavano via oggi sono storicizzati in automatico. L'agenzia per l'Italia digitale "AGID" ha avviato progetti molto importanti anche per la salvaguardia del dato. La nuova agenzia per la Cybersecurity "ACN" ha inserito campagne per aumentare la sicurezza dei vari enti pubblici, ha implementato appositi TEAMS per aiutare le aziende durante o dopo gli attacchi informatici subiti, ha introdotto campagne di "alert" per le nuove vulnerabilità. Tutto questo è stato fatto grazie a nuovi investimenti del governo e ultimamente grazie ai fondi PNRR. Tramite questi fondi anche le aziende con grossi problemi finanziari hanno potuto rimodernare i propri asset per essere in linea con i tempi.

Le Regioni stanno alacremente lavorando per l'interoperabilità dei fascicoli sanitari regionali con l'obiettivo di convogliare tutte le informazioni nel fascicolo sanitario Nazionale. Per fare questo hanno rivoluzionato le modalità di interazione anche all'interno delle stesse aziende sanitarie. Sono stati implementati i più moderni protocolli di comunicazione vedi ad esempio HL7, SOAP, ecc. Hanno avviato processi di unificazione degli applicativi più importanti vedi ad esempio Immagini Radiologiche, Software economico/finanziari, Software per il consenso, software per la rilevazione presenze e per gli stipendi. In questo modo tutte le aziende pubbliche hanno iniziato a parlare la stessa lingua tecnologica e lo scambio di dati ha avuto un'impennata positiva. Ora posso andare nel mio fascicolo sanitario e verificare gli esami fatti, i vaccini, ritirare i referti, depositare documentazione aggiuntiva.

Tutte le attività di sviluppo sono strettamente realizzate in linea con le normative vigenti in termini di sicurezza e privacy, in particolar modo per quanto concerne

l'applicazione del GDPR. Tutte le transazioni devono essere autenticate e tracciate sui sistemi informativi. Oggi, qualunque attività eseguita dagli operatori sanitari sui sistemi, è tracciata e regolamentata dai concetti di presa in carico che vincola la visibilità della cartella clinica e dei singoli esami dei pazienti di propria competenza. Questo garantisce eventuali controlli e contestazioni da parte delle autorità e aumenta il rapporto di fiducia tra l'utente finale e la pubblica amministrazione.

All'interno delle aziende i software coprono ormai tutte le aree, ad esempio il protocollo, gestione delibere, gestione determine, rilevazione presenze, controllo temperature frigoriferi, controllo centrali termiche, affrancatura automatizzata, gestione magazzini e in diversi altri ambiti. In quello sanitario tra i principali si riscontrano cartelle verticali quali quelle di cardiologia, quelle per la refertazione degli esami EEG, per gli esami ECG, sistemi PACS per la gestione delle immagini di radiologia, cardiologia e anatomia patologica. In anatomia patologica infatti il problema più grosso in assoluto è la conservazione e ricerca dei vetrini. Tramite le nuove tecnologie ora è possibile archiviare tutto in modalità digitale. È stato superato il problema della grandezza di questi archivi, la tecnologia digitale ha permesso di migliorare la risoluzione in modo da permettere l'incremento dei fattori di espansione delle immagini a supporto di diagnosi più efficaci.

Tutto questo però ha portato ovviamente anche delle criticità, le aziende non erano pronte a questo processo di digitalizzazione, non avevano le risorse economiche, non avevano la conoscenza, non erano formate. Quindi ogni azienda ha dovuto affrontare in urgenza i problemi scaturiti creando appositi settori per riuscire a superare le varie difficoltà e creare efficienza.

Ad esempio sono stati istituiti specifici settori per la formazione digitale, per la privacy e soprattutto delle componenti informatiche; le aree ICT (Information and Comunication Tecnology) hanno creato a loro volta dei sotto settori specializzati quale ad esempio il settore per la Cybersecurity. Sono stati implementati veri e propri SOC (Security Operation Center).

Oggi non è più sufficiente avere un antivirus installato sul proprio pc, non basta più acquisire un Firewall, non bastano più utente e password. Ad oggi bisogna cercare di pensare alla sicurezza a 360 gradi, acquisendo Firewall NG (Next Generation) in grado di controllare singoli pacchetti di trasmissione che meglio riescono ad intercettare eventuali attacchi. I sistemi Waf (Web Application Firewall) che si utilizzano oggi prevedono l'autenticazione a due fattori chiamata anche MFA (Multi factor authentication). Nei sistemi antiintrusione si

ragiona in termini di malware, di EDR (Endpoint Detection and Response), di XDR (eXtended Detection and Response). Inoltre tutti questi software ed apparecchiature devono essere aggiornate in tempo reale. I sistemi di protezione prevedono continui aggiornamenti in tempo reale, si basano su appositi servizi di auto aggiornamento o di allarme per l'uscita di una nuova patch.

Per quanto riguarda in generale le infrastrutture invece AGID ha avviato processi per la normalizzazione di tutti i data center pubblici. Ha imposto regole severe per l'implementazione e manutenzione dei vari data center spengendo molto una migrazione sul Cloud. A tal proposito bisogna citare il PSN (Polo Strategico Nazionale) che è un insieme di data center nazionali con l'obbiettivo di ospitare tutti i sistemi della pubblica amministrazione.

Ma i vari operatori del settore come hanno reagito? Hanno reagito cercando di stare al passo il più possibile alle varie direttive ma con gli strumenti e la cultura che avevano a disposizione. Di fatto si sono creati una loro burocrazia di strada "Street Level Bureaucracy". Ad esempio per i data center hanno cercato di migliorli dedicandoli quasi solo, per la parte Sanitaria, agli elettromedicali (visto che le direttive non erano chiare in tal senso); hanno aderito subito a servizi esterni di Soc cercando nel frattempo di acquisire le conoscenze necessarie per essere autonomi; hanno puntato molto sui corsi di Cybersecurity per loro e per l'utente finale.

Come parte finale ma decisiva della mia tesi ho voluto sperimentare per la seconda volta il significato di creare un vero e proprio questionario personalizzato che ha prodotto ottimi risultati permettendo un'analisi accurata sul tema. Anche se non era la prima volta il percorso è stato arduo ma con il forte supporto del mio relatore ritengo di aver aumentato ulteriormente la mia esperienza. Questa volta abbiamo raggiunto un numero consistente di adesioni che ha riportato risultati statisticamente molto interessanti.

Il poter toccare con mano le opinioni dei non addetti ai lavori è stato molto formativo. Solitamente noi informatici tendiamo a vedere eventuali grandi problemi, per gli altri, come dei piccoli ostacoli temporanei, ad esempio "ma si, fai il refresh del browser e tutto torna a posto", "sì ma è normale per un servizio appena partito avere un po' di lentezza", "svuota la cache e tutto riparte", il problema è che lato utente vediamo semplicemente non funzionare un applicativo, una pagina web , vediamo un ostacolo molto grosso che ci fa pensare che i servizi funzionino malissimo e che dall'altra parte ci siano degli incompetenti in materia.

Questo percorso è stato plasmato attraverso una serie di indagini online, la consultazione di testi, riviste e partecipazioni a seminari, ma soprattutto tramite l'analisi di questionari preesistenti e delle loro strutture. La creazione di ciascuna domanda e delle relative opzioni di risposta è stata un'esperienza coinvolgente che mi ha reso estremamente attivo. Oltre a discutere con il mio relatore, ho confrontato le domande con colleghi e amici per valutare il loro potenziale coinvolgimento per i futuri compilatori del questionario. Ho dedicato particolare attenzione alle condizioni di ciascuna domanda, alle varie risposte (singole, multiple, ecc.) e alla loro disposizione. Nonostante l'impegno nella formulazione delle domande, ho riscontrato un alto tasso di abbandono del questionario prima del completamento. Facendo delle brevi indagini ho scoperto che molte volte gli utenti si collegavano, iniziavano il questionario, poi facevano un altro lavoro e lo abbandonavano. Successivamente, in molti casi, iniziavano un altro questionario e lo compilavano sino alla fine.

Nello specifico ho fatto un’attenta analisi dei risultati del questionario. Nella prima sezione di domande indirizzate agli intervistati ma come cittadini/utenti ho avuto delle conferme ma anche dei risultati inaspettati. Per quanto riguarda le conferme, al primo posto ci sono i giovani che hanno confermato di avere più familiarità con il concetto di informatizzazione/digitalizzazione. Gli stessi riscontrano ovviamente ancora grossi problemi derivanti dalla burocrazia.

Per quanto riguarda i risultati inaspettati, troviamo le donne che in teoria dovrebbero essere quelle ad apprezzare di più i servizi digitali in modo da poter dedicare più tempo ad altre responsabilità, invece hanno dato l’impressione di essere meno appagate dalle evoluzioni della digitalizzazione nella PA. Stessa cosa per l’Area Sanitaria che nonostante le spinte da parte del Governo e soprattutto da parte dell’Europa è stata riscontata una minor sensibilità sul tema della Digitalizzazione. Mi è anche dispiaciuto apprendere che nonostante tutti gli sforzi degli addetti ai lavori dei servizi digitali, quasi tutti gli intervistati hanno criticato la digitalizzazione nei confronti degli anziani.

Per quanto riguarda la sezione sui lavoratori non sono stati riscontrati grossi problemi di salute derivanti dall’utilizzo di terminali o computer. I più giovani hanno sfruttato al meglio l’opportunità dello Smart Working.

Per quanto riguarda la Cybersecurity, tutti hanno dimostrato di conoscerne le terminologie ed i concetti però hanno ancora la percezione che la sicurezza li rallenti. Inoltre,

anche in questo caso, nonostante gli sforzi dei Governi ed i molteplici investimenti vi è ancora una scarsa partecipazione ai corsi. Corsi che potrebbero anche variare la percezione in merito ad un argomento così importante come la Cybersecurity. Nell'Azienda ove lavoro abbiamo subito un attacco informatico e posso dire che con la collaborazione di tutti si può garantire la continuità dei servizi e la sicurezza dei dati dei cittadini e degli addetti ai lavori. È un lavoro molto arduo ma fattibile aiutato anche dal fatto che la digitalizzazione e la sicurezza dei propri dati è un argomento ormai toccato da tutti, vedi ad esempio l'utilizzo dei social che sono in tutte le case del mondo.

In conclusione, spero che l'interesse per la digitalizzazione e soprattutto la sicurezza informatica aumenti ancora e venga compreso come punto saldo e fondamentale del nuovo mondo che ormai si sta quasi totalmente digitalizzando. Desidero sottolineare che la stesura di questa tesi ha suscitato in me nuovamente un interesse non solo per l'argomento trattato, ma anche per il mondo delle ricerche e dei questionari, che spero di continuare ad approfondire nel mio futuro.

6. Bibliografia

Agostino D. – Arnaboldi M. – Lema M.D. (2020), New Development: COVID-19 as an Accelerator of Digital Transformation in Public Service Delivery, in «Public Money & Management», pp. 1-4, doi: 10.1080/095 40962.2020.1764206.

Anthopoulos L.G. – Siozos P. – Tsoukalas I.A. (2007), Applying Participatory Design and Collaboration in Digital Public Services for Discovering and Re- designing e-Government Services, in «Government Information Quarterly», 24, pp. 353-376, doi: 10.1016/j.giq.2006.07. 018.

Asgarkhani M. (2005), Digital Government and its Effectiveness in Public Management Reform: A Local Government Perspective, in «Public Management Review», vol. 7, n. 3, pp. 465-487, doi: 10.1080/147190305 00181227.

Bovaird T. (2003), E-government and E-governance: Organisational Implications, Options and Dilemmas, in «Public Policy and Administration», vol. 18, n. 2, pp. 37-56.

Bovens M. – Zouridis S. (2002), From Street-level to System-level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control, in «Public Administration Review», vol. 62, n. 2, pp. 174-184, doi: 10. 1111/0033-3352.00168.

Busemeyer M.R. (2020), Digitalizzazione, automazione e il futuro del welfare state democratico: profili per un' agenda di ricerca, in «Rivista Italiana di Politiche Pubbliche», n. 1, pp. 123-143.

Campbell J.L. (2004) Institutional Change and Globalization, Princeton, Princeton University Press.

Capano G. – Galanti M.T. (2020), From Policy Entrepreneurs to Policy Entrepreneurship: Actors and Actions in Public Policy Innovation, in «Policy & Politics», 00(00), pp. 1-22, doi: 10.1332/030557320x159068 42137162.

Capano G. – Pavan E. (2019), Designing Anticipatory Policies through the Use of ICTs, in «Policy and Society», 38(1), pp. 96-117, doi: 10.1080/14494035.2018.1511194.

Castelnovo W. – Sorrentino M. (2018), The Digital Government Imperative: A Context-aware Perspective, in «Public Management Review», vol. 20, n. 5, pp. 709-725, doi: 10.1080/14719037.2017.1305693.

Casula M. – Leonardi C. – Zancanaro M. (2020), How Does Digital Technology Impact on the Co-production of Local Services? Evidence from a Childcare Experience, in «Public Money and Management», pp. 1-11. doi: 10.1080/09540962.2020.1728066.

Clarke A. – Craft J. (2017), The Vestiges and Vanguards of Policy Design in a Digital Context, in «Canadian Public Administration», vol. 60, n. 4, pp. 476-497, doi: 10.1111/capa.12228.

Clarke A. – Margetts H. (2014), Governments and Citizens Getting Know Each Other? Open, Closed, and Big Data in Public Management Reform, in «Policy and Internet», vol. 6, n. 4, pp. 393-417, doi: 10.1002/1944- 2866.POI377.

Clausen T.H. – Demircioglu M.A. – Alsos G.A. (2020), Intensity of Innovation in Public Sector Organizations: The Role of Push and Pull Factors, in «Public Administration», vol. 98, n. 1, pp. 159-176, doi: 10.1111/padm.12617.

De Blasio E. – Selva D. (2016), Why Choose Open Government? Motivations for the Adoption of Open Government Policies in Four European Countries, in «Policy and Internet», vol. 8, n. 3, pp. 225-247, doi: 10.1002/poi3.118.

De Vries H. – Bekkers V. – Tummers L. (2016), Innovation in the Public Sector: A Systematic Review and Future Research Agenda, in «Public Administration», vol. 94, n. 1, pp. 146-166, doi: 10.1111/padm.12209.

Demircioglu M.A. (2019), Why Does Innovation in Government Occur and Persist? Evidence from the Australian Government, in «Asia Pacific Journal of Public Administration», vol. 41, n. 4, pp. 217-229, doi: 10.1080/23276665.2019.1692570.

Demircioglu M.A. – Audretsch D.B. (2017), Conditions for Innovation in Public Sector Organizations, in «Research Policy», vol. 46, n. 9, pp. 1681- 1691, doi: 10.1016/j.respol.2017.08.004.

Di Giulio M. – Vecchi G. (2019), Multilevel Policy Implementation and the Where of Learning: The Case of the Information System for School Buildings in Italy, in «Policy Sciences», vol. 52, n. 1, pp. 119-135, doi: 10.1007/s11077-018-9326-4.

Dunleavy P. – Margetts H. – Bastow S. – Tinkler J. (2006a), Digital Era Governance: IT Corporations, the State, and e-Government, Oxford, Oxford University Press, doi: 10.1093/acprof:oso/9780199296194.001.0001.

Dunleavy P. – Margetts H. – Bastow S. – Tinkler J. (2006b), New Public Management is Dead – Long Live Digital-era Governance, in «Journal of Public Administration Research and Theory», vol. 16, n. 3, pp. 467-494, doi: 10.1093/jopart/mui057.

Dunleavy P. – Evans M. (2019), Australian Administrative Elites and the Challenges of Digital-era Change, in «Journal of Chinese Governance», vol. 4, n. 2, pp. 181-200, doi: 10.1080/23812346.2019.1596544.

European Commission (2003), The Role of eGovernment for Europe's Future, Brussels, 26.9.2003.

European Commission (2019), eGovernment Benchmark 2019: Empowering Europeans Through Trusted Digital Public Services, Brussels, European Commission, doi: 10.2759/950318.

Falch M. – Henten A. (2000), Digital Denmark: From Information Society to Network Society, in «Telecommunications Policy», vol. 24, n. 5, pp. 377- 394, doi: 10.1016/S0308-5961(00)00028-8.

Gallego-Álvarez I. – Rodríguez-Domínguez L. – García-Sánchez I.M. (2010), Are Determining Factors of Municipal E-government Common to a Worldwide Municipal View? An Intra-country Comparison, in «Government Information Quarterly», vol. 27, n. 4, pp. 423-430. doi: 10.1016/j.giq.2009.12.011.

Gauld R. – Goldfinch S. – Horsburgh S. (2010), Do They Want it? Do They Use It? The «Demand-Side» of e-Government in Australia and New Zealand, in «Government Information Quarterly», vol. 27, n. 2, pp. 177- 186. doi: 10.1016/j.giq.2009.12.002.

Gil-Garcia J.R. – Dawes S.S. – Pardo T.A. (2018), Digital Government and Public Management Research: Finding the Crossroads, in «Public Management Review», vol. 20, n. 5, pp. 633-646, doi: 10.1080/147190 37.2017.1327181.

Giritli Nygren K. (2012), Narratives of ICT and Organizational Change in Public Administration, in «Gender, Work and Organization», vol. 19, n. 6, pp. 615–630. doi: 10.1111/j.1468-0432.2010.00531.x.

Grant M.J. – Booth A. (2009), A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies, in «Health Information and Libraries Journal», John Wiley & Sons, Ltd, pp. 91-108, doi: 10.1111/ j.1471-1842.2009.00848.x.

Greve B. (2019), The Digital Economy and the Future of European Welfare States, in «International Social Security Review», vol. 72, n. 3, pp. 79-94, doi: 10.1111/issr.12214.

Hall P.A. (1993), Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain, in «Comparative Politics», vol. 25, n. 3, pp. 275-296.

Hameduddin T. – Fernandez S. – Demircioglu M.A. (2020), Conditions for Open Innovation in Public Organizations: Evidence from Challenge.gov, in «Asia Pacific Journal of Public Administration», vol. 42, n. 2, pp. 111-131, doi: 10.1080/23276665.2020.1754867.

Hansen H.-T. – Lundberg K. – Syltevik L.J. (2018), Digitalization, Street- level Bureaucracy and Welfare Users' Experiences, in «Social Policy & Administration», vol. 52, n. 1, pp. 67-90, doi: 10.1111/spol.12283.

Heeks R. (2006), Implementing and Managing eGovernment: An International Text, London, SAGE Publications, doi: 10.1177/0894439 306287246.

Heeks R. – Bailur S. (2007), Analyzing E-government Research: Perspectives, Philosophies, Theories, Methods, and Practice, in «Government Information Quarterly», vol. 24, n. 2, pp. 243-265, doi: 10.1016/j.giq. 2006.06.005.

Helbig N. – Ramón Gil-García J. – Ferro E. (2009), Understanding the Complexity of Electronic Government: Implications from the Digital Divide Literature, in «Government Information Quarterly», vol. 26, n. 1, pp. 89-97, doi: 10.1016/j.giq.2008.05.004.

Homburg V. (2018), ICT, E-Government and E-Governance Bits & Bytes for Public Administration, in E. Ongaro – S. van Thiel (eds.), The Palgrave Handbook of Public Administration and Management in Europe. London, Palgrave Macmillan, pp. 347-361

Hood C. (1983), The Tools of Government, London and Basigstoke, The Macmillan Press LTD, doi: 10.1007/978-1-349-17169-9_3.

Hood C. (1991), A Public Management for All Seasons?, in «Public Administration», vol. 69, pp. 3-19.

Hood C. – Margetts H.Z. (2007), The Tools of Government in the Digital Age, Basingstoke, Palgrave Macmillan, doi: 10.1017/CBO978110741 5324.004.

Huang B. – Yu J. (2019), Leading Digital Technologies for Coproduction: the Case of «Visit Once» Administrative Service Reform in Zhejiang Province, China, in «Journal of Chinese Political Science», vol. 24, n. 3, pp. 513- 532, doi: 10.1007/s11366-019-09627-w.

Hur J.-Y. – Cho W. – Lee G. – Bickerton S.H. (2019), The «Smart Work» Myth: How Bureaucratic Inertia and Workplace Culture Stymied Digital Transformation in the Relocation of South Korea's Capital, in «Asian Studies Review», vol. 43, n. 4, pp. 691-709, doi: 10.1080/10357823.2019.1663786.

Jacobs A.M. – Weaver R.K. (2015), When Policies Undo Themselves: Self-Undermining Feedback as a Source of Policy Change, in «Governance», vol. 28, n. 4, pp. 441-457, doi: 10.1111/gove.12101.

Jacobsen D.I. (2018), Adopting and Refining E-services – The Role of Organization Size, in «Public Organization Review», vol. 18, n. 1, pp. 111-123, doi: 10.1007/s11115-016-0364-0.

Kingdon J.W. (1984), Agendas, Alternatives, and Public Policy, New York, Harper Collins.

Lau T.Y. – Aboulhoson M. – Lin C. – Atkin D.J. (2008), Adoption of E- government in Three Latin American Countries: Argentina, Brazil and Mexico, in «Telecommunications Policy», vol. 32, n. 2, pp. 88-100, doi: 10.1016/j.telpol.2007.07.007.

Lember V. – Kattel R. – Tõnurist P. (2018), Technological Capacity in the Public Sector: The Case of Estonia, in «International Review of Administrative Sciences», vol. 84, n. 2, pp. 214-230, doi: 10.1177/0020 852317735164.

Lim J.H. – Tang S.-Y. (2008), Urban E-Government Initiatives and Environmental Decision Performance in Korea, in «Journal of Public Administration Research and Theory», vol. 18, n. 1, pp. 109-138, doi: 10.1093/jopart/mum005.

Margetts H. – Dunleavy P. (2013), The Second Wave of Digital-era Governance: A Quasi-paradigm for Government on the Web, in «Philosophical Transactions of the Royal Society», 371, doi: 10.1098/rsta.2012.0382.

Meijer A. – Bolivar M.P.R. – Gil-Garcia J.R. (2018), From E-Government to Digital Era Governance and Beyond: Lessons from 15 Years of Research into Information and Communications Technology in the Public Sector, in «Journal of Public Administration Research and Theory», pp. 1-6.

Nam T. (2018), Examining the Anti-corruption Effect of E-government and the Moderating Effect of National Culture: A Cross-country Study, in «Government Information Quarterly», vol. 35, n. 2, pp. 273-282, doi: 10.1016/j.giq.2018.01.005.

Nasi G. – Cucciniello M. – Degara V. (2018), Evaluation of Innovation Performance in the Public Sector: A Systematic Review of Studies, in E. Borgonovi – E. Anessi-Pessina – C. Bianchi (eds.), Outcome-Based Performance Management in the Public Sector, Cham, Springer, doi: 10.1007/978-3-319-57018-1_1.

Natali D. – Guardiancich I. (2020), Le politiche pubbliche nell'era digitale: introduzione alle principali sfide di analisi, in «Rivista Italiana di Politiche Pubbliche», n. 1, pp. 5-22.

Natali D. – Raitano M. (2020), Il cambiamento tecnologico e le sfide per le politiche pensionistiche, in «Rivista Italiana di Politiche Pubbliche», n. 1, pp. 49-76.

Natalini A. – Stolfi F. (2012), Mechanisms and Public Administration Reform: Italian Cases of Better Regulation and Digitalization, in «Public Administration», vol. 90, n. 2, pp. 529-543, doi: 10.1111/j.1467- 9299.2011.01998.x.

O'Neill R. (2009), The Transformative Impact of E-Government on Public Governance in New Zealand, in «Public Management Review», vol. 11, n. 6, pp. 751-770, doi: 10.1080/14719030903318939.

OECD (2003), The e-Government Imperative, Paris, OECD e-Government Studies, OECD Publishing. Available at: www.SourceOECD.org,.

OECD – Public Governance Committee (2014), Recommendation of the Council on Digital Government Strategies, Adopted by the OECD Council on 15 July 2014.

OECD (2016), Digital Government Strategies for Transforming Public Services in the Welfare Areas. Paris, OECD Publishing, doi: 10.1063/1.3689939.

Park C.H. – Kim K. (2020), E-government as an Anti-corruption Tool: Panel Data Analysis Across Countries, in «International Review of Administrative Sciences», vol. 86, n. 4, pp. 691-707, doi: 10.1177/0020 852318822055.

Petridou E. – Mintrom M. (2020), A Research Agenda for the Study of Policy Entrepreneurs, in «Policy Studies Journal», pp. 1-25, doi: 10.1111/ psj.12405.

Petropoulos G. – Marcus J.S. – Bergamini E. (2019), Digitalisation and European Welfare States, Brussels, Bruegel Bluerpint Series.

Petticrew M. – Roberts H. (2006), Systematic Reviews in the Social Sciences: A Practical Guide, Oxford, Blackwell Publishing, doi: 10.1002/978047 0754887.

Pierson, P. (2004), Politics in Time: History, Institutions, and Social Analysis, Princeton, Princeton University Press.

Pina V. – Torres L. – Royo S. (2007), Are ICTs Improving Transparency and Accountability in the EU Regional and Local Governments? An Empirical Study, in «Public Administration», vol. 85, n. 2, pp. 449-472, doi: 10.1111/j.1467-9299.2007.00654.x.

Pissin A. (2019), Digital Welfare for Children in China: Human Needs and Sustainability, in «Critical Social Policy», pp. 1-21, doi: 10.1177/026101 8319858569.

Schou J. – Hjelholt M. (2019), Digitalizing the Welfare State: Citizenship Discourses in Danish Digitalization Strategies from 2002 to 2015, in «Critical Policy Studies», 13(1), pp. 3-22. doi: 10.1080/19460171. 2017.1333441.

Schou J. – Pors A.S. (2019), Digital by Default? A Qualitative Study of Exclusion in Digitalised Welfare, in «Social Policy & Administration», vol. 53, n. 3, pp. 464-477, doi: 10.1111/spol.12470.

Schwab K. (2016), The Fourth Industrial Revolution, Cologny/Geneva, World Economic Forum.

Shanahan E.A. – Jones M.D. – McBeth M.K. – Radaelli C.M. (2018), The Narrative Policy Framework, in C.M. Weible – Sabatier P.A. (eds.), Theories of the Policy Process, New York, Routledge, pp. 173-214.

Spensberger F. (2019), The Digitalization of a Social Work Theory: Experiences of a German Child Welfare Social Worker, in «International Social Work», vol. 62, n. 6, pp. 1575-1579, doi: 10.1177/0020872819865018.

Stevenson S. (2009), Digital Divide: A Discursive Move Away from the Real Inequities, in «Information Society», vol. 25, n. 1, pp. 1-22, doi: 10.1080/01972240802587539.

Streeck W. – Thelen K. (2005), Introduction: Institutional Change in Advanced Political Economies, in W. Streeck – K. Thelen (eds.), Beyond Continuity: Institutional Change in Advanced Political Economies, New York, Oxford University Press, pp. 1-39

Tolbert C.J. – Mossberger K. – McNeal R. (2008), Institutions, Policy Innovation, and E-Government in the American States, in «Public Administration Review», vol. 68, n. 3, pp. 549-563, doi: 10.1111/j.1540- 6210.2008.00890.x.

Tregeagle S. – Darcy M. (2007), Child Welfare and Information and Communication Technology: Today's Challenge, in «British Journal of Social Work», vol. 38, n. 8, pp. 1481-1498, doi: 10.1093/bjsw/bcm048.

Weible C.M. – Sabatier P.A. (eds.) (2018), Theories of the Policy Process. New York, Routledge.

Welch E.W. (2005), Linking Citizen Satisfaction with E-government and Trust in Government, in «Journal of Public Administration Research and Theory», vol. 15, n. 3, pp. 371-391, doi: 10.1093/jopart/mui021.

Welch E.W. – Feeney M.K. (2014), Technology in Government: How Organizational Culture Mediates Information and Communication Technology Outcomes, in «Government Information Quarterly», vol. 31, n. 4, pp. 506-512, doi: 10.1016/j.giq.2014.07.006.

Welch E.W. – Pandey S.K. (2007), E-government and Bureaucracy: Toward a Better Understanding of Intranet Implementation and Its Effect on Red Tape, in «Journal of Public Administration Research and Theory», vol. 17, n. 3, pp. 379-404, doi: 10.1093/jopart/mul013.

West D.M. (2005), Digital Government: Technology and Public Sector Performance, Princeton, Princeton University Press.

Wirtz B.W. – Birkmeyer S. (2015), Open Government: Origin, Development, and Conceptual Perspectives, in «International Journal of Public Administration», vol. 38, n. 5, pp. 381-396, doi: 10.1080/01900692.2014.942735.

Wirtz B.W. – Daiser P. (2018), A Meta-analysis of Empirical E-government Research and its Future Research Implications, in «International Review of Administrative Sciences», vol. 84, n. 1, pp. 144-163, doi: 10.1177/ 0020852315599047.

Wirtz B.W. – Weyerer J.C. – Geyer C. (2019), Artificial Intelligence and the Public Sector—Applications and Challenges, in «International Journal of Public Administration», vol. 42, n. 7, pp. 596-615, doi: 10.1080/01900 692.2018.1498103.

Wong W. – Welch E. (2004), Does E-government Promote Accountability? A Comparative Analysis of Website Openness and Government Accountability, in «Governance», vol. 17, n. 2, pp. 275-297.

World Bank (2002), The E-government Handbook for Developing Countries, Washington, D.C., World Bank.

Zhao X. – Xu H.D. (2015), E-Government and Corruption: A Longitudinal Analysis of Countries, in «International Journal of Public Administration», vol. 38, n. 6, pp. 410-421, doi: 10.1080/01900692. 2014.942736.

Zheng Y. (2016), The Impact of E-participation on Corruption: A Cross- country Analysis, in «International Review of Public Administration», vol. 21, n. 2, pp. 91-103, doi: 10.1080/12294659.2016.1186457.

7. Appendice

7.1 Questionario

1	**Quale è il tuo sesso? ***
	Scegli **solo una** delle seguenti: • Maschio • Femmina • Preferisco non rispondere DESCRIZIONE: Questa domanda prevede anche il "Preferisco non rispondere" per garantire la privacy. Il sesso in ogni intervista, questionario, survey è comunque un elemento molto importante per le analisi successive.
2	**Età? ***
	Ogni risposta deve essere al più uguale a 99 Solo valori interi possono essere ammessi in questi campi. Scrivere la/le proprie risposta/e qui: DESCRIZIONE: L'età è molto importante per capire se ha influito negativamente soprattutto nell'utilizzo degli strumenti informatici, vedi ad esempio aumento problemi tecnici o di salute.
3	**A quale area funzionale appartiene? ***
	Scegli **solo una** delle seguenti: • Area Tecnica • Area Amministrativa • Area Sanitaria DESCRIZIONE: La domanda serve per capire quale sia il settore che ha fruito maggiormente dei vantaggi della digitalizzazione.
4	**Appartiene all'area? ***
	Scegli **solo una** delle seguenti: • Dirigenza • Comparto DESCRIZIONE: Altro elemento significativo per individuare i settori che hanno sfruttato maggiormente la digitalizzazione e la Sicurezza Informatica
	In qualità di cittadino/utente, quale è il suo rapporto con la digitalizzazione nella Pubblica Amministrazione?

5	**Ha familiarità con il concetto di digitalizzazione nella Pubblica Amministrazione? ***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda molto significativa che permette di capire il grado di conoscenza dell'argomento come cittadino/utente.
6	**Quanto ritiene di essere informato/a riguardo ai processi di digitalizzazione attuali dalla Pubblica Amministrazione?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda molto significativa che permette di capire il grado di conoscenza dell'argomento come cittadino/utente.
7	**Ritiene che la pandemia da Covid-19 abbia accelerato la digitalizzazione?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Questa domanda server per capire quanto la pandemia abbia aiutato il processo di digitalizzazione visto anche l'introduzione dello smart working.
8	**Quanto le sue aspettative, rispetto alla digitalizzazione nella Pubblica Amministrazione, sono state appagate?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda che serve a capire quante aspettative avevano gli intervistati e se sono state appagate.

9	**Ritiene che la digitalizzazione abbia migliorato l'accessibilità della Pubblica Amministrazione? ***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda che serve a valutare l'apprezzamento del cittadino/utente nei confronti della digitalizzazione.
10	**Hai riscontrato benefici personali nell'utilizzo dei servizi digitali rispetto a quelli tradizionali?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda di confronto tra servizi digitali e tradizionali. Server a capire l'apprezzamento dei servizi digitali ma paragonandolo a quelli tradizionali.
11	**Secondo lei la digitalizzazione ha contribuito a ridurre la burocrazia nella Pubblica Amministrazione?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda molto significativa per capire quanto possa eventualmente contribuire la digitalizzazione a diminuire la burocratizzazione del paese.
12	**Incontra spesso difficoltà nell'utilizzo dei servizi digitali della Pubblica Amministrazione?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza

- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire se, nonostante l'esistenza di servizi digitali sia ha difficoltà nel loro utilizzo.

13 Secondo lei, le informazioni in merito ai servizi di digitalizzazione della Pubblica Amministrazione sono state sufficienti?*

Scegli **solo una** delle seguenti:

- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire se le informazioni ed istruzioni che da la Pubblica Amministrazione nella pubblicazione dei vari servizi sia sufficiente oppure no.

14 Pensa, che la digitalizzazione della Pubblica Amministrazione penalizzi gli anziani nell'accesso, soprattutto, ai servizi sanitari?*

Scegli **solo una** delle seguenti:

- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Ultimamente il governo ha investito molto per migliorare l'accesso degli anziani ai servizi della Pubblica Amministrazione. Questa domanda vuol catturare le percezioni degli intervistati su questo tema.

15 Quanto si sente sicuro riguardo alla protezione dei suoi dati personali quando utilizza servizi online della Pubblica Amministrazione?*

Scegli **solo una** delle seguenti:

- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire quanto siano sereni o preoccupati gli intervistati per i dati inseriti o archiviati sui sistemi della Pubblica Amministrazione.

In qualità di lavoratore/lavoratrice, quale è il suo rapporto con l'utilizzo di strumenti di lavoro digitali?*

16 A seguito del lavoro su un computer/terminale ha riscontrato fastidi/problemi di

salute che prima non manifestava?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire se la digitalizzazione e quindi il maggior utilizzo di computer/terminali ha portato fastidi/problemi.

17 Ha riscontrato benefici personali nell'utilizzo dei servizi digitali rispetto a quelli tradizionali?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Questa domanda è identica a quella della sezione del cittadino e serve anche per paragonare le differenti valutazioni di cittaino oppure da lavoratore.

18 Ha riscontrato problemi muscolo-scheletrici usando un computer/trminale? *

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire che tipo di problemi di salute possa dare la digitalizzazione.

19 Ha riscontrato problemi di cefalea usando un computer/terminale?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire che tipo di problemi di salute possa dare la digitalizzazione.

20 Ha riscontrato problemi visivi usando un computer/terminale?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire che tipo di problemi di salute possa dare la digitalizzazione.

21 A suo parere il lavoro sul computer può rappresentare forme di dipendenza da web?

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire la percezione degli intervistati in merito ad argomenti sociali tipo la dipendenza da Web.

22 Quante volte, nell'ultimo anno, ha dovuto utilizzare una procedura manuale per malfunzionamento dei servizi informatici della sua azienda o nazionali?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire quanto la digitalizzazione, in caso di disservizi, crei grossi problemi ai lavoratori.

23 La digitalizzazione utilizzata in Smart Working, quanto ha migliorato il suo lavoro?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Domanda per capire quanti possano sfruttare lo smart working e quanto lo apprezzino.

	Quali sono le sue opinioni ed esperienze su Cybersecurity (sicurezza informatica) nel suo ambiente di lavoro?*
24	**Ha partecipato a eventi o corsi sulla Cybersecurity nell'Azienda Pubblica ove lavora?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda per capire quale sia la partecipazione ai corsi proposti dalla Pubblica Amministrazione.
25	**I progetti di sicurezza informatica vedi MFA (Multi Factor Authentication/Autenticazione a più fattori) con OTP le danno maggiore tranquillità nell'utilizzo dei sistemi digitali?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Domanda per capire se i sistemi di sicurezza che implementano oggi le Pubbliche Amministrazioni siano visti positivamente o negativamente.
26	**Quanto ha sentito parlare di attacchi informatici o di Hackers?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: L'argomento degli attacchi informatici e degli Hackers è conosciuto?
27	**Pensa che l'implementazione di nuove misure di sicurezza siano utili per il suo lavoro ed i dati che inserisce/utilizza?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto

- Moltissimo

DESCRIZIONE: Le misure di sicurezza implementate nelle Azienda Pubbliche per difendere i pc e le identità digitali sono viste positivamente o negativamente?

28 Crede che siano state adottate adeguate misure di sicurezza informatica?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Da lavoratore si ha la percezione che ci siano sistemi digitali di lavoro sicuri?

29 Ritiene che la Cybersecurity sia un importante nella digitalizzazione dei sistemi?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Valutazione su Cybersecurity all'interno del processo di digitalizzazione dei sistemi di lavoro.

28 Crede che siano state adottate adeguate misure di sicurezza informatica?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Da lavoratore si ha la percezione che ci siano sistemi digitali di lavoro sicuri?

29 Ritiene che la Cybersecurity sia un importante nella digitalizzazione dei sistemi?*

Scegli **solo una** delle seguenti:
- Per nulla
- Poco
- Abbastanza
- Molto
- Moltissimo

DESCRIZIONE: Valutazione su Cybersecurity all'interno del processo di digitalizzazione dei sistemi di lavoro.

30	**Ritiene che l'introduzione di sistemi di Sicurezza Informatica abbiano rallentato e/o complicato l'accesso ai sistemi quali ad esempio la posta elettronica?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Questa domanda server per capire quanto gli operatori pubblici pensano che la Sicurezza informatica rallenti gli accessi ai servizi digitali.
31	**Quanto percepisce la Cybersecurity come necessità che cresce di pari passo con la digitalizzazione?***
	Scegli **solo una** delle seguenti: • Per nulla • Poco • Abbastanza • Molto • Moltissimo DESCRIZIONE: Questa domanda vuole catturare la percezione degli intervistati in merito alla crescita della Cybersecurity.