Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a 2023/2024

Titolo tesi: Amministrazione Digitale e Sicurezza Informatica

Relatore: Prof. Clemente Pio Santacroce

Studente: Clara Rosina

Ai miei nonni mi mancate

Alla mamma e papà

Sommario

INTRODUZIONE

Il seguente elaborato offre al lettore un approfondimento sul tema relativo all'amministrazione digitale e la sicurezza informatica. Da tempo è in atto un processo di cambiamento spinto dalla tecnologia, il quale ha inesorabilmente coinvolto anche la P.A. Essendo diffuso l'utilizzo della tecnologia anche da parte del servizio pubblico, crescono le insidie sul piano della sicurezza informatica, le quali appaiono più impattanti e pervasive di un tempo, sia per il ruolo che la P.A ricopre nel sistema paese e che ne fa una vittima, sia per la mole di dati e informazioni posseduti. Per questi motivi, la P.A è tenuta, in virtù dei principi a cui la stessa è chiamata ad essere amministrata, a garantire la continuità, sicurezza e disponibilità di quei servizi erogati nell'interesse della cittadinanza.

Il primo capitolo è dedicato al tema della sicurezza informatica, partendo dall'etimologia del termine e suo sviluppo, si vuole sottolineare come oramai il processo di digitalizzazione non può escludere la messa in sicurezza della tecnologia. Si volge lo sguardo al cyberspazio, il quale è la conseguenza della nascita delle tecnologie che permettono la connessione internet. Tale dimensione, in un primo momento, si presenta come *alios* ma successivamente viene a costituirsi come realtà nella quale l'uomo stesso conduce la propria vita e in virtù di ciò, nasce la necessità che tale "spazio" venga regolato e che siano garantiti gli stessi principi costituzionali. A chiusura del capitolo si trova una panoramica concernente il manifestarsi della sicurezza informatica utile al lettore per una comprensione prima di tutto della tipologia di attacchi e minacce e, in secondo luogo, di quelle contromisure, metodologie e processi tipici della cibersicurezza.

Il secondo capitolo si addentra nello snodo centrale dell'elaborato, in un primo passaggio l'attenzione si concentra sul ruolo della transizione digitale per la pubblica amministrazione, attraverso le principali tappe della digitalizzazione insieme ai principi dell'amministrazione digitale. Segue un secondo passaggio, il quale riguarda la presentazione di alcune delle possibili interpretazioni concernenti il legame tra la P.A e la sicurezza informatica. La prima, partendo da una riflessione sul concetto di cittadinanza e appurando la presenza del digitale in modo trasversale in ogni sua

"forma", muove verso il principio del Buon andamento dell'amministrazione di cui all'art.97 Cost. Quel che si vuole sottolineare è la necessità della pubblica amministrazione di offrire un servizio ad una cittadinanza oramai digitale, in virtù dei principi a cui la stessa è chiamata ad essere amministrata, quali l'efficienza, efficacia ed economicità. In aggiunta, in virtù del rapporto strumentale tra la PA e il cittadino, sembra potersi configurare un diritto ad una "buona amministrazione" in relazione al quale le tecniche di sicurezza informatica possono garantire la continuità del servizio e la realizzazione di quei diritti (anche in forma digitale) del cittadino. Il secondo passaggio invece, verte sul tema della sicurezza e ordine pubblico, nella definizione dei quali, la cibersicurezza rientra nei confini di sicurezza pubblica come una componente dell'ordine pubblico materiale.

Il terzo capitolo approfondisce lo sviluppo normativo in materia di cibersicurezza, ponendo attenzione alle strategie per la PA, sono percorse le principali disposizioni in materia fino alla creazione, post pandemica, di un'architettura nazionale di cibersicurezza. Dalla lettura emerge la sempre crescente consapevolezza nel legislatore di accentrare e rendere efficiente l'organizzazione cyber italiana. Infatti, in un primo momento la stessa era suddivisa tra varie agenzie e ministeri per poi passare gradualmente all'Agenzia per la Cybersicurezza Nazionale. Infine, uno sguardo è dedicato ai recenti sviluppi per quanto concerne la legge n.90 del 24 giugno del 2024, e a chiusura, una riflessione sui prossimi adempimenti in merito alla normativa europea e al futuro della sicurezza informatica nella pubblica amministrazione.

CAPITOLO I

LA SICUREZZA INFORMATICA

In questo capitolo si offre al lettore una panoramica sulle origini e gli sviluppi della sicurezza informatica. Verrà inoltre esaminato come l'avvento del cyberspazio e la trasformazione digitale abbiano reso sempre più urgente la necessità di risposte adeguate a tale cambio di paradigma. Successivamente, l'attenzione viene rivolta alle principali tipologie di attacco, alle vulnerabilità, in particolare alle minacce rivolte al settore pubblico e alle metodologie di risposta e contromisure.

1. ETIMOLOGIA ED EVOLUZIONE

1.1 Origini della cibersicurezza

La sicurezza informatica o cibersicurezza e meglio nota nella sua terminologia anglosassone *cybersecurity* ha origini nella "computer security" la quale risale ai primi anni del 1960. Il confisso "cyber" risale dall'etimologia greca del termine κυβερνήτης[1] (kybernetes) il quale aveva il significato letterale di "timoniere", "pilota di una nave" e per estensione "colui che guida e governa una città o uno Stato[2]". Il confisso venne impiegato dal matematico statistico statunitense Robert Wiener, riconosciuto come padre della cibernetica, nel testo "Introduzione alla cibernetica, l'uso umano degli esseri umani" del 1950. Nel tempo il confisso, partendo da un nesso con la teoria dei sistemi di controllo automatico, e quindi da uno studio comparato del controllo dell'uomo e della macchina, è andato a legarsi allo sviluppo di quei sistemi "autonomi" che oggi rintracciamo nella tecnologia e in particolare nell'Intelligenza artificiale.

Accanto all'etimologia del confisso *cyber* vi è la difficoltà di circoscrivere l'espressione "*security*", oggigiorno sembra riferirsi al concetto di sicurezza nazionale ma pare potersi anche espandere al concetto di protezione di diversi valori legati alla trasformazione digitale. L'origine del termine, essendo legata alla sicurezza dei computer, ha subito ulteriori evoluzioni a seguito dello sviluppo tecnologico, come la *network security* e

[1] Utilizzato da Platone nella sua accezione politica di guida della polis.

[2] Accademia della Crusca.

l'*information security*, la prima legata non solo alla dimensione del computer ma anche del sistema informatico nella sua interezza, la seconda è allacciata alla salvaguardia delle informazioni. L'accezione attuale di *cybersecurity* include un concetto di sicurezza onnicomprensiva, ed è stato utilizzato in relazione alla protezione del cyberspazio sottolineando il passaggio della materia da una visione ristretta, legata ai sistemi informatici e alle reti, ad una visione olistica e consapevole della nuova realtà[3]. Di conseguenza la cibersicurezza racchiude in sé diverse sfaccettature della sicurezza, basti pensare alla *data protection* definita dal regolamento europeo sulla protezione dei dati personali (GDPR) o alla sicurezza delle informazioni dettate dallo standard ISO /IEC 27001, o al riferimento alla cibersicurezza dei sistemi di I.A secondo l'art. 15 del Regolamento europeo sull'Intelligenza Artificiale (AI Act). Ne consegue che il termine, nella sua totalità, appare "non cristallizzato", per via della sua dimensione olistica (da olismo che deriva a sua volta dal greco ὅλος cioè, "tutto, intero, totale") la quale fa rientrare nel termine sicurezza informatica i concetti di sicurezza nazionale, ordine pubblico, sicurezza personale dell'individuo, privacy e sicurezza dei dati, interessi economici e la preservazione dei diritti fondamentali[4]. Invero, una "minaccia cyber" non solo comporta un rischio per i sistemi informatici ma oramai è in grado di «ledere dei diritti e libertà delle persone, alterare gli equilibri politici di una nazione e, se sono colpite infrastrutture critiche, determinare gravi conseguenze per comunità, istruzioni e imprese[5] ».

Avendo presentato quanto sopra, possiamo affermare che la cibersicurezza si prefigge di garantire tre fattori[6] la riservatezza, ovvero il controllo e protezione delle informazioni sensibili e personali; l'integrità, in quanto salvaguardia dell'accuratezza, affidabilità e coerenza di una informazione o sistema informatico; la disponibilità ovvero la possibilità utilizzare un dato sistema o di accedere a delle informazioni[7]. Dal punto di vista operativo e tecnico, questi tre fattori, sono perseguibili attraverso la predisposizione di

---

[3] R. BRIGHI e C. PIER GIORGIO, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* Federalismi, p.19, n.21, 8 settembre 2021.

[4] L. TOSONI, *The Fundamental Right to Cybersecurity, Inception, Implications and Limits*, University of Oslo, p. 27 – 32, 2023.

[5] L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, Federalismi, p. 67, n.25/2022.

[6] Si veda la triade CIA, "Confidentiality, Integrity and Availability".

[7] R. CASTROREALE, *Cybersecurity per tutti*, EPC editore, p.22, 2024.

misure di prevenzione dagli attacchi, misure di monitoraggio e tecniche di risposta e di ripristino. Insieme alla parte "tecnica" della sicurezza informatica, rientrano anche il governo la gestione e la cultura cyber, questi fattori si articolano in numerose azioni quali, lo sviluppo normativo, l'analisi del rischio, formazione e consapevolezza, il piano di risposta, la definizione di una strategia di ruoli e responsabilità[8]. Sulla scia di ciò, un aspetto essenziale della sicurezza informatica, ripreso poi nel corso dell'elaborato, è l'essere una «responsabilità condivisa[9]», sia come impegno del singolo, il quale ha il compito di adottare un comportamento diligente volto alla sicurezza; sia come compito dello Stato, il quale non deve limitare il suo ruolo a quello di erogatore di servizi, ma deve fungere anche da motore di crescita digitale-culturale[10]. Per questi motivi, la sicurezza informatica si concatena sempre di più al concetto di digitalizzazione, in quanto un contesto sempre più digitalizzato non può prescindere dalla sicurezza degli strumenti adoperati, soprattutto se questi vengono adottati dalla società.

1.2 Cyberspazio e tutela dei diritti

In seguito alla diffusione delle tecnologie in grado di connettersi alla rete Internet, è nata una nuova realtà chiamata cyberspazio. Si tratta di una dimensione che ha origine dall'unione delle reti e dati e dall'interconnessione tra gli uomini grazie agli strumenti tecnologici e alla connessione di rete[11]. Di conseguenza, la progressiva digitalizzazione della società ha comportato la possibilità di condurre azioni analogiche nel mondo del cyberspazio, il quale non è una realtà parallela ma si configura come luogo inscindibilmente interconnesso al mondo reale. Infatti, sono numerose le azioni che si compiono grazie all'ingresso nel cyberspazio; come agevolare i movimenti tra paesi di beni, servizi e persone, la possibilità di comunicare, stringere accordi «a tal punto che la

[8] Un approfondimento sul tema può essere svolto attraverso la lettura del nuovo aggiornamento del NIST Cybersecurity Framework (CSF) 2.0, pubblicato il 26 febbraio del 2024 dall'agenzia americana per la gestione dell'innovazione e tecnologia, ovvero il National Institute of Standards and Technology.

[9] R. BRIGHI e C. PIER GIORGIO, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, Federalismi, p.41, 8 settembre 2021 n.21.

[10] R. FORSI, *Cyber, una PA più sicura farà lezione degli errori passati,* Agenza Digitale. Eu, 2024. https://www.agendadigitale.eu/sicurezza/levoluzione-della-cybersicurezza-nella-pa-lezioni-dal-passato-e-prospettive-future/

[11] L.MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale,* Il Mulino - rivisteweb, *p.*63, n. Politica & Società Fascicolo 1, gennaio-aprile 2018.

nostra vita quotidiana, i diritti fondamentali, le economie […] sono strettamente dipendenti dal regolare funzionamento delle tecnologie […][12]».

Nel corso degli anni, questa dimensione ha rappresentato, come i movimenti libertari hanno aspirato, quel mondo privo di un controllo e di una regolamentazione, ma anzi, incarnasse quel luogo auto organizzato dove le libertà e i diritti potessero essere espressi senza impedimenti, a riguardo di ciò ricordiamo il lavoro di J.P Barlow "Dichiarazione di Indipendenza del Cyberspazio".

Tuttavia, ben presto è emerso il carattere utopistico della visione libertaria del cyberspazio, in quanto, l'influenza di alcuni attori diviene strategicamente pericolosa quando mira a modellare la realtà tramite l'utilizzo improprio della tecnologia. A fronte di ciò, l'Intelligenza artificiale[13] si pone come uno strumento a doppio taglio; se da un lato infatti rappresenta il culmine attuale in cui la digitalizzazione viene a trovarsi, dall'altro, si presta come uno strumento di attacco altamente dannoso. Tale caratteristica è dovuta a due fattori, il primo concerne lo stesso funzionamento dell'I.A, in quanto non sempre comprensibile all'uomo e quindi fonte di una maggiore difficoltà del suo controllo[14]; il secondo, è legato alla capacità dell'I.A di generare attacchi differenti da quelli precedentemente conosciuti rispetto a sistemi informatici tradizionali[15], infatti l'Intelligenza artificiale è capace di simulare il comportamento umano.

Avendo, detto ciò, il cyberspazio è divenuto, più che una realtà "libera da pregiudizi e controlli", il nuovo campo di battaglia tra potenze mondiali (*cyberwar*) e per criminali (*cybercrime*) e non si tratta solo di attacchi ai singoli partecipanti, ma soprattutto di attacchi diretti alle strutture statali e governative, aziendali e industriali, dal momento che costituiscono il motore di qualsiasi paese. Lo scontro geopolitico si sta sempre più spostando verso la dimensione del cyberspazio, come testimoniato dai recenti conflitti[16]

---

[12] L. V. MARIA SALAMONE, *La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'intelligence e prospettive de iure condendo*, p.4, Federalismi n.23/2017.

[13] C.A CIARALLI, *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, p. 41, n. 15/2023.

[14] Ci si riferisce al fenomeno delle *Black Box* ovvero quando il funzionamento dei sistemi di Intelligenza artificiale appare comprensibile rispetto al comportamento esterno, ma rimane non conoscibile, da qui il termine scatola nera, il funzionamento interno e le modalità con cui il sistema ha prodotto l'output.

[15] ENISA, *Cybersecurity of AI in the AI Act*, 2023.

[16] Per un approfondimento sul tema si veda il testo, *Il Fronte Cyber, Uno speciale sulla cyberwarfare tra guerra in ucraina e Medio Oriente*, dell'ebook di Guerre di Rete.

in Ucraina e alla guerra tra Israele e Hamas, molteplici sono gli attacchi a strutture, servizi essenziali e ad apparati governativi in grado di dirigere il paese.

Per questi motivi, appare quanto mai necessario garantire l'esistenza e l'esercizio dei valori costituzionali[17] anche all'interno del cyberspazio, il quale, come presentato, non costituisce più una dimensione scissa dall'analogico ma la realtà in cui la società vive e agisce. Non si tratta quindi di limitare il cyberspazio, ma di garantire quei diritti fondamentali proteggendo la società e gli stati stessi dalle minacce del mondo cyber.

Perciò, la sicurezza informatica si erge come fondamentale strumento[18] e inoltre, l'evoluzione stessa del termine *cybersecurity*, nella sua accezione olistica, non fa sembrare equivoco constatare come la stessa possa e debba essere ricompresa all'interno dei concetti di sicurezza interna ed esterna menzionati all'articolo 117 comma 2 lettera h) della Costituzione italiana[19].

2. FENOMENOLOGIA

2.1 Criminalità Informatica

Quanto ad attacchi e tipologie di minacce cyber occorre soffermarsi sull'evoluzione che gli stessi hanno subito nel corso del tempo. Inizialmente il fenomeno era circoscritto all'utilizzo dei primi computer, si parla infatti negli anni '90 di *computercrime*, i quali verranno introdotti con la legge n. 547 del 21 dicembre del 1993 nel Codice penale italiano. Dopodiché, con l'avvento di Internet e la nascita del cyberspazio, si riscontra una nuova tipologia di attacchi informatici, i cosiddetti *cybercrime*. Questi ultimi si distinguono per la possibilità di essere realizzati da chiunque abbia accesso al *web*[20] in quanto si servono del cyberspazio. Tale evoluzione tecnologica è stata sottolineata anche sul piano giuridico, come evidenziato dalla pubblicazione della Convenzione di

[17] M.BETZU, Convegno del Gruppo di Pisa il diritto costituzionale e le sfide dell'innovazione tecnologica Università degli studi di Genova 18-19 giugno 2021, *Poteri Pubblici E Poteri Privati Nel Mondo Digitale,* La rivista "Gruppo di Pisa", p.171, Fascicolo n. 2/2021.

[18] A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, A. CADOPPI, *Cybercrime,* p. 53, Milano: UTET Giuridica; 2019.

[19] L.MORONI, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, p. 181, n. 14/2024.

[20] A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, A. CADOPPI, Cybercrime, p. 53, Milano: UTET Giuridica; 2019.

Budapest sulla repressione della criminalità informatica nel 2001, uno dei primi accordi internazionali sui reati commessi tramite Internet o reti elettroniche.

Venendo all'analisi degli autori degli attacchi, spesso si tratta di gruppi di criminali oppure di singoli individui, i quali, per diverse motivazioni, agiscono per ottenere informazioni, chiedere o interrompere servizi, causare danni, effettuare furti di denaro e di identità digitali con lo scopo di compiere truffe o estorsioni[21]. In base alle motivazioni, i cyber attaccanti si dividono in diverse categorie, si parla infatti di cybercriminali quando il gruppo o il singolo sono mossi da scopi economici; seguono i gruppi di terroristi spinti da una violenza ideologica; vi sono poi i cosiddetti *insider threats*, si tratta di minacce provenienti da soggetti interni alle organizzazioni; vi sono anche gli hacktivisti i quali, essendo spinti da ideali politici e sociali, si ergono a giustizieri del mondo cyber, in quanto intervengono in quei contesti giudicati essere immorali o ingiusti; ci sono poi i *thrill-seekers* i quali agiscono per puro divertimento e infine, nel contesto della *cyberwar*, troviamo come attori gli stessi stati-nazioni, in questi casi gli attacchi hanno come oggetto interessi di tipo economico, politico, risorse statali e infrastrutture critiche[22].

Di seguito vengono presentate le principali pratiche di attacco, tra le più frequenti vi sono lo *Spoofing* che permette, grazie ad un mascheramento dell'indirizzo IP o dell'identità, di ingannare sistemi informatici e/o persone apparendo come fonte sicura e affidabile. A riguardo di ciò, vi sono pratiche di *spoofing* che attaccano i *server DNS*, ovvero quei server che traducono l'*URL* digitato in un *browser web* in un unico indirizzo di protocollo *Internet* (IP). Un'ulteriore tecnica di attacco, molto diffusa, consiste nel *Phishing*, attraverso l'invio di *e-mail* e messaggi l'utente è convinto ad aprire file e allegati i quali però contengono un *software* malevolo. In certi casi il soggetto viene ingannato con l'utilizzo di messaggi personalizzati facenti uso di informazioni ricavabili con la pratica del *social engineering*[23], la quale, sfruttando il fattore umano, utilizza tecniche per manipolare e ricavare informazioni personali. Con l'utilizzo dell'Intelligenza artificiale, il *social engineering* ha registrato un aumento della capacità di impatto, in quanto, grazie

[21] R. CASTROREALE, *Cybersecurity per tutti*, p.32, EPC Editore 2024.

[22] Canadian Centre Cyber Security, *An introduction to the Cyber Threat Environment p.2, 2023 – 2024*.

[23] Per un approfondimento sul tema si veda F. SALAHDINE and N. KAABOUCH, *Social Engineering Attacks: A Survey*, Future Internet 2019, School of Electrical Engineering and Computer Science, University of North Dakota.

all'I.A è possibile generare contenuti video, vocale e immagine realistici e altamente in grado di ingannare la vittima. Successivamente vi sono quelle pratiche che mirano all'interruzione dell'erogazione dei servizi, rendendoli indisponibili come il *Distribuited Denial of Service (DDoS)* per poi procedere con una richiesta di riscatto.

I *Malware* invece, tramite virus e *software* dannosi, possono rubare, criptare, danneggiare o prendere il controllo dei dati e del sistema. Nei casi di tentativi di accesso a sistemi o *file*, si parla di *Brute Force Attack* (attacco di forza bruta) si tratta di attacchi ripetuti nel tentativo di indovinare la *password* di protezione. Infine, vi sono i casi di *password sniffing* e *network sniffing*, si tratta dell'individuazione di password e traffico di rete che non utilizzano sistemi adeguati di sicurezza, ad esempio informazioni in transito su reti Wi-Fi libere e chiavi di accesso condivise senza aver impiegato tecniche crittografiche.

Le pratiche presentante sono solo alcune delle strategie principali di attacco a sistemi e soggetti, è importante sottolineare come il tema della sicurezza informatica includa in modo significativo il comportamento umano e non solo la capacità di resilienza dei sistemi informatici[24].

2.1.1 Attacchi alle strutture pubbliche

Le strutture pubbliche sono tra gli obiettivi più colpiti sia da cybercriminali sia nel contesto della *cyberwar*. Le principali ragioni sono di tipo strategico, infatti tali strutture fungono da coordinamento dell'assetto statale, un ulteriore punto, consiste nel fatto che le pubbliche amministrazioni detengono una grande mole di dati, si pensi al solo settore sanitario o anche alle amministrazioni comunali, la quantità di dati personali e sensibili è davvero significativa. Per la criminalità informatica, ma anche in un contesto di scontro che esula dai confini, si pensi quindi alla cyberguerra, i dati entrano nel mirino degli attaccanti proprio per il valore delle informazioni contenute in essi. Da un lato la loro sottrazione comporta la conoscenza di informazioni strategiche (si pensi a informazioni militari o di sicurezza statale), dall'altro, come dimostra la prassi, la loro detrazione comporta richieste di riscatto a cui segue la minaccia di rendere indisponibili tali preziose informazioni. Nello stesso Rapporto CLUSIT sulla Sicurezza ICT in Italia 2024

[24] L. PIER MONTESSORO, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, Istituzioni del Federalismo, p.784, 2019.

si è sottolineata la portata di questo fenomeno «siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'ICT e della stessa Cyber Security, ed hanno impatti profondi, duraturi e sistemici[25]». Difatti, come emerso nel rapporto, essendo mutato lo scenario geopolitico, l'Italia sembra essere entrata nel mirino di gruppi di cybercriminali, in particolare di quelle organizzazioni affiliate a stati che vedono il continente Europeo come nemico. Inoltre, emerge come siano in aumento i *cybercrime*, anche se una percentuale consistente di attacchi, è originata dalle vulnerabilità nei sistemi[26] il cui impatto critico ha registrato un incremento rispetto agli anni precedenti.

Per quanto concerne il settore pubblico, anch'esso registra un importante aumento degli attacchi in virtù del fatto che «I rischi cyber hanno ormai assunto una natura esistenziale, ed è urgente adeguare al nuovo scenario le misure di prevenzione e protezione, a tutti i livelli (pubblica amministrazione, aziende pubbliche e private), onde evitare di subire danni inevitabilmente crescenti[27]». Le pubbliche amministrazioni, sia centrali sia a livello locale, si trovano in difficoltà in quanto non dispongono ancora di una struttura e governance "cyber" adeguate, per questo negli ultimi anni vi sono stati passi decisivi per una politica della digitalizzazione volta alla creazione di un vero e proprio apparato di sicurezza informatica nazionale. Lo scenario è da attenzionare come dimostrato nel caso Westpole[28], infatti, a dicembre 2023 il provider di servizi *Westpole* ha subito un attacco *ransomware* da parte del gruppo criminale *Lockbit*[29] che ha reso per diversi giorni indisponibili i servizi che il provider fornisce a PA Digitale[30], la quale a sua volta serve circa più di un migliaio di pubbliche amministrazioni e all'incirca cinquecento comuni. Alcune amministrazioni sono state forzate a ritornare ad un'attività analogica per

[25] Clusit Rapporto 2024 sulla Sicurezza ICT in Italia.

[26] Ibidem p.29.

[27] Ibidem p.10.

[28] Sul caso si veda *Westpole PA digitale il vero conto del disastro enorme*. https://www.cybersecurity360.it/nuove-minacce/westpole-pa-digitale-il-vero-conto-del-disastro-enorme/

[29] Di seguito si veda il seguente articolo inerente il gruppo cybercriminale Lockbit. https://www.corriere.it/tecnologia/23_dicembre_19/chi-sono-i-russi-di-lockbit-hacker-che-hanno-bloccato-la-pubblica-amministrazione-politica-contano-solo-i-soldi-695b2492-8908-4e12-993c 5cb23941dxlk.shtml

[30] Si tratta del sito del Dipartimento per la trasformazione digitale che permette alla PA di accedere ai fondi di Italia digitale 2026. Il sito è il punto di accesso per avere informazioni sugli avvisi dedicati alla digitalizzazione della PA, alla richiesta di accesso ai fondi e rendicontare l'avanzamento dei progetti. Può essere richiesta assistenza diretta per tutte le informazioni sulle azioni di accompagno previste dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri.

affrontare le difficoltà riscontrate, i settori colpiti hanno riguardato i servizi di pagamento digitali offerti ai cittadini, posta elettronica certificata, sistema di gestione delle carte di identità e anagrafe e lo sportello unico attività produttive. Il caso Westpole è uno degli eventi più eclatanti e recenti ma è opportuno ricordare come giornalmente vi siano tentativi di attacco di cui solo una parte ha successo.

In conclusione, appare chiaro come le amministrazioni pubbliche debbano richiamare l'attenzione sulla sicurezza informatica quanto a vulnerabilità, prevenzione, resilienza dei sistemi e formazione del personale. Tale attività non deve avvenire al solo interno ma anche e soprattutto tramite un'azione di accertamento del rispetto delle misure di sicurezza anche nei confronti dei terzi e fornitori di servizi, in modo da adottare un approccio olistico della sicurezza informatica.

CAPITOLO II

LA CENTRALITÀ DELLA DIGITALIZZAZIONE PER LA P.A

In questo capitolo viene sottolineata l'importanza della digitalizzazione per la pubblica amministrazione, portando il lettore a riflettere sul concetto di amministrazione digitale, la quale deve essere in grado di garantire l'esercizio dei diritti dei cittadini anche in un contesto sempre più digitale. Verranno affrontate le tappe fondamentali di tale percorso e le difficoltà attuative, per approdare ad un punto snodale dell'elaborato; si tratta di evidenziare il legame tra l'amministrazione digitale e la cibersicurezza partendo dal concetto stesso di cittadinanza e dai significati racchiusi dentro essa. Il nesso è individuabile, in prima battuta, nel principio costituzionale del Buon andamento della pubblica amministrazione, e in secondo luogo, nella sicurezza pubblica e ordine pubblico.

1. AMMINISTRAZIONE DIGITALE

1.1 Pubblica amministrazione e digitalizzazione

Negli ultimi decenni, si è assistito a un significativo cambio di paradigma, le cui radici affondano nello studio della cibernetica dei primi anni '50. Questo cambiamento è stato ulteriormente accelerato dall'invenzione di *Internet*, dalla diffusione delle Tecnologie dell'Informazione e della Comunicazione (TIC), dai primi mezzi di comunicazione digitali e, più recentemente, dallo sviluppo dell'Intelligenza Artificiale. Siamo partecipi di un cambiamento segnato dalla tecnologia, la quale permea ogni circostanza della nostra vita e, come emerso in vari studi, si sta delineando una nuova "realtà", si è parlato infatti di «mondo-dato[31]», «infosfera e onlife[32]» cyberspazio e «dataismo[33]».

Tuttavia, dal momento che la digitalizzazione coinvolge molteplici aspetti della vita di ogni individuo e della società in sé, è inevitabile chiedersi come tale cambiamento

[31] C. SARRA, *Il Mondo-dato, Saggi su datificazione e diritto,* Cleup, 2019.

[32] L. FLORIDI, *La quarta rivoluzione come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017.

[33] Y. N. HARARI, *Homo Deus Breve storia del futuro*, Bompiani, p.449, 2015.

influisca sulla «soddisfazione delle scelte dei cittadini e di quelle collettive[34]» ovvero alla funzione svolta dalla pubblica amministrazione. Se si guarda alla storia dell'evoluzione statale italiana, l'amministrazione pubblica ha esteso la propria funzione in numerosi ambiti; pensiamo alla sanità, trasporti e all'istruzione, facendo uso del digitale seppure con qualche ritardo rispetto al settore privato. Inoltre, l'utilizzo da parte della collettività delle tecnologie e dell'informatica, esorta, in prima battuta, l'apparato pubblico a una forma di comunicazione differente ma soprattutto poi ad un cambio di forma di organizzazione e di prospettiva[35]. A sostengo di ciò vi è il pensiero di Lessing, il quale aveva identificato nel potere pubblico quel soggetto più «drammaticamente segnato dal passaggio dall'azione umana[36]». Tale affermazione risuona con una tale evidenza, in un contesto in cui le possibilità del digitale sembrano avvicinare ancor di più il servizio pubblico alle esigenze del cittadino.

Si evince come sia cruciale il ruolo della pubblica amministrazione in quanto assume un «ruolo guida nella impostazione e definizione di un modello desiderabile di applicazione delle tecnologie emergenti ai cittadini[37]» in quanto, essendo lo Stato a direzionare tale cambiamento per il proprio assetto, il diritto amministrativo funge da esempio anche per gli altri settori del diritto. Oltretutto, nella storia dello Stato non si era ancora registrata l'azione di un agente esterno, come la tecnologia, così impattante da richiedere un riassetto organizzativo e strutturale. La tecnologia progredisce e avanza inesorabilmente a tal punto che la sua velocità ha influenze sulla regolamentazione, il controllo, e questi ultimi sono soggetti al rischio di divenire in breve obsoleti, per questi motivi il potere pubblico sembra fronteggiare un inevitabile cambiamento comprensivo di ogni ambito della vita[38].

---

[34] G. PESCE, *Dottrina e attualità giuridiche, Diritto amministrativo e intelligenza artificiale: problemi*, Giurisprudenza Italiana, p. 1509, Giugno 2022.

[35] F. MUSELLA, *Digital regulation: come si cambia la Pubblica Amministrazione*, Rivista di Digital Politics, fascicolo gennaio-agosto 2022.

[36] G. PESCE, *Dottrina e attualità giuridiche, Diritto amministrativo e intelligenza artificiale: problemi*, Giurisprudenza Italiana, p. 1510, Giugno 2022.

[37] Ibidem.

[38] L.TORCHIA, *Lo Stato digitale, Una introduzione*, Il Mulino, p.21, 2023.

1.2 Le tappe fondamentali del percorso verso un'amministrazione digitale

Il «processo di digitalizzazione»[39] non è nuovo ma è frutto di un percorso che ha le sue radici negli anni Sessanta, al tempo la tecnologia non presentava il carattere pervasivo oggi più che mai attuale, ma, era assunta, come quell'elemento di novità fonte di preoccupazioni per la tutela della riservatezza e sull'uso di informazioni personali da parte della pubblica amministrazione. Se da un lato, l'elaboratore elettronico poteva rafforzare, per quanto discretamente, il funzionamento delle attività della pubblica amministrazione, dall'altro si era testimoni di una «informatica costretta ad adeguarsi all'amministrazione»[40], ciò dovuto anche alla difficoltà nel reperire la strumentazione tecnologica. Le pubbliche amministrazioni si affacciavano al preludio della digitalizzazione, la quale avrebbe portato, attraverso una serie di riforme e piani di azione, all'amministrazione digitale di cui oggi siamo attori e partecipi. Nonostante le prime titubanze, vi era chi percepiva nella tecnologia quella spinta al cambiamento, come sottolineato dallo studioso Vittorio Frosini in merito all'elaboratore elettronico applicato ai servizi amministrativi. È in questo periodo che si delinea, insieme all'avanzare della tecnologia, la necessità di un cambiamento dell'organizzazione, formazione e cultura amministrativa, come già evidenziato nel Rapporto Giannini del 1979. È da notare come lo stesso autore avesse rilevato «[…] che i sistemi informativi non servono più alle amministrazioni per fatti di gestione interna, ma servono proprio per amministrare, si proiettano cioè sempre più verso l'esterno»[41] sottolineando non solo l'utilità strumentale, ma anche la funzionalità dell'elaboratore elettronico, funzionalità che si estende al cittadino e non rimane racchiusa all'interno del contesto istituzionale.

A partire dagli anni Ottanta, si assiste ad un incremento della spesa pubblica nelle tecnologie, tuttavia, la produttività delle amministrazioni fornisce scarsi risultati. Questo slancio ha trovato impreparate le pubbliche amministrazioni, e le proposte contenute nel rapporto Giannini, seppur ambiziose, non hanno avuto uno sviluppo concreto[42]. Come

---

[39] F. MUSELLA, *Digital regulation: come si cambia la Pubblica amministrazione*, (Rivista di Digital Politics, Fascicolo 1-2, p. 3, gennaio-agosto 2022.

[40] A. NATALINI, *Come il passato influenza la digitalizzazione delle amministrazioni pubbliche,* Rivista di Diritto Pubblico n.1, p.98, 2022.

[41] Rapporto GIANNINI, paragrafo 3.7, 1979.

[42] F. MUSELLA, *Digital regulation: come si cambia la Pubblica amministrazione*, (doi: 10.53227/105064), Rivista di Digital Politics (ISSN 2785-0072) Fascicolo 1-2, p. 5, gennaio-agosto 2022. Si veda per maggiori

evidenziato da Sabino Cassese nel rapporto[43] del 1993 questa prima spinta innovativa sembra avere corrisposto più ad un fine di offerta in un contesto di interventi per lo sviluppo dell'informatica invece di andare ad agire sulla rigidità dell'organizzazione amministrativa.

Bisognerà aspettare gli anni Novanta perché si possa trattare di un concreto avvio alla digitalizzazione. È in questa fase che riemergono le proposte evidenziate da Giannini, con la creazione dell'Autorità per l'informatica nella pubblica amministrazione (AIPA)[44] presso la Presidenza del consiglio nel 1993 con l'obiettivo di favorire l'utilizzo delle ICT. Inoltre, vede avvio il progetto per una Rete Unitaria della pubblica amministrazione (RUPA), con il fine di stabilire una connessione, compartecipazione tra le amministrazioni[45]. Un ulteriore sviluppo avviene con la pubblicazione delle Leggi Bassanini, in particolare l. 15 marzo del 1997 artt. 15 e 20 nei quali si sancisce il pari valore tra il documento elettronico e cartaceo, oltre alla necessità e ai vantaggi di un impiego maggiore delle tecnologie verso gli amministrati. È infatti da questo momento che l'azione del digitale pone l'accento sulla comunicazione, non solo tra pubbliche amministrazioni ma anche verso i cittadini.

Negli anni Duemila i governi Berlusconiani apportano un cambiamento significativo alla *governance* della funzione pubblica, di fatti in precedenza, la direzione era in capo del Ministro per la funzione pubblica, ora viene affidata al nuovo Ministero per l'innovazione e le tecnologie. Quello che preme sottolineare è l'ingresso di figure del settore privato come conduttori della politica digitale, primo fra tutti Lucio Stanca, il quale sarà apripista di una scelta politica che verrà portata avanti anche dai governi successivi. In questi anni hanno fatto seguito ulteriori norme in materia di comunicazione pubblica, riordino delle disposizioni pubbliche, l'accesso di utenti con

---

approfondimenti A. Natalini, *Come il passato influenza la digitalizzazione delle amministrazioni pubbliche,* Rivista di Diritto Pubblico n.1, p.100-102, 2022.

[43] Etica PA, La PA è la comunità dei cittadini. https://www.eticapa.it/eticapa/la-foresta-incantata-rapporto-cassese-del-1993-sulle-condizioni-delle-pubbliche-amministrazioni/#more-5021

[44] AIPA venne istituito con il d. lgs. 39/1993, con lo scopo di coordinare le pubbliche amministrazioni all'utilizzo e formazione in materia di informatica. Successivamente con il d. lgs.196/2003 (Codice in materia di protezione dei dati personali) ha trasformato l'AIPA nel Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA). Infine, con il d. legisl. 177/2009, il CNIPA è stato trasformato nell'Ente nazionale per la Digitalizzazione della Pubblica Amministrazione (DigitPA) poi soppresso dal Governo Monti che istituì l'agenzia per l'Italia Digital (AGID).

[45] A. NATALINI, *Come il passato influenza la digitalizzazione delle amministrazioni pubbliche,* Rivista di Diritto Pubblico n.1, p.104, 2022.

disabilità e l'istituzione della Posta Elettronica Certificata[46]. Di particolare importanza è stato il riordino, nel 2005, delle disposizioni amministrative vigenti nel Codice dell'Amministrazione Digitale[47] (CAD) il quale metterà in luce non solo il concetto di digitalizzazione del servizio pubblico ma anche il tema dei diritti digitali e la sicurezza informatica. Tuttavia, come evidenziato da Natalini, spesso il CAD subirà modifiche e integrazioni normative, le quali sembrano essere più il frutto della volontà dei governi succedutisi di comunicare ai cittadini «[…] l'impegno profuso a colmare i ritardi della digitalizzazione del settore pubblico»[48]. Inoltre, l'azione dei governi successivi ha portato ad una dualità dei vertici amministrativi, che di fatto ha separato le politiche di riforma organizzative delle amministrazioni dal percorso di digitalizzazione[49].

Nonostante la difficoltà nella *governance* pubblica, tra il 2010 - 2019 si sono poste importanti basi per lo sviluppo delle piattaforme digitali quali PagoPA e SPID. Inoltre, con la legge 7 agosto 2015 n.124, Legge Madia, si è sottolineato il passaggio dalla digitalizzazione della comunicazione, al potenziamento dei diritti del cittadino, ciò sottolineato dall'adozione della Carta della cittadinanza digitale.

Un'ulteriore presa di coscienza avviene con la pandemia nel 2020, in questo caso la pubblica amministrazione dovette forzatamente cambiare paradigma non solo nella comunicazione con l'amministrato, ma anche nel modo in cui la stessa svolgeva le proprie funzioni. A livello europeo, è stato adottato il Next Generation EU corrispondente a livello nazionale al Piano nazionale di ripresa e resilienza PNRR, si tratta di una «riforma strumentale al conseguimento degli obiettivi contenuti nei tre assi strategici: transizione digitale, la transizione ecologica e l'inclusione sociale all'interno della quale stanno le politiche per ridurre il divario territoriale[50]». Tra gli obiettivi vi sono una strategia *cloud* nazionale, il potenziamento delle infrastrutture digitali,

---

[46] G. ZICCARDI e P. PERRI, *Tecnologia e Diritto Volume II, Informatica Giuridica Data Governance, protezione dei dati e GDPR, mercato unico digitale, blockchain, Pubblica Amministrazione digitale,* Giuffrè Francis Lefebvre, p. 220, 2019.

[47] D.lgs 7 marzo 2005, n.82.

[48] A. NATALINI, *Come il passato influenza la digitalizzazione delle amministrazioni pubbliche,* Rivista di Diritto Pubblico n.1, p.107, 2022.

[49] Ci si riferisce al caso in cui il governo Renzi ha dato luce a due strategie di rinnovo separate tra l'AGID e il nuovo team per la trasformazione digitale affiancato alla Presidenza del Consiglio dei Ministri, poi confluito con il governo Conte I nel neo dipartimento per la Trasformazione digitale di supporto al ministro per l'innovazione tecnologica e la transizione digitale.

[50] N. GIANNELLI, *Il cammino delle riforme della pubblica amministrazione nella svolta pragmatica del PNRR*, p. 45, 2021.

interoperabilità e dati, l'incremento dei servizi digitali e cittadinanza digitale, supporto alla trasformazione della PA locali, previsione di un piano per le competenze digitali di base, e infine misure di rafforzamento della sicurezza informatica, tema che, come vedremo, assumerà sempre di più un ruolo essenziale e strumentale per l'amministrazione.

1.2.1 Amministrazione digitale i principi del CAD: alcune riflessioni

Dopo un excursus sulle tappe fondamentali della digitalizzazione si volge lo sguardo al tema dell'amministrazione digitale, la quale, come si vedrà, ha radici nel testo costituzionale.

L'articolo 117, secondo comma, lettera "r" della Costituzione, riconduce la potestà legislativa in materia di sistemi informativi-statistici e informatici dei dati alla pubblica amministrazione; con l'obiettivo di promuovere un uso condiviso che non sia caratteristica di solo alcune realtà, ma che sappia portare ad una condivisione di metodologie in considerazione anche delle Regioni e autonomie. Ancora una volta, si manifesta il ruolo guida del diritto amministrativo nella rivoluzione digitale.

Successivamente, la legge generale sul procedimento amministrativo (l. n. 241/1990) è stata modificata con l'aggiunta dell'articolo 3 – bis (Legge 11 febbraio 2005, n. 15) il quale, è stato modificato dall'art. 12, comma 1, lett. b) del D.L. 16 luglio 2020, n. 76 (convertito con modificazioni dalla L. 11 settembre 2020, n. 120) e «stabilisce una connessione fra il ricorso all'informatica e l'efficienza amministrativa[51]». Tale connessione, nella formulazione più recente è stata rivista in modo assertivo in quanto «le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati[52]», infatti non si tratta più "incentivare all'uso della telematica" ma di un "utilizzo" da parte della stessa P.A, sottolineando la strumentalità della tecnologia sia per il funzionamento dell'amministrazione sia nei rapporti con il cittadino.

Arrivando alla disciplina del CAD, il testo si prefigge di riordinare e raccogliere la normativa relativa alla trasformazione digitale, applicabile alle pubbliche

[51] L.TORCHIA, *Lo Stato digitale, Una introduzione*, il Mulino, p.98, 2022.

[52] Art. 3 bis legge sul procedimento amministrativo. https://www.brocardi.it/legge-sul-procedimento-amministrativo/capo-i/art3bis.html

amministrazioni, gestori dei servizi pubblici e alle società in controllo pubblico escluse quelle quotate in borsa.

Una delle prime tematiche trattate concerne i diritti dei cittadini nei confronti dell'amministrazione digitale, in capo ai quali viene riconosciuto il diritto di utilizzare la tecnologia e come tale, deve essere accessibile ed efficace. Di conseguenza le comunicazioni con l'amministrazione devono avvenire tramite l'utilizzo delle tecnologie, ma non solo, anche l'esercizio del diritto di accesso alle informazioni soggette al trattamento e al procedimento amministrativo. A fronte di ciò, sono previsti degli obblighi in capo alle amministrazioni, come il garantire servizi online semplici e integrati (Art. 7) anche attraverso l'utilizzo dei dispositivi mobili con autenticazione tramite l'identità digitale, l'obbligo di connettività alla rete negli uffici pubblici (Art. 8-bis) e l'obbligo di utilizzo di un fascicolo informatico (art. 41). Le amministrazioni pubbliche sono chiamate a rispettare apposite norme in materia di privacy, trasmissione dei dati e trattamento, garantendo l'accesso e la trasparenza e; dal momento che le amministrazioni sono detentrici di una mole considerevole di dati personali e sensibili, sono necessarie misure di cibersicurezza col fine di prevenire e monitorare accessi abusivi e veri e propri furti di dati.

In relazione a ciò, le amministrazioni, secondo la disciplina del CAD, devono acquisire i sistemi informatici sulla base di principi come l'economicità ed efficienza, la tutela degli investimenti, la neutralità tecnologica e il riuso (Art. 68). Le pubbliche amministrazioni sono quindi chiamate ad effettuare una valutazione sugli strumenti tecnologici da adottare, con particolare riguardo alle caratteristiche del prodotto come la tecnologia, compresa l'Intelligenza artificiale, la progettazione e la sicurezza informatica.

Avendo dato uno sguardo sulle tappe e politiche di digitalizzazione e ai principi istituiti dal CAD, occorre svolgere una riflessione sulle difficoltà affrontate dalle pubbliche amministrazioni nel garantire un servizio digitale come lo stesso CAD stabilisce. Il primo punto riguarda la governance della digitalizzazione, la quale è stata spesso oggetto di frammentazioni e di un coordinamento che non ha saputo imprimere con efficacia l'obiettivo posto dal legislatore. Inoltre, il susseguirsi di governi ha fatto si che ogni rappresentanza politica imprimesse la propria strategia, portando, in alcune occasioni, a netti cambi di direzione. Il risultato è stato quello di una digitalizzazione a macchia di leopardo che ha evidenziato un divario tra le regioni del nord, centro e sud Italia e di

una troppa procedimentalizzazione che di fatto ha reso tale processo farraginoso. Ulteriormente, è da chiedersi se gli approcci alla digitalizzazione (il più recente costituito dal PNRR) «di rilevanza sistemica e standardizzati[53]» siano la strategia più efficace per rispondere ad una digitalizzazione differenziata sia geograficamente sia dal punto di vista delle realtà amministrative. In seguito, il divario tra il settore privato e quello pubblico rischia di accentuarsi ancora di più se non si attuano strategie di partenariato che pongano al centro l'amministrazione, cioè la realizzazione di piani di digitalizzazione che tengano in considerazione le vere esigenze pubbliche e seguano un approccio a lungo termine; in modo da realizzare un'amministrazione che non abbia necessità di un aiuto di tipo strutturale, ma strumentale da parte dell'azione privata. Un ulteriore punto ha come oggetto le competenze digitali del settore pubblico, le cui difficoltà sono emerse in occasione della pandemia. Infatti, la gestione delle risorse umane necessita di piani di formazione e competenza che superino il legame con l'analogico e abbiano un approccio a lungo termine. Questo comporta non solo fondamentali cambiamenti in merito alla forza lavoro ma alla stessa organizzazione, la quale deve essere idonea a rispondere alle esigenze dei cittadini. Tuttavia, è bene notare come negli ultimi anni si è registrato un andamento positivo con l'emergere di nuove realtà digitali anche nel mezzogiorno, come testimoniato dall'"Indagine sulla maturità digitale dei Comuni capoluogo[54]" del 2024. Ulteriormente, come sottolineato nel *Report on the State of the Digital Decade 2024*[55], si è registrata una graduale crescita dei servizi online offerti dalle pubbliche amministrazioni, grazie alla realizzazione di piattaforme digitali e numerosi progetti in corso, anche se è necessario attenzionare maggiormente alcuni temi. In questi ultimi, rientrano le competenze digitali, il divario digitale e l'adozione dell'intelligenza artificiale «*Italy made progress in the area of e-government, in particular in e-health and key digital public services for businesses and continued to advance on*

[53] E. SORRENTINO e A.F SPAGNUOLO, *Le sfide degli enti locali: tra PNRR e gap digitali,* Federalismi rivista di diritto pubblico italiano, comparato, europeo, p. 169, 9 agosto 2023.

[54] I risultati della ricerca sono stati presentati il 22 Maggio 2024 al "FORUM PA 2024". La ricerca, realizzata da FPA per Deda Next, società di Dedagroup, ha analizzato lo stato di avanzamento delle amministrazioni comunali italiane negli obiettivi di digitalizzazione individuati dalle strategie nazionali, secondo il modello Ca.Re. (*Cambiamento Realizzato*) di Deda Next.

[55] Si veda il Report sul sito ufficiale della Commissione Europea. https://digital-strategy.ec.europa.eu/en/policies/2024-state-digital-decade-package

gigabit networks roll-out. […] particularly important challenges persist in digital skills, while Italian enterprises lag behind in the adoption of advanced technologies such as AI[56]».

Inoltre, come sottolineato nel primo capitolo, relativamente al "fattore umano", le amministrazioni sono tra le più soggette ad attacchi informatici. Inoltre, la sicurezza non dipende solamente dall'organizzazione pubblica, ma anche dalla sicurezza dei singoli[57], la quale rientra nell'alveo delle competenze digitali in quanto è fondamentale la crescita di una consapevolezza digitale e la percezione del rischio.

2. LA P.A E IL LEGAME CON LA SICUREZZA INFORMATICA

2.1 Polimorfismo della cittadinanza

Una riflessione che va di pari passo rispetto a quella sul tema della digitalizzazione verte sulla cittadinanza digitale, tale termine è apparso ripetutamente anche nel nostro ordinamento giuridico[58]. Il concetto di cittadinanza ha matrice nello status di appartenenza ad uno stato-ordine politico, ed è strettamente connesso alla sovranità e quindi ad un contesto in cui il riconoscimento del concetto di persona non trova ancora piena espressione. Tuttavia, essendo lo stesso concetto di cittadinanza legato alla persona, nei secoli lo stesso ha subito un'ineluttabile evoluzione, la quale ha portato a "forme" differenti di cittadinanza. Attraverso cambiamenti culturali, sociali, storici, filosofici, politici, il concetto di cittadinanza si è disancorato dall'appartenenza ad un ordine sovrano, il quale ha oppresso l'espansione del patrimonio giuridico della persona. Vediamo infatti che, accanto ad una cittadinanza nazionale, si è affiancata, ed è per sua stessa natura complementare, una cittadinanza europea prima e una cittadinanza cosmopolita poi. Allo stesso tempo si è originata una cittadinanza amministrativa, la

[56] Commissione Europea, Pacchetto sullo stato del decennio digitale 2024, allegato 3 "Corte relazioni dei 27 Stati membri dell'UE" Italy. https://digital-strategy.ec.europa.eu/it/policies/2024-state-digital-decade-package

[57] R. BRIGHI e C. PIER GIORGIO, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* Federalismi, 8 settembre, n.21, 2021.

[58] Si veda il d.lgs 82/2005 Codice dell'Amministrazione Digitale nel quale si fa riferimento al fascio di diritti e doveri del cittadino introdotti e con le modifiche e integrazioni del d.lgs 217/2017 alla II sezione denominata "Carta della cittadinanza digitale" e anche nel nuovo Codice degli Appalti Pubblici.

quale ha come fondamento l'appartenenza della persona ad una comunità e idoneità ad esercitare un fascio di diritti e doveri in capo al cittadino.

Avendo premesso ciò, è possibile identificare come la digitalizzazione attraversi le varie forme di cittadinanza «in modo trasversale[59]». La motivazione riguarda la realtà in cui il cittadino si trova, la quale non vede una scissione tra il piano analogico e digitale, ma osserva il consolidamento tra queste due realtà destinata ad evolvere in infosfera[60], dove il denominatore comune è ricondotto alla digitalizzazione. Lo stesso Consiglio d'Europa accoglie la definizione di cittadinanza digitale definendola come la capacità «*to partecipate actively, continuously and responsibly in communities (local, national, global, online and offline) all levels (political, economic, social, cultural and intercultural)*[61]». In questo passaggio viene in luce l'evoluzione della cittadinanza, la quale muove verso una natura meno esclusiva e di appartenenza alla sovranità. Infatti, in tale definizione emerge il polimorfismo[62] del concetto di cittadinanza, facendo richiamo ai due piani – *online e offline* – e non solo ma anche alle dimensioni – locale, nazionale e globale – le quali sono tutte concatenate tra loro.

2.1.1 Cittadinanza digitale e Principio del Buon andamento della P.A

Ulteriore passaggio, di fondamentale importanza, consiste nel legame tra la cittadinanza digitale e la sicurezza informatica, connessione che, in virtù della centralità della digitalizzazione per la pubblica amministrazione, della polimorfia del significato di cittadinanza, si può ricondurre ai principi di Buon andamento e imparzialità della nostra Costituzione presenti all'articolo 97. Tali principi racchiudono in sé l'obbligo delle pubbliche amministrazioni di amministrare e agire in modo trasparente, efficace,

---

[59] E.N. FRAGALE, *La cittadinanza amministrativa al tempo della digitalizzazione,* Rivista di Diritto amministrativo n.2, p.481, 2022.

[60] Come lo stesso Luciano Floridi riferisce in *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*. Milano Raffaello Cortina Editore, 2017. "È il mondo che si sta adattando all'AI e non viceversa".

[61] Citato in M. PIETRANGELO, *Sui "diritti di cittadinanza digitale". Note a margine di un opaco percorso normativo,* n.8, p.131, 3 aprile 2024.

[62] A riguardo si veda il passaggio di E.N. FRAGALE, *La cittadinanza amministrativa al tempo della digitalizzazione,* Rivista di Diritto amministrativo n.2, p.487, 2022. L'autore tratteggia il polimorfismo assunto dai diritti di cittadinanza amministrativa all'interno della Dichiarazione Europea dei principi e diritti digitali.

responsabile, secondo il criterio dell'economicità per la realizzazione dei diritti dei cittadini affinché le decisioni vengano prese nell'interesse migliore della collettività.

Sebbene la ratio del testo costituzionale non abbia come centralità la definizione dei diritti del cittadino nei confronti dell'amministrazione, ma stabilisca i poteri e principi per l'esercizio della funzione pubblica, sembra potersi delineare un diritto della persona o una pretesa soggettiva "alla buona amministrazione". Ciò sarebbe possibile in virtù del «rapporto di strumentalità immediato e necessario esistente tra la (buona) amministrazione e la realizzazione degli interessi fondamentali inerenti alla persona[63]». La strumentalità di cui si discute (la quale trova fondamento anche nella Carta dei diritti fondamentali dell'Unione Europea Art. 43 Diritto ad una buona amministrazione[64]), consiste nel creare un'amministrazione sempre più vicina al cittadino, che sia in grado di consentire allo stesso una partecipazione attiva al perseguimento di un interesse generale (Articolo 118 Costituzione)[65] in ragione di un contesto digitale e di una partecipazione digitale del cittadino (si veda la cittadinanza digitale)

Per cui, una buona amministrazione, al giorno d'oggi, deve essere intesa come necessariamente digitale e quindi anche capace di offrire un servizio continuo, sicuro e accessibile. Per questi motivi è possibile includere la sicurezza informatica nel concetto di Buona amministrazione[66], in quanto un'amministrazione per utilizzare e offrire servizi digitali al cittadino deve in modo necessario dotarsi di piani di cibersicurezza. Oramai, il non disporre di tali piani comporta, in caso di attacco, una possibile lesione dei diritti

[63] Ivi p.492.

[64] Art. 43 Diritto ad una buona amministrazione 1. Ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione. 2. Tale diritto comprende in particolare: a) il diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio; b) il diritto di ogni persona di accedere al fascicolo che la riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale e commerciale; c) l'obbligo per l'amministrazione di motivare le proprie decisioni. 3. Ogni persona ha diritto al risarcimento da parte dell'Unione dei danni cagionati dalle sue istituzioni o dai suoi agenti nell'esercizio delle loro funzioni, conformemente ai principi generali comuni agli ordinamenti degli Stati membri. 4. Ogni persona può rivolgersi alle istituzioni dell'Unione in una delle lingue dei trattati e deve ricevere una risposta nella stessa lingua. https://fra.europa.eu/it/eu-charter/article/41-diritto-ad-una-buona-amministrazione

[65] Il principio di sussidiarietà orizzontale prevede per la sua realizzazione che vengano tessuti rapporti fra soggetti pubblici e soggetti privati per il perseguimento di un interesse comune ad entrambi, l'interesse generale.

[66] E. SALERNO, *La cybersecurity amministrativa il buon andamento informatico,* Privacy e Cybersecurity, p.16, 2020.

fondamentali del cittadino, basti pensare al furto di dati o all'inoperatività dei sistemi di pagamento pubblico digitale, le cui conseguenze possono comportare una lesione della privacy, ritardi nei pagamenti, rispetto al diritto di accesso, nell'avvio del procedimento amministrativo, il tutto ricorda una meccanicità tipica di un'amministrazione legata all'analogico.

2.2 Ordine pubblico e sicurezza pubblica

Il termine ordine pubblico e sicurezza pubblica vengono introdotti dal Regio Decreto all'Art. 2 del Testo unico delle leggi di pubblica sicurezza (TULPS) del 1926. Il testo fa riferimento alla facoltà attribuita al Prefetto di adottare provvedimenti indispensabili, in caso di urgenza o grave necessità pubblica «[…] per la tutela dell'ordine e della sicurezza pubblica[67]». Il lemma, emerso nel TULPS, risale al periodo fascista ed è connotato dalla necessità di consolidare quelle attività di controllo della polizia esercitate da parte del regime. A seguito dell'instaurazione della Repubblica, nel testo costituzionale, fino al 2001, era presente solamente il termine "sicurezza pubblica", ma a seguito della riforma costituzionale è stato introdotto l'articolo 117. Al secondo comma alla lettera h) vi si ritrova l'espressione "ordine pubblico e sicurezza" all'interno delle competenze esclusive statali, tale espressione viene infatti definita una «endiadi[68]» con il fine di sottolineare come la sicurezza e l'ordine pubblico vengano considerati «in senso collettivo[69]».

Quindi, prima della riforma costituzionale dei primi anni Duemila, i concetti di ordine pubblico e sicurezza pubblica si trovavano ad essere disgiunti, ma con quanto sostenuto dalla Corte costituzionale[70], si perviene ad un chiarimento del rapporto tra i due concetti «non si tratta di sinonimi, ma di espressioni da valorizzarsi nel loro contenuto autonomo, sebbene esse risultino parzialmente sovrapponibili e tra loro complementari[71]». Sicché il

---

[67] Quaderni istituzionali, *La funzione di sicurezza nella legalità costituzionale*, n. 4, 2014, p.989-998 citato nel testo di O. CARAMASCHI, *Dall'ordine pubblico alla sicurezza: una prospettiva di teoria costituzionale* rivista Democrazia e Sicurezza, n.1, p.102, 2023.

[68] G. SESSA, *L'esigenza di sicurezza pubblica: tra diritto e partecipazione,* Iusinitinere, p.2, 2022.

[69] E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica,* Nuovi problemi di amministrazione pubblica G. Giappichelli editore - Torino, p.79, 2023.

[70] Sentenza n. 77/1987.

[71] Cit. O. CARAMASCHI, *Dall'ordine pubblico alla sicurezza: una prospettiva di teoria costituzionale*, Rivista Democrazia e Sicurezza, p.106, n.1 2023.

concetto di ordine pubblico viene declinato in due eccezioni; la prima attiene all'ordine pubblico in senso civilistico, ovvero in riferimento ai principi e alle regole; dall'altra parte troviamo un concetto di ordine pubblico di diritto di polizia, il quale fa riferimento al «limite del lecito giuridico[72]». La sicurezza pubblica[73] invece, come emerso anche nel primo capitolo, porta con sé significati molteplici e la sua polisemia si ritrova anche nella Costituzione all'Art.117 quanto ai riferimenti di "sicurezza nazionale e pubblica". La prima ha come fine la protezione degli interessi statali come collettività, la seconda invece, è intesa in senso materiale a protezione dell'«incolumità fisica e l'integrità patrimoniale dei cittadini[74]». In questo senso la sicurezza pubblica diviene una componente dell'ordine pubblico materiale e ciò è sottolineato dal ruolo della stessa sicurezza pubblica, la quale è al servizio delle funzioni di prevenzione e repressione per il mantenimento di una convivenza serena[75].

2.2.1 Sicurezza pubblica e sicurezza cibernetica

Possiamo quindi definire il fine della pubblica sicurezza con il brocardo altino - *ne cives ad arma ruant* - con cui si indica quell'attività volta a garantire una convivenza pacifica e l'ordine pubblico. Avendo premesso ciò, la cibersicurezza diviene rilevante quando si tratta di sicurezza pubblica in quanto l'utilizzo distorto delle tecnologie, come precedentemente evidenziato, comporta nuovi rischi che vanno a minare il quieto vivere sia del privato cittadino sia della collettività sia dello Stato quanto a sicurezza nazionale. Come evidenziato da Buoso, si assiste a «un ritorno di poteri regolativi, preventivi e sanzionatori molto pesanti per garantire la sicurezza interna ed esterna, quella individuale e collettiva[76]» in un momento in cui lo sviluppo della tecnologia porta a possibilità maggiori di liberalizzazione. Proprio per questi motivi la sicurezza

---

[72] Cit. E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica,* Nuovi problemi di amministrazione pubblica G. Giappichelli Editore - Torino, 2023, p.77. In particolare, l'autrice evidenzia una particolarità dell'ordine pubblico di polizia, e che è bene sottolineare, in quando viene definito come un concetto «destinato a dilatarsi e a restringersi per ragioni storiche o scelte politiche».

[73] Per un approfondimento sul tema si veda G. SESSA, *L'esigenza di sicurezza pubblica: tra diritto e partecipazione*, Rivista giuridica Iusinitinere, 2022.

[74] Cit. O. CARAMASCHI, *Dall'ordine pubblico alla sicurezza: una prospettiva di teoria costituzionale*, Rivista Democrazia e Sicurezza, n.1, p.104, 2023.

[75] F. ALICINO, *Sicurezza, ordine pubblico e libertà religiosa di fronte al terrorismo internazionale*, Rivista semestrale di libertà religiosa, laicità, diritti dal 1978, Coscienza e Libertà, n. 67, p.176, 2024.

[76] C:\Users\HP\AppData\Local\Microsoft\Teams\current\resources\app.asar\assets\icons\icn_close.svg

informatica si lega al fascio di compiti pubblici, il quale è necessario per garantire la sicurezza e il quieto vivere della collettività.

CAPITOLO III

STRUTTURA NORMATIVA DELLA CIBERSICUREZZA ITALIANA

Quest'ultima sezione si propone di offrire al lettore un approfondimento sull'evoluzione normativa in materia di sicurezza informatica, dalle sue origini fino all'accentramento dell'architettura nazionale. In particolare, si noti come il comune denominatore delle disposizioni abbia radici nel legame tra la pubblica amministrazione e sicurezza informatica, in questi paragrafi tale interconnessione risulterà sul piano operativo e dall'attenzione posta dal legislatore al settore pubblico.

1. I PRIMI PASSI VERSO UNA STRUTTURA NAZIONALE DI CIBERSICUREZZA

1.1 I primi passi della sicurezza informatica

La struttura italiana di cibersicurezza è relativamente recente, i primi passi vi sono stati già un quindicennio addietro, e ancor prima nel contesto dell'Alleanza Atlantica e dell'Unione Europea[77]. Prima di allora non esisteva una vera e propria architettura di sicurezza informatica nazionale, sebbene vi fossero state numerose iniziative volte ad assicurare le comunicazioni e le strutture pubbliche. Ricordiamo infatti, la Rete Unitaria della Pubblica Amministrazione (RUPA) la quale diverrà successivamente il Sistema Pubblico di Connettività (SPC), questo organismo ha svolto un ruolo importate in termini di sicurezza e compartecipazione tra le pubbliche amministrazioni. Faranno seguito iniziative volte a costituire gruppi di lavoro per la sicurezza delle reti e delle comunicazioni, i quali vedono una concretizzazione con la Direttiva della Presidenza del Consiglio dei Ministri 16 gennaio 2002 concernente la sicurezza informatica delle comunicazioni nelle pubbliche amministrazioni. Successivamente, con Decreto Interministeriale 24 luglio 2002, viene istituito il Comitato Tecnico Nazionale sulla Sicurezza Informatica e delle Comunicazioni nelle Pubbliche Amministrazioni, il quale

[77] A. MARRONE, ESABATINO, O. CREDI, *L'Italia e la difesa cibernetica, Istituto Affari Internazionali*, p.5, 2021.

avrebbe dovuto confluire nel Centro Nazionale per la sicurezza informatica agganciato alla proposta di creare un CERT per la P.A[78]. A seguito di alcune direttive comunitarie venne adottato, il 1 agosto 2003, con D.lgs. n.259 il Codice delle Comunicazioni Elettroniche il quale ha previsto la nascita del CERT Nazionale presso il MISE (Istituito poi nel 2014)[79].

Ulteriore passo avviene con la legge 3 agosto 2007, n. 124[80], recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto" la quale segna uno dei primi passi verso la costruzione di una disciplina improntata alla sicurezza delle infrastrutture del paese con la nascita del Dipartimento delle informazioni per la sicurezza (DIS). Inoltre, all'Art.5 è prevista l'istituzione presso la Presidenza del Consiglio dei ministri, del Comitato interministeriale per la sicurezza della Repubblica (CISR), il quale è l'organo cui competono le nomine dei vertici delle agenzie d'intelligence. È importante ricordare anche quanto inserito nel CAD, infatti all'art.51, ora denominato, a seguito di modifiche e adeguamenti, "Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", nel quale si fa esplicito riferimento all'assicurare i dati gestiti dalle PA.

La svolta si registra quando nel 2010 viene approvata una relazione sulla sicurezza cibernetica del Copasir (Comitato parlamentare che ha la funzione di controllo sui servizi di informazione) nella quale emerge la necessità di prevedere una difesa delle infrastrutture critiche del paese. Dalla relazione si evidenzia la necessità di una legge che designasse un'autorità del governo, la quale potesse dirigere e organizzare le attività di cibersicurezza sia in ambito pubblico sia in quello privato, anche in luce del ritardo del paese rispetto ai paesi membri dell'Unione Europea. Fa seguito il DPCM 5 maggio

[78] Istituito poi nel 2004 presso il CNIPA, precedentemente nominato AIPA, la quale poi diverrà nel 2009 con il d. lgs. N. 177/2009, l'Ente nazionale per la Digitalizzazione della Pubblica Amministrazione (DigitPA) poi soppresso dal Governo Monti che istituì l'agenzia per l'Italia Digital (AGID).

[79] Successivamente, con il DPCM dell'8 agosto 2011 pubblicato su G.U. n.262 del 8 novembre 2019 vengono fornite, in un unico decreto, le disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano, nel frattempo i due CERT (Computer Emergency Response Team) ovvero il CERT nazionale italiano (presso il MISE) e quello della Pubblica Amministrazione (CERT-PA presso AgID) rafforzano sempre di più la loro collaborazione, per svolgere congiuntamente il ruolo e le funzioni del CSIRT. Infine, in conseguenza del DPCM 8 Agosto 2019 le funzioni di CERT-PA e CERT-Nazionale sono trasferite allo CSIRT Italia.

[80] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2007-08-03;124

2010[81] "Organizzazione nazionale per la gestione di crisi" con l'istituzione all'Art.5 del Nucleo interministeriale situazione e pianificazione (NISP) e infine, la legge 7 agosto 2012, n.133[82] modifica e rafforza le previsioni della legge 3 agosto del 2007 n.124.

1.2 DPCM Monti 2013 e il DPCM Gentiloni 2017

Grazie allo slancio legislativo del 2012 ha fatto seguito il Decreto del Presidente del Consiglio dei ministri Monti, il quale vede una direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale del 24 gennaio del 2013[83], esso è stato il primo atto ad aver delineato una serie di compiti, procedure e indirizzi. L'intervento delinea una struttura suddivisa in tre diversi piani. Il primo di questi, di carattere politico, è affidato al CISR, infatti all'Art. 1 comma primo e all'Art.3, viene stabilito che su deliberazione del CISR, il Presidente del Consiglio dei ministri adotta il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali. All'Art.4 sono elencate le funzioni di supporto del CISR, tra le quali l'esercitare l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico, ed elaborare gli indirizzi fondamentali per la sicurezza cibernetica nazionali. Il secondo piano, invece, concerne un supporto operativo e amministrativo, affidato dall'Art.8 al Nucleo per la Sicurezza Cibernetica (NSC) con lo scopo di fungere da congiunzione tra gli enti e organi interessati. Il Nucleo è presieduto dal Consigliere militare e composto dal rappresentante del DIS[84], dell'AISE[85], dell'AISI[86], dal Ministero degli affari esteri, dal Ministero dell'interno, dal Ministero della difesa, dal Ministero dello sviluppo economico, dal Ministero dell'economia e delle finanze, dal Dipartimento della protezione civile e dall'AgID. I compiti di tale Nucleo sono delineati all'Art. 9, tra i quali vi sono le funzioni di prevenzione e pianificazione, di risposta e ripristino. Infine, il terzo piano è rappresentato dalla gestione delle crisi affidato al Tavolo interministeriale di crisi cibernetica, il quale raccoglie i dati relativi agli stati di crisi informando il Presidente del Consiglio, esso è attivato dal Nucleo per la sicurezza cibernetica.

[81] https://www.gazzettaufficiale.it/eli/id/2010/06/17/10A07594/sg
[82] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133
[83] https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg
[84] Dipartimento delle informazioni per la sicurezza fondato il 28 agosto 2007.
[85] Agenzia informazioni e sicurezza esterna fondata il 28 agosto del 2007.
[86] Agenzia informazioni e sicurezza interna fondata il 28 agosto 2007.

Dalla l'altra parte, il DPCM del presidente del consiglio Gentiloni, del 17 febbraio del 2017,[87] abroga e sostituisce il precedente DPCM Monti. Anch'esso ha lo scopo di «razionalizzare e semplificare l'architettura istituzionale» stabilita con il DPCM precedente e «migliorare le funzioni di coordinamento e raccordo[88]». Le principali modifiche attengono il rafforzamento del ruolo del CISR (Art.4), il quale si avvale del supporto e coordinamento interministeriale delle amministrazioni, del CISR Tecnico di cui all'Art.5 e del DIS. Viene mantenuto il ruolo del Presidente del Consiglio quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica di cui all'Art.3. Anche il ruolo del Nucleo per la Sicurezza Cibernetica viene rafforzato (Art.8), i suoi compiti sono specificati all'Art.9 esso viene trasformato in un hub operativo di 24 ore e assume la gestione dei rischi e compiti e viene integrato nel Dipartimento delle informazioni per la sicurezza (DIS), questi cambiamenti semplificano l'organizzazione e spostano il fulcro della sicurezza cibernetica all'interno del DIS. Al direttore generale del DIS viene affidato il compito di definire le linee di azione per assicurare adeguati livelli di sicurezza di quei sistemi di interesse strategico nazionale, sia pubblici sia privati. Inoltre, è previsto un maggiore coinvolgimento e interazione con l'AgID, il Dipartimento della Funzione Pubblica, il Ministero dello Sviluppo Economico, il Ministero dell'Interno, il Ministero della Difesa e con il Ministero dell'Economia e Finanze. Al secondo comma dell'Art. 11 vi è la nascita, presso il MISE, del Centro di Valutazione e Certificazione Nazionale (CVCN). Ulteriori modifiche riguardano l'inclusione, nell'Art.11, tra gli "operatori privati" anche di quelli definiti nella direttiva europea *Directive on security of network and information systems* NIS UE/2016/1148 del 6 luglio del 2016 (attuata con D.lgs n.65 del 18 maggio 2018[89]) anche se non vengono definiti quali siano effettivamente e come debbano interfacciarsi con le autorità pubbliche. Altro punto che emerge è all'Art. 2, il quale manca di una definizione di "infrastruttura critica" anche se viene introdotta la definizione, di matrice NIS, di "operatori di servizi essenziali". Infine, come sottolineato da Chittaro e Setola, sembra mancare un riferimento al fattore umano, il quale come già evidenziato, costituisce un

[87] https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2017-04-13&atto.codiceRedazionale=17A02655

[88] Ibidem.

[89] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;65

elemento chiave sia con risvolto positivo sia negativo, in quelle fasi che possano riguardare la certificazione, valutazione e validazione, formazione e *cyber culture* sia di operatori pubblici sia privati[90].

2. LA NASCITA DELLA STRUTTURA CYBER ITALIANA

2.1 Il Perimetro Nazionale di Sicurezza Cibernetica

Un'ulteriore svolta avviene con il D.L n.105 del 21 settembre 2019[91] il quale definisce il Perimetro Nazionale di Sicurezza Cibernetica (PSNC) le cui modalità di individuazione sono successivamente definite dal DPCM n.131 del 30 luglio 2020[92].

Il decreto-legge fa seguito al recepimento della direttiva europea 2016/1148[93] del 6 luglio 2016 NIS - *Network and Information Security*. Il D.L n.105 ha lo scopo di creare un sistema di organi e misure che sia in grado di assicurare la sicurezza cibernetica quanto a quei servizi ritenuti strategici per l'interesse nazionale comprese le reti 5G, istituendo un perimetro entro il quale far rientrare tali beni e servizi.

Fanno parte del PSNC le amministrazioni pubbliche, gli enti e operatori nazionali anche privati quando gli stessi esercitino una funzione essenziale dello stato e l'esercizio o la prestazione di tale servizio dipenda da reti, sistemi informativi e servizi informatici il cui funzionamento, interruzione o attacco comporti un danno per la sicurezza nazionale e l'ordine pubblico. Si tratta di soggetti operanti nel settore governativo in particolare nelle attività di amministrazione dello stato, attività delle amministrazioni del Comitato Interministeriale per la Sicurezza della Repubblica (CISR) e di quei soggetti pubblici e privati (quando non ricompresi nel settore governativo) attinenti alla difesa, interno, energia, spazio e aerospazio, telecomunicazioni, trasporti, economia e finanza, servizi

---

[90] A. CHITTARO e R. SETOLA, *Nuova direttiva per la protezione cibernetica e la sicurezza informatica*, Sicurezza e Giustizia, 2/2017.

[91] Italia, Decreto-legge 21 settembre 2019, n. 105: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.

[92] Presidenza del Consiglio dei Ministri, Decreto 30 luglio 2020, n. 131: Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

[93] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016L1148

digitali, enti previdenziali e lavoro e trasporti[94]. Inoltre, al comma 6 dell'Art. 1, il Centro di Valutazione e Certificazione Nazionale (CVCN) assume un ruolo cardine, in quanto è data facoltà di imporre test e valutazioni di software e hardware con la possibilità di sospendere o meno l'affidamento del contratto ad un soggetto in base al risultato di tale valutazione e infine, il CVCN potrà rivalutare e rielaborare le modalità di certificazioni utilizzate. Al comma 9 dell'Art.1 è presentato il regime sanzionatorio per coloro che si rendano inadempienti rispetto alle previsioni del decreto-legge, la cui urgenza è sottolineata dalla sanzione pecuniaria massima pari a 1.800.00 euro. Segue poi il DPCM 81/2021[95] il quale si concentra sulle misure volte a garantire la sicurezza dei beni ICT inclusi nel perimento e ad indicare le modalità di notifica degli incidenti, questi ultimi devono essere segnalati al gruppo di intervento per la sicurezza informatica (CSIRT).

2.2 Agenzia per la cybersicurezza nazionale e gli sviluppi normativi del 2022-2023

Un'ulteriore regolazione per la sicurezza informatica nazionale è l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), la quale è stata creata al di fuori dei reparti dell'intelligence con il decreto-legge del 14 giugno 2021 n.82[96] convertito con modificazioni nella legge 4 agosto 2021, n. 10[97] recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale».

All'Art.5 viene istituita l'Agenzia le cui funzioni ricadono all'interno del testo dell'art.7, agli artt. 1 - 4 viene definita l'architettura nazionale di sicurezza la cui figura apicale corrisponde al Presidente del Consiglio in linea con le precedenti disposizioni. A quest'ultimo sono attribuite l'alta direzione e la responsabilità generale delle politiche di cibersicurezza, la nomina e la revoca del direttore generale e del vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale, l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato Interministeriale per la Cybersicurezza (CIC),

[94] https://lineaamica.gov.it/docs/default-source/missione-1/digitalizzazione-innovazione-competitivit%C3%A0/dossier_la-cybersicurezza-nell'ordinamento-italiano.pdf?sfvrsn=4da83b6f_7

[95] https://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.del.presidente.del.consiglio.dei.ministri:2021-04-14;81!vig=2021-06-30

[96] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14;82

[97] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2021-08-04;109

quest'ultimo è stato istituito all'Art. 4 e si tratta di un organismo che ha funzioni di consulenza, proposta e vigilanza. Il CISR ovvero il Comitato Interministeriale della sicurezza della Repubblica, viene affiancato al nuovo CIC, dall'altra parte invece, vi è lo spostamento del sistema di sicurezza cibernetica nazionale dal DIS all'Agenzia, compreso il Nucleo di Sicurezza Cibernetica[98].

L'Agenzia ha il compito di coordinare i soggetti pubblici e privati promuovendo la realizzazione di azioni per la sicurezza cibernetica nazionale, «ponendo la cybersicurezza a fondamento della trasformazione digitale» e la sicurezza delle pubbliche amministrazioni. Inoltre, la stessa realizza l'attività di vigilanza del mercato in ambito nazionale, ad esempio il vigilare su fornitori e fabbricanti che emettono le dichiarazioni UE di conformità, su coloro che sono titolari di certificati europei di sicurezza informatica e sugli organismi di valutazione della conformità in concerto con le Forze dell'Ordine[99]. Fanno seguito poi il DPR 54/2021[100] il quale individua le modalità e le procedure relative al funzionamento del CVCN e i criteri per l'individuazione delle categorie di quei soggetti inclusi nel PSNC che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT (allegato 1 del DPCM 3[101]).

L'ACN è regolamentata dal DPCM 9 dicembre n.233 del 2021[102], ed è suddivisa in quattro rami, il Computer Security Incident Response Team (CISRT), il Centro di Valutazione e certificazione nazionale (CVCN), il Centro Nazionale di Coordinamento e l'Organismo di Certificazione della Sicurezza Informatica (OCSI). Ai vertici troviamo il comitato tecnico-scientifico presieduto dal Direttore generale, il comitato si occupa di questioni in materia di sviluppo di competenze, innovazione, partecipazione e programmi e progetti di cibersicurezza sia internazionali sia nazionali. I compiti invece del CSIRT[103]sono definiti dal D.lgs 18 maggio n.65 del 2018 e si tratta di attività di monitoraggio di incidenti a livello nazionale, l'emissione di preallarmi, allerte, annunci e divulgazione di

---

[98] A. MARRONE, ESABATINO, O. CREDI, *L'Italia e la difesa cibernetica*, Istituto Affari Internazionali, p.8, 2021.

[99] https://lineaamica.gov.it/docs/default-source/missione-1/digitalizzazione-innovazione-competitivit%C3%A0/dossier_la-cybersicurezza-nell'ordinamento-italiano.pdf?sfvrsn=4da83b6f_7

[100] https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg

[101] https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg

[102] https://www.normattiva.it/uri-res/N2Ls?urn:nir:presidente.consiglio:decreto:2021;223

[103] https://www.csirt.gov.it/

informazioni alle parti interessate in merito a rischi e incidenti, intervento in caso di incidente, analisi dinamica dei rischi e degli incidenti e la sensibilizzazione situazionale e la partecipazione alla rete dei CSIRT. Il CVCN adotta metodologie utilizzate nel processo di valutazione come, ad esempio, l'analisi del rischio affinché possa essere stabilito un livello di affidabilità che si articola in una triplice classificazione: affidabilità di base, sostanziale ed elevata. Si trova poi l'OCSI il quale, a seguito di una valutazione basata sugli standard internazionali di sicurezza informatica, vedi ISO/IEC e i criteri europei ITSEC e ITSEM, rilascia certificati di sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione. Infine, il Centro Nazionale di Coordinamento supporta il Centro europeo (ECCC) di competenza in cybersecurity, funge da punto di contatto tra i vari soggetti nel settore della sicurezza informatica.

Nel 2022 si è invece conclusa l'attuazione della normativa del Perimetro di Sicurezza Nazionale Cibernetica con la pubblicazione del DPCM 18 maggio 92/2022[104], il quale ha come temi, le procedure, le modalità e i termini da seguire in ordine alla gestione dei raccordi del CVCN (il quale ha preso operatività dal 30 giugno 2022) con i Laboratori Accreditati di Prova (LAP) e i Centri di Valutazione (CV) del Ministero dell'interno e del Ministero della Difesa. Per quanto concerne la segnalazione degli incidenti, con le disposizioni di cui all'articolo 37-quater del decreto-legge n. 115 del 2022[105], è stato esteso l'obbligo di segnalazione con l'introduzione del comma 3-bis all'art.1 del D.L m.105 del 2019 per gli incidenti che coinvolgano beni fuori dal Perimetro ma di pertinenza di soggetti inclusi nello stesso. Il 2023 è stato sottolineato dalla partecipazione allo *European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe)[106], l'ACN ha partecipato alle attività di esercitazione, le quali hanno lo scopo di innalzare il livello di resilienza aumentando la consapevolezza e la capacità di gestione in caso di eventi e incidenti cyber. Si è tenuta anche l'esercitazione NATO denominata *Crisis Management Exercise* nei

[104] https://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.del.presidente.del.consiglio.dei.ministri:2022-05-18;92

[105] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:2022;115~art33ter!vig

[106] Nasce da un progetto promosso da Italia e Francia, ha lo scopo di sostenere la gestione coordinata degli incidenti e delle crisi cyber su vasta scala, garantendo il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organi e le agenzie dell'Unione, ponendosi anche come elemento di collegamento tra la componente tecnica e il livello politico. All'Agenzia dell'Unione europea per la cibersicurezza (ENISA) è affidato il segretariato di CyCLONe, che viene presieduto dallo Stato membro che detiene la Presidenza di turno del Consiglio dell'Unione.

primi mesi del 2023 e a novembre si è tenuta la *European Election Cyber Excerise* in vista delle elezioni del parlamento europeo di giugno 2024. Seguono poi una serie di decreti ACN in materia di cloud per la PA e di passaggio di funzioni da AgID all'ACN, prosegue l'impegno nell'accompagnare la pubblica amministrazione verso la resilienza cyber, un'adeguata struttura cloud, oltre che di un piano di *awareness* e formazione.

3. L'ACCENTRAMENTO E GLI ADEMPIMENTI FUTURI PER LA CIBERSICUREZZA NAZIONALE

3.1 La legge n.90 del 2024 e le prospettive in ambito europeo

Il 2 luglio 2024 viene pubblicata in Gazzetta Ufficiale la legge 28 giugno 2024 n. 90[107] in merito a disposizioni in materia di rafforzamento della cibersicurezza nazionale e di reati informatici la cui elaborazione parte da inizio anno con l'approvazione del disegno di legge C1717. La *ratio* del testo di legge mira a sottolineare il necessario adeguamento alle misure e *best practice* di sicurezza informatica anche per quei soggetti pubblici e privati non compresi nel PSNC[108], oltre a preparare il terreno per l'attuazione della direttiva (EU) 2022/2555 NIS 2[109] da recepire entro il 17 ottobre 2024.

Il Capo I concerne i temi della sicurezza informatica tracciando una serie di adempimenti volti ad accrescere la resilienza dei soggetti inclusi. Il testo prevede obblighi di segnalazione e notifica degli incidenti al CSIRT Italia[110] riconducibili ad una delle tipologie individuate nella tassonomia di cui all'articolo 1, co. 3-bis, del D.L. n. 105/2019, ossia gli incidenti riconducibili agli ICP-C di cui alla sezione "Soggetti PSNC".

Una delle prime disposizioni concerne il mancato o ritardo adeguamento alle segnalazioni dell'ACN di cui all'Art.2, tuttavia si ravvisa la possibilità di un «difficile

---

[107] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2024-06-28;90

[108] Si tratta delle PA Centrali (elenco ISTAT), Regioni, Province autonome, Comuni capoluogo di regione, Comuni > 100.000 abitanti, ASL, Società in House, Città metropolitane, Società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, Società in house che forniscono servizi di raccolta, smaltimento o trattamento di acque reflue (urbane, domestiche o industriali) e di gestione dei rifiuti.

[109] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555

[110] Per un approfondimento si veda la "Guida alla notifica degli incidenti informatici" redatta dall'ACN suddivisa in base ai requisiti per i soggetti ricadenti all'interno del PSNC, soggetti legge n.90/2024, operatori TELCO, OSE e SFD e ulteriori soggetti. https://www.csirt.gov.it/contenuti/guida-alla-notifica-degli-incidenti-informatici

coordinamento[111]» data la formulazione del suddetto articolo. Quest'ultimo prevede una sanzione nel caso in cui i soggetti non abbiano sanato quelle specifiche vulnerabilità segnalate dall'ACN alle quali gli stessi siano "potenzialmente esposti"; proprio la potenzialità e non la certezza che tali soggetti siano esposti fa si che anche quelle segnalazioni, non verificabili o non con evidenze di rischio, ricadano anche in quelle puntuali. In secondo luogo, all'Art. 8 viene trattato il tema del rafforzamento della resilienza delle pubbliche amministrazioni con la nascita della figura del "Referente per la cybersicurezza" nelle PA. Quest'ultimo, disponendo di una conoscenza e competenze in ambito informatico oltre ad una visione completa della normativa di riferimento, ha il compito di monitorare il rilevamento delle minacce *cyber*, adottare misure di protezione, diffondere la cultura *cyber* e le *best practise*, lo sviluppo di piani di risposta e infine l'adeguamento alla normativa garantendo la conformità. Si tratta di una figura poliedrica la cui nascita sottolinea la spinta che si intende imprimere alle pubbliche amministrazioni, non si tratta solo di un approccio olistico alla sicurezza ma di un più profondo e necessario cambio di mentalità all'interno delle PA. Tuttavia, è bene sottolineare come la previsione all'Art.8 possa tradursi in una criticità per la PA nell'individuare il personale adeguato e sufficientemente formato per tale ruolo, vista la carenza sia nel settore privato sia pubblico[112], e soprattutto alla luce delle difficoltà riscontrate con il Responsabile per la transizione digitale disciplinato dal CAD. È previsto inoltre un rafforzamento della sicurezza dei dati tramite l'impiego di tecniche di crittografia[113] come disciplinato agli Artt. 9 e 10, si tratta di un metodo per proteggere dati e informazioni sensibili attraverso la trasformazione dei dati leggibili in un formato illeggibile (cifrato) utilizzando algoritmi matematici.

Al Capo II troviamo gli articoli 16, 17 e 19 i quali introducono nuove ipotesi di reato e circostanze aggravanti assieme all'introduzione della facoltà per l'ACN, di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche nelle forme di incidente probatorio in caso di accertamenti tecnici non ripetibili per i delitti di cui art. 371- bis.

---

[111] M.GIANNELLI, *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, p.18, 2024.

[112] Per un approfondimento sul tema si veda il report Fortinet. https://www.fortinet.com/it/corporate/about-us/newsroom/press-releases/2024/fortinet-annual-skills-gap-report-reveals-growing-connection-between-cybersecurity-breaches-and-skills-shortages

[113] Per un approfondimento sul tema si veda le *Linee guida funzioni crittografiche.* https://www.acn.gov.it/portale/crittografia

Tuttavia, una partecipazione simile dell'ACN in situazioni in cui vi è la possibilità di tessere collaborazioni con i servizi di intelligence, sembra poter rappresentare un problema per l'indipendenza delle indagini e alla trasparenza delle procedure giudiziarie[114]. Inoltre, la nuova legge *cyber* apporta modifiche anche alla disciplina della responsabilità amministrativa da reato ex D.lgs n.231/2001[115] per quanto concerne i delitti informatici e trattamento illecito di dati. L'Art.20 modifica l'Art. 24 -bis D.lgs 231/2001 portando un innalzamento delle sanzioni pecuniarie, (comma 1 lettera a) in relazione alla commissione di uno dei reati informatici contemplati. Alla lettera c) del comma 1, viene modificato il comma 2 sempre del suddetto art.24-bis D.lgs n.231/2001, in cui il riferimento all'art.625-quinquies è stato abrogato e sostituito con l'art.635-quater.1 il quale presenta contenuti simili ma caratterizzati da un acuirsi delle circostanze aggravanti. Infine, viene introdotto nell'art.24-bis il comma 1 -bis che presenta la fattispecie di estorsione mediante reati informatici[116] (art.629 comma 3, c.p)[117] questa nuova fattispecie di reato punisce l'uso illecito delle tecnologie informatiche per ottenere vantaggi economici, con pene severe per chi costringe individui o aziende a compiere o omettere determinate azioni a proprio svantaggio. A conclusione, la legge presenta uno dei primi passi per il consolidamento di una strategia nazionale di sicurezza informatica sia per il contrasto dei crimini informatici sia per la nascita di un apparato di sicurezza informatica pubblico comprensivo anche di quelle realtà amministrative più piccole e in considerazione delle difficoltà della PA rapportate ad una strategia nazionale di accentramento in considerazione anche dello scenario normativo europeo in materia.

L'Italia ha dovuto affrontare e sarà tenuta nei prossimi anni a seguire un processo di recepimento delle nuove direttive e adozione dei regolamenti in materia impattanti

---

[114] Unione Camere Penali Italiane, *Le nuove disposizioni in materia di cybersicurezza – Luci e ombre della Legge 90/2024*, Osservatorio "Scienza, processo e Intelligenza artificiale", p.1, 2024.

[115] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2001-06-08;231!vig=

[116] Per un approfondimento si veda G. FIORINELLI, *Il ransomware nel DDL Cybersicurezza: dalla fattispecie di estorsione "informatica" al coordinamento tra indagini e incident response,* Rivista italiana di informatica e diritto, 1/2024. Sulla fattispecie di estorsione informatica si veda il passo seguente «nella "estorsione informatica" la violenza e la minaccia, che costituiscono le condotte tipiche produttive della costrizione nella fattispecie di estorsione "comune" (Marini 1990), sono sostituite dal riferimento alle condotte di una serie di reati informatici (Accesso abusivo, Intercettazione, impedimento, etc. […] o Falsificazione, alterazione, etc. […] di comunicazioni informatiche, Danneggiamento di informazioni, dati e programmi informatici, Danneggiamento di sistemi informatici, anche di pubblica utilità), ovvero alla «minaccia di compierle».

[117] S. LIISTRO, *Legge 90/2024 sulla Cybersicurezza e compliance integrata: gli impatti su Modello 231 e privacy*, 2024.

soprattutto sull'apparato pubblico. Possiamo cominciare un breve excursus delle principali normative in arrivo, a gennaio 2023 è entrata in vigore la direttiva NIS 2 (UE) 2022/2555, la quale abroga la precedente NIS 2016/1148 relativa alle misure di cibersicurezza nell'Unione (da recepire entro il 17 ottobre 2024) in relazione alla quale il governo italiano ha approvato i decreti attuativi ad agosto 2024[118]. Ulteriore Regolamento europeo entrato in vigore a gennaio 2023, è il DORA *Digital Operation Resilience Act* con l'obiettivo di accelerare le capacità di resilienza cibernetica delle istituzioni finanziarie. Si ravvisa poi il lavoro sui decreti attuativi della Direttiva CER (UE) 2022/2557[119] in materia di resilienza dei soggetti critici, per la quale entro il 17 luglio 2026 ogni stato ha obbligo di individuare i soggetti critici. Segue poi il Regolamento *Cyber Resiliance Act*[120] la cui versione è stata pubblicata a dicembre 2023 con obbligo di applicazione dal gennaio 2027. A luglio 2024 è stato pubblicato il Regolamento europeo sull'Intelligenza Artificiale[121] *(Artificial Intelligence Act)*, il quale contiene a sua volta i requisiti di sicurezza informatica specifici per quei sistemi di IA classificati ad alto rischio. Il testo infatti pone al Capo II una serie di articoli indirizzati alla sicurezza e resilienza di tali sistemi, all'Art. 9 "Sistema di gestione dei rischi" e all'Art. 15 "Accuratezza, robustezza e cibersicurezza". Infine, troviamo il *Cyber Solidarity act*[122] il quale ha come fine l'organizzazione di centri operativi di sicurezza connessi in tutta l'UE i cui negoziati per l'approvazione del regolamento e la realizzazione del cosiddetto scudo informatico europeo sono stati avviati a gennaio 2024.

3.2 Il futuro della sicurezza informatica della PA

Infine, come riscontrabile da quanto emerso finora nell'elaborato, saranno cruciali nei prossimi anni la strategia e le scelte in ambito cyber per la Pubblica Amministrazione in quanto essenziali per il corretto «funzionamento del Sistema Paese[123]». L'esigenza di indirizzare la PA verso un cambiamento radicale e di mentalità emerge soprattutto dal

---

[118] Schema decreto attuativo NIS (UE) 22022/2555. https://www.cybersecitalia.it/wp-content/uploads/2024/06/DRAFTING_Schema-DLgs-NIS2-7-giugno-ore-18-05-post-riunione.pdf

[119] Schema di decreto attuativo direttiva CER. https://documenti.camera.it/leg19/dossier/pdf/AC0253.pdf?_1725887554014

[120] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

[121] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689

[122] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209

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

Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026 (il quale incorpora i contenuti del Piano Nazionale di Ripresa e Resilienza), con particolare attenzione al Capitolo 7 riguardante il tema della Sicurezza Informatica. È previsto il supporto di AgID alle PA tramite piattaforme e servizi, l'ACN invece, riveste un ruolo primario quanto alla definizione degli obiettivi e risultati attesi in tema *cyber*.

In primo luogo, uno dei punti primari consiste nell'"Adottare una governance della cybersicurezza diffusa nella PA" con il target di individuare e rendere noti ruoli e responsabilità nel 2025, con attenzione al responsabile della sicurezza informatica e anche alla definizione di un riferimento normativo in materia che sia di supporto alle PA. In secondo luogo, vi è l'obiettivo di "Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti", si tratta di definire e approvare i requisiti di sicurezza nei processi di acquisto di soluzioni IT con lo scopo di delineare, per il 2025, sia la procedura sia la definizione di contratti con terze parti e fornitori per il rispetto dei requisiti cyber. Affianco alla definizione della procedura di approvvigionamento vi è quella di monitoraggio, si tratta delle verifiche in ambito *audit* per la valutazione dei fornitori con il fine, nel 2026, di definire le azioni di controllo e verifica su terzi e fornitori (per giugno 2025 sono previste delle linee guida dall'ACN per la realizzazione degli *audit* e verifiche di sicurezza). In terzo luogo, di vitale importanza è la "Gestione mitigazione del rischio cyber" la quale si articola nella definizione del *framework* per la gestione del rischio con attività e processi di *cyber risk* (calcolo del rischio informatico) e *security by design* (cibersicurezza considerata fin dallo sviluppo e progettazione) e nella definizione delle modalità di monitoraggio del rischio cyber le cui indicazioni verranno fornite dall'ACN. In quarto lugo, si riscontra l'obiettivo di "Potenziare le modalità di prevenzione e gestione degli incidenti informatici" con la definizione di una architettura documentale relativa alla gestione degli incidenti e quindi dei presidi e la formalizzazione dei processi, assieme alla definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti. Infine, gli ultimi due obiettivi riguardano l'"Implementazione di attività di sensibilizzazione cyber del personale" in modo da adottare piani di formazione in base ai ruoli posizioni organizzative e responsabilità ricoperti, e la distribuzione di indicatori di compromissione alle PA per "Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA", ovvero l'utilizzo di strumenti atti all'esecuzione dei piani di

autovalutazione dei sistemi esposti, tali strumenti sono a disposizione sul portale CERT-AgID e si prevede per il 2026 che la totalità delle PA ne fruiscano[124]. Infine, occorre soffermarsi su un aspetto cruciale riguardante la realizzazione degli obiettivi fin qui enunciati, si tratta di dotare le PA di quegli strumenti necessari per effettuare tale cambiamento. Spesso nella storia legislativa italiana si è assistito ad una fiorente nascita di disposizioni, le quali hanno però mancato di un effetto concreto per una mancanza di conoscenze, competenze, strutture e strumenti, tutto ciò ha comportato ad uno sviluppo digitale e *cyber* disconnesso, venendo meno una visione comprensiva e omogenea. Le disposizioni recenti, sia in ambito europeo sia nazionale, pongono un tracciato favorevole, soprattutto in considerazione dei piani di investimento derivanti dal PNRR, saranno quindi cruciali gli investimenti e gli indirizzi del legislatore nell'applicare concretamente le strategie in ragione della dimensione sistemica della cibersicurezza.

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

CONCLUSIONE

A conclusione del percorso intrapreso, possiamo convenire sul fatto che la sicurezza informatica stia divenendo estremamente essenziale nell'organizzazione amministrativa, sia per quanto concerne la sicurezza nazionale, l'ordine pubblico fino alla tutela del cyberspazio. Oramai gli attaccanti sfruttano tecniche, le quali fanno leva sul fattore umano e le pubbliche amministrazioni, in quanto più deboli, divengono un bersaglio. Nasce, insieme alla necessità di tutelare il patrimonio informativo, anche quella di creare una cultura volta alla cybersecurity, in ragione della dimensione assunta dalla digitalizzazione sempre più pervasiva vista la crasi tra il piano dell'online e offline. Da qui la pubblica amministrazione, in quanto struttura guida di un paese, ha il compito di indirizzare e fungere da esempio per un'adeguata digitalizzazione, inoltre, la sua efficienza consiste nel fornire un servizio sempre più vicino al cittadino, continuo e sicuro. La sicurezza informatica si lega al principio del buon andamento della pubblica amministrazione e rientra nell'alveo dei concetti di sicurezza ed ordine pubblico, assistendo quindi ad un ritorno di quei poteri regolatori su una realtà digitale che al contempo ha portato ad una connessione e liberalizzazione maggiori. Il legislatore italiano ha accolto tale necessità e, come emerso nell'ultimo quinquennio, l'architettura nazionale cyber è venuta a costituirsi e il suo recente accentramento sottolinea una volontà di rafforzare la resilienza del Paese in particolare la tutela del servizio pubblico. Per queste motivazioni, le scelte del legislatore e gli indirizzi a livello europeo saranno strategici e fondamentali per la costituzione di un quadro normativo in grado di indirizzare nella sicurezza informatica gli *stakeholder* pubblici e privati. Nel contesto italiano di fondamentale importanza sarà attenzionare quelle aree della pubblica amministrazione più in difficoltà, con lo scopo di superare un *modus operandi* e una *forma mentis* legate all'analogico.

BIBLIOGRAFIA

A. BANFI, G. GALLI, *La digitalizzazione delle pubbliche amministrazioni*, OCPI, 2020 https://osservatoriocpi.unicatt.it/cpi-archivio-studi-e-analisi-la-digitalizzazione-delle-pubbliche-amministrazioni-1941/cpi-Digitalizzazione%20PA(1).pdf

A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, A. CADOPPI, *Cybercrime*, Milano: UTET Giuridica, consultabile su Wolter Kluwer, 2019

A. CHITTARO e R. SETOLA, *Nuova direttiva per la protezione cibernetica e la sicurezza informatica*, Sicurezza e Giustizia, 2/2017 https://www.sicurezzaegiustizia.com/nuova-direttiva-per-la-protezione-cibernetica-e-la-sicurezza-informatica/

A. MARRONE, E. SABATINO, O. CREDI, *L'Italia e la difesa cibernetica*, Istituto Affari Internazionali, 2021 https://www.iai.it/it/pubblicazioni/litalia-e-la-difesa-cibernetica

A. NATALINI, *Come il passato influenza la digitalizzazione delle amministrazioni pubbliche*, Rivista di Diritto Pubblico n.1, 2022 https://www.irpa.eu/articolo/come-il-passato-influenza-la-digitalizzazione-delle-amministrazioni-pubbliche/

A. PACE, *La funzione di sicurezza nella legalità costituzionale*, Forum di Quaderni istituzionali, n. 4, 2014 https://biblio.liuc.it/scripts/essper/ricerca.asp?tipo=autori&codice=11010153

A. PITTAU, *Social engineering: è in atto una campagna di Phishing ai danni di privati e P.A. L'AgID lancia l'allarme. Ecco come individuarle e difendersi*, Redazione DirICTo, 2020 https://www.diricto.it/?p=1426305

A. SIMONCINI, E. CREMONA, *La AI fra pubblico e privato*, DPCE online, 1/2022 https://www.dpceonline.it/index.php/dpceonline/article/view/1571

ACN, *Guida alla notifica degli incidenti informatici*, https://www.csirt.gov.it/contenuti/guida-alla-notifica-degli-incidenti-informatici

ACN, *Linee guida funzioni crittografiche* https://www.acn.gov.it/portale/crittografia

ACN, Relazione annuale al parlamento 2022 https://www.acn.gov.it/portale/relazione-annuale

ACN, Relazione annuale al parlamento 2023 https://www.acn.gov.it/portale/relazione-annuale-2023

ACN, Strategia nazionale di cybersicurezza 2022 – 2026 https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

AGENZIA EUROPEA PER I DIRITTI FONDAMENTALI, Art. 43 Diritto alla buona amministrazione https://fra.europa.eu/it/eu-charter/article/41-diritto-ad-una-buona-amministrazione

AGID Piano Triennale per l'informatica nella PA 2024 - 2026 https://www.agid.gov.it/it/agenzia/piano-triennale

AGID *Regolamento per l'adozione di Linee Guida per l'attuazione del Codice dell'Amministrazione Digitale* (ai sensi degli artt. 14-bis e 71 del Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82). Allegato alla Determinazione AgID del 17 maggio 2018, n. 160, https://www.agid.gov.it/sites/default/files/repository_files/regolamento-adozione-linee-guida-attuazione-cad.pdf

AGID, Guida Dei Diritti Di Cittadinanza Digitali, D. Lgs. N. 82/2005, Art. 17, comma 1-quinquies, https://www.agid.gov.it/sites/default/files/repository_files/guida_riepilogo_diritti_cittadinanza_digitale_03-2022-acc.pdf

AGID, *Strategia Italiana per l'Intelligenza Artificiale 2024-2026* https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf

C. DE LUVIO, *Il grave attacco informatico alla pubblica amministrazione,* Il POST, 2023 https://www.ilpost.it/2023/12/19/attacco-informatico-westpole-pa/

C. MELONI, *La nuova architettura di cybersicurezza in Italia,* La Comunicazione - Note, Recensioni e Notizie n. 67, 2023 https://atc.mise.gov.it/images/documenti/Rivista/2023/La_nuova_architettura_di_cybersicurezza_in_Italia.pdf

C. MENEGHETTI, *CyberItalia: l'evoluzione normativa della cybersecurity in Italia, cosa bisogna sapere,* Diritto al digitale, 2023 https://dirittoaldigitale.com/2023/10/09/cybersecurity-italia-cyberitalia-evoluzione-normativa/

C. SARRA, *Il Mondo-dato, Saggi su datificazione e diritto,* Cleup, 2019

C.A CIARALLI, *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, n. 15/2023 https://federalismi.it/nv14/articolo-documento.cfm?artid=49045

CANADIAN CENTRE CYBER SECURITY, *An introduction to the Cyber Threat Environment* 2023 – 2024 https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

CLUSIT, Rapporto 2024 sulla Sicurezza ICT in Italia https://clusit.it/rapporto-clusit/

COMMISSIONE EUROPEA, *Cyber Resilience Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

COMMISSIONE EUROPEA, *Cyber Solidarity Act* https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:52023PC0209

COMMISSIONE EUROPEA, Pacchetto sullo stato del decennio digitale 2024, allegato 3 "Corte relazioni dei 27 Stati membri dell'UE" Italy https://digital-strategy.ec.europa.eu/it/policies/2024-state-digital-decade-package

COMMISSIONE EUROPEA, Report Digital Decade Package, https://digital-strategy.ec.europa.eu/en/policies/2024-state-digital-decade-package

COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico*, https://www.sicurezzacibernetica.it/db/[2010]%20Relazione%20COPASIR%20-%20Sulle%20possibili%20implicazioni%20e%20minacce%20per%20la%20sicurezza%20nazionale%20derivanti%20dallo%20spazio%20cibernetico.pdf

CORRIERE DELLA SERA, Lockbit https://www.corriere.it/tecnologia/23_dicembre_19/chi-sono-i-russi-di-lockbit-hacker-che-hanno-bloccato-la-pubblica-amministrazione-politica-contano-solo-i-soldi-695b2492-8908-4e12-993c 5cb23941dxlk.shtml

CORTE COSTITUZIONALE, sentenza n. 77/1987, https://giurcost.org/decisioni/1987/0077s-87.html?titolo=Sentenza%20n.77

CSIRT, https://www.csirt.gov.it/

CYBERSECURITY 360, *Westpole PA digitale il vero conto del disastro enorme* https://www.cybersecurity360.it/nuove-minacce/westpole-pa-digitale-il-vero-conto-del-disastro-enorme/

DEDAGROUP, *La maturità digitale dei comuni capoluogo*, 2024, https://www.deda.group/media/comunicati-stampa/cresce-la-maturita-digitale-dei-comuni-capoluogo-2024

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE, *Programma Strategico Intelligenza Artificiale 2022-2024*, 24 novembre 2021 https://innovazione.gov.it/

E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica,* Nuovi problemi di amministrazione pubblica G. Giappichelli editore - Torino, 2023

E. CREMONA, *Fonti private e legittimazione democratica nell'età della tecnologia,* Numero speciale, i sistemi normativi post-vestfaliani ..., DPCE online, 2021 https://www.dpceonline.it/index.php/dpceonline/article/view/1521

E. SALERNO, *La cybersecurity amministrativa il buon andamento informatico,* Privacy e Cybersecurity, 2020 https://www.researchgate.net/publication/341343901_La_Cybersecurity_amministrativa_il_buon_andamento_informatico_-_Cybersecurity_in_public_sector_a_good_digital_administration

E. SORRENTINO e A.F SPAGNUOLO, *Le sfide degli enti locali: tra PNRR e gap digitali,* Federalismi rivista di diritto pubblico italiano, comparato, europeo, 9 agosto 2023 https://www.federalismi.it/nv14/articolo-documento.cfm?artid=49302

E.N. FRAGALE, *La cittadinanza amministrativa al tempo della digitalizzazione,* consultabile su Rivista di Diritto amministrativo n.2, 2022

ENISA, *Cybersecurity of AI in the AI Act,* 2023, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

ETICA PA, La PA è la comunità dei cittadini https://www.eticapa.it/eticapa/la-foresta-incantata-rapporto-cassese-del-1993-sulle-condizioni-delle-pubbliche-amministrazioni/#more-5021

F. ALICINO, *Sicurezza, ordine pubblico e libertà religiosa di fronte al terrorismo internazionale*, Rivista semestrale di libertà religiosa, laicità, diritti dal 1978, Coscienza e Libertà, n. 67, 2024 https://coscienzaeliberta.it/coscienza-e-liberta/rivista-n-67/francesco-alicino-sicurezza-ordine-pubblico-e-liberta-religiosa-di-fronte-al-terrorismo-internazionale-n-67-anno-2024/

F. DELERUE, A. SUKUMAR AND D. BROEDERS, *Responsible Behaviour In Cyberspace*, Global narratives and practice, Luxembourg: Publications Office of the European Union, 2023 https://op.europa.eu/en/publication-detail/-/publication/d1baf40a-1c6c-11ee-806b-01aa75ed71a1/language-en

F. ITALO, Cap.1 *La P.A al servizio dei cittadini*, Manuale del nuovo diritto amministrativo, 2008

F. MUSELLA, *Amministrazione 5.0*, Rivista di Digital Politics, politica internazionale, Il Mulino - rivisteweb, n. Politica & Società Fascicolo 1, gennaio-aprile 2018 https://www.academia.edu/85882868/Administration_5_0

F. MUSELLA, *Digital Regulation: come si cambia la Pubblica Amministrazione*, consultabile su Rivista di Digital Politics, fascicolo gennaio-agosto 2022

F. SALAHDINE and N. KAABOUCH, *Social Engineering Attacks: A Survey*, Future Internet 2019, School of Electrical Engineering and Computer Science, University of North Dakota https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey

FORTINET https://www.fortinet.com/it/corporate/about-us/newsroom/press-releases/2024/fortinet-annual-skills-gap-report-reveals-growing-connection-between-cybersecurity-breaches-and-skills-shortages

G. CALZETTA, *Hacker russi chiedono riscatto per il massiccio attacco alla Pa. Agenzia cybersicurezza: stipendi saranno pagati*, Il Sole 24 Ore, 2023 https://www.ilsole24ore.com/art/cosa-sappiamo-finora-dell-attacco-hacker-che-sta-bloccando-servizi-pa-AF9Y173B

G. FIORINELLI, *Il ransomware nel DDL Cybersicurezza: dalla fattispecie di estorsione "informatica" al coordinamento tra indagini e incident response*, Rivista italiana di informatica e diritto, 1/2024 https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/196/170

G. PESCE, *Dottrina e attualità giuridiche, Diritto amministrativo e intelligenza artificiale: problemi*, consultabile su Rivista Giurisprudenza Italiana, Giugno 2022

G. SESSA, *L'esigenza di sicurezza pubblica: tra diritto e partecipazione*, Rivista giuridica Iusinitinere, 2022 https://www.iusinitinere.it/lesigenza-di-sicurezza-pubblica-tra-diritto-e-partecipazione-42154

G. ZICCARDI e P. PERRI, *Tecnologia e Diritto Volume II, Informatica Giuridica Data Governance, protezione dei dati e GDPR, mercato unico digitale, blockchain, Pubblica Amministrazione digitale*, Giuffrè Francis Lefebvre, 2019

GAZZETTA UFFICIALE , D.L 30 luglio 2020, n. 131 Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, https:// www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

GAZZETTA UFFICIALE, D.L 21 settembre 2019, n. 105: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg

GAZZETTA UFFICIALE, DPCM 14 aprile 2021, n. 81, Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. (21G00089) (GU Serie Generale n.138 del 11-06-2021) https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

GAZZETTA UFFICIALE, DPCM 15 giugno 2021, Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (21A05087) (GU Serie Generale n.198 del 19-08-2021) https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg

GAZZETTA UFFICIALE, DPCM 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. (17A02655) (GU Serie Generale n.87 del 13-04-2017) https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2017-04-13&atto.codiceRedazionale=17A02655

GAZZETTA UFFICIALE, DPCM 18 maggio 2022, n. 92, Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (22G00099) (GU Serie Generale n.164 del 15-07-2022) https://www.gazzettaufficiale.it/eli/id/2022/07/15/22G00099/sg

GAZZETTA UFFICIALE, DPCM 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale. (13A02504) (GU Serie Generale n.66 del 19-03-2013) https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

GAZZETTA UFFICIALE, DPCM 5 maggio 2010, Organizzazione nazionale per la gestione di crisi. (10A07594) (GU Serie Generale n.139 del 17-06-2010) https://www.gazzettaufficiale.it/eli/id/2010/06/17/10A07594/sg

GAZZETTA UFFICIALE, DPR 5 febbraio 2021, n. 54, Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (21G00060) (GU Serie Generale n.97 del 23-04-2021) https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg

IL FRONTE CYBER, *Uno speciale sulla cyberwarfare tra guerra in ucraina e Medio Oriente*, dell'ebook di Guerre di Rete https://www.guerredirete.it/il-fronte-cyber-ecco-il-nostro-ebook/

J. AHMAD, A. AMELIO, D.H GERNSBACK E D. F. SIVILLI, *Intelligenza artificiale spiegabile: sicurezza informatica, usabilità, metaverso e sfide giuridiche,* Federalismi, 2024 https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=50280&content=&content_author=

K. CHAŁUBIŃSKA–JENTKIEWICZ, *Cybersecurity as a Public Task in Administration,* Cybersecurity in Poland, 2022 https://www.researchgate.net/publication/366682791_Cybersecurity_as_a_Public_Task_in_Administration

L. FLORIDI, *La quarta rivoluzione come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017

L. FRANCHINA, *Agenzia per la cyber security, una svolta per l'Italia digitale: ma ora lavorare sulle competenze*, 2021 https://www.agendadigitale.eu/sicurezza/agenzia-per-la-cybersicurezza-nazionale-litalia-prova-a-colmare-il-ritardo-i-modelli-di-francia-e-germania/

L. GOLISANO, *Il governo del digitale: strutture di governo e innovazione digitale*, consultabile su Giornale di diritto amministrativo, 6/2022

L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale,* Il Mulino - rivisteweb, *p.*63, n. Politica & Società Fascicolo 1, gennaio-aprile 2018 https://www.cssii.unifi.it/upload/sub/quinta%20dimensione%20conflittualit%C3%A0%20cyberspazio%20MARTINO.pdf

L. MORONI, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, n. 14/2024 https://www.federalismi.it/nv14/articolo-documento.cfm?artid=50689

L. PIER MONTESSORO, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, Istituzioni del Federalismo, 2019

https://www.regione.emilia-romagna.it/affari_ist/rivista_3_2019/Montessoro.pdf

L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, Federalismi, n.25/2022 https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=47823

L. TORCHIA, *Lo Stato digitale, Una introduzione*, Il Mulino, 2023

L. TOSONI, *The Fundamental Right to Cybersecurity, Inception, Implications and Limits*, University of Oslo, 2023 https://kudos.dfo.no/documents/49639/files/32079.pdf

L. V. MARIA SALAMONE, *La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'intelligence e prospettive de iure condendo*, Federalismi, n.23/2017 https://federalismi.it/nv14/articolo-documento.cfm?artid=35245

LINEA AMICA, PNRR Dossier https://lineaamica.gov.it/docs/default-source/missione-1/digitalizzazione-innovazione-competitivit%C3%A0/dossier_la-cybersicurezza-nell'ordinamento-italiano.pdf?sfvrsn=4da83b6f_7

M. BIANCHI, *Adeguati assetti e digitalizzazione degli enti locali, limiti e prospettive*, consultabile su Azienditalia, n.1/2024

M. D. CAVELTY, A. WENGER, *Cybersecurity politics, socio-technological transformations and political fragmentation*, 2022 https://library.oapen.org/bitstream/id/20a53302-dee5-4834-9d98-8f9c07f0a602/9781000567113.pdf

M. KARPIUK, *Cybersecurity as an element in the planning activities of public administration*, University of Warmia and Mazury in Olsztyn, 2020 https://www.cybersecurityandlaw.com/Cybersecurity-as-an-element-in-the-planning-activities-of-public-administration,142179,0,2.html

M. PIETRANGELO, *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, n. 1/2024, 2024 https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/191

M. PIETRANGELO, *Sui "diritti di cittadinanza digitale". Note a margine di un opaco percorso normativo*, n.8, 3 aprile 2024 https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=50373&content=&content_author=

M. PROTTO, *Diritto amministrativo e nuove tecnologie*, Dottrina e attualità giuridiche, consultabile su Giurisprudenza Italiana - Giugno 2022 https://dialnet.unirioja.es/ejemplar/611517

M. S. GIANNINI, Rapporto 1979, https://www.tecnichenormative.it/RapportoGiannini.pdf

M. SFORZA, *Social engineering, combatterlo con un approccio multi disciplinare (umano-tecnico): ecco come*, Digital 360, 2019 https://www.agendadigitale.eu/sicurezza/social-engineering-combatterlo-con-un-approccio-multi-disciplinare-umano-tecnico-ecco-come/

M.B FORNACIARI, *Sistema delle fonti e definizione dello spazio giuridico europeo*, Federalismi, 2021 https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=45155

M.BETZU, Convegno del Gruppo di Pisa il diritto costituzionale e le sfide dell'innovazione tecnologica Università degli studi di Genova 18-19 giugno 2021, *Poteri Pubblici E Poteri Privati Nel Mondo Digitale*, La rivista "Gruppo di Pisa", Fascicolo n. 2/2021 https://gruppodipisa.it/eventi/convegni/484-18-19-giugno-2021-genova-il-diritto-costituzionale-e-le-sfide-dell-innovazione-tecnologica

M.GIANNELLI, *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, Rivista Italiana di Informatica e Diritto, 2024 https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/193

N. GIANNELLI, *Il cammino delle riforme della pubblica amministrazione nella svolta pragmatica del PNRR*, Studi Urbinati, A - Scienze Giuridiche, Politiche Ed Economiche, 2021 https://journals.uniurb.it/index.php/studi-A/article/view/3254

NORMATTIVA, D.L 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. (21G00098) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14;82

NORMATTIVA, D.L 9 agosto 2022, n. 115, Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali. (22G00128) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:2022;115~art33ter!vig

NORMATTIVA, D.lgs 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi

nell'Unione. (18G00092) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;65

NORMATTIVA, D.lgs 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, D.lgs 7 marzo 2005, n.82 https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82

NORMATTIVA, D.lgs 8 giugno 2001, n. 231, Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300 https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2001-06-08;231!vig=

NORMATTIVA, DPCM 9 dicembre 2021, n. 223, Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale. (21G00246) https://www.normattiva.it/uri-res/N2Ls?urn:nir:presidente.consiglio:decreto:2021;223

NORMATTIVA, LEGGE 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. (24G00108) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2024-06-28;90

NORMATTIVA, LEGGE 3 agosto 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2007-08-03;124

NORMATTIVA, LEGGE 4 agosto 2021, n. 109, Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. (21G00122) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2021-08-04;109

NORMATTIVA, LEGGE 7 agosto 2012, n. 133, Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto. (12G0156) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133

O. CARAMASCHI, *Dall'ordine pubblico alla sicurezza: una prospettiva di teoria costituzionale*, Rivista Democrazia e Sicurezza, n.1 2023 https://romatrepress.uniroma3.it/wp-content/uploads/2024/01/5.-Caramaschi-Dallordine-pubblico-alla-sicurezza.pdf

PARLAMENTO EUROPEO E COMMISSIONE, *European Declaration on Digital Rights and Principles for the Digital Decade*, The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights

and Principles for the Digital Decade https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

PARLAMENTO EUROPEO E CONSIGLIO, Direttiva (UE) 2016/1148, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016L1148

PARLAMENTO EUROPEO E CONSIGLIO, direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555

PARLAMENTO EUROPEO E CONSIGLIO, REGOLAMENTO (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689

R. BRIGHI e C. PIER GIORGIO, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* Federalismi, n.21, 8 settembre 2021 https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=45896

R. CASTROREALE, *Cybersecurity per tutti*, EPC Editore, 2024

R. FORSI, *Cyber, una PA più sicura farà lezione degli errori passati,* Agenza Digitale. Eu, 2024 https://www.agendadigitale.eu/sicurezza/levoluzione-della-cybersicurezza-nella-pa-lezioni-dal-passato-e-prospettive-future/

S. DOMINIONI, Cybersecurity: l'architettura della difesa italiana, ISPI90, 2019 https://www.ispionline.it/it/pubblicazione/cybersecurity-larchitettura-della-difesa-italiana-24546

S. LIISTRO, *Legge 90/2024 sulla Cybersicurezza e compliance integrata: gli impatti su Modello 231 e privacy*, NT Plus Diritto, 2024 https://ntplusdiritto.ilsole24ore.com/art/legge-902024-cybersicurezza-e-compliance-integrata-impatti-modello-231-e-privacy-AF8FWtuC

S. PIETROPAOLI, *Un altro modo di fare la guerra. La cyberwar come problema giuridico*, Ars interpretandi, Fascicolo 1, gennaio-giugno 2023 https://www.carocci.it/prodotto/un-altro-modo-di-fare-la-guerra-la-cyberwar-come-problema-giuridico

S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza-la Repubblica, Roma-Bari 2014 https://www.laterzalibropiuinternet.it/materiali_download_free.php?id=24630&isbn=9788842100111

S. ROSSA, *Cyber Attacchi E Incidenti Nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario,* 2024 https://research.uniupo.it/it/publications/cyber-attacchi-e-incidenti-nella-pubblica-amministrazione-fra-org

SCHEMA DECRETO ATTUATIVO NIS (UE) 22022/2555 https://www.cybersecitalia.it/wp-content/uploads/2024/06/DRAFTING_Schema-DLgs-NIS2-7-giugno-ore-18-05-post-riunione.pdf

SCHEMA DI DECRETO ATTUATIVO DIRETTIVA CER https://documenti.camera.it/leg19/dossier/pdf/AC0253.pdf?_1725887554014

UNIONE CAMERE PENALI ITALIANE, *Le nuove disposizioni in materia di cybersicurezza – Luci e ombre della Legge 90/2024*, Osservatorio "Scienza, processo e Intelligenza artificiale", 2024 https://www.camerepenali.it/cat/12590/le_nuove_disposizioni_in_materia_di_cybersicurezza_-_luci_e_ombre_della_legge_902024.html

V. GUARIELLO, *Cybersecurity: Una Sfida Tra Pubblica Sicurezza E Sicurezza Nazionale*, Cammino Diritto rivista di informazione giuridica, 2022 https://rivista.camminodiritto.it/public/pdfarticoli/8123_2-2022.pdf

VARENNA, *La digitalizzazione della vita dell'amministrazione del processo*, Foro Amministrativo - n. 10 – 2016 https://www.astrid-online.it/static/upload/madd/maddalena_varenna_2016.pdf

Y. N. HARARI, *Homo Deus Breve storia del futuro*, Bompiani, 2015