UNIVERSITA' DEGLI STUDI DI PADOVA

Dipartimento di Giurisprudenza

Corso di Laurea in Diritto e Tecnologia

Anno Accademico 2023/2024

DAI DIRITTI FONDAMENTALI DEGLI INDIVIDUI ALLE INFRASTRUTTURE CRITICHE: L'EVOLUZIONE DELLA CYBERSECURITY

Relatore:
Prof. Giuseppe Bergonzini

Laureanda: Irene Benedetti
matricola: 2036914

SOMMARIO

beanTech srl

La beanTech è una PMI innovativa che affianca le aziende nelle sfide della *digital transformation* aiutandole ad effettuare un percorso di crescita. La beanTech supporta le aziende a gestire l'intera filiera del dato con un'offerta di soluzioni che vanno dall'acquisizione dati all'architettura IT, agli sviluppi software personalizzati alla gestione dei processi interni, dall'analisi del business all'implementazione di sofisticati algoritmi di intelligenza artificiale[1].

L'obiettivo di questo progetto di tesi è la comprensione del ruolo e dell'importanza delle diverse attività di Cybersecurity in un'azienda medio/grande. Verranno sviluppate conoscenze legate alla strategia aziendale di *awareness*, alla creazione, erogazione e valutazione del *training* sul tema, alle attività legate alla compliance alla ISO 27001 e sul ciclo di vita, le tipologie e i framework di *threat intelligence*.

[1] https://www.beantech.it/en/.

1. INTRODUZIONE

La trasformazione digitale sta interessando tutti i settori della nostra vita e ha profondamente cambiato la società, le nostre relazioni e il modo di fare industria.

La sicurezza nel cyberspazio è rilevante non solo come valore in sé, ma nell'ottica del bene comune della sicurezza nazionale, della protezione delle infrastrutture critiche, dello sviluppo del mercato digitale e della tutela del sistema di diritti fondamentali[2].

Le strategie europee nel campo della sicurezza informatica stanno attraversando un processo di costante evoluzione. Perché si realizzi un adeguato livello di protezione, l'Unione promuove un approccio strategico di tipo globale, caratterizzato da aggiornamenti progressivi che mirano a rafforzare gli approcci di protezione e resilienza, tenendo conto dei progressi tecnologici e delle dinamiche mutevoli delle minacce, sempre più estese e sistematiche[3]. Per tali ragioni, il nuovo quadro legislativo in materia di cybersicurezza si è arricchito di regole per la tutela dei sistemi e dei servizi online, promuovendo misure normative riguardanti la protezione delle infrastrutture ICT e degli attori essenziali. Nelle società che dipendono dall'infrastruttura digitale per funzionare, la solidità dei sistemi è un requisito essenziale e richiede una progettazione accurata e test continui per lo studio delle nuove vulnerabilità e la prevenzione di possibili attacchi. Al centro dell'approccio europeo vi è l'analisi preventiva dei rischi, la notifica degli incidenti da parte degli operatori pubblici e privati, la verifica dei livelli di sicurezza dei prodotti attraverso sistemi di certificazione e standard.

In questa rivoluzione, dove ognuno di noi è potenzialmente un destinatario diretto o indiretto di un attacco cibernetico, il ruolo degli standard, assieme alle norme di carattere nazionale e comunitario è pertanto centrale.

---

[2] R. BRIGHI, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, 8 settembre 2021.

[3] A. TONOLO, *"Evoluzione delle Strategie di Cyber Security: Uno Sguardo a Confronto tra Europa e Stati Uniti",* 16 gennaio 2024.

2. CYBERSECURITY

La cybersecurity ha raggiunto un nuovo livello di rilevanza e ha assunto un ruolo in primo piano nell'Agenda di Governi, Istituzioni, Aziende, diventando una delle principali priorità dei paesi dell'Unione Europea, in accordo alle quali devono essere definite le strategie di sviluppo, attraverso azioni di coordinamento normativo, tecnico e operativo. Il motivo principale è che gli attacchi informatici mirano a danneggiare le informazioni, i dati personali e i diritti di imprese e cittadini. Non si tratta di un problema che riguarda solo la sicurezza pubblica, ma anche la difesa del sistema giuridico e della nazione che lo sostiene.[4]

Il termine cybersecurity è stato definito dal Regolamento (UE) 2019/881[5] relativo all'ENISA[6] come *"l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e le altre persone interessate alle minacce informatiche"*. La *mission* è quindi la protezione di qualsiasi evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone. Nessun anello della catena di sicurezza deve essere tralasciato, incluso l'utente finale che spesso è esso stesso, con il suo comportamento, fonte di vulnerabilità.

La cybersecurity, inoltre, è stata definita dagli standard ISO 27000[7] come: *"la conservazione della confidenzialità dei dati, integrità e disponibilità dell'informazione (CIA[8]). Inoltre, dispone di altre caratteristiche, tra cui l'autenticità, la responsabilità e*

[4] ACCREDIA, *Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata*, 14 novembre 2022.

[5] PARLAMENTO EUROPEO E CONSIGLIO, *relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (Testo rilevante ai fini del SEE).*

[6] Istituita nel 2004, l'ENISA (European Union Agency for Cybersecurity) contribuisce alla politica dell'UE in materia di sicurezza nel settore IT, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC. Coopera inoltre con gli Stati Membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche.

[7] La serie ISO/IEC 27000 comprende gli standard di sicurezza delle informazioni, le quali forniscono un quadro riconosciuto a livello globale delle best practice per la gestione della sicurezza delle informazioni.

[8] Per confidenzialità del dato si intende la protezione durante tutto il loro ciclo di vita. Per integrità si intende la capacità di mantenere originali i dati e le risorse affinché non vengano in nessun

l'affidabilità del dato, che possono essere utilizzate per spiegare il concetto di cybersecurity". Detti principi sono i fattori chiave per la gestione e pianificazione della sicurezza.

Con l'avvento dei dispositivi mobili si sono resi necessari nuovi approcci alla cybersecurity e tra questi troviamo il NIST Cybersecurity Framework[9], definito come un insieme di cinque attività, che vanno svolte in modo concomitante e continuo per formare una cultura operativa che affronti il rischio dinamico della cybersecurity:

- Identificazione: viene sviluppato e compreso l'ambiente, le risorse che devono essere protette e i rischi cibernetici a cui sono esposte;
- Protezione: vengono implementate adeguate misure di sicurezza per garantire la continuità delle operazioni aziendali e per ridurre l'impatto delle potenziali minacce cibernetiche;
- Rilevazione: vengono sviluppate attività per una rapida identificazione della presenza di minacce;
- Risposta: vengono identificati i possibili interventi in caso di incidente di sicurezza rilevato;
- Recupero: vengono implementate attività appropriate per mantenere i piani di resilienza e per ripristinare qualsiasi capacità o servizio che sia stato compromesso a causa di un incidente di sicurezza.

La sicurezza informatica di una nazione non si basa esclusivamente sulle misure di protezione adottate dalle entità governative e aziendali, ma anche dalla sicurezza individuale degli utenti. La vulnerabilità individuale è legata alla consapevolezza del rischio e al livello di abilità tecnologica. Spesso si sottovaluta il pericolo legato all'uso scorretto dei dati personali, con ripercussioni sulla propria identità, sulla propria reputazione e sulla sicurezza dei propri dati.

---

modo modificate o cancellate. Il principio di disponibilità è indice del diritto all'accesso alle risorse garantite agli utenti (impedire interruzioni di servizio).

[9] Il NIST (National Institute of Standards and Technology) è un'agenzia non regolamentare che promuove l'innovazione attraverso il progresso della scienza, degli standard e della tecnologia delle misurazioni. Il NIST Cybersecurity Framework consiste in standard, linee guida e best practice per aiutare le organizzazioni a migliorare la loro gestione dei rischi per la sicurezza informatica https://www.nist.gov/cyberframework

Tra i possibili attaccanti non vengono quasi mai considerati familiari o conoscenti che in un contesto di abusi possono comunque avvantaggiarsi di un accesso facilitato al dispositivo della vittima. L'*asset* da proteggere da abusi e manipolazioni diventa dunque la persona[10].

Oltre alla comprensione del termine cybersecurity, bisogna comprendere quali sono le tipologie di attacchi informatici che si possono subire e il loro impatto nella vita di ciascuno di noi. In un mondo in cui tutte le informazioni sono dematerializzate, l'uomo deve fare i conti con il veloce progredire della tecnologia e con le sue conseguenze, positive e negative. Un valore crescente del mercato è stato accompagnato dalla comparsa di tentativi fraudolenti di impossessarsi di queste informazioni e alla nascita del cosiddetto cybercrime, inteso come un'attività criminale caratterizzata dall'abuso di componenti tecnologiche informatiche, sia hardware che software. Comprende quindi tutti quei reati che sfruttano tecnologie digitali e sistemi informatici per provocare danni a privati, aziende ed enti. Tra le tipologie di attacchi più diffusi[11] si indicano:

- Attacco malware: ovvero software malevoli, come spyware, ransomware, virus e worm. Il malware viola una rete sfruttandone una vulnerabilità. Una volta all'interno del sistema il malware può bloccare l'accesso ai componenti principali della rete, installare malware o altri software dannosi o interferire con alcune componenti e rendere il sistema inutilizzabile.
- Attacco di *Social Engineering*[12]: basato sullo studio del comportamento delle persone col fine di manipolarle e carpire informazioni confidenziali. Il procedimento si basa sulla psicologia umana e sfrutta la fiducia, la mancanza di conoscenza e, in generale, la vulnerabilità della vittima per ottenere dati

[10] Comportamenti lesivi quali molestie, odio, bullismo e stalking hanno nella dimensione online un forte potenziale lesivo della reputazione in virtù della persistenza delle informazioni e della loro potenziale diffusione virale.

[11] MICROSOFT, "*Che cos'è un attacco informatico*?", https://www.microsoft.com/it-it/security/business/security-101/what-is-a-cyberattack

[12] Una delle tecniche di Social Engineering più sfruttate è l'attacco phishing. Tramite l'invio di mail fraudolente, messaggi, telefonate o siti web progettati per indurre l'utente a scaricare malware, condividere informazioni sensibili o dati personali, gli attaccanti ingannano l'utente ottenendo le informazioni desiderate.

confidenziali. Il social Engineering può manifestarsi sotto varie forme e viene utilizzato tramite canali utilizzati quotidianamente dalle persone, come e-mail, social media, servizi cloud o app di messaggistica.

- Attacco ad Applicazioni Web: attraverso lo sfruttamento di vulnerabilità e punti deboli presenti nelle applicazioni web, vengono eseguiti comandi dannosi (iniezioni SQL o esecuzioni di codice remoto).
- Attacco Man in the Middle: noti anche come attacchi di intercettazione, si verificano quando gli hacker si inseriscono in una comunicazione fra due parti. Una volta che hanno interrotto il traffico, i criminali possono filtrare e rubare dati.
- Attacco Zero-day: colpisce non appena viene scoperta una vulnerabilità nella rete, ma prima che sia possibile implementare una patch o una soluzione. Gli hacker prendono di mira la vulnerabilità rilevata durante questa finestra temporale.
- Attacco DDoS: (Distributed Denial-of-Service), avviene tramite il sovraccarico di un sito web, un server o una risorsa di rete con traffico dannoso. Di conseguenza, il sistema preso di mira si blocca o non riesce a funzionare, negando il servizio agli utenti legittimi.

Queste attività non si limitano all'accesso non autorizzato ai sistemi informatici. La grande quantità di condotte che sono racchiuse nella definizione di cybercrime rispecchia la complessità del fenomeno e le sue infinite declinazioni. Il panorama delle minacce si è ampliato in modo significativo e l'esposizione di soggetti e organizzazioni è in continuo aumento specialmente a causa dell'introduzione del *cloud computing*[13], dei dispositivi mobili e dell'*IoT*[14], offrendo numerosi potenziali vettori con cui un criminale può agire.

[13] Il *cloud computing* è un modello di elaborazione basato su Internet che consente agli utenti di accedere a risorse informatiche condivise (come server, storage, applicazioni e servizi) tramite una rete di server remoti ospitati su internet, piuttosto che utilizzare un server locale.

[14] *IoT (Internet of Things)* è una rete di oggetti e dispositivi connessi, dotati di sensori e altre tecnologie che consentono loro di trasmettere e ricevere dati, da e verso altre cose e sistemi.

2.1. LO STRETTO RAPPORTO TRA PRIVACY E CYBERSECURITY

I dati rappresentano il cuore del modello di business dell'intero ecosistema digitale e la questione della privacy gioca un ruolo chiave nella vita delle persone, nella società, nei mercati e nelle democrazie. Secondo il "The Global Risk Report 2023"[15] del World Economic Forum (WEF), la cybersecurity e il diritto alla privacy emergono, a livello globale, quali aree di forte criticità a causa dell'inasprimento degli episodi di criminalità informatica e del diffondersi di un senso di "cyber insecurity" sotto il profilo della protezione dei dati personali [16].

Il motivo è molto semplice da capire: in un mondo digitale i dati che identificano i nostri comportamenti sono digitalizzati; se non riusciamo a tutelare questi dati digitali, non riusciamo a tutelare i nostri comportamenti. Se la privacy è l'altra faccia della cybersecurity è anche vero che la privacy è un diritto fondamentale dell'UE, mentre la cybersecurity non lo è.

Eppure, in un contesto in cui ogni azione viene trasformata in dato, la salvaguardia di quei dati che riflettono le nostre attività quotidiane diventa fondamentale[17].

Questo complesso rapporto si sta sviluppando come un incrocio di innovazioni, dibattiti e possibili scontri tra istituzioni.

In risposta alla crescita esponenziale dell'importanza della rete in molteplici attività umane, si verifica un analogo incremento parallelo della quantità e della qualità dei dati online, molti dei quali sensibili e strettamente riservati (informazioni sanitarie o personali, dati genetici, dati biometrici, dati finanziari). L'accesso non autorizzato a tali dati, la loro esposizione senza previo consenso, la loro alterazione o distruzione sono tutti eventi in grado di dare vita a conseguenze negative per il titolare dei dati stessi. Nonostante i professionisti in materia lavorino duramente per colmare le lacune

---

[15] https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

[16] TECH4FUTURE, "*Dati e sicurezza: la violazione del diritto alla privacy il rischio maggiormente percepito*", 18 gennaio 2023.
https://tech4future.info/cyber-security-diritto-privacy-rischi/

[17] A. DI CORINTO, *Data Commons: privacy e cybersecurity sono diritti umani fondamentali*, in *Rivista italiana di informatica del diritto*, 2022, pp. 33-34.

della sicurezza[18], gli aggressori sono sempre alla ricerca di nuovi modi per aggirare le misure di difesa e sfruttare le debolezze emergenti.

Un esempio addizionale dell'ampliamento delle frontiere di interazione tra l'ambiente e i sistemi informativi è rappresentato dall'Internet of Things[19]. Questi sistemi, che stanno assumendo un ruolo sempre più rilevante sia nel settore pubblico, come nelle infrastrutture critiche, sia in quello privato, sono dispositivi capaci di interagire costantemente con l'ambiente fisico in cui operano, mediante sistemi di sensori e attuatori interconnessi. Una delle principali preoccupazioni associate ai dispositivi è la mole di dati personali che raccolgono. Ogni cosa, dalla nostra posizione, al nostro comportamento, alle preferenze e allo stato di salute, può essere catturata da questi dispositivi, creando un'impronta digitale che può essere sfruttata.

Di conseguenza, IoT comporta una modifica del paradigma nell'approccio alla sicurezza: ogni attacco cibernetico ai sistemi IoT ha un effetto diretto su tutti gli oggetti fisici interconnessi.

Da tempo il diritto è entrato nella società tecnologica, con tutti i suoi temi e problemi derivanti dall'applicazione delle tecniche giuridiche. Nel Ventunesimo Secolo, una delle sfide principali per il costituzionalismo è rappresentata dalla tecnologia: come garantire forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica e dai suoi derivati in ambito giuridico.

Si è discusso altresì di un "nuovo costituzionalismo" e si potrebbe riformulare l'antico brocardo latino con: *ubi societas (technologica), ibi ius*[20].

[18] Le entità criminali stanno diventando sempre più potenti e le tecniche utilizzate per portare a segno attacchi cyber sono divenute, infatti, sempre più raffinate ed all'avanguardia, al punto da essere in grado, in molti casi, di superare o aggirare i sistemi e le procedure di sicurezza implementate proprio per contrastarle.

[19] NETWORK DIGITAL360, "*IoT. Internet of Things:cos'è, come funziona ed esempi*", 16 novembre 2022.

[20] T.E. FROSINI, *Apocalittici e integrati. La dimensione costituzionale della società digitale*, Modena, 2021, p. 9.

2.2. SECURITY OPERATIONS CENTER (SOC)

Tanto più la tecnologia diventa indispensabile, tanti più dati e informazioni sensibili vengono processati e custoditi al suo interno. La protezione delle informazioni passa necessariamente attraverso una corretta tutela dei dispositivi che le processano. Tuttavia, questo scopo non si raggiunge semplicemente applicando sofisticate tecnologie. Innanzitutto, c'è bisogno di approcciare alla sicurezza da più angolazioni: da quella tecnica, a quella legislativa, passando per un'incessante azione di formazione e sensibilizzazione[21] di utenti e personale.[22]

Il SOC (Security Operations Center) è un'entità organizzativa che si caratterizza, principalmente, per le capacità difensive in contrasto ad attività non autorizzate condotte contro gli *assets* oggetto di protezione. Viene considerato come la realizzazione più tangibile e visibile dalla *real-time security situational awareness*[23] e, data l'accelerazione evolutiva della minaccia digitale, è oggi un asset fondamentale per ogni organizzazione.[24]

In questa crescente richiesta si è inserita la beanTech, composta, tra le diverse Business Unit, da un SOC, il quale eroga servizi mirati alla sicurezza dei sistemi informativi e garantisce una sicurezza informatica costante. Tra le attività svolte dal SOC:

- Prevenzione e Rilevamento: rileva le minacce, le classifica in base alla gravità e previene possibili attività dannose;
- Indagine: vengono analizzate le attività sospette per determinare le misure delle minacce. Le informazioni raccolte vengono poi combinate sulla rete

[21] "*Security awareness*" rimanda al concetto di consapevolezza: essa va acquisita attraverso un processo di formazione puntuale e costante destinato a tutti gli utenti di dispositivi connessi e, più in particolare, ai dipendenti considerati figure centrali nel tradurre in pratica quotidiana quanto contenuto nelle policy di security aziendale.

[22] CYBERMENT*, "il legame intrinseco tra Cybersecurity e Privacy", 14 giugno 2023.* https://www.pqa.it/news/il-legame-intrinseco-tra-cybersecurity-e-privacy/

[23] È uno dei principali obiettivi del *SOC team*, ossia consolidare flussi di dati tramite aggregazione, associazione, contestualizzazione e presentazione di una visione costante della *security posture*.

[24] IBM, "*SOC (Security Operations Center)"*

dell'organizzazione con le più recenti threat intelligence globali, che includono informazioni specifiche su strumenti, tecniche e tendenze degli aggressori;

- Analisi e Risposta: viene definito l'insieme degli strumenti di reazione e segnalazione per reagire a eventuali eventi critici. In presenza di un attacco è necessario rispondere nel minor tempo possibile;
- Reportistica e Presentazione: la fase reportistica è fondamentale per dimostrare il lavoro svolto, rispettando gli accordi presi con il cliente. Il report è considerato uno strumento di comunicazione tra SOC e il cliente[25].

L'azione del SOC è possibile tramite la collaborazione di elementi quali:

- Tecnologia[26]: possono essere utilizzate diverse tecnologie, quali ad esempio sistemi di Security Information Event Management (SIEM), Database Active Monitoring (DAM), Intrusion Detection/Prevention System (IDS/IPS), Malware Protection, Sandbox e simili. Data la natura estremamente dinamica nel panorama delle minacce cyber, è estremamente importante per il SOC avvalersi costantemente di tecnologie di sicurezza;
- Persone: sono il fattore centrale e distintivo del SOC e di solito esiste una struttura multilivello all'interno dell'organizzazione per lo svolgimento di azioni diverse e complementari;
- Processi: divisi in quattro categorie, tra cui business, tecnologici, operativi e analitici;

La *Digital Transformation* espone l'informazione a rischi direttamente proporzionali alla dinamica di crescente centralità delle ICT ed è sempre più urgente attivare adeguate capacità di difesa contro attacchi e minacce. Il SOC è l'eccellenza operativa di tali capacità e gestisce quindi gli incidenti di sicurezza e coordina la risposta ai cyber-attacchi esterni ed interni, al fine di garantire la CIA dei dati e dei suoi clienti.

[25] F.LA TROFA, "cos'è e a che cosa serve un Security Operation Center". *https://universeit.blog/soc-security-operation-center/*

[26] Le tecnologie utilizzate da un Security Operation Center (SOC) si riferiscono agli strumenti, sistemi e piattaforme che aiutano i professionisti della sicurezza a monitorare, rilevare, analizzare e rispondere alle minacce informatiche. Queste tecnologie sono essenziali per proteggere le infrastrutture IT, i dati e le operazioni aziendali dalle violazioni della sicurezza e dagli attacchi informatici.

3. DIRITTI FONDAMENTALI E NUOVE TECNOLOGIE: BILANCIAMENTO TRA SICUREZZA E LIBERTÀ.

I diritti fondamentali vengono riconosciuti non come una vicenda conclusa ma come un continuo impegno, che richiede un costante bilanciamento tra i principi fondamentali e le mutevoli esigenze richieste dalla realtà.

E così avvengono gli sviluppi della giurisprudenza italiana. Lo sviluppo di nuovi mezzi di comunicazione, le conquiste scientifiche, l'affermarsi di una consapevolezza sociale rispetto ai temi legati all'innovazione. L'evoluzione della tecnologia, unitamente alla forte spinta data dalla pandemia, rende indispensabile una riflessione sul ruolo della rete nella prospettiva dei diritti fondamentali garantiti dalla Costituzione. Una prospettiva ampia e problematica, che porta a interrogarsi sull'attualità dei principi costituzionali rispetto al mondo della rete, contraddistinto dall'innovazione e dalla dinamicità[27].

Molti giuristi sostengono che un ridimensionamento in tema di diritti potrebbe avere forti implicazioni a livello etico e sociale legati alla tutela dei diritti fondamentali in una società sempre più liquida, globalizzata, digitale e ora algoritmica.

A partire dalla rivoluzione industriale, le "nuove" tecnologie hanno progressivamente investito ogni aspetto dell'organizzazione sociale. Essa ha fatto emergere nuove prospettive per l'esercizio di diritti fondamentali già riconosciuti.

Oltre alle interferenze con il diritto alla riservatezza, si avverte come con il progressivo affermarsi di questo nuovo paradigma di efficienza, fondato sul potenziale dei dati e degli algoritmi, possa essere inficiata la tenuta di alcune garanzie fondamentali, come i principi di tutela contro le diseguaglianze, il giusto processo, la partecipazione e il controllo pubblico rispetto all'agire pubblico e, più in generale, la trasparenza di tutti quei procedimenti decisionali che a diverso titolo, per mano di attori pubblici o privati, possono produrre effetti significativi sulla sfera giuridica dei soggetti interessati e nel godimento dei loro diritti.

[27] A. FONZI, *Il principio di autodeterminazione dell'utente al cospetto delle nuove tecnologie*, in *Rivista on-line diritti fondamentali*, n. 3/2021, pp. 570-572.

Il progresso tecnologico, nelle sue varie fasi, ha inevitabilmente influenzato da un lato, l'insieme delle azioni umane e l'organizzazione delle società civile, e dall'altro l'organizzazione e l'azione dello stato e dei poteri pubblici, impattando di conseguenza, anche i diritti fondamentali[28]. Questa estensione della sfera di azione pone sfide concettuali più esigenti per i giuristi.

Riportando le parole della vicepresidente del Garante della privacy: "È vero che il progresso tecnologico in generale e l'evoluzione delle tecnologie digitali, delle biotecnologie e dei sistemi di comunicazione elettronica negli ultimi vent'anni hanno creato enormi opportunità a livello globale per consolidare società prospere sotto il profilo economico, più inclusive e giuste; ma al contempo, senza un nuovo contratto sociale e un quadro normativo adattato alle nuove tecnologie dall'effetto dirompente, sono emerse numerose gravi minacce per l'umanesimo, prima che per l'umanità (violazioni della vita privata, distorsioni algoritmiche dovute a dati di cattiva qualità, volatilità dei mercati, perdita del lavoro a causa dei progressi nell'automazione e della sua diffusione, etc.)" [29].

Per più di vent'anni, l'analisi etico-politica delle diverse fasi della rivoluzione digitale è stata in gran parte positiva, nel senso che le nuove opportunità sembrano superare di gran lunga i rischi e le minacce per i diritti umani. Tuttavia, negli ultimi anni, è emersa invece una percezione diversa dei problemi e le valutazioni pessimistiche hanno guadagnato terreno rispetto a quelle ottimistiche.

Di fronte ad una diversa visione del rapporto fra diritti fondamentali e nuove tecnologie, è sorta l'esigenza sempre più avvertita di norme giuridiche chiare e coerenti, condivise ed efficaci, ci si trova spesso di fronte ad un vero e proprio "disorientamento giuridico" in cui le stesse categorie tradizionali subiscono un effetto di riformulazione[30].

Le nuove tecnologie hanno creato nuove forme e nuove opportunità per i diritti fondamentali già riconosciuti dalle Costituzioni contemporanee, ma hanno anche

---

[28] M. OLIVETTI, *Diritti Fondamentali e Nuove tecnologie: una mappa del dibattito italiano*, in *Revista Estudos Institucionais*, n. 2/2020, pp. 395-398.

[29] Ginevra Cerrina Ferroni, vicepresidente del Garante della Privacy, *PNRR, digitale: gli impatti sui diritti e ordinamento costituzionale- intervento di Ginevra Cerrina Ferroni,* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9815604

[30] C. CASONATO, *Bioetica e pluralismo nello Stato Costituzionale*, in *Forum di Quaderni costituzionali*, 2006, p. 2.

favorito l'emergere di nuove minacce. In particolare, le tecniche informatiche permettono di controllare l'intero svolgimento della vita delle persone. Tutte le attività realizzate da un individuo attraverso connessione alla rete sono tracciabili. Un ulteriore aspetto critico è la sorveglianza di massa. Se da un lato la sicurezza pubblica può beneficiare della sorveglianza tecnologica, dall'altro lato molte volte l'uso dei dati raccolti non è conforme alle leggi e questo rappresenta un chiaro esempio dei limiti e degli abusi in materia di diritti individuali.

La rapidità dell'evoluzione tecnologica spesso supera la capacità delle leggi esistenti di tenere il passo. A fronte di questo tipo di minacce si è sviluppato il diritto alla tutela dei dati personali, il GDPR (Regolamento Generale sulla protezione dei dati personali), entrato in vigore nel 2016 in tutti gli Stati membri dell'UE.

Osservando l'impatto della rivoluzione digitale sul diritto, l'emergere della cosiddetta "identità digitale" è un elemento in grado di confermare l'esigenza di regole adeguate a tutelare gli individui partecipanti del cyberspazio. Se informazioni diverse su un utente circolano per scopi più disparati sulla rete, è possibile che alcuni frammenti di informazione che sarebbero irrilevanti per certe finalità, risultino pericolosi laddove acquisiti da certi soggetti con l'intento di farne uso improprio.

La forma più rilevante di impatto delle nuove tecnologie sul diritto è tuttavia rappresentata dall'emersione di nuovi[31] diritti fondamentali[32], utili per proteggere la persona da minacce rilevanti dalle nuove tecnologie, mentre in altri sono finalizzate a rendere effettivamente fruibili le nuove opportunità che le nuove tecnologie hanno generato rispetto ai diritti fondamentali già esistenti[33].

Il quadro sopra descritto evidenzia l'importanza e l'urgenza di un'azione di preparazione agli attacchi, ma anche di capacità di rilevamento, contenimento e risposta. L'azione del sistema deve pertanto tendere a migliorare la postura della

[31] Si parla qui di «nuovi» diritti in due diversi sensi: si tratta di diritti nuovi in quanto non previsti dalla Costituzione; si tratta altresì di diritti nuovi in quanto emersi in reazione alle nuove tecnologie.

[32] Come i diritti che proteggono la persona da minacce provenienti dall'uso delle nuove tecnologie da parte di soggetti pubblici o, più spesso, privati e che operano seguendo la logica delle libertà tra cui - il diritto alla protezione dei dati personali, il diritto all'oblio, il diritto a non essere oggetto di decisioni esclusivamente automatizzate.

[33] M. OLIVETTI, *Diritti Fondamentali e Nuove tecnologie: una mappa del dibattito italiano*, 2020, p. 401.

sicurezza globale, ma questo necessariamente passa attraverso un intervento che coinvolga diversi comparti della società e del mondo produttivo.

Le principali innovazioni hanno avuto origine in ambito europeo, sia mediante l'adozione di atti normativi dell'Unione Europea, sia mediante pronunce della Corte di giustizia dell'Unione europea[34]. A fronte delle nuove minacce generate dalle nuove tecnologie, in Italia sono state introdotte nuove norme legislative finalizzate a proteggere alcuni interessi umani fondamentali, che hanno generato nuovi limiti e nuove restrizioni di alcuni diritti fondamentali già riconosciuti, come la libertà di espressione, per bilanciare gli effetti nocivi causati dalle tecnologie. Continua a prevalere la riflessione dottrinale, divisa fra coloro che hanno segnalato l'emersione di nuovi e specifici diritti e coloro che invece sostengono, sulla base dell'interpretazione dei principi costituzionali italiani, un "macro-diritto informatico".

Tuttavia, la rapidità dell'evoluzione tecnologica spesso supera la capacità delle leggi esistenti di tenere il passo. L'intelligenza artificiale e la sorveglianza di massa sollevano questioni complesse riguardo alla responsabilità e alla discriminazione algoritmica al fine di trovare il giusto equilibrio tra innovazione e tutela dei diritti. Le tecnologie emergenti presentano quindi questioni significative per la privacy e per la protezione dei dati personali. Le leggi sulla privacy devono essere adeguate e adattate all'evoluzione tecnologica, garantendo il giusto equilibrio tra innovazione e tutela dei diritti individuali. Solo attraverso una regolamentazione robusta e consapevole possiamo garantire che le tecnologie emergenti siano utilizzate in modo etico e rispettoso della privacy delle persone[35].

[34] Si v. ad es. le sentenze quelle adottate nei casi *Digital rights Ireland* (8.4.2014), *Google Spain* (13.5.2014) e *Maximillian Schrems v Data Protection Commissioner*, Judgement of the Court (Grand Chamber) 6.10.2015.

[35] LEGAL ENZDR, Tecnologia e Privacy: u*n bilanciamento Necessario tra Individuazione e tutela dei Diritti Individuali*, 17 maggio 2023 *https://www.linkedin.com/pulse/tecnologia-e-privacy-un-bilanciamento-necessario-tra-innovazionel*

4. LE POLITICHE DELL'UNIONE EUROPEA IN MATERIA DI CYBERSICUREZZA

L'UE ha da tempo intrapreso azioni per garantire una sempre maggiore protezione dei mercati *online*, incentivare gli investimenti in ricerca e innovazione ed assicurare uno sviluppo costante e rapido delle reti e dei servizi di comunicazione elettronica. La necessità di regolamentare la sicurezza delle reti e delle applicazioni digitali è stata chiara fin dall'inizio, quando si è compreso che il problema del rischio informatico avrebbe avuto effetti diretti sulle informazioni, sui dati e sui servizi che queste reti e applicazioni forniscono e quindi, effetti diretti e catastrofici sulla società e sulle libertà costituzionali.

Le prime azioni risalgono all'inizio di questo secolo con la pubblicazione sul *Cybercrime* del 2001[36], relativa alla sicurezza delle infrastrutture dell'informazione e alla lotta al crimine informatico. Questa comunicazione è stata successivamente integrata da quella sulla *Network Information Security* (NIS)[37], definita come: *".... la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema…"*.

La definizione offerta dalla NIS è accompagnata da un quadro generale che mostra le varie tipologie di pericoli che possono influire sulla sicurezza delle reti, classificate in base alla loro natura e che includono l'intercettazione delle comunicazioni, l'accesso non consentito a computer e reti informatiche e le cosiddette interruzioni di rete, l'esecuzione di software "maligni" che alterano o distruggono i dati,

[36] COMMISSIONE EUROPEA, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica*. eEurope 2002 (COM(2000)890), 26 gennaio 2001.

[37] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni. Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, Bruxelles, 6.6.2001 COM(2001)298 definitivo, p. 10.

l'appropriazione indebita delle identità personali e gli incidenti ambientali e eventi imprevisti.[38]

Sempre nei primi anni 2000 vennero approvate tre importanti Direttive in materia NIS: la Direttiva 2002/21/CE[39] relativa all'accesso e alle autorizzazioni per le reti e i servizi di comunicazione elettronica, la Direttiva 2002/19/CE[40] relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime e la Direttiva 2002/20/CE[41], relativa alle autorizzazioni per le reti ed i servizi di comunicazione elettronica. Nel 2009 però, vennero abrogate con l'emissione della Direttiva Quadro 2009/140/CE[42], la quale impone agli Stati membri di predisporre misure interne che garantiscano la sicurezza delle reti e la costituzione di un'apposita autorità nazionale[43].

Il 2004 fu un anno molto importante per l'avanzamento della cybersecurity in Europa. In un contesto socio-economico in cui l'Information technology (IT) aveva già dimostrato di svolgere un ruolo determinante, l'Unione Europea ha manifestato la crescente preoccupazione nei confronti della minaccia cibernetica con l'istituzione dell'ENISA (*European Union Agency for Network and Information Security*), avvenuta con il Regolamento (CE) n. 460/2004[44], sottolineando in questo modo, l'importanza di adottare misure efficaci in materia di sicurezza delle reti di comunicazione e dei sistemi informativi.

---

[38] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni. Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, p. 3.

[39] Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), GU L 108 del 24.04.2002.

[40] Direttiva 2002/19/CE del Parlamento europeo e del Consiglio, del 24 aprile 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime (direttiva accesso), GU L 108 del 24.04.2002.

[41] Direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni), GU L 108 del 24.04.2002.

[42] Direttiva 2009/140/CE del 25 novembre 2009 recante modifiche alle direttive 2002/21/CE, 2002/19/CE e 2002/20/CE, GU L 260 del 03.10.2009.

[43] A. CONTALDO, D. MULA (a cura di), Cybersecurity Law. *Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020, p. 19.

[44] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004, relativo all'istituzione dell'Agenzia europea per la sicurezza delle reti e dell'informazione, art. 1.1.

L'Agenzia ha il compito di assistere la Commissione e la comunità degli Stati membri, accrescendone le capacità di prevenire e affrontare i problemi di sicurezza delle reti e dell'informazione e di reagire, fornendo loro assistenza e consulenza e contribuendo allo sviluppo generale di un alto livello di competenze. Infine, l'agenzia contribuisce a promuovere e diffondere una nuova cultura della sicurezza, affinché la questione della cybersicurezza venga adeguatamente affrontata a livello europeo e soprattutto nazionale[45].

La prima legislazione orizzontale dell'UE ad affrontare le sfide in materia di cybersicurezza, che ha rivoluzionato la resilienza e la cooperazione Europea è stata la Direttiva sulla sicurezza delle reti e delle informazioni (Direttiva EU n.2016/1148)[46], nota come NIS (*Network and Information Security*)[47], emanata dalla Commissione Europea come parte della strategia di cybersecurity dell'Unione. L'obiettivo della Direttiva è quello di migliorare la sicurezza informatica e delle informazioni in tutta l'Unione, imponendo agli Stati membri una serie di obblighi, per conseguire un livello comune elevato di sicurezza delle reti e dei sistemi informativi della UE. La Direttiva ha tre obiettivi principali: migliorare le capacità nazionali di cybersicurezza, rafforzare la cooperazione a livello dell'UE, promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare per gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e fornitori di servizi digitali, armonizzando le relative capacità nazionali in materia, la collaborazione transfrontaliera e la supervisione dei settori critici in tutta l'UE. Dopo l'approvazione della Direttiva NIS, ogni nazione Europea ha cominciato a implementare le leggi nazionali per la determinazione di obiettivi strategici e misure attuative, godendo di un certo margine di manovra per adattarsi a situazioni nazionali, come per esempio la possibilità di riutilizzare le strutture organizzative già esistenti o di allinearsi alla legislazione nazionale preesistente.

---

[45] C. CENCETTI, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Roma, 2014, p.25.

[46] JACCHIA, DE BERTI, "*La cybersecurity in Europa: fonti e legislazione*" 2017. p. 9.

[47] 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.

I settori che rientrano nell'ambito di applicazione della direttiva NIS riguardano l'energia, i trasporti, le banche, i mercati finanziari, la sanità, la fornitura e la distribuzione di acqua potabile, le infrastrutture digitali, i motori di ricerca, i servizi cloud e le piattaforme di commercio elettronico[48].

Il ruolo dell'ENISA nell' assistenza agli Stati membri è stato notevolmente ampliato grazie alla Direttiva NIS: non solo supporta i Paesi dell'Unione Europea a gestire le questioni comuni di cybersicurezza e a concordare gli approcci e le procedure comuni da seguire, ma individua anche le buone pratiche degli Stati membri e sostiene il processo di segnalazione per gli incidenti di sicurezza.

Considerando l'evoluzione della minaccia, era inevitabile che il testo della Direttiva NIS subisse delle modifiche, soprattutto per estendere il suo ambito di applicazione e preparare le imprese a fronteggiare le sfide presenti e future relative alla sicurezza delle reti e dei sistemi informativi. Questo ha portato la Commissione a proporre una revisione della Direttiva, sotto il nome di NIS2[49]. La proposta è volta a migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti di soggetti pubblici e privati, delle Autorità competenti e dell'UE nel suo complesso, nel campo della Cybersecurity e delle infrastrutture critiche. Nella revisione è stato ridefinito l'ambito di applicazione delle norme in materia, sono state rafforzate le autorità e le attività di supervisione a livello UE, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica. La Direttiva detta anche i requisiti minimi che i soggetti coinvolti saranno chiamati a garantire: devono analizzare e valutare i rischi di sicurezza dei sistemi informativi con operazioni di *vulnerability assessment* e di *penetration test*, gestire gli incidenti di sicurezza con un piano e un'attività di monitoraggio continuo e di *incident response*; dotarsi di un piano di continuità di

[48] *https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new*.

[49] La nuova direttiva NIS2 prevede il coinvolgimento, fra gli altri, dei seguenti settori di attività: infrastrutture digitali e digital provider; finanza; salute; reti idriche; energia; olio e gas; trasporti; pubblica amministrazione; reti e servizi per la comunicazione elettronica pubblica; servizi postali; aerospace; prodotti medicali, prodotti chimici, prodotti farmaceutici e dispositivi medicali; rifiuti; filiera agro-alimentare; data center e social network *https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/*

business e gestione delle crisi. Uno degli aspetti più rilevanti della NIS2 riguarda la gestione degli incidenti e la segnalazione alle autorità competenti[50].

La gestione degli incidenti ha anche un'importante connessione con il Regolamento UE 2016/679 (GDPR)[51], che disciplina la protezione dei dati personali nell'Unione Europea. L'obiettivo del Regolamento è quello di stabilire norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione dei dati. Un considerevole contributo, atto ad aumentare la fiducia e la sicurezza dei consumatori nel mercato è stato dato proprio dal GDPR, poiché il rispetto dei principi di privacy e protezione dei dati personali è una componente fondamentale della fiducia, che sta alla base della relazione tra utenti e fornitori di servizi digitali. Il diritto alla protezione dei dati personali[52] è sancito dall'art. 8 della Convenzione Europea dei Diritti dell'uomo[53] e dall'art. 16 del Trattato sul funzionamento dell'UE. Questo Regolamento è di grande importanza perché rivede gli strumenti volti a tutelare i dati personali di fronte alle nuove sfide tecnologiche e trattandosi di un Regolamento, esso non necessita di un recepimento da parte degli Stati ed è trattato allo stesso modo in tutti i paesi dell'UE senza margini di libertà nell'adattamento, pur lasciando spazi di manovra ai legislatori nazionali in alcune materie, in particolare quelle che investono in via diretta l'esercizio dei pubblici poteri.[54]

Nel Regolamento Generale sulla Protezione dei Dati, la definizione di "dato personale" assume un ruolo centrale delineando il perimetro entro il quale operano le normative sulla privacy e la protezione dei dati. Secondo l'art. 4 del GDPR[55], un dato personale è qualsiasi informazione relativa a una persona fisica identificata o

[50] È previsto un processo di segnalazione dell'evento entro 24 ore, con successiva notifica dell'incidente entro 72 ore.

[51] Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio dell'Unione Europea del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*.

[52] Il diritto alla protezione dei dati si è sviluppato a partire dal diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza; la dignità della persona umana, infatti, è il valore dominante di tutte le carte dei diritti.

[53] (*https://fra.europa.eu/it/eu-charter/article/8-protezione-dei-dati-di-carattere-personale*).

[54] B. SAETTA, "*Diritto alla protezione dei dati personali*", 22 luglio 2018.

[55] (*https://www.altalex.com/documents/news/2018/04/12/articolo-4-gdpr-definizioni*).

identificabile, direttamente o indirettamente, tramite riferimenti a un identificativo come il nome, un numero di identificazione, dati sulla localizzazione, o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. La definizione è ampia e inclusiva e stabilisce che qualsiasi informazione che possa essere collegata a un individuo è considerata un dato personale. Ciò include il numero di telefono, il codice fiscale, l'indirizzo e-mail, dati meno ovvi come l'indirizzo IP, o dati generati da app di tracking.

L'interessato ha il diritto di chiedere al titolare del trattamento (soggetto pubblico, impresa, associazione, partito o persona fisica) se sia in corso o meno un trattamento di dati personali che lo riguarda e, qualora il trattamento sia confermato, di ottenere una copia di tali dati e di essere informato su una serie di elementi, quali le finalità del trattamento, le categorie di dati personali trattate, i destinatari dei dati e il periodo di conservazione degli stessi, la loro origine, gli estremi identificativi di chi li tratta (titolare, responsabile, rappresentante), l'esistenza di un processo decisionale automatizzato, compresa la profilazione, ed infine, i diritti previsti dal regolamento[56].

Da questa disposizione normativa emerge il duplice obiettivo, ovvero la protezione delle persone fisiche per quanto riguarda il trattamento dei dati personali e la libera circolazione dei dati. Questi obiettivi vengono fortemente correlati da altri importanti principi che reggono l'elaborazione dei dati: la liceità, la correttezza e la trasparenza nel trattamento dei dati[57]; Inoltre, i dati dovranno essere trattati solo per uno scopo legittimo e specifico, oltre che esplicito, e dovranno essere poi adeguati, rilevanti, necessari rispetto alle finalità e trattati in modo sicuro e in modo da non subire alterazioni o accessi non autorizzati.

Il Regolamento pone anche l'accento sulla responsabilizzazione (*accountability*)[58] dei titolari e dei responsabili del trattamento, ossia sull'adozione di

[56] (*https://www.garanteprivacy.it/home/i-miei-diritti/diritti.)*

[57] Il trattamento di dati personali è lecito solo quando si fonda su una base legittima come il consenso oppure se il trattamento è necessario per l'esecuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali per una persona fisica o di interesse pubblico, il perseguimento di un legittimo interesse, ove non prevalgano diritti e libertà del soggetto interessato.

[58] «Accountability (responsabilizzazione)»: *https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili*.

comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento: la novità sta nel fatto che viene affidato ai titolati il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati dal regolamento. Il primo tra i criteri è sintetizzato dall'espressione inglese *data protection by default and by design*[59].

Ai sensi dell'articolo 25, paragrafo 1, del GDPR, per privacy by design si intende l'obbligo per il titolare, di mettere in atto "misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati".

L'articolo 25, paragrafo 2, del GDPR, prevede poi che "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento".

Le autorità di controllo e in particolare il Comitato Europeo per la protezione dei dati, svolgono un ruolo cruciale per assicurare un approccio uniforme e per fornire strumenti interpretativi e analitici. Infatti, il Comitato è incaricato di elaborare linee guida e altri documenti orientativi su queste e altre tematiche connesse, al fine di garantire gli adeguamenti necessari in risposta all'evoluzione delle tecnologie e dei sistemi di trattamento dei dati.

Nel 2016, la Commissione ha poi introdotto un pacchetto di misure volte a potenziare la cybersicurezza europea con nuove iniziative operanti sotto il triplice profilo della resilienza, deterrenza e difesa (*Cybersecurity Package*[60]). Collocandosi nella cornice della normativa di matrice europea in materia di sicurezza informatica, al fianco delle disposizioni della Direttiva (UE) n.2016/1148 "Direttiva NIS" e, di quelle del Regolamento (UE) n.2016/679 "GDPR", si colloca il Cybersecurity Act, relativo

[59] AGENDA DIGITALE. "*Privacy by design e by default: cosa sono, vantaggi e sfide*", 8 agosto 2023.

[60] COMMISSIONE EUROPEA, *Comunicazione congiunta al Parlamento europeo e al Consiglio, Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 (anche nota come "Cybersecurity package").

all'ENISA, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione[61]. Il Regolamento costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali.

Il Cybersecurity Act si compone di due parti: nella prima vengono specificati il ruolo e il mandato dell'ENISA[62], la quale assume un ruolo diretto nella prevenzione dei cyber-attacchi, rafforzando la propria posizione. Fino ad oggi il compito dell'ENISA è stato quello di assistere in termini tecnici gli Stati membri e le istituzioni europee nell'elaborazione di politiche in materia di sicurezza delle reti e dei sistemi informativi e a rafforzare la propria capacità di prevenire, rilevare e reagire agli incidenti informatici. La gestione operativa degli incidenti informatici rimane però una competenza esclusiva degli Stati membri. Il Cybersecurity Act intende rafforzare il ruolo dell'ENISA garantendole un mandato permanente e consentendole di svolgere non solo compiti di consulenza tecnica, come è stato finora, ma anche attività di supporto alla gestione operativa degli incidenti informatici da Parte degli Stati membri[63].

Un altro punto chiave del Regolamento riguarda l'introduzione di un sistema europeo di certificazione della sicurezza informatica dei prodotti e dei servizi digitali. La costituzione di schemi di certificazione specifici per prodotti e sistemi ICT[64] non è di per sé una novità. Infatti, numerosi schemi di questo tipo già esistono nella maggior parte degli Stati membri. Ad esempio, in Italia, l'Istituto Superiore delle Comunicazioni

---

[61] PARLAMENTO EUROPEO E CONSIGLIO, *Regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*

[62] Istituita il 13 marzo 2004 con il regolamento (CE) n. 2004/460 del Parlamento Europeo e del Consiglio del 10 marzo 2004; il suo scopo è quello "di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione".

[63] Agenda Digitale. "*Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT",* 7 giugno 2019.

[64] La definizione di Information Technology consiste nell'applicazione della tecnologia per risolvere problemi aziendali o organizzativi su vasta scelta. Il settore IT si basa su diversi servizi principali che sono i pilastri dell'information technology. «Servizi IT: cosa sono, cos'è l'Information Technology» (*https://sceglifornitore.it/blog/servizi-it-cosa-sono-cose-linformation-technology/*).

e delle Tecnologie dell'informazione già certifica la sicurezza informatica di prodotti e sistemi ICT secondo lo schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione. Tuttavia, molti schemi di certificazione esistenti non vengono riconosciuti all'estero, o almeno in tutti gli Stati membri. Ciò obbliga ad esplorare vari processi di certificazioni per operare a livello transnazionale.

Il Cybersecurity Act intende ovviare a tali problemi introducendo un quadro complessivo di regole che disciplinano gli schemi europei della sicurezza informatica. Tale attività è stata affidata principalmente all'ENISA, attraverso compiti e funzioni di promozione dell'uso delle suddette certificazioni e di incremento della trasparenza del livello di sicurezza dei prodotti ICT. Lo European Union Cyber Security Scheme on Common Criteria (EUCC)[65] è un sistema di certificazione e adesione volontaria, adottato proprio seguendo l'iter previsto dal Cybersecurity Act, secondo cui dopo l'iniziale richiesta formulata dalla Commissione, l'ENISA ha predisposto il sistema di certificazione oggi approvato[66].

Nelle intenzioni del legislatore europeo, l'istituzione di un sistema europeo comune di certificazione di questo tipo dovrebbe favorire la cosiddetta "security by design", ovvero la presa in considerazione della sicurezza informatica fin dagli stadi iniziali della progettazione dei prodotti ICT, inclusi quei dispositivi di consumo connessi alla rete che costituiscono il cosiddetto "Internet of Things"[67].

Le imprese e i singoli consumatori dovrebbero disporre di informazioni precise sul livello di affidabilità con cui è stata certificata la sicurezza dei propri prodotti, servizi e processi ICT.

Sono necessari ulteriori sforzi per accrescere la consapevolezza dei cittadini, delle organizzazioni e delle imprese circa le questioni riguardanti la cybersicurezza. In aggiunta, dato che gli incidenti minano la fiducia nei fornitori di servizi digitali e nel

[65] CYBERSECURITY 360, "*sistema UE di certificazione della cyber security: come adeguarsi al nuovo mercato digitale*", 8 febbraio 2024.

[66] ACCREDIA "*Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata*", 14 novembre 2022, p. 13.

[67] C. BOSCHIERO, "*Intelligenza Artificiale e cybersecurity*"), 14 giugno 2021. (*https://www.italiaoggi.it/news/intelligenza-artificiale-e-cybersecurity-2522679*).

mercato unico digitale, essa dovrebbe essere ulteriormente rafforzata fornendo informazioni in maniera trasparente in merito al livello di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC che evidenzi persino un livello elevato di certificazione della cybersicurezza. Un aumento di fiducia può essere agevolato da una certificazione a livello di Unione[68].

In quest'ottica, il Cybersecurity Act, affiancandosi alla direttiva NIS, ha come principale obiettivo quello di aumentare il coordinamento, anche attraverso l'aumento di un eguale livello di consapevolezza in tutta l'area euro comunitaria. Inoltre, la coesistenza di certificazioni pubbliche e le già esistenti certificazioni private (ISO) ambisce a creare le conoscenze e le abilità operative necessarie per garantire un livello appropriato di sicurezza. Il Regolamento tratta esplicitamente tre possibili livelli di affidabilità: livello base, sostanziale ed elevato[69]. Il livello di affidabilità è commisurato al rischio associato al previsto uso del prodotto, servizio o processo ICT, in termini di probabilità e impatto di un incidente[70]. I requisiti di sicurezza corrispondenti a ogni livello vengono indicati nel sistema europeo di certificazione della cybersecurity pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la specificità corrispondenti alla valutazione a cui deve essere sottoposto il prodotto, servizio o processo.

---

[68] PARLAMENTO EUROPEO E CONSIGLIO, *relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (Testo rilevante ai fini del SEE).*

[69] Nel primo caso il certificato ha lo scopo di assicurare che i prodotti, servizi e processi TIC siano stati valutati ad un livello sufficiente a ridurre i rischi informatici derivanti da noti di incidenti o attacchi informatici; il livello di affidabilità sostanziale, invece, certifica standard più elevati, comprese le funzionalità di sicurezza e ad un livello inteso a limitare i rischi noti di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. In questo caso, le attività di valutazione aumentano e diventa necessario procedere con un riesame per dimostrare il perdurare dell'assenza di vulnerabilità pubblicamente note. Infine, il certificato di livello elevato assicura che i prodotti, i servizi e i processi TIC rispettino i requisiti di sicurezza e siano stati valutati per ridurre al minimo i rischi derivanti da attacchi informatici.

[70] Per i prodotti, servizi e processi ICT con livello di rischio elevato la certificazione può essere rilasciata solo dall'Autorità nazionale di cybersecurity, oppure, in determinati casi, da un organismo di valutazione della conformità.

4.1. PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

In Italia, l'architettura nazionale di cybersecurity viene definita nel d.l. n. 82/2021, che istituisce il Sistema Nazionale di Sicurezza cibernetica e l'Agenzia per la Cybersicurezza Nazionale (ACN)[71]. L'Agenzia ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza informatica nello spazio cibernetico, uno dei fondamentali ambiti sui quali il Piano nazionale di ripresa e resilienza (PNRR) si è concentrato. La sicurezza cibernetica rappresenta infatti il primo dei 7 investimenti della Digitalizzazione della PA, pilastro principale della Componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "digitalizzazione, innovazione, competitività e turismo"[72].

Il Perimetro di Sicurezza nazionale Cibernetico, rappresenta per il nostro Paese un'innovazione epocale nella normativa di settore ed una opportunità unica per accrescere la competitività delle imprese strategiche nel nostro Paese.

La strategia nazionale di cybersecurity non è solo una lista con cui un governo identifica obiettivi astratti e programmatici, bensì è una vera e propria espressione della visione nazionale, dei principi e delle priorità che guideranno lo Stato nell'avanzamento dei propri interessi nella sfera cyber e in tutti gli ambiti con un'importante componente digitale.[73] Il panorama delle minacce continua a caratterizzarsi per l'elevata remuneratività dello strumento cyber per i malintenzionati, in ragione dell'ampia disponibilità di tool offensivi e dei bassi livelli di rischio operativo. Dal monitoraggio delle Tecniche, Tattiche e Procedure (TTP)[74] utilizzate è emerso un elevato livello di

[71] *https://www.acn.gov.it/portale/chi-siamo*.

[72] Missione 1 - la cybersicurezza nell'ordinamento italiano.

[73] Redazione, «Sviluppo di strategie nazionali di cybersecurity, la guida», CyberSecurity Italia (blog), 23 dicembre 2021 (*https://www.cybersecitalia.it/sviluppo-di-strategie-nazionali-di-cybersecurity-la-guida-di-un-gruppo-i-lavoro-internazionale/15869/*).

[74] Con l'acronimo di tattiche, tecniche e procedure (TTPs) si identifica una metodologia d'analisi delle minacce APT che consente di superare il tradizionale approccio alla cyber security basato sulla risposta agli incidenti per introdurre uno proattivo in grado di prevenire e respingere i nuovi e sempre più devastanti attacchi informatici. Ecco di cosa si tratta.

complessità e sofisticatezza delle azioni. In tale contesto, lo sforzo più significativo posto in essere dai responsabili d'intelligence ha riguardato il contrasto di campagne di spionaggio digitale.

Nel 2013 l'Italia ha delineato per la prima volta la sua architettura di sicurezza cibernetica, provvedendo a sintetizzare, sia pure con la legislazione vigente, le molteplici competenze di settore distribuite tra i diversi attori istituzionali. Ciò ha consentito l'avvio dell'accrescimento delle capacità cyber nazionali, opportunamente guidato dagli atti di indirizzo strategico e operativo[75].

I recenti attacchi informatici che hanno colpito il nostro Paese nel contesto di una guerra ibrida hanno fornito evidenze di danni economici e reputazionali per le imprese, blocco dell'operatività di infrastrutture energetiche, malfunzionamenti di sistemi informativi impiegati da aziende ospedaliere e sanitarie, fino alla diffusione di dati personali di figure pubbliche, giornalisti e attivisti politici col fine di screditare mettendole talvolta in pericolo. Per far fronte alle crescenti sfide che caratterizzano il panorama globale in ambito cyber, a livello nazionale sono state delineate una serie di normative al fine di innalzare il livello di sicurezza dei settori considerati essenziali per il Paese. Il fenomeno dei cyber attacchi non ha ovviamente lasciato indifferenti le istituzioni che hanno, nel corso del tempo, istituito svariati organismi di contrasto. Questo scenario ha portato all'approvazione, nel 2021, della Strategia nazionale di cybersicurezza 2022-2026[76], con annesso il Piano di Implementazione del comitato ministeriale per la Cybersicurezza (CIC). Nel corso della riunione del CIC è stato approvato anche l'ultimo DPCM per la realizzazione del Perimetro di sicurezza nazionale cibernetica gestito dall'Agenzia per la Cybersicurezza Nazionale (ACN) e nel quale rientrano tutti quei soggetti pubblici e privati che svolgono attività essenziali per lo Stato.

Punto di partenza della Strategia Nazionale di Cybersicurezza 2022-2026 è la considerazione che, da un lato, la migrazione verso il digitale sia un elemento

[75] AGID, "*Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali*", 13 febbraio 2020, p. 9.

[76] CYBERSECURITY360, "*strategia nazionale di cybersicurezza, gli obiettivi da raggiungere entro il 2026 per la resilienza del Paese*", 25 maggio 2022.

fondamentale nelle società contemporanee e, dall'altro, che tale processo non è privo di rischi e che, anzi, nel corso degli anni i pericoli in materia di cybersicurezza si sono ampliati e sono divenuti più complessi[77]. Il Decreto legislativo 82/2021 ha dato vita ad una nuova architettura nazionale, che si sviluppa su quattro pilastri principali. In primo luogo, è stata istituita l'Agenzia per la cybersicurezza nazionale, con competenze in ambito di cybersicurezza e resilienza. È stata poi rafforzata la prevenzione e il contrasto alla criminalità informatica, realizzata da una serie di corpi e servizi della Polizia di Stato, con l'inserimento di specifiche attività di difesa e ricerca affidate al comparto di Intelligence[78].

In tale contesto, con il d.l. n. 105/2019 ed i successivi decreti attuativi, è stato istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), con lo scopo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e di quelli informatici di alcune pubbliche amministrazioni e di aziende private opportunamente individuate. Il PSNC rappresenta per il nostro Paese un'innovazione epocale nella normativa di settore ed un'opportunità unica per accrescere la competitività delle imprese strategiche del nostro Paese, cercando di mettere in opera, a livello nazionale, tutte le prescrizioni e le disposizioni imposte dagli attuali regolamenti europei in tema di cybersecurity, in particolar modo alla direttiva NIS e dal Cybersecurity Act[79].

Tale Piano Nazionale costituisce una mappa per l'adozione, da parte dei soggetti pubblici e privati, delle misure prioritarie per l'implementazione del Quadro Strategico Nazionale, sulla base di un dialogo attivo e interattivo che vede nella protezione cibernetica e nella sicurezza informatica nazionali non solo un obiettivo ma, soprattutto, un processo che coinvolge tutti gli attori interessati, a vario titolo, alla tematica cyber.

Nel quadro di un intervento di sistema, coerente e definito, occorre poi fare leva sulle competenze e sulle responsabilità degli attori pubblici titolari di competenze

---

[77] tra questi: attacchi cyber dovuti a cybercriminali, rischi che provengono da tecnologie impiegate sviluppate e prodotte da grandi realtà aziendali influenzate da Governi, diffusione di fake news, deep fake o campagne di disinformazione.

[78] AVVISO PUBBLICO, "*Strategia Nazionale di cybersicurezza 2022-2026*", (https://www.avvisopubblico.it/home/home/cosa-facciamo/informare/documenti-tematici/mafie/strategia-nazionale-di-cybersicurezza-2022-2026-sintesi-del-documento/).

[79] Perimetro di sicurezza nazionale cibernetica (PSNC) (https://www.acn.gov.it/portale/faq/nis-e-psnc).

primarie a livello nazionale nel settore cyber. In tale contesto, si mira a semplificare la *governance*[80], attraverso l'accorciamento della catena decisionale e la razionalizzazione dei processi di lavoro, sia di carattere ordinario, sia per la risposta emergenziale ad eventi cibernetici, ponendosi altresì quale fulcro della cooperazione tra le amministrazioni che compongono lo stesso Nucleo. La visione sistematica che informa il presente piano d'azione volta ad assicurare la messa in sicurezza degli *assets* nazionali secondo una progressione dettata da una scala di criticità:

- al primo livello si colloca la Sicurezza nazionale dello stato (comparto di Intelligence, Difesa, Interno, Amministrazioni CISR);
- al secondo livello si trovano le infrastrutture critiche nazionali (TLC, utilities, settore finanziario, trasporto);
- al terzo livello si trova il tessuto produttivo nazionale, cittadinanza.

A rendere complessa l'analisi del documento è l'introduzione di un "Piano di Azione" che raccoglie le iniziative individuate per garantire il necessario ed effettivo cambio di passo in termini di innalzamento dei livelli di sicurezza dei sistemi e delle reti del nostro Paese. Comprendere il rischio del sistema Paese connesso con la minaccia cyber è un elemento fondamentale per una corretta identificazione delle azioni da adottare. Questo si declina mediante l'individuazione di una metodologia di cyber risk management univoca e condivisa a livello strategico e l'adozione del piano di valutazione dei rischi (come previsto dalla Direttiva NIS)[81].

Si mira a creare un'approfondita conoscenza delle vulnerabilità non solo del fattore tecnologico ma anche di quello umano e delle minacce cibernetiche che le sfruttano mediante una valutazione in continuo delle stesse che includa sia soggetti istituzionali, che soggetti privati. In merito alla collaborazione tra soggetti pubblici e privati, obiettivo del Piano è quello di potenziare il coordinamento e la cooperazione tra questi, con la consolidazione di canali di dialogo e consultazione tra le istituzioni ed i

[80] Con il termine *Governance* si fa riferimento all'insieme di principi, regole e procedure che riguardano la gestione di una società, di un'istituzione, di un fenomeno collettivo.

[81] R. SETOLA, *Il piano nazionale per la protezione cibernetica e la sicurezza informatica*, in Sicurezza e Giustizia, n. 3/2017, p. 31.

settori privati nell'ottica dell'approccio "Sistema Paese". La rapida evoluzione tecnologico-informatica comporta un altrettanto veloce obsolescenza delle norme che disciplinano materie correlate alle tecnologie dell'informazione e della comunicazione. Pertanto, esse necessitano di periodiche revisioni e aggiornamenti anche alla luce della necessità di finalizzare il quadro normativo relativo alle infrastrutture critiche nazionali informatizzate, nonché di identificare gli strumenti tecnici, inclusi quelli relativi all'indirizzamento necessari all'attribuzione di responsabilità in caso di violazioni di sicurezza[82].

Un comune livello di protezione informatica è garantito anche dalla compliance a standard e protocolli di sicurezza. Occorre però provvedere all'identificazione, adozione, aggiornamento e verifica degli standard di riferimento, delle best practices a delle misure e requisiti minimi per la sicurezza delle reti. Per gestire correttamente un evento cyber con un impatto significativo sulla popolazione è necessario predisporre un coordinamento sulla *Situational Awareness* dei contenuti e delle informazioni, allo scopo di rendere efficaci i flussi comunicativi al fine di essere in grado di fornire, ove necessario o opportuno, un'informazione completa, corretta e veritiera. Il Perimetro di sicurezza nazionale cibernetica risulta composto da attori privati e pubblici che esercitano funzioni essenziali dello Stato o assicurano un servizio essenziale alle attività fondamentali per l'interesse dello Stato stesso[83].

In particolare, il decreto del 30 luglio chiarisce che un soggetto esercita una funzione essenziale dello Stato laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti[84]. Invece, un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o

---

[82] *https://www.sicurezzaegiustizia.com/il-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/*.

[83] CYBERSECURITY360, "*Dalla percezione alla consapevolezza: il ruolo critico della formazione nella cyber security",* 26 settembre 2023.

[84] CYBERSECURITY360, "P*erimetro di sicurezza nazionale cibernetica: regole e criteri di attuazione* ", 30 ottobre 2020.

economiche fondamentali per gli interessi dello Stato laddove realizzi una serie di attività che vengono ivi elencate, tra cui le attività strumentali all'esercizio di funzioni essenziali dello Stato, e le attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica. I soggetti suddetti sono individuati tra gli operatori dei vari settori: interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche ed enti previdenziali/lavoro[85].

Il Decreto prevede che, per ogni settore, il ministero di competenza agisca in quattro direzioni.

Innanzitutto, l'amministrazione preposta deve individuare le funzioni e i servizi essenziali che dipendono da reti, sistemi informativi o sistemi informatici la cui interruzione possa compromettere la sicurezza nazionale. In secondo luogo, con riguardo ad un'interruzione della funzione o del servizio essenziale, la P.A. deve valutare l'estensione territoriale della funzione essenziale, il numero di utenti e le possibili ricadute economiche. Quanto agli effetti di una compromissione della funzione o del servizio essenziale, l'amministrazione dovrà prendere in esame le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati per il loro svolgimento. Ancora, è necessario valutare le possibilità di mitigazione per il ripristino dello svolgimento della funzione o del servizio in condizioni di totale sicurezza. Infine, la terza direttiva prevede che il ministero di competenza individui le funzioni e i servizi essenziali per i quali, in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è massimo e le possibilità di mitigazione minime[86].

In conclusione, la normativa in settore è in continua evoluzione e si attendono numerosi interventi normativi, sia da parte dell'ACN, sia in termini di implementazione di direttive europee.

---

[85] Bird&Bird, "*DPCM 131/2020: nuove disposizioni in materia di cybersecurity*".

[86] CYBERSECURITY 360, "*Perimetro di sicurezza nazionale cibernetica: regole e criteri di attuazione*", 30 ottobre 2020.

5. INFRASTRUTTURE CRITICHE NEL MIRINO DEGLI HACKER

La iper-digitalizzazione ha reso molto più complesso definire ciò che è critico per il funzionamento e la stabilità di un Paese. Per anni si è parlato di infrastrutture critiche, ma oggi è più opportuno parlare di servizi considerati essenziali non solo dai governi, ma anche dai cittadini. Inoltre, stiamo passando da una difesa preventiva, finalizzata a prevenire gli attacchi, a una difesa dinamica e proattiva che si comporta in modo simile al sistema immunitario: si parla di resilienza, concetto molto noto in ambito finanziario, ma sempre più popolare anche nel dominio più ampio della difesa di nazioni, sistemi economici ed ecosistemi digitali[87].

Le infrastrutture critiche sono sempre più sotto attacco, ma anche sempre più vulnerabili, essenzialmente per il mancato coordinamento delle attività di protezione e la mancanza di investimenti in sicurezza. Lo sostiene il Rapporto presentato il 27 aprile scorso alla trentottesima Assemblea generale annuale dell'International Security Ligue, "Cyber-Physical Security e and Critical Infrastructure". Il nuovo rapporto è un progetto congiunto della Ligue, fondata nel 1934 e che rappresenta le principali società di sicurezza del mondo, e della Confederazione dei servizi di sicurezza europei (CoESS), ed ha visto il contributo di Antonello Villa, vicepresidente di Univ e componente di giunta di ConFederSicurezza e Servizi.

Il rapporto descrive le strategie di supervisione e gestione necessarie per proteggere le società nell'era dei sistemi connessi e delle minacce ibride (fisiche/logiche). Enucleando le sfide che devono affrontare le infrastrutture critiche mondiali, il rapporto approfondisce le questioni più critiche con l'ausilio di esperti di sicurezza su temi come la governance della sicurezza integrata, il ruolo della legislazione e della regolamentazione, i *penetration test* e la valutazione del rischio e la necessaria partnership tra pubblico e privato. Il rischio per le infrastrutture critiche cresce man mano che i sistemi legacy delle infrastrutture critiche vengono aperti alla comunicazione e spinti verso il cloud, offrendo agli aggressori nuove opportunità di

[87] FORTUNE ITALIA, "*Cybersecurity e infrastruttura critica, dalla prevenzione alla resilienza*", 19 maggio 2023.

attacco, e possono verificarsi anche in conseguenza di tensioni geopolitiche, a scopo di riscatto o di terrorismo[88].

I dati del rapporto Clusit[89], rilevano che nel 2023 in Italia gli attacchi informatici sono cresciuti del 65%. Oltre la metà sono stati classificati come critici o di elevata gravità. L'Italia ha subito l'11% degli attacchi gravi a livello mondiale, mostrando una crescente vulnerabilità nel panorama globale della cybersecurity e una marcata escalation di episodi legati *all'hacktivism*[90] e al cybercrime.

L'incidenza di attacchi informatici è in continuo aumento e nei recenti sei mesi si è osservato un significativo incremento di cyber attacchi che hanno causato notevoli disagi in diversi settori, soprattutto in quelli legati alle infrastrutture critiche. I settori cruciali quali energia, produzione critica, gestione delle risorse idriche e impianti nucleari sono tra le categorie di infrastrutture critiche spesso bersagliate in gran parte degli incidenti riportati[91]. Nonostante gli sviluppi recenti, connotati da una forte consapevolezza sia dei decisori politici che dei *board* aziendali, con l'adozione conseguente di stringenti misure di difesa e resilienza, la sicurezza informatica, all'interno della Pubblica amministrazione e delle infrastrutture critiche, sembra costituire tuttora un *vulnus* evidente come testimoniano tutti gli attacchi sin qui avvenuti. La numerosità di questi eventi – ovvero gli attacchi alle strutture critiche, in primo luogo sanitarie ma anche imprese private di ogni ordine e grado – non ha fatto che rendere di pubblica evidenza quello che si poteva facilmente ipotizzare già in precedenza. Vale a dire che esisteva un problema di messa in sicurezza di tali infrastrutture[92].

---

[88] FEDER SICUREZZA, "*Infrastrutture critiche sotto attacco: il nuovo White Paper del CoESS*". 8 maggio 2023.

[89] INNOVATIONPOST, *"Italia sempre più nel mirino dei criminali informatici: attacchi in crescita del 65%", 6 marzo 2024. (https://www.innovationpost.it/attualita/italia-sempre-piu-nel-mirino-dei-criminali-informatici-attacchi-in-crescita-del-65/#:~:text=Il%20nostro%20Paese%20appare%20sempre,del%2065%25%20rispetto%20al%202022.)*

[90] Derivato dall'unione delle parole 'Hack' e 'Activism', l'hacktivism è l'atto di hackerare, o di introdursi in un sistema informatico, per scopi politicamente o socialmente motivati.

[91] Report Clusit 2023.

[92] *https://www.ictsecuritymagazine.com/articoli/le-infrastrutture-critiche-allintersezione-tra-dispositivi-cyber-fisici-e-cyber-threat-intelligence/.*

Uno scenario riguardo al quale Gabriele Faggioli, presidente Clusit e CEO Digital 360, ha spiegato: "le strategie adottate oggi, anche a livello normativo, sono state sicuramente utili e importanti per cercare di limitare la crescita del fenomeno ma per far rallentare il trend e cercare di stabilizzarlo, e possibilmente ridurlo, devono essere concepite e adottate strategie nuove che si fondino sul *knowledge sharing*, sulla messa a fattor comune degli investimenti e sulla assunzione di responsabilità verso la comunità per chi deliberatamente decide di non proteggere adeguatamente la propria struttura con ciò arrecando danno all'intero ecosistema Paese"[93]. Il tema centrale, per gli stati, le aziende e i singoli cittadini, dovrebbe concentrarsi non tanto su quali sono i controlli da implementare per prevenire l'attacco, ma piuttosto capire come riuscire a riprendersi il prima possibile e limitare impatti e conseguenze.

In tale contesto, a tutela delle infrastrutture critiche del Paese, è cruciale il ruolo che può svolgere la Cyber Threat Intelligence[94], l'attività di raccolta di dati provenienti da varie fonti in merito ad attacchi che colpiscono o sono potenzialmente in grado di offendere la sicurezza di un'organizzazione. La Threat Intelligence implica che i "messaggi lasciati" nel mondo Cyber debbano essere gestiti adeguatamente per prevenire e contrastare le minacce informatiche. Vanno definite poi delle *Standard Operating Procedures*, che vanno eseguite utilizzando le risorse specifiche in base alle competenze e/o strumenti in dotazione al team: può essere ad esempio una chiave d'accesso o un tool per eseguire una procedura informatica nel caso di un *Computer Security Incident Response Team* (CSIRT), magari insieme ad una squadra di manutenzione Emergency Response Team (ERT) che va sul campo, per comandare manualmente un azionamento che – se manomesso – potrebbe causare danni a persone e/o cose. L'elaborazione di una strategia per la sicurezza nel Cyber Space richiede una crescente collaborazione internazionale e nuove sfide fra governi, imprese e mondo accademico e della ricerca scientifica".

[93] CYBERSECURITY360, "*Attacchi cyber, l'italia più vulnerabile:i dati del rapporto Clusit 2024*".

[94] La Threat intelligence è il processo di identificazione e analisi delle cyberminacce. Il termine "threat intelligence" si riferisce sia ai dati raccolti su una potenziale minaccia sia ai processi di aggregazione, interpretazione e analisi di quei dati per una migliore comprensione delle minacce. La Threat intelligence prevede ordinare i dati, esaminarli in maniera contestuale per individuare i problemi e mettere in campo soluzioni specifiche al problema trovato (*https://www.kaspersky.it/resource-center/definitions/threat-intelligence*).

"Il Cyber Space, imprescindibile nei settori strategici del Paese, è un nuovo campo di battaglia e di competizione geopolitica nel XXI secolo – evidenzia Leporale – La rivoluzione nel campo delle tecnologie dell'informazione e della comunicazione sta trasformando la natura del potere e delle relazioni internazionali, con nuovi tipi di conflittualità e di minaccia alla sicurezza degli Stati e del sistema internazionale. La comprensione dei rischi inediti derivanti dal Cyber Space rappresenta una grande sfida intellettuale a livello mondiale per la tutela di infrastrutture critiche di aziende, pubbliche amministrazioni e Stati".

E l'Europa si è attrezzata con il varo della direttiva NIS che nel febbraio 2023, è stata aggiornata con la NIS 2: le regole puntano a creare un livello comune elevato di cybersicurezza e migliorare la resilienza e le capacità di risposta agli incidenti dell'Ue[95].

I temi della sicurezza cibernetica, della protezione dei dati personali e della protezione delle infrastrutture critiche, pongono il sistema paese, le istituzioni e le aziende di fronte a responsabilità e profili di sicurezza inediti. Ne è testimone l'attuale inedito assetto normativo, delineato dalle due norme pilastro GDPR e NIS (recepita quest'ultima in Italia dal D.Lgs. n. 65/2018) e dall'ulteriore tessuto normativo di recente attuazione, composto dal D.L. n. 105/2019 recante Disposizioni in materia di perimetro di sicurezza nazionale cibernetica e dalla recente modifica apportata al D.L. n. 21/2012 (c.d. "Decreto golden power")[96], che ha esteso l'esercizio dei poteri speciali del Governo anche al processo di approvvigionamento dei servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

Occorre dunque un cambio di marcia nel dotarsi di procedure e di strumenti necessari ad affrontare con efficacia eventuali attacchi cyber che, colpendo le infrastrutture critiche, possono mettere in ginocchio il Paese.

[95] CorCom. "*Cyber Intelligence cruciale per la tutela delle infrastrutture critiche del Paese*". 5 dicembre 2023.

[96] *https://www.assonime.it/Eventi/Pagine/Cybersecurity-nelle-Infrastrutture critiche.aspx*.

6. RISK MANAGEMENT E COMPLIANCE: LA CONSAPEVOLEZZA DEL RISCHIO CYBER E LA CONFORMITA' AGLI STANDARD INTERNAZIONALI.

Il rischio deriva da un insieme di variabili che possono essere sia interne sia esterne all'azienda, difficili da prevedere per l'uomo e soprattutto da controllare. L'impresa si trova quotidianamente ad affrontare un cospicuo numero di situazioni incerte e di rischio che possono mettere in dubbio il conseguimento di un adeguato equilibrio economico, patrimoniale e finanziario e, nel medio e lungo termine, la creazione di valore e la sopravvivenza della stessa azienda.

La protezione dei dati interessa ognuno di noi, inteso come individuo o come organizzazione. Come realizzare un efficace sistema di protezione, invece, presenta un ampio margine di discrezionalità, solo in parte giustificato dalle caratteristiche del business ma principalmente per l'impossibilità di una soluzione certa e condivisa. In generale, il modo per affrontare la questione di sicurezza è quello di affidarsi ad una metodologia riconosciuta internazionalmente e di aggiustare la soluzione, gradualmente nel tempo, con l'aiuto di una ciclica valutazione del rischio.

La gestione del rischio è il processo di identificazione, valutazione e controllo delle minacce al capitale, agli utili e alle operazioni di un'organizzazione. Questi rischi derivano da una varietà di fonti, tra cui incertezze finanziarie, responsabilità legali, problemi tecnologici, errori di gestione strategica, incidenti e disastri naturali. Diventa quindi molto importante investire principalmente sulla consapevolezza degli utenti e indicare delle linee guida e delle *best practices* da adottare. Se infatti le aziende possono dotarsi di tutte le tecnologie più sofisticate, l'aspetto più importante rimane comunque la formazione degli utenti[97] e la capacità di non cascare nei tranelli dei cybercriminali. Il fattore umano è sempre l'anello debole della catena[98].

[97] L'emergenza legata al Covid ha accelerato il processo di digitalizzazione, modificando i comportamenti degli utenti con una maggiore spinta verso la sfera digitale. Questo spostamento ha portato ad un aumento dell'attività da parte di cyber criminali. Secondo un report di Check Point research, nel 2021, in tutto il mondo gli attacchi informatici verso le aziende sono cresciuti del 40% rispetto al 2020; settimanalmente le aziende italiane ne subiscono mediamente 903e hanno visto crescere la percentuale del 36% rispetto al 2020. CybergON Blog, "cyber security Awareness".

[98] RISK MANAGEMENT 360, "*Gestione del rischio: quali sono le best practices e gli strumenti necessari per le aziende*", 13 giugno 2023.

La maggior parte delle minacce proviene proprio dalla poca attenzione che le persone mettono nel compiere azioni di routine: l'utilizzo delle proprie credenziali, la navigazione non sicura o la poca attenzione nella gestione della posta elettronica.

Non si può mai essere sicuri di evitare completamente un attacco informatico, ma esistono diverse azioni da mettere in atto per cercare di ridurre al minimo questo rischio[99].

Innanzitutto, per aumentare la soglia di attenzione dei dipendenti, andrebbero erogati training specifici i quali sono di fondamentale importanza per limitare il rischio e creare una maggiore consapevolezza della pericolosità che un attacco può provocare, non solo all'azienda, ma anche al singolo individuo. La formazione deve essere continua e nell'arco di un lungo periodo, in modo da tenere sempre alta la sensibilità degli utenti sull'argomento. Durante il tirocinio presso la beanTech, sono stati condotti corsi di formazione per l'intera azienda, non solo come misura efficace e indispensabile per tutti i dipendenti, ma anche come passaggio importante per garantire la conformità agli standard ISO 27001[100].

Settimanalmente, la beanTech condivide dei report in merito alla "Cyber threat intelligence"[101], i quali forniscono un'analisi dettagliata delle minacce cibernetiche emergenti. Questi bollettini contengono informazioni utili per delineare le minacce informatiche che colpiscono o che potrebbero colpire un'organizzazione, prevedendo eventuali rischi e vulnerabilità. Includono dettagli sui nuovi tipi di ransomware, sui loro comportamenti, sui vettori di attacco e sulle possibili conseguenze. Includono inoltre una sezione specifica sulle notizie dal cybercrime, ossia una sezione dedicata ad aggiornamenti su notizie relative al crimine informatico e una sezione dedicata ai

[99] CYBERGON, "*Cyber Security Awareness: quando il fattore umano può ridurre il rischio di un attacco informatico*". 4 aprile 2022.

[100] la norma ISO/IEC 27001 delinea e fornisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS), specifica una serie di migliori pratiche e descrive in dettaglio i controlli di sicurezza che possono aiutare a gestire i rischi legati alle informazioni.

[101] La Cyber Threat Intelligence (CTI), o semplicemente Threat Intelligence, è l'attività di raccolta delle informazioni provenienti da diverse fonti, che vengono analizzate ed elaborate, per scoprire tendenze e relazioni degli attacchi informatici per comprendere in modo approfondito minacce effettive e potenziali. Lo scopo è fornire delle informazioni accurate per intraprendere azioni efficaci al fine di prevenire gli attacchi e rendendo la protezione proattiva.

"Cyber tip of the week", ossia consigli e suggerimenti per una migliore comprensione sulla sicurezza dei propri dati personali e dei propri sistemi. Altre buone pratiche consistono nella creazione di *phishing test ad hoc* che simulino attacchi di *phishing* per testare il livello di preparazione dei propri dipendenti. Queste campagne mirate, del tutto innocue, risultano molto utili per fornire una fotografia del livello di vulnerabilità del fattore umano all'interno dell'azienda. I risultati ottenuti sono utili per capire come impostare i corsi di formazione.

Un ulteriore elemento di valutazione delle vulnerabilità aziendali è l'analisi OSINT, ricerca di informazioni private appartenenti all'azienda o al singolo individuo che vengono fatte per capire l'esposizione dei dati disponibili su Internet. Partendo da semplici dati come il nome e cognome è possibile impersonare un soggetto condurre all'inganno tramite tecniche efficaci di social engineering. L'OSINT si rivela quindi uno strumento estremamente utile ed efficace per investigare la presenza di informazioni e il rischio connesso al riutilizzo di tali dati a fini malevoli[102].

Dopo un'adeguata formazione, gli utenti dovrebbero essere in grado di riconoscere i diversi casi di *social engineering* e quindi, seguendo le procedure di policy interne all'azienda, riportare un maggior numero di incidenti direttamente al dipartimento IT. Negli ultimi anni sta cambiando notevolmente l'approccio delle aziende verso il concetto di cybersecurity: sono infatti le stesse organizzazioni che, in seguito al costante aumento di attacchi subiti, stanno investendo sulla formazione erogata ai propri dipendenti.

Il fattore umano rimane comunque un primo passo per una protezione efficace contro il cyber crimine, che deve poi proseguire con l'analisi e la gestione dei rischi da parte di specialisti del settore, che con l'utilizzo di strumenti a loro disposizione, saranno in grado di ridurre l'esposizione ai rischi cyber[103].

[102] AGENDA DIGITALE, "*Open Source Intelligence (OSINT): cos'è, a chi serve e come usarla*", 23 aprile 2024.

[103] CYBERGON, "*Cyber Security Awareness: quando il fattore umano può ridurre il rischio di un attacco informatico*", 4 aprile 2022.

La storia degli incidenti degli ultimi anni ci dice che nella gran parte dei casi, sia il verificarsi dell'incidente in sé, sia soprattutto l'ampiezza dell'impatto, sono dovuti dall' inadeguatezza di misure di sicurezza fondamentali e da fattori non controllabili esterni all'azienda. Tale inadeguatezza spesso non è dovuta da una mancanza di risorse in senso assoluto, ma dalla scarsa percezione della criticità dei rischi di cyber security, percepita come una tematica della "Direzione IT", piuttosto che come una tematica di rischio per l'intera infrastruttura.

La Direttiva NIS2 è la legislazione a livello UE sulla sicurezza informatica. Fornisce una serie di misure legali per aumentare il livello generale di sicurezza informatica nell'UE. Le norme UE sulla sicurezza informatica introdotte nel 2016 sono state aggiornate dalla Direttiva NIS2 entrata in vigore nel 2023. Ha modernizzato il quadro giuridico esistente per tenere passo con la crescente digitalizzazione e un panorama di evoluzione delle minacce alla sicurezza informatica[104]. Estendendo l'ambito di applicazione delle norme sulla sicurezza informatica a nuovi settori ed entità, si migliora ulteriormente la resilienza e le capacità di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'UE nel suo insieme[105].

La Direttiva sulle misure per un livello comune elevato di cybersicurezza nell'Unione prevede misure giuridiche per aumentare il livello generale di cybersicurezza garantendo:

- la preparazione degli Stati membri, chiedendo loro di essere adeguatamente attrezzati. Ad esempio, con un Computer Security Incident Response Team(CSIRT) e un'autorità nazionale competente per le reti e i sistemi informativi (NIS).
- cooperazione tra tutti gli Stati membri, istituendo un gruppo di cooperazione per sostenere e facilitare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri.

[104] Cybersecurity360, *"NIS 2 e ISO/IEC 27001: i requisiti di governance contro il rischio di incidenti cyber*", 28 febbraio 2024.

[105] *https://www.cybersecurity360.it/legal/nis-2-e-iso-iec-27001-i-requisiti-di-governance-contro-il-rischio-di-incidenti-cyber/.*

- una cultura della sicurezza in tutti i settori che sono vitali per la nostra economia e società e che dipendono fortemente dalle TIC.[106]

L'articolo 20 "Governance", al comma 1 indica che gli organi di gestione dei soggetti in perimetro dovranno approvare "*le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21*". L'articolo 21 afferma che "*l'organo di gestione sarà tenuto a seguire una formazione per far si che acquisisca conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto*"[107].

L'esigenza di gestire i temi di cybersecurity e i requisiti posti più esplicitamente dalla Direttiva NIS, non si esauriscono in generale con attività svolte dalla Direzione IT.

Dal maggio 2018, con l'applicazione del GDPR, è entrato in vigore un severo quadro normativo sulla protezione dei dati, che è uno dei contesti chiave della sicurezza informatica, da applicare per tutte le aziende che operano con cittadini dell'UE e spostando temi su una prospettiva *legal-tech*, il GDPR regola il trattamento e la diffusione di dati personali relativi alle persone fisiche e giuridiche, identificativi di ruoli e responsabilità, richiedendo esplicitamente alle organizzazioni di dimostrare di aver incorporato il principio della protezione dei dati fin dalla progettazione e per impostazione predefinita, adottando misure tecniche e organizzative adeguate a garantire che il trattamento di tali dati sia conforme al Regolamento[108]. La sicurezza delle informazioni è fondata su tre aspetti principali: riservatezza, disponibilità e integrità. per garantire il successo e la continuità dell'azienda e minimizzare l'impatto di eventi negativi, la sicurezza delle informazioni implica l'uso e la gestione di adeguate misure di sicurezza, prendendo in considerazione un'ampia varietà di minacce e implementando una serie di misure di controllo selezionate in base al processo di gestione del rischio e gestite utilizzando un framework che comprenda politiche,

[106] https://digital-strategy.ec.europa.eu/it/policies/nis2-directive
[107] *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555*
[108] *https://www.ictsecuritymagazine.com/articoli/gdpr-compliance-e-iso-27001-sistemi-di-gestione-della-sicurezza-oltre-la-formalita/.*

processi, procedure, strutture organizzative, software e hardware, al fine di proteggere la risorse informative identificate come a rischio. Un ISMS (*Information Security Management System*), o ISO/IEC 27001[109], è una norma volontaria per la gestione della sicurezza dei dati e dei sistemi informatici riconosciuta a livello internazionale e applicabile a organizzazioni di differenti dimensioni e operanti in qualsiasi settore. I benefici di un modello di ISMS sono evidenti perché consentono di avere una visione complessiva e centrale della sicurezza aziendale che spazia oltre il perimetro IT includendo anche persone e processi secondo un approccio olistico ma permette anche di ottenere una corretta visione sullo stato della security e diventa uno strumento fondamentale per l'ottimizzazione dell'allocazione del budget indirizzandolo verso le iniziative che restituiscono un maggior ritorno in termini di riduzione del rischio[110].

Il più diffuso modello di riferimento per costruire e monitorare un sistema di sicurezza informatica è lo standard internazionale ISO/IEC 27001, contenente requisiti per la gestione della sicurezza delle informazioni. Si integra in maniera coerente ed efficace con altri sistemi di gestione, quali ad esempio quelli relativi alla qualità (ISO 9001), all'ambiente (ISO 14001), alla gestione dei servizi IT (ISO/IEC 20000) e in combinazione con la ISO 27001, permette ad un'organizzazione di rispondere agli obiettivi previsti dal GDPR. Un sistema di gestione della sicurezza dei dati secondo la ISO 27001 consente non solo un miglioramento continuo dei sistemi di gestione ma anche un miglioramento in efficacia e in efficienza dei processi[111].

Come passaggio base, richiede l'analisi nel contesto esterno e interno, al fine di individuare minacce, vulnerabilità, ma anche opportunità e punti di forza esistenti. Attraverso questa analisi vengono acquisiti elementi utili ad indirizzare efficacemente le attività di prevenzione e protezione del cyberspazio. Il secondo passaggio è l'analisi dei processi e la mappatura dell'infrastruttura adottata per supportare i processi

[109] La norma ISO/IEC 27001 delinea e fornisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS), specifica una serie di migliori pratiche e descrive in dettaglio i controlli di sicurezza che possono aiutare a gestire i rischi legati alle informazioni.

[110] CYBERSECURITY360, *"ISMS: cos'è, a cosa serve e come strutturare un Information Security Management System*". 21 gennaio 2020.

[111] CYBERSECURITY360, "*ISO 27001 e NIST Cybersecurity Framework: binomio vincente per un'efficace protezione dei dati*".

medesimi. Queste informazioni, correlate alla conoscenza di pericoli e minacce, sono la base dei processi di valutazione dei rischi e di analisi di continuità operativa, che per un'organizzazione operante nel mercato attuale significa capacità di sopravvivenza a fronte di molteplici incidenti informatici e di sicurezza oggi ipotizzabili. Definiti i rischi e i beni dell'organizzazione che possono essere esposti o comunque impattati da relativi eventi,si potranno progettare e applicare misure organizzative e tecniche atte a mitigare i rischi, dette anche "controlli operativi". L'esistenza di tali rischi sarà intesa più come elemento base per lo sviluppo di un percorso ottimale, per tenere sotto controllo l'organizzazione.

L'audit interno, svolto in beanTech è stato un processo fondamentale per garantire la conformità alle norme di sicurezza delle informazioni. Nella fase iniziale viene definito il piano di audit, che identifica le aree chiave da esaminare e stabilisce un calendario chiave per le revisioni. Durante l'audit, un team esterno esamina i processi, le politiche e i controlli dell'azienda per verificare se rispettano gli standard ISO 27001. Questo può includere l'analisi delle politiche di backup, i controlli delle misure di protezione fisica, la gestione delle password e dei log. Gli auditor raccolgono poi le prove dell'audit e le valutano per identificare eventuali non conformità. Il processo di audit non solo aiuta l'azienda a mantenere la conformità agli standard, ma contribuisce anche a creare una cultura di sicurezza all'interno dell'organizzazione, aumentando la consapevolezza del rischio cyber.

L'integrazione di NIS2 e ISO/IEC 27001 rappresenta dunque una scelta strategica per le Organizzazioni che desiderino rafforzare la propria sicurezza informatica, ottimizzare le risorse e migliorare la postura di sicurezza. Il modello "ibrido" proposto consente di combinare la tempestività e il coordinamento normativo della NIS2 con la flessibilità e l'adattabilità organizzativa dello standard sui sistemi di gestione della sicurezza delle informazioni.

Tale sinergia potenzia l'efficacia delle strategie di risposta e fortifica la gestione degli incidenti a tutto il mondo, sia la protezione delle infrastrutture critiche che la continuità operativa.

7. CONCLUSIONI

La cybersecurity è rilevante non solo come valore in sé, ma nell'ottica di bene comune della sicurezza nazionale, della protezione delle infrastrutture critiche, dello sviluppo del mercato digitale e della tutela delle libertà fondamentali. Il campo della cybersecurity in Europa rappresenta un *work in progress*. La lotta al cybercrime e la protezione delle infrastrutture critiche informatizzate, gli aspetti più importanti della sicurezza cibernetica richiedono un'adeguata trattazione, non solo a livello nazionale, ma anche a livello europeo. Perché si realizzi un adeguato livello di protezione, a fronte di sfide globalizzate e minacce sempre più transnazionali, l'Unione Europea promuove un approccio strategico di tipo globale, fondato sulla cooperazione internazionale e sulla condivisione di informazioni a tutti i livelli, ridistribuendo la responsabilità tra settore pubblico e privato[112].

Nelle società che dipendono dall'infrastruttura digitale per funzionare, l'integrità dei sistemi è un elemento essenziale. La robustezza dei sistemi gestita nell'interesse pubblico, in un quadro d'insieme caratterizzato dalla centralità dei diritti fondamentali, può avere effetti diretti e indiretti sullo sviluppo della società: dal funzionamento delle infrastrutture critiche alla protezione delle attività che i cittadini concludono online. La pratica dell'*information sharing*, concetto largamente percepito come principio della cybersecurity, a livello europeo e nazionale è alla base del consolidamento di un atteggiamento costruttivo finalizzato al coordinamento politico e al progresso tecnologico, fondamentale per la trattazione adeguata della sicurezza cibernetica. Lo scambio di informazioni ed esperienze dovrebbe coinvolgere le istituzioni europee e gli attori statali, ma anche le imprese e i singoli cittadini.

La cybersecurity è una responsabilità condivisa tra chi progetta sistemi, chi fornisce requisiti di sicurezza da implementare e chi ne gestisce le funzionalità. È infatti compito del settore pubblico stabilire norme, procedure di certificazione e verifiche in grado di garantire un livello sufficiente di sicurezza.[113]

---

[112] C. CENCETTI, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, 2014.

[113] M. BROLLI. "*Sicurezza Informatica: una responsabilità condivisa*". 29 maggio 2019, ICT Security Forum.

Dall'altra parte il settore privato è responsabile della progettazione di sistemi robusti e dello sviluppo di nuovi metodi di sicurezza. Ai cittadini invece dovrà essere attribuita la responsabilità di adottare comportamenti consapevoli. Si rende necessaria, dunque, per tutte le organizzazioni, l'adozione di paradigmi "di comunità" o "olistici" per la cybersecurity, che promuovano la consapevolezza dei requisiti di conformità cui fare riferimento in ambito di prodotti, processi e sicurezza, al fine di garantire idonei livelli di gestione del rischio in un contesto sempre più vantaggioso. Al centro dell'approccio europeo vi è l'analisi preventiva dei rischi, la notifica degli incidenti da parte degli operatori pubblici e privati, la verifica dei livelli di sicurezza dei prodotti attraverso le certificazioni e standard. In questo contesto, l'Italia vuole essere un esempio nella comunità europea. I tre DPCM di attuazione del Perimetro Nazionale di Sicurezza Cibernetica e la costituzione dell'Agenzia per la cybersicurezza nazionale (ACN) testimoniano, da una parte, l'esigenza di "tutela rafforzata avvertita in relazione ad ambiti ritenuti maggiormente sensibili ed afferenti alla sicurezza degli apparati dello Stato non "coperti" dalla direttiva NIS in tutte le componenti essenziali" e, dall'altra, la volontà dell'esecutivo e del Parlamento di dotare la nazione di una Autorità nazionale avente personalità giuridica di diritto pubblico volta a ricomprendere il *Computer security incident response* team italiano (CSIRT) e il Centro di valutazione e certificazione nazionale (CVCN)[114].

È nell'impegno della beanTech, azienda ospitante del tirocinio formativo, sulla base dei nuovi equilibri che si stanno ridisegnando nei rapporti commerciali ed economici, quello di erogare servizi capaci di assicurare alle aziende partner, un'infrastruttura sempre all'avanguardia, innovativa e scalabile in base alle proprie esigenze[115].

[114] G. CARRER, *Con il sì del Senato, l'Agenzia cyber in rampa di lancio*, in Formiche.net, 03/08/2021

[115] *https://www.beantech.it/aree-di-business/infrastructure-services/*.

BIBLIOGRAFIA

beanTech srl, https://www.beantech.it/en/

R. BRIGHI, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, 8 settembre 2021.

A. TONOLO, *"Evoluzione delle Strategie di Cyber Security: Uno Sguardo a Confronto tra Europa e Stati Uniti",* 16 gennaio 2024.

ACCREDIA, *Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata*, 14 novembre 2022, pag.1.
https://www.accredia.it/app/uploads/2022/11/01_2022_Osservatorio_ACCREDIA_Cybersecurity_DEF.pdf

NIST, *cybersecurity Framework*, https://www.nist.gov/cyberframework.

"ISO/IEC 27001: 2022. *"information security, cybersecurity and privacy protection-Information security management system"*.
ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

MICROSOFT, "*Che cos'è un attacco informatico*?",
https://www.microsoft.com/it-it/security/business/security-101/what-is-a-cyberattack

THE GLOBAL RISK REPORT,
https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

TECH4FUTURE, "*Dati e sicurezza: la violazione del diritto alla privacy il rischio maggiormente percepito*", 18 gennaio 2023
https://tech4future.info/cyber-security-diritto-privacy-rischi/.

A. DI CORINTO, *Data Commons: privacy e cybersecurity sono diritti umani fondamentali*, in *Rivista italiana di informatica del diritto*, 2022, pp. 33-34

NETWORK DIGITAL360, "*IoT. Internet of Things:cos'è, come funziona ed esempi*", 16 novembre 2022

T.E. FROSINI, *Apocalittici e integrati. La dimensione costituzionale della società digitale*, Modena, 2021, p.9.

NETWORK DIGITAL360. "*IoT. Internet of Things:cos'è, come funziona ed esempi*".
https://www.internet4things.it/iot-library/internet-of-things-gli-ambiti-applicativi-in-italia/

CYBERMENT srl "*Legame intrinseco tra Cybersecurity e Privacy*", 14 giugno 2023 https://www.pqa.it/news/il-legame-intrinseco-tra-cybersecurity-e-privacy/

IBM, "*SOC (Security Operations Center)*. https://www.ibm.com/it-it/topics/security-operations-center

F. La Trofa. *"cos'è un Security Operation Center*", UniverseIT. https://universeit.blog/soc-security-operation-center/

A. FONZI, *Il principio di autodeterminazione dell'utente al cospetto delle nuove tecnologie*, in *Rivista on-line diritti fondamentali*, n. 3/2021, pp. 570-572.

M. OLIVETTI, *Diritti Fondamentali e Nuove tecnologie: una mappa del dibattito italiano*, in Revista Estudos Institucionais, n. 2/2020, pp. 395-398.

Ginevra Cerrina Ferroni, vicepresidente del Garante della Privacy, *PNRR, digitale: gli impatti sui diritti e ordinamento costituzionale- intervento di Ginevra Cerrina Ferroni*, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9815604

C. CASONATO, *Bioetica e pluralismo nello Stato Costituzionale*, in *Forum di Quaderni costituzionali*, 2006, p. 2.

LEGAL ENZDR, Tecnologia e Privacy: "u*n bilanciamento Necessario tra Individuazione e tutela dei Diritti Individuali"*, 17 maggio 2023. https://www.linkedin.com/pulse/tecnologia-e-privacy-un-bilanciamento-necessario-tra-innovazione/?originalSubdomain=it

A. CONTALDO, D. MULA (a cura di), Cybersecurity Law. *Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020, p. 19.

C. CENCETTI, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Roma, 2014, p.25.

*NIS Directive:*https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

Jacchia, De berti. "*La cybersecurity in Europa: fonti e legislazione*". https://www.dejalex.com/wpcontent/uploads/2017/06/PUBBL_20170306_Cybersecurity.pdf

https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Agenda Digitale. "*Nis2, come adeguarsi ai nuovi obblighi cyber: i punti chiave*". 25 gennaio 2024. https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/

https://fra.europa.eu/it/eu-charter/article/8-protezione-dei-dati-di-carattere-personale

B. Saetta. "*Diritto alla protezione dei dati personali*". 22 luglio 2018. https://www.altalex.com/documents/news/2018/04/12/articolo-4-gdpr-definizioni

(https://www.garanteprivacy.it/home/i-miei-diritti/diritti.)

«Accountability(responsabilizzazione)»,https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

Agenda Digitale. "*Privacy by design e by default: cosa sono, vantaggi e sfide*", 8 agosto 2023.

«Servizi IT: cosa sono, cos'è l'Information Technology» https://sceglifornitore.it/blog/servizi-it-cosa-sono-cose-linformation-technology/.

Agenda Digitale. "*Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT",* 7 giugno 2019. https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

CYBERSECURITY 360, "*sistema UE di certificazione della cyber security: come adeguarsi al nuovo mercato digitale*", 8 febbraio 2024.

C. BOSCHIERO, "*Intelligenza Artificiale e cybersecurity*"), 14 giugno 2021. https://www.italiaoggi.it/news/intelligenza-artificiale-e-cybersecurity-2522679.

Osservatorio ACCREDIA "*Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata*", 2022, p.13

https://www.acn.gov.it/portale/chi-siamo.

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

Redazione, «Sviluppo di strategie nazionali di cybersecurity, la guida», CyberSecurity Italia (blog), 23 dicembre 2021, https://www.cybersecitalia.it/sviluppo-di-strategie-nazionali-di-cybersecurity-la-guida-di-un-gruppo-di-lavoro-internazionale/15869/.

Cybersecurity360, "*strategia nazionale di cybersicurezza, gli obiettivi da raggiungere entro il 2026 per la resilienza del Paese*". 25 maggio 2022.

AGID. "*Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali*", 13 febbraio 2020, p.9

Avviso Pubblico, *"Strategia Nazionale di cybersicurezza 2022-2026"*, https://www.avvisopubblico.it/home/home/cosa-facciamo/informare/documenti-tematici/mafie/strategia-nazionale-di-cybersicurezza-2022-2026-sintesi-del-documento/

Perimetro di sicurezza nazionale cibernetica, https://www.acn.gov.it/portale/faq/nis-e-psnc

R. SETOLA, *Il piano nazionale per la protezione cibernetica e la sicurezza informatica*, in Sicurezza e Giustizia, n. 3/2017, p. 31.

https://www.sicurezzaegiustizia.com/il-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/

Cybersecurity360. "*Dalla percezione alla consapevolezza: il ruolo critico della formazione nella cyber security",* 26 settembre 2023.

Cybersecurity360. "P*erimetro di sicurezza nazionale cibernetica: regole e criteri di attuazione*", 30 ottobre 2020.

Bird&Bird. "*DPCM 131/2020: nuove disposizioni in materia di cybersecurity*".

Cybersecurity360. "*Cyber security delle infrastrutture critiche: tendenze e normative UE*", 17 novembre 2023.

FEDER SICUREZZA, "*Infrastrutture critiche sotto attacco: il nuovo White Paper del CoESS*". 8 maggio 2023.

INNOVATIONPOST, *"Italia sempre più nel mirino dei criminali informatici: attacchi in crescita del 65%", 6 marzo 2024. (*https://www.innovationpost.it/attualita/italia-sempre-piu-nel-mirino-dei-criminali-informatici-attacchi-in-crescita-del-65/#:~:text=Il%20nostro%20Paese%20appare%20sempre,del%2065%25%20rispetto%20al%202022*.)*

https://www.ictsecuritymagazine.com/articoli/le-infrastrutture-critiche-allintersezione-tra-dispositivi-cyber-fisici-e-cyber-threat-intelligence/.

https://www.assonime.it/Eventi/Pagine/Cybersecurity-nelle-Infrastrutture critiche.aspx.

Cybersecurity360, "*Attacchi cyber, l'italia più vulnerabile:i dati del rapporto Clusit 2024*". https://www.cybersecurity360.it/news/attacchi-cyber-nei-dati-clusit-uno-scenario-fosco-nel-2023-piu-12-per-cento/

CorCom. "*Cyber Intelligence cruciale per la tutela delle infrastrutture critiche del Paese*". 5 dicembre 2023. https://www.corrierecomunicazioni.it/cyber-security/limportanza-della-cyber-intelligence-nella-protezione-delle-infrastrutture-critiche-nazionali/

https://www.kaspersky.it/resource-center/definitions/threat-intelligence

Risk Management 360. "*Gestione del rischio: quali sono le best practices e gli strumenti necessari per le aziende*". 13 giugno 2023. *https://www.riskmanagement360.it/risk-analysis/gestione-del-rischio-tutto-quello-che-bisogna-sapere/*

CYBERGON. "*Cyber Security Awareness: quando il fattore umano può ridurre il rischio di un attacco informatico*". 4 aprile 2022. *https://blog.cybergon.com/posts/cyber-security-awareness-quando-il-fattore-umano-puo-ridurre-il-rischio-di-un-attacco-informatico/*

Agenda Digitale. "*Open Source Intelligence (OSINT): cos'è, a chi serve e come usarla*". 23 aprile 2024. *https://www.agendadigitale.eu/sicurezza/open-source-intelligence-osint-cose-a-chi-serve-e-come-usarla/*

Cybersecurity360. *"NIS 2 e ISO/IEC 27001: i requisiti di governance contro il rischio di incidenti cyber*". 28 febbraio 2024. *https://www.cybersecurity360.it/legal/nis-2-e-iso-iec-27001-i-requisiti-di-governance-contro-il-rischio-di-incidenti-cyber/*

https://www.cybersecurity360.it/legal/nis-2-e-iso-iec-27001-i-requisiti-di-governance-contro-il-rischio-di-incidenti-cyber/.

https://digital-strategy.ec.europa.eu/it/policies/nis2-directive.

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

https://www.ictsecuritymagazine.com/articoli/gdpr-compliance-e-iso-27001-sistemi-di-gestione-della-sicurezza-oltre-la-formalita/

Cybersecurity360. *"ISMS: cos'è, a cosa serve e come strutturare un Information Security Management System*". 21 gennaio 2020. *https://www.cybersecurity360.it/soluzioni-aziendali/isms-cose-a-cosa-serve-e-come-strutturare-un-information-security-management-system/*

Cybersecurity360. "*ISO 27001 e NIST Cybersecurity Framework: binomio vincente per un'efficace protezione dei dati*". *https://www.cybersecurity360.it/soluzioni-aziendali/iso-27001-e-nist-cybersecurity-framework-binomio-vincente-per-unefficace-protezione-dei-dati/*

C. Cencetti. "*Cybersecurity: Unione Europea e Italia. Prospettive a confronto*". Quaderni IAI

M. Brolli. "*Sicurezza Informatica: una responsabilità condivisa*". 29 maggio 2019, ICT Security Forum.