UNIVERSITÀ DEGLI STUDI DI GENOVA

SCUOLA DI SCIENZE SOCIALI

DIPARTIMENTO DI GIURISPRUDENZA

CORSO DI LAUREA IN

GIURISPRUDENZA

Tesi di laurea in

Diritto Pubblico Comparato

"LA TRANSIZIONE DIGITALE SOTTO IL PROFILO DELLA CYBERSICUREZZA"

Relatrice:

Prof.ssa Patrizia Magarò

Candidata:

Camilla Lendaro

Anno accademico 2022/2023

Ai miei nonni Cosimo e Gianna,

per tutto l'amore che mi hanno sempre dato.

Indice

Abstract

Con l'aumento del numero dei dispositivi connessi a Internet e del numero e della tipologia di software malevoli, negli ultimi anni i cyber attacchi si sono riprodotti in maniera esponenziale. Per questo motivo è importante implementare delle giuste procedure che mettano al riparo le informazioni e tutti i dati più sensibili. I cyber attacchi vengono messi a punto per mettere a repentaglio la sicurezza informatica ed è per questo che sono molto pericolosi e vanno assolutamente prevenuti e, quando non si può fare nulla per evitarli, vanno minimizzati nel minor tempo possibile per provare a limitare i danni. L'obiettivo dell'elaborato è quello di sviluppare un'analisi comparativa tra la normativa italiana e quella spagnola in materia di cybersicurezza per proteggere le proprie infrastrutture critiche e strategiche per l'economia e la sicurezza.

Partendo da un primo esame sul panorama europeo, in cui crescono di giorno in giorno la consapevolezza e la sensibilità nei confronti di questi temi, sono analizzati gli obblighi prescritti dalla Direttiva (UE) 2016/1148 (cosiddetta NIS) e dal Regolamento (UE) 2019/881 (noto come Cybersecurity Act) in capo agli Stati membri con la finalità precipua di assicurare un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea. Proprio per far fronte a tale scenario, nonché alle crescenti sfide che caratterizzano il panorama globale in ambito cyber, nei contesti nazionali italiano e spagnolo sono state delineate una serie di normative al fine innalzare il livello di sicurezza dei settori considerati essenziali per i Paesi, i quali svolgono un servizio o una funzione essenziale per gli interessi dello Stato che rendono necessario prevedere maggiori garanzie. A tal fine, nel presente documento saranno analizzate in una prospettiva comparatistica la pianificazione delle misure di sicurezza, il sistema di notificazione degli incidenti a danno di infrastrutture critiche e servizi essenziali, nonché la procedura di valutazione dei beni ICT.

Introduzione

La cybersecurity, o in italiano cybersicurezza, è definita dal Regolamento UE 2019/881 come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche". Più precisamente, è l'insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, dati e reti telematiche di uno Stato o di altro ente (privato o pubblico) da eventuali intrusioni perpetrate per via informatica. La protezione agisce, dunque, su tre ambiti: il primo è quello dei contenuti, dei dati e delle informazioni; il secondo riguarda la protezione degli hardware[1]; il terzo, infine, è quello relativo ai software[2] intesi quali programmi, reti, database, archivi digitali ed altre impostazioni tecnologiche similari. Data la crescente pericolosità della minaccia cibernetica, in tema di cybersecurity è richiesto un costante aggiornamento delle tecniche e delle metodologie della protezione. Infatti, al di là della terminologia, la cybersecurity è una disciplina molto pratica: si occupa di proteggere i sistemi informatici da minacce concrete che hanno una probabilità significativa di realizzarsi, fra le tante che sarebbero concepibili. In questo, la si può vedere come uno strumento di gestione dei rischi. Questi infatti non sono praticamente mai nulli e le misure di sicurezza sono utilizzate per ridurre tali rischi, quasi mai per eliminarli[3]. Il termine cybersicurezza è piuttosto giovane e la sua origine proviene dal cosiddetto "cyber spazio", ossia l'insieme dei collegamenti e relazioni tra

[1] L' hardware del computer è composto dai componenti fisici del computer. Un componente hardware è una parte del computer che può essere effettivamente toccata e pesata. Alcuni esempi di hardware sono il disco fisso, la scheda madre, la Cpu, ecc. *«L'Hardware del computer - Okpedia», https://www.okpedia.it/hardware.*

[2] Il software, è l'insieme di informazioni memorizzate su un dispositivo ed utilizzate da quest'ultimo per svolgere operazioni più o meno complesse: è comunemente riconosciuto come la controparte dell'hardware. In un PC faranno parte del software, a titolo esemplificativo, il sistema operativo, il programma usato per scrivere e quello per sentire la musica, cioè tutte quelle componenti che danno informazioni alla macchina allo scopo di svolgere precise istruzioni, come cambiare i pixel dello schermo, muovere la stampante, comporre musica ecc. Il software, perciò, è la parte fondamentale grazie alla quale è possibile utilizzare a pieno l'hardware. A seconda delle possibilità più o meno concrete di un hardware si possono creare dei software per impartire comandi ad una macchina. *Luca Giudice, «Che cos'è il software e a cosa serve?», Internetto, 16 settembre 2018, https://www.internetto.it/che-cose-il-software-e-a-cosa-serve/.*

[3] «Cyber security: cos'è e come garantire la sicurezza dei sistemi informatici e delle reti», Cyber Security 360 (blog), 5 settembre 2018, https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-la-guida-definitiva-per-la-corretta-implementazione-in-azienda/.

oggetti accessibili attraverso una rete di telecomunicazioni generalizzata, i quali presentano interfacce che consentono il loro controllo remoto nonché l'accesso ai dati. La sicurezza informatica è stata creata e utilizzata da professionisti IT, consulenti, lobbisti e politici proprio per affrontare problemi di sicurezza nel cyber spazio[4].

Quando si parla di cybersecurity si intende una serie di azioni pensate per difendere sistemi elettronici, reti, server[5] e dispositivi da attacchi hacker. Si tratta, in buona sostanza, di una serie di azioni e provvedimenti pensati per la sicurezza informatica e delle informazioni. Gli hacker sono coloro i quali minacciano le informazioni, i sistemi e le reti e pertanto è necessario prendere delle precauzioni, così la sicurezza informatica diventa fondamentale[6]. Trascurarla espone, infatti, a una serie di rischi perché le minacce si moltiplicano con un ritmo allarmante, che raddoppia quasi anno dopo anno. Naturalmente ci sono settori più colpiti, come quello medico e finanziario, ma è bene prestare attenzione in qualsiasi ambito e in ogni momento. Ultimamente sono proprio questi i settori più esposti ai rischi perché più attraenti agli occhi degli hacker; tuttavia, se si pensa allo spionaggio industriale è utile sottolineare che nessun settore è al sicuro. Per questo motivo è importante implementare delle giuste procedure che mettano al riparo le informazioni e tutti i dati più sensibili. Il cybercrimine è infatti una minaccia invisibile e impalpabile, che però può mettere in crisi aziende, enti e governi. Si parla di cybercrimine quando si vogliono intendere degli attacchi messi a punto da uno o più hacker con l'obiettivo di un ritorno economico o, ancora, finalizzato a produrre interruzioni della continuità produttiva di un'azienda. A questo punto è utile anche definire la figura del cybercriminale, anche noto come hacker: si tratta di colui che viene spinto da intento criminale che lo muove a effettuare attacchi informatici attraverso internet. La rete, quindi, diventa il punto di accesso per questi criminali che hanno come obiettivo quello di un guadagno o, come

[4] Redazione, «Cybersecurity e digital divide, investiamo anche sul territorio con una regia nazionale», Formiche.net, 2 agosto 2022, https://formiche.net/2022/08/cybersecurity-digital-divide-investiamo-territorio-regia-nazionale/.

[5] Il server (servitore in inglese) è un elemento informatico e delle telecomunicazioni che elabora e gestisce le informazioni su una rete, restituendole a tutti coloro che ne fanno richiesta. Altrimenti detto, il server è gestore virtuale delle informazioni che stanno su una rete. *Nadia Kasa, «Che cos'è un server? La spiegazione semplice», Kasa della comunicazione (blog), 15 settembre 2020, https://www.kasadellacomunicazione.it/server/.*

[6] «Nuove minacce alla sicurezza informatica tra malware e attacchi hacker», Cyber Security 360 (blog), https://www.cybersecurity360.it/nuove-minacce/.

detto, di mettere in crisi l'operatività di una azienda, di un ente o altro. Spesso alla base di tutto questo sussistono motivazioni politiche che spingono l'hacker all'azione. I cyberattacchi vengono messi a punto per mettere a repentaglio la sicurezza informatica ed è per questo che sono molto pericolosi e vanno assolutamente prevenuti e, quando non si può fare nulla per evitarli, vanno minimizzati nel minor tempo possibile per provare a limitare i danni[7]. In altre parole, la cybersecurity può essere definita come l'insieme delle attività poste in essere per la difesa e la sicurezza degli strumenti informatici, delle reti e delle informazioni, da attacchi volti a creare un danno o il blocco degli stessi. Secondo l'art. 2, punto 1) del Regolamento (UE) 2019/881 relativo all'ENISA[8], per cybersecurity si intende "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[9]. Le azioni di cybersicurezza, pertanto, hanno quale missione la protezione dalle minacce informatiche, intese come "qualsiasi circostanza, 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"[10]. La cybersecurity inoltre, secondo quanto previsto dagli standard ISO 27000[11], si occupa della "conservazione della

[7] «Cybersecurity: Definizione, Significato e Perché Serve | Alteredu», https://www.alteredu.it/cybersecurity-definizione-e-significato/.

[8] Il Regolamento (UE) 2019/881, noto come "regolamento sulla cibersicurezza" o "Cybersecurity Act", introduce nell'Unione europea un quadro di certificazione della cibersicurezza armonizzato per superare la frammentazione attuale del mercato interno dei certificati di cibersicurezza e rendere maggiormente affidabili per il consumatore i prodotti e i servizi che utilizzano tecnologie dell'informazione e della comunicazione (ICT). Il regolamento mira a realizzare un modello di "security by design" volto a garantire la sicurezza informatica dei prodotti e dei servizi digitali fin dalla fase di progettazione degli stessi. *«Le novità introdotte con l'entrata in vigore del regolamento UE 2019/881 "Cybersecurity Act" – Casella Scudier», 27 luglio 2019, https://www.casellascudier.it/le-novita-introdotte-con-lentrata-in-vigore-del-regolamento-ue-2019-881-cybersecurity-act/.*

[9] Redazione InSic, «Tutto quello che devi sapere sulla Cybersecurity», InSic (blog), 5 marzo 2021, https://www.insic.it/privacy-e-sicurezza/security-articoli/cybersecurity-definizione-e-provvedimenti/.

[10] Riferimento all'articolo 2, punto 8) del Regolamento (UE) 2019/881, relativo all'ENISA.

[11] ISO è un acronimo che sta per International Organization for Standardization. È la più importante organizzazione mondiale che si occupa di definire le cosiddette norme tecniche, dette anche norme ISO oppure standard ISO. Tutte le imprese realizzano prodotti o erogano servizi; tali prodotti e/o servizi possono avere requisiti e caratteristiche diverse a seconda delle esigenze dei clienti, delle norme cogenti applicabili e di ciò che l'organizzazione intende offrire al proprio mercato. Tuttavia, esistono alcune caratteristiche che, invece, devono essere assolutamente rispettate se si intende immettere sul mercato un prodotto o un servizio standardizzato, cioè realizzato nel rispetto di alcuni requisiti che sono riconosciuti a livello internazionale. Tali requisiti sono quelli contenuti negli Standard ISO.
La realizzazione di prodotti o servizi avviene attraverso una sequenza di processi che ogni azienda può gestire nel modo che ritiene più opportuno. Uno dei metodi che questa può scegliere è quello proposto nelle Norme Tecniche definite dall'ISO. L'adesione alle linee guida dettate dalle certificazioni aziendali hanno carattere volontario, per cui non vi sono obblighi di legge, ma queste certificazioni presentano numerosi vantaggi, in quanto si occupano di attestare la conformità

confidenzialità dei dati, integrità e disponibilità dell'informazione, inoltre altre caratteristiche tra cui l'autenticità, la responsabilità e l'affidabilità del dato possono essere utilizzate per spiegare il concetto di cybersecurity"[12]. Le tre caratteristiche citate riguardano le nozioni di "confidentiality", la quale indica che l'informazione non è rivelata ai soggetti non autorizzati, di "integrity", ossia accuratezza dell'informazione, e di "availability of information", quindi la disponibilità dell'informazione da parte dei soggetti autorizzati[13]. I principi di integrità, confidenzialità e disponibilità sono i fattori chiave per la gestione in sicurezza dell'informazione. Detti fattori, noti anche come CIA factors (dall'inglese Confidentiality, Integrity e Availability), resi dal NIST[14], sono pertanto gli elementi da considerare quando si individuano i parametri attraverso i quali si pianifica e si esegue una corretta impostazione della sicurezza informatica[15]. Di contro, data la complessità ormai raggiunta dall'ecosistema digitale, sussistono innumerevoli minacce ai fattori CIA e, conseguentemente, altrettante possibilità di perdita di valore del dato e del sistema che lo gestisce. Queste possibilità, per chi gestisce la security, sono analizzate congiuntamente agli impatti sui sistemi informatici e sulle informazioni qualora si concretizzino[16].

---

di un'azienda a determinati criteri valutativi, indicando nello specifico la presenza di alcuni elementi qualitativi all'interno dell'organizzazione aziendale e dei suoi processi interni. Quindi, gli standard ISO sono una raccolta di "best practice" che promuovono la compatibilità dei prodotti, la condivisione di soluzioni e l'identificazione dei problemi di sicurezza. Le norme presentano un approccio che è stato concordato da esperti internazionali. *«Norme ISO: cosa sono e a cosa servono», 4 giugno 2019, https://www.bcbcertificazioni.com/blog/norme-iso-cosa-sono-e-a-cosa-servono* e *We-learn, «Cosa sono gli Standard ISO», We Learn, 1 ottobre 2021, https://www.we-learn.it/cosa-sono-le-norme-iso/.*

[12] Redazione InSic, «Tutto quello che devi sapere sulla Cybersecurity», InSic (blog), 5 marzo 2021, https://www.insic.it/privacy-e-sicurezza/security-articoli/cybersecurity-definizione-e-provvedimenti/.

[13] Gianluca Lombardi, «Sicurezza informatica: cybersecurity e ISO 27001», Mondo 27001, 23 novembre 2020, https://www.mondo27001.it/sicurezza-informatica-cybersecurity-e-iso-27001/.

[14] Il National Institute of Standards and Technology (NIST, in origine National Bureau of Standards [NBS]) è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie. Fa parte del Dipartimento del Commercio e il suo compito è la promozione dell'economia americana attraverso la collaborazione con l'industria al fine di sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio. Il NIST si sta occupando attivamente delle tessere di identificazione per i dipendenti federali, al fine di controllare e prevenire il terrorismo, i criminali, e tutti gli accessi non autorizzati all'interno di strutture governative e dei loro sistemi informatici. Negli ultimi anni il NIST è tra i principali riferimenti autorevoli relativamente alla cybersecurity.

[15] «Sicurezza delle informazioni: i tre principi per gestire il cyber risk», Agenda Digitale, 21 giugno 2023, https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-i-tre-principi-per-gestire-il-cyber-risk/.

[16] ENISA Overview of Cybersecurity and Related Terminology', September 2017.

È solo dalla seconda metà del 2019 che il quadro normativo europeo e nazionale in materia ha assunto maggiore concretezza: a livello europeo con il citato Regolamento (UE) 2019/881 e sul piano nazionale con il Decreto Legge n. 105 del 2019, convertito con modificazioni dalla legge 18 novembre 2019, n. 133 e ss.mm.ii. I due atti non hanno un diretto legame normativo – nel D.L. 105/2019 non c'è alcun riferimento al Reg. 881/19 –, tuttavia il decreto ha introdotto disposizioni che, senza trascurare il necessario raccordo con la Direttiva NIS, mirano ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi di rilievo strategico. Con il Decreto Legge n. 105 del 2019 è stato definito il Perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale[17]. Come indicato nel DPCM 31 luglio 2020, n. 131, i soggetti pubblici e privati – che forniscono tali servizi o esercitano tali funzioni – sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici (interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro) dalle Amministrazioni competenti nei rispettivi settori. I soggetti inclusi nel Perimetro di sicurezza cibernetica nazionale sono tenuti a predisporre annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi essenziali e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT (Computer Security Incident Response Team) attivo presso l'Agenzia per la Cybersicurezza Nazionale[18]. Le misure di sicurezza, che i soggetti inclusi nel Perimetro sono

[17] Corrado Pisano, «Perimetro sicurezza», Ministero delle Imprese e del Made in Italy, https://atc.mise.gov.it/index.php/sicurezza/perimetro-sicurezza.

[18] «Cybersecurity», Dipartimento per le Politiche Europee, http://www.politicheeuropee.gov.it/it/comunicazione/europarole/cybersecurity/.

tenuti ad adottare, e le modalità di notifica degli incidenti sono state definite con il DPCM 14 aprile 2021, n. 81.

Il concetto di cybersecurity non è quindi da confondere con quello di cyberdefense[19]; infatti, la difesa informatica si concentra sulla prevenzione e le sue attività sono pressoché interamente devolute alla piena operatività del comparto difesa e militare. Con l'aumento del numero dei dispositivi connessi a Internet (ad esempio, smartphone, notebook e laptop) e del numero e della tipologia di software malevoli (ransomware, cryptolocker, virus, worm e trojan), negli ultimi anni i cyber attacchi si sono riprodotti in maniera esponenziale[20]. Di conseguenza, sono continue le minacce basate su nuovi software sempre più sofisticati ed è richiesta una risposta immediata affinché i pericoli siano neutralizzati. Lo standard ISO/IEC 27002:2022 sulla "Sicurezza delle informazioni, sicurezza informatica e protezione della privacy – Controlli di sicurezza delle informazioni" arriva nove anni dopo ISO/IEC 27001:2013 e porta con sé alcune novità[21]. I controlli, ossia le misure che mantengono e/o modificano il rischio, sono riformati da un punto di vista strutturale: non più aggregati per ambiti, come in passato, ma per macro-temi corrispondenti ai quattro controlli centrali della sicurezza delle informazioni (fisici, tecnologici, organizzativi e delle persone)[22]. A cambiare è anche il numero di controlli, che vengono ridotti attraverso l'accoppiamento di alcuni e l'introduzione di nuovi. Gli obiettivi principali che si pone la norma sono, in primo luogo, quelli di mappare i punti deboli del sistema puntando a ridurre i rischi nonché la probabilità che si verifichino eventi negativi; inoltre, è necessario limitare il danno qualora gli eventi negativi si verifichino ed imparare dall'esperienza – propria e altrui – migliorando attraverso l'introduzione di procedure o prassi

[19] La definizione di cyberdefense data dal CCDCOE (Cooperative Cyber Defense Centre of Excellence della Nato, avente sede a Tallinn in Estonia) consiste in una misura proattiva per rilevare od ottenere informazioni su un'infrazione informatica, attacco informatico o imminente operazione informatica ovvero per determinare l'origine di un'operazione che comporta l'avvio di una contromisura preventiva o informatica contro la fonte d'aggressione.

[20] «Cyber security: cos'è e come garantire la sicurezza dei sistemi informatici e delle reti», Cyber Security 360 (blog), 5 settembre 2018, https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-la-guida-definitiva-per-la-corretta-implementazione-in-azienda/.

[21] Amministratore, «ISO/IEC 27002: cosa cambia nel nuovo standard», Mondo 27001, 7 marzo 2022, https://www.mondo27001.it/iso-iec-27002-cosa-cambia-nel-nuovo-standard/.

[22] «International Standard ISO/IEC 27000», s.d.

aggiornate[23]. Ancora, è importante puntare sulla formazione e sulla competenza per ridurre l'errore umano e aumentare la consapevolezza[24]. In aggiunta, è da segnalare la differenza tra "security" e "safety". Con Safety si intende l'insieme di tutte quelle soluzioni volte alla sicurezza delle persone in assenza di atti criminosi; al contrario, con Security si intende l'insieme di procedure, processi, tecnologie ed elementi fisici volti alla prevenzione di atti criminosi nei confronti di persone o cose[25]. I sistemi antintrusione o il controllo degli accessi sono le declinazioni classiche della security, ognuna delle quali si traduce in una specifica applicazione caratterizzata da obiettivi e caratteristiche differenti[26]. La cybersecurity è una particolare branca della Security che riguarda la Sicurezza logica, ossia l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei dati e dei beni o asset informatici. Le aziende e gli enti pubblici si trovano a dover fronteggiare un numero sempre più crescente di minacce: accanto a cyber attacchi eclatanti e noti quali, ad esempio, quelli che hanno coinvolto l'Agenzia delle Entrate[27] e la Regione Lazio[28], è stimato un totale di oltre 13 milioni di attacchi giornalieri di ogni entità a danno di imprese ed enti pubblici. Le "nuove" minacce consistono in documenti Office malevoli (macro-less malware), tecniche di evasione capaci di eludere sistemi antivirus basici, attacchi basati su script utilizzati da programmi downloader e dropper. La conseguenza è che si rendono indispensabili strutture in grado di contrastare i rischi cibernetici: per garantire sufficienti livelli di sicurezza occorre mantenere i sistemi di difesa costantemente aggiornati

[23] «Cybersecurity», Dipartimento per le Politiche Europee, http://www.politicheeuropee.gov.it/it/comunicazione/europarole/cybersecurity/.

[24] 14:00-17:00, «ISO/IEC 27002:2022», ISO, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/56/75652.html.

[25] Linda Lovo, «Convergenza tra Safety, Security e Cybersecurity», Italsicurezza (blog), 1 giugno 2020, https://www.italsicurezza.it/convergenza-tra-safety-security-e-cybersecurity/.

[26] «Cybersecurity, il Consiglio Ue: "Contro gli attacchi rafforzare la cooperazione"», CorCom, 23 maggio 2022, https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-il-consiglio-ue-contro-gli-attacchi-rafforzare-la-cooperazione/.

[27] L'episodio è avvenuto nel luglio 2022: si fa riferimento all'attacco hacker all'Agenzia delle Entrate da parte di LockBit, che ha sottratto tramite malware 78 giga byte di dati intimando un ultimatum di cinque giorni, pena la diffusione di questi ultimi.

[28] Vicenda avvenuta nell'Ottobre 2021: attacco cibernetico al sistema della Regione Lazio per la prenotazione dei vaccini contro il COVID-19. *«Attacco informatico all'Agenzia delle Entrate, la Procura di Roma apre un'inchiesta», RaiNews, https://www.rainews.it/articoli/2022/07/attacco-informatico-allagenzia-delle-entrate-countdown-fissato-a-5gg-0e679af7-e070-46bf-b663-bfbbb4d62783.html.*

con continui avanzamenti delle tecnologie[29]. Gli Stati Uniti e l'Unione europea hanno accelerato l'adozione di misure volte ad incrementare la sicurezza dei propri sistemi e delle proprie reti, come conseguenza del crescente numero di attacchi informatici rivolti alle infrastrutture critiche. Per quanto riguarda l'Unione europea, negli ultimi mesi in seguito al conflitto russo-ucraino, il Consiglio e il Parlamento europeo hanno raggiunto un accordo sulla cosiddetta Direttiva NIS2[30], la normativa europea che si prefigge di migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti del settore pubblico, privato e dell'Unione nel suo complesso attraverso misure per un livello comune elevato di cybersicurezza, che introducono nuovi requisiti di sicurezza per la protezione dei servizi essenziali e di quelli digitali nell'UE[31]. L'attuazione della Direttiva NIS, invece, è stata un passo importante per la cooperazione nella rete dei CSIRT europei per la protezione di infrastrutture critiche in settori come l'energia, i trasporti, le banche.

Il lavoro di ricerca che è stato svolto propone un primo esame circa le politiche dell'Unione europea, vincolanti e non, in materia di cybersicurezza per la protezione delle infrastrutture critiche e dei dati personali, attraverso l'analisi delle principali norme sul tema che sono, fra le altre, la Direttiva NIS, il Regolamento GDPR ed il Cybersecurity Act. In ambito europeo gioca un ruolo fondamentale l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), la cui missione è migliorare la sicurezza informatica e delle reti di telecomunicazioni dell'Unione europea. Grazie al nominato Cybersecurity Act tra le sue competenze si annovera quella di ente di certificazione europea, conferendo affidabilità ai sistemi, servizi e processi informatici. Dopo un primo esame sul panorama europeo, verrà analizzata la cybersicurezza in Italia. In primo luogo, è stato visionato il Codice dell'Amministrazione Digitale di cui si servono le Pubbliche Amministrazioni, grazie al ruolo importassimo svolto dalle Linee guida di AgID che forniscono norme tecniche in materia di amministrazione digitale. In secondo luogo, verrà ampiamente

[29] Redazione, «Sicurezza e gestione del rischio online e offline. Cosa devono fare aziende e Pa», Formiche.net, 1 settembre 2022, https://formiche.net/2022/09/rischio-online-offline-cyber-pa/.

[30] Gli obiettivi della NIS2 sono la lotta contro la criminalità informatica e le frodi, la protezione dei minori on line, la sicurezza delle reti 5G, la resilienza dei soggetti critici, i sistemi di certificazione della cybersicurezza.

[31] European Network and Information Security Agency. 'Definition of Cybersecurity - Gaps and Overlaps in Standardisation', 1 July 2016.

ispezionata la disciplina del Perimetro Nazionale di Sicurezza Cibernetica con i suoi decreti attuativi, allo scopo di esaminare i compiti affidati ai soggetti rilevanti per la cybersicurezza nazionale, quali l'Agenzia per la Cybersicurezza nazionale, il Centro di Valutazione e di Certificazione nazionale e i Computer Security Incident Response Teams. Per completare il panorama italiano, saranno altresì vagliati gli interventi recenti per lo sviluppo informatico (tra cui il Decreto Aiuti e il PNRR), l'impatto dei Golden Power sull'economia italiana ed infine il Framework nazionale creato dal CINI. Intorno, invece, all'aspetto comparatistico della ricerca, è stato deciso di analizzare la disciplina spagnola in materia di cybersicurezza al fine di confrontarla con la normativa italiana discussa precedentemente. A tal proposito, verranno esaminate le Strategie nazionali di cybersicurezza, la normativa contenuta nel cosiddetto Codice del diritto di cybersicurezza ed infine i temi della protezione dei dati e della garanzia dei diritti digitali. In Spagna la protezione dei dati è strettamente collegata con la normativa di cybersicurezza. Ancora, viene analizzato l'impatto che la Direttiva NIS ha avuto sul sistema spagnolo in materia di notificazioni degli incidenti cibernetici a livello nazionale ed in materia di certificazione di sistemi, servizi e processi informatici. Infine, sarà valutato il ragionamento operato dalla Spagna in merito ad un ulteriore rafforzamento rispetto alla sicurezza imposta dalla Direttiva NIS, improntata alla difesa degli enti che svolgono funzioni essenziali per lo Stato, adottato in Italia grazie all'introduzione di una normativa speciale che istituisce il Perimetro nazionale di cybersicurezza.

Capitolo I: Le politiche dell'Unione europea in materia di cybersicurezza

Le crisi cibernetiche sono una minaccia sistemica concreta che interessa tutte le società avanzate, dunque anche l'Unione europea, generando rischi per tutti gli attori socioeconomici, incluse le pubbliche amministrazioni, e risultando in costi rilevanti per il mercato unico. Le conseguenze negative delle crescenti e sempre più sofisticate minacce cyber non sono solo di stampo economico, ma possono arrivare fino a minacciare la vita dei cittadini[32]; per far fronte a tali pericoli, l'Unione deve dotarsi di una visione e di strumenti comuni, andando verso l'istituzione di un'unità congiunta per il cyberspazio. L'Autorità europea per la cybersicurezza (ENISA) sottolinea come gli attacchi siano cresciuti in sofisticazione e impatto, a causa della costante crescita del digitale, incentivata anche dalla pandemia di covid-19, della transizione verso soluzioni infrastrutturali connesse e basate sul cloud e dello sfruttamento di nuove tecnologie emergenti, quali l'intelligenza artificiale[33].

La prima misura in ambito di cybersicurezza, a livello europeo, è stata la comunicazione della Commissione europea sulla sicurezza delle reti del 2001, adottata a seguito della Convenzione di Budapest del Consiglio sulla criminalità informatica; la Commissione ha evidenziato come "le misure politiche in tale ambito possono avere un duplice beneficio: rafforzare dal punto di vista economico il mercato interno e allo stesso tempo migliorare il quadro giuridico". La comunicazione sottolinea inoltre l'importanza di avere un approccio coordinato, non solo a livello europeo, ma anche a livello internazionale[34]. Da allora, l'Unione si è avvalsa di politiche,

[32] Ciò è stato dimostrato dal ransomware che ha compromesso le reti del sistema sanitario irlandese nel maggio 2022, impedendo l'accesso ai registri sanitari in alcuni ospedali e causando l'annullamento di trattamenti medici, tra cui servizi per il trattamento di cancro e ictus. Un attacco simile, ma di proporzioni più contenute, ha interessato anche l'Italia, dove il sistema sanitario della Regione Lazio è stato compromesso nell'estate 2021.

[33] «Cybersecurity, Commissione europea: "Ecco la nostra risposta coordinata"», Agenda Digitale, 10 gennaio 2022, https://www.agendadigitale.eu/sicurezza/cybersecurity-verso-una-risposta-europea-quadro-delle-minacce-azioni-e-lacune-da-colmare/.

[34] «Norme cybersecurity in Europa, che caos: i nodi da risolvere», Agenda Digitale, 3 gennaio 2020, https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/.

normative e risorse finanziarie per accrescere la propria cyberresilienza. A fronte di un numero crescente di gravi attacchi e incidenti informatici, dal 2013 l'attività al riguardo si è intensificata e, parallelamente, gli Stati membri hanno adottato le prime strategie nazionali per la cybersicurezza[35]. Sin dalle sue primissime comunicazioni, la Commissione ha sempre sottolineato la necessità di armonizzare, a livello europeo, le misure sostanziali, che si identificano nella definizione di crimini e dei protocolli di sicurezza, e procedurali, quindi organizzative, tra i vari stati dell'Unione per assicurare un adeguato livello di cybersicurezza[36]. La strategia dell'Unione europea del 2013 (EUCSS 2013) comprende una serie d'iniziative legislative, vincolanti e non, volte a stabilire un cyberspazio aperto, sicuro e protetto; a tal fine, gli atti che compongono la strategia sviluppano azioni volte a combattere il cybercrimine, proteggendo al tempo stesso le infrastrutture critiche e rinforzando la sicurezza delle reti[37]. Fanno parte dell'EUCSS 2013 la direttiva NIS e la comunicazione della Commissione che sottolinea l'importanza della cooperazione tra il settore pubblico e privato riconoscendo il valore strategico della *partnership*[38].

Nel novembre 2009 è stato proposto di introdurre misure di sicurezza nel campo delle comunicazioni elettroniche varando la direttiva 2009/140/CE, che emenda la precedente 2002/21/CE, e che regolamenta i servizi e le reti di comunicazione elettronica disponendone la sicurezza e l'integrità. Successivamente, il 7 febbraio 2013, al fine di armonizzare il sistema di

---

[35] Brp_cybersecurity_it.pdf https://www.eca.europa.eu/Lists/ECADocuments/Brp_cybersecurity/Brp_cybersecurity_it.pdf

[36] «Norme cybersecurity in Europa, che caos: i nodi da risolvere», Agenda Digitale, 3 gennaio 2020, https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/.

[37] Oggi per combattere in maniera efficace la criminalità è importante che i fornitori di servizi conservino determinati dati, oltre a quelli raccolti a fini strettamente commerciali, che possano essere divulgati a determinate condizioni rigorose per finalità di lotta contro la criminalità. Tuttavia, la conservazione dei dati può violare i diritti fondamentali della persona, in particolare i diritti alla riservatezza e alla protezione dei dati personali secondo l'interpretazione della Corte di giustizia dell'Unione europea. Nelle cause Digital Rights c/ Irlanda del 2014 e Tele2 del 2016, la CGUE ha vietato all'Unione europea e ai suoi Stati membri di definire norme che comportino una conservazione generalizzata e indifferenziata dei dati. *«Conservazione dei dati per combattere la criminalità: il Consiglio adotta conclusioni»,https://www.consilium.europa.eu/it/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/.*

[38] L'intera discussione su questo argomento scaturisce dall'importanza di fornire strumenti efficaci di lotta alla criminalità, da una parte, e dalla necessità di rispettare i diritti fondamentali, in particolare i diritti alla riservatezza, alla protezione dei dati personali, alla non discriminazione e alla presunzione di innocenza, dall'altra.

sicurezza cibernetico europeo, è stata adottata la Strategia dell'Unione europea per la sicurezza cibernetica, contenente l'invito rivolto a tutti gli Stati membri ad adottare specifiche normative nazionali al fine di prevenire e rispondere alle perturbazioni e agli attacchi che colpiscono i sistemi di telecomunicazioni in Europa. Pochi mesi dopo, il 12 settembre 2013, il Parlamento europeo approva la risoluzione n. 2013/2606 "sulla strategia dell'Unione europea per la cybersicurezza: un cyberspazio aperto e sicuro"[39].

Sin dal 2017, la Commissione ha affermato la necessità di sviluppare un quadro europeo di risposta agli incidenti e alle crisi di cybersicurezza su vasta scala. È necessario trasferire in maniera veloce e accurata l'informazione dagli esperti tecnici ai decisori politici, passando attraverso il livello operativo dei *policy officers* e dei gestori di crisi: l'obiettivo principale è agire in maniera coordinata e supportare gli Stati membri che siano in difficoltà[40]. Comunicare tempestivamente le cause, l'impatto e le possibili contromisure a una crisi cibernetica significa limitare al minimo i pericoli per i cittadini e i possibili danni economici per l'economia dell'Unione. Per questo, il quadro europeo prevede di consentire una risposta efficace e coordinata; ciò richiede, in linea con l'ambizione dichiarata nella strategia europea di cybersicurezza, una sistematica e completa condivisione delle informazioni. In concreto, quindi, gli *stakeholder* attivi nel cyberspazio europeo dovrebbero acquisire una consapevolezza situazionale condivisa, prepararsi adeguatamente attraverso esercizi e formazione comuni e concordare principi di comunicazione pubblica. Questa visione, proposta dalla Commissione, ha permesso negli ultimi anni di strutturare al meglio la cooperazione operativa tra gli Stati membri; nonostante questo, il sistema è ancora incompleto e ci sono lacune da colmare al più presto, sfruttando a pieno gli strumenti attualmente a nostra disposizione[41].

---

[39] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), pag. 19.

[40]«Cybersecurity, il Consiglio Ue: "Contro gli attacchi rafforzare la cooperazione"», CorCom, 23 maggio 2022, https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-il-consiglio-ue-contro-gli-attacchi-rafforzare-la-cooperazione/.

[41] Particolari priorità in tal senso consistono: in primo luogo, nell'implementare il mandato di ENISA nel supporto alla cooperazione operativa (in base alla legislazione Europea, ENISA può supportare gli esperti tecnici parte della rete di gruppi nazionali di intervento in caso di incidente (CSIRTs), ad esempio fornendo assistenza nella gestione tecnica degli incidenti e nell'analisi di vulnerabilità, sostenendo gli Stati membri in indagini tecniche ex-post e contribuendo ad esercitazioni); in secondo luogo, nell'intensificare la cooperazione tra le istituzioni, agenzie ed enti europei responsabili

Secondo la raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cybersicurezza su vasta scala, l'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali in tutti i settori di attività economica, dato che imprese e cittadini sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero. Un incidente di cybersicurezza che interessa le organizzazioni di più Stati membri o addirittura l'intera Unione, con potenziali gravi perturbazioni del mercato interno e più in generale delle reti e dei sistemi informativi dai quali dipendono l'economia, la democrazia e la società dell'Unione, è uno scenario per il quale gli Stati membri e le istituzioni dell'UE devono essere ben preparati[42].

Un incidente di cybersicurezza può essere considerato una crisi a livello unionale quando le conseguenti perturbazioni sono talmente ampie da non poter essere gestite autonomamente dallo Stato membro interessato o quando interessa due o più Stati membri o, ancora, ha un impatto di rilevanza tecnica o politica di così vasta portata da richiedere un coordinamento e una risposta tempestivi a livello politico. Gli incidenti di cybersicurezza possono innescare crisi più ampie, con ripercussioni su altri settori di attività al di là dei sistemi informativi e delle reti di comunicazione; per reagire adeguatamente è necessario intervenire con attività di

per la cybersicurezza (lo stesso incidente, soprattutto se su larga scala, ha ricadute sia sulla comunità civile, identificabile con le autorità NIS, che sulle forze di polizia, sul corpo diplomatico e, talvolta, sulle forze militari). Il protocollo d'intesa tra Agenzia Europea per la Difesa (EDA), ENISA, CERT-EU ed EUROPOL pone le basi per una più efficace cooperazione tra gli enti europei che rappresentano queste differenti comunità, consente l'adozione di relazioni tecniche approfondite in merito a incidenti e minacce, così come iniziative coordinate di esercitazione e formazione. In aggiunta, ENISA e il CERT delle istituzioni EU (CERT-EU) sono impegnati in attività di cooperazione strutturata che includono l'apertura di uffici adiacenti a Bruxelles. Infine, in terzo luogo, una priorità consiste nell'incrementare lo scambio d'informazioni e la mutua assistenza tra autorità civili nazionali: la rete di CSIRTs nazionali e quella di collegamento per le crisi informatiche (CyCLONe), possono incrementare il livello di cooperazione attraverso piattaforme sicure per lo scambio d'informazioni, l'individuazione di ruoli, responsabilità e procedure ben definite che possano collegare queste due reti con il livello politico, rappresentato dal Consiglio. A tal fine, attraverso la revisione della Direttiva NIS, la Commissione ha proposto sia d'istituzionalizzare CyCLONe, che di definire quadri nazionali di gestione delle crisi di cybersicurezza e piani nazionali di risposta agli incidenti e alle crisi. *«Cybersecurity, Commissione europea: "Ecco la nostra risposta coordinata"», Agenda Digitale, 10 gennaio 2022, https://www.agendadigitale.eu/sicurezza/cybersecurity-verso-una-risposta-europea-quadro-delle-minacce-azioni-e-lacune-da-colmare/.*

[42] «Cybersecurity, Commissione europea: "Ecco la nostra risposta coordinata"», Agenda Digitale, 10 gennaio 2022, https://www.agendadigitale.eu/sicurezza/cybersecurity-verso-una-risposta-europea-quadro-delle-minacce-azioni-e-lacune-da-colmare/.

attenuazione concernenti sia l'ambito informatico sia altri settori[43]. Dal momento in cui gli incidenti di cybersicurezza sono imprevedibili e spesso si verificano ed evolvono in tempi molto ridotti, i soggetti colpiti e coloro che hanno la responsabilità di reagire e di attenuare gli effetti conseguenti devono coordinare la loro risposta rapidamente. Inoltre, spesso tali incidenti non sono circoscritti a una determinata area geografica e possono verificarsi simultaneamente o diffondersi all'istante in molti paesi[44]. Quindi, per far fronte agli incidenti e alle crisi di cybersicurezza è necessaria una cooperazione a livello unionale, la quale si approccia su tre livelli differenti: politico, operativo e tecnico. Ciascun livello della cooperazione mira a conseguire, quali obiettivi principali, di consentire una risposta efficace, di condividere la conoscenza situazionale e concordare i principali messaggi di comunicazione pubblica.

Le comunicazioni in caso di crisi svolgono un ruolo essenziale nel limitare gli effetti negativi degli incidenti di cybersicurezza per dare efficacia alla risposta politica, ma un messaggio appropriato che segnala chiaramente le possibili conseguenze di una risposta diplomatica può anche servire a influenzare il comportamento dei (potenziali) aggressori. Di particolare importanza è la diffusione ai cittadini di informazioni accurate e utilizzabili su come attenuare le conseguenze di un incidente (ad esempio, applicando aggiornamenti di sicurezza o

---

[43] *«Raccomandazione (UE) 2017/1584 della Commissione - del 13 settembre 2017 - relativa alla risposta coordinata agli incidenti e alle crisi di cybersicurezza su vasta scala», s.d.* In particolare, riferimento ai considerando (1), (2), (3) e (4).

[44] La risposta agli incidenti di cybersicurezza può assumere molte forme, che vanno dall'individuazione di misure tecniche che possono comportare la ricerca congiunta - da parte di due o più soggetti - delle cause tecniche dell'incidente (ad esempio, analisi dei programmi malevoli, noti anche come malware) o l'identificazione dei modi in cui le organizzazioni possono valutare se sono state colpite (ad esempio, indicatori di compromissione) alle decisioni operative sull'applicazione di tali misure e, a livello politico, sulla scelta di ricorrere ad altri strumenti, ad esempio al quadro relativo a una risposta comune alle attività informatiche dolose o al protocollo operativo dell'UE per contrastare le minacce ibride, in funzione dell'incidente. In aggiunta, la fiducia dei cittadini e delle imprese europee nei servizi digitali è essenziale per un mercato unico digitale fiorente; pertanto, la comunicazione in caso di crisi riveste un ruolo particolarmente importante nell'attenuazione degli effetti negativi degli incidenti e delle crisi di cybersicurezza. La comunicazione può essere utilizzata anche nell'ambito del quadro relativo a una risposta diplomatica comune come strumento per influenzare il comportamento dei (potenziali) aggressori che agisce da paesi terzi. L'allineamento della comunicazione pubblica per attenuare gli effetti negativi degli incidenti e delle crisi di cybersicurezza e l'uso della comunicazione pubblica per influenzare un aggressore sono essenziali per dare efficacia alla risposta politica. *«Raccomandazione (UE) 2017/1584 della Commissione - del 13 settembre 2017 - relativa alla risposta coordinata agli incidenti e alle crisi di cybersicurezza su vasta scala», s.d.* In particolare, riferimento ai considerando (21), (22) e (23).

effettuando azioni complementari per evitare la minaccia)[45]. Nelle conclusioni, il Consiglio evidenzia le cinque funzioni fondamentali dell'Unione nel settore informatico: l'UE deve rafforzare la resilienza e le capacità di protezione, rafforzare la solidarietà e la gestione globale delle crisi, promuovere la propria visione sul cyberspazio, rafforzare la cooperazione con i Paesi partner e le organizzazioni internazionali e, infine, prevenire, difendere e rispondere agli attacchi informatici. I ministri hanno invitato la Commissione a proporre requisiti comuni di sicurezza informatica per i dispositivi connessi, nonché i processi e servizi associati; invitano inoltre le autorità competenti, come l'ENISA, a formulare raccomandazioni per rafforzare la resilienza delle reti e delle infrastrutture di comunicazione all'interno dell'UE; infine, sottolineano l'importanza di istituire esercitazioni informatiche periodiche, al fine di testare e sviluppare la risposta interna ed esterna ad attacchi informatici su larga scala[46].

L'Unione europea si sta adoperando su più fronti per promuovere la cyberresilienza, combattere la criminalità e rafforzare la diplomazia informatica e la cyberdifesa. Settori critici quali i trasporti, l'energia, la sanità e la finanza dipendono sempre più dalle tecnologie digitali per la gestione delle loro attività principali: se è vero che la digitalizzazione porta con sé enormi opportunità e offre soluzioni a molte delle sfide che l'Europa deve affrontare, non da ultimo durante la crisi covid-19, altresì essa espone l'economia e la società a minacce informatiche. Una risposta più forte in materia di cybersicurezza volta alla creazione di un cyberspazio aperto e sicuro può contribuire a una maggiore fiducia dei cittadini negli strumenti e nei servizi digitali[47]. Nel dicembre 2020 la Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova strategia dell'UE in materia di cybersicurezza. L'obiettivo è rafforzare la resilienza dell'Europa a fronte delle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e

[45] «Raccomandazione (UE) 2017/1584 della Commissione - del 13 settembre 2017 - relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala», s.d.

[46] «Cybersecurity, il Consiglio Ue: "Contro gli attacchi rafforzare la cooperazione"», CorCom, 23 maggio 2022, https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-il-consiglio-ue-contro-gli-attacchi-rafforzare-la-cooperazione/.

[47] «Cybersicurezza: la risposta dell'UE alle minacce informatiche», https://www.consilium.europa.eu/it/policies/cybersecurity/.

attendibili; la nuova strategia include proposte concrete per l'introduzione di strumenti normativi, strategici e di investimento. Il 22 marzo 2021 il Consiglio ha adottato conclusioni sulla strategia, sottolineando che la cybersicurezza è essenziale per costruire un'Europa resiliente, verde e digitale: in altre parole, i ministri hanno stabilito l'obiettivo fondamentale di raggiungere l'autonomia strategica mantenendo allo stesso tempo un'economia aperta. La strategia copre la sicurezza di servizi essenziali come ospedali, reti energetiche, ferrovie e il numero sempre crescente di oggetti connessi nelle nostre case, uffici e fabbriche, e mira a costruire capacità collettive per rispondere ai principali attacchi informatici; delinea, inoltre, i piani per lavorare con partner in tutto il mondo per garantire la sicurezza e la stabilità internazionali nel cyberspazio, e prevede che un'unità informatica comune possa garantire la risposta più efficace alle minacce informatiche utilizzando le risorse collettive e le competenze a disposizione degli Stati membri e dell'Unione europea. A seguito dei progressi compiuti nell'ambito delle strategie precedenti, la strategia in esame contiene proposte concrete per l'attuazione di tre strumenti principali, quali le iniziative normative, di investimento e politiche; esse affronteranno, a loro volta, tre ambiti d'azione: in primo luogo, il settore della resilienza, sovranità tecnologica e leadership; in secondo luogo, la capacità operativa di prevenire, scoraggiare e rispondere; e da ultimo, la cooperazione per far progredire un cyberspazio globale e aperto[48]. Il quadro strategico dell'Unione europea in materia di cyberdifesa è stato adottato dal Consiglio il 18 novembre 2014 e da allora, attraverso la sua attuazione, risultati concreti hanno contribuito a rafforzare in modo significativo le capacità di cyberdifesa degli Stati membri. La strategia globale pone l'accento sulla necessità di accrescere le capacità di proteggere i cittadini e di rispondere alle crisi esterne, nonché di rafforzare l'Unione in quanto comunità di sicurezza[49].

---

[48] «La Strategia Di Cybersicurezza | Plasmare Il Futuro Digitale Dell'Europa», https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

[49] La criminalità informatica assume varie forme e molti reati comuni sono favoriti dall'informatica stessa; ad esempio, i criminali possono: acquisire il controllo di dispositivi personali utilizzando malware, sottrarre o compromettere dati personali e proprietà intellettuale per commettere frodi online, utilizzare internet e le piattaforme dei social media per distribuire contenuti illegali oppure utilizzare la "darknet" per vendere beni illeciti e servizi di pirateria informatica. Nel quadro di Europol è stato istituito un Centro europeo per la lotta alla criminalità informatica specializzato che aiuta i paesi dell'UE a indagare i reati online e a smantellare le reti criminali. La piattaforma multidisciplinare europea di lotta

Da ultimo, è importante menzionare il Cyber Resilience Act, proposto dalla Commissione nel settembre 2022, il cui scopo è garantire che i prodotti con elementi digitali immessi sul mercato europeo presentino meno vulnerabilità e i produttori siano responsabili della sicurezza informatica per tutto il ciclo di vita di un prodotto. È un passo fondamentale per aumentare la consapevolezza dell'importanza della cybersecurity in tutti gli aspetti del ciclo di vita di un prodotto: dalla fase di concept a quella di design, di implementazione e infine di testing. A seguire saranno anche interessate le fasi di post-sviluppo e produzione[50]. I dispositivi IoT[51] espongono i consumatori a rischi informatici perché spesso non possiedono sistemi sicuri di archiviazione e trasferimento dei dati, né queste attività vengono monitorate. La conseguenza è duplice: nuove opportunità per i cyber criminali e incapacità di identificare e affrontare le

alle minacce della criminalità (EMPACT) è un'iniziativa in materia di sicurezza portata avanti dagli Stati membri e tesa a individuare, classificare in ordine di priorità e affrontare le minacce provenienti dalla criminalità organizzata internazionale. Contrastare gli attacchi informatici è una delle sue priorità.

Il Centro europeo per la lotta alla criminalità informatica (EC3) è stato istituito da Europol per rafforzare la risposta delle autorità di contrasto alla criminalità informatica nell'UE e contribuire così a proteggere i cittadini, le imprese e i governi europei dalla criminalità online. Dalla sua istituzione nel 2013, EC3 ha dato un contributo significativo alla lotta contro il crimine informatico ed è stato coinvolto in molte operazioni di alto profilo e centinaia di implementazioni di supporto operativo. EC3 si concentra sui seguenti tipi di crimini informatici: criminalità ciberdipendente, sfruttamento sessuale minorile e frode nei pagamenti. Il supporto fornito si estende anche alla lotta alla criminalità sul Dark Web e piattaforme alternative.

Nel 2010 Europol, insieme alla Commissione europea e agli Stati membri dell'UE, ha istituito la task force dell'Unione europea sulla criminalità informatica (EUCTF), una rete basata sulla fiducia il cui ruolo è individuare, discutere e classificare in ordine di priorità le principali sfide e azioni nella lotta contro la criminalità informatica.

EC3 ospita e supporta la Joint Cybercrime Action Task-force (J-CAT), composta da funzionari di collegamento informatico di vari Stati membri dell'UE, partner delle forze dell'ordine non UE e EC3. I membri della task force propongono, selezionano e lavorano insieme su casi di alto profilo per le indagini. Il Consiglio di Programma EC3 fornisce al Centro indicazioni su come raggiungere al meglio i suoi obiettivi e adempiere ai compiti ufficialmente assegnati, basandosi su partnership, responsabilità condivisa e cooperazione con tutti i membri del Consiglio.

Sono stati creati gruppi consultivi dedicati al fine di promuovere una più stretta cooperazione tra l'EC3 e i principali partner non appartenenti alle forze dell'ordine in settori chiave come la sicurezza di Internet, le telecomunicazioni e i servizi finanziari.

Infine, EC3 lavora per garantire che ogni partner globale possa svolgere un ruolo nella lotta congiunta contro il crimine informatico. Ha quindi istituito la piattaforma sicura per esperti accreditati di criminalità informatica (SPACE), in cui gli esperti possono scambiare le migliori pratiche e ampliare ulteriormente la base di conoscenze globali sulla criminalità informatica. *«European Cybercrime Centre - EC3», Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.*

[50] https://www.cybersecurity360.it/giornalista/andrea-razzini, «Cyber Resilience Act: requisiti fondamentali e prodotti coinvolti», Cyber Security 360 (blog), 22 settembre 2022, https://www.cybersecurity360.it/legal/cyber-resilience-act-requisiti-fondamentali-e-prodotti-coinvolti/.

[51] L'Internet of Things, o IoT, è un sistema di dispositivi informatici in grado di raccogliere e trasferire dati su una rete wireless senza bisogno dell'intervento umano.

aggressioni. Anche i *device* basati sull'AI sono soggetti alle medesime minacce, con, in più, una maggiore difficoltà nell'individuare eventuali compromissioni[52].

[52] «Il Cyber Resilience Act: i nuovi requisiti di cybersecurity europei», Futuro Digitale (blog), 21 ottobre 2022, https://futurodigitale.infocert.it/pillole-normative/il-cyber-resilience-act-i-nuovi-requisiti-di-cybersecurity-europei/.

1. Le infrastrutture critiche

Quando si parla di infrastrutture critiche bisogna guardare non solo alla protezione, in termini di prevenzione e contrasto delle minacce, ma anche all'idoneità al ripristino della capacità operativa e più in generale della *service continuity* in un'ottica di resilienza integrata[53]. Le autorità nazionali sono prevalentemente responsabili della protezione delle infrastrutture critiche; tuttavia le perturbazioni di queste possono avere effetti al di là delle frontiere nazionali, ed è per questo che si rende necessaria una dimensione unionale per aiutare a gestire tali rischi. Nel 2007, il Consiglio dell'Unione europea ha adottato conclusioni relative a un programma europeo per la protezione delle infrastrutture critiche, il quale punta a migliorare la loro tutela contro tutti i tipi di minacce e pericoli. La perturbazione o la distruzione delle infrastrutture critiche assume un impatto significativo a livello unionale quando il danno derivante da queste, a causa di calamità naturali, terrorismo, attività criminali o comportamenti dolosi, si riversa su almeno due degli Stati membri, causando una consistente criticità alla sicurezza dell'Unione europea e al benessere dei suoi cittadini[54]. Ridurre la loro vulnerabilità e aumentarne la resilienza è uno dei principali obiettivi dell'Unione; occorre infatti garantire un livello adeguato di protezione e limitare il più possibile gli effetti negativi delle perturbazioni sulla società[55].

Il programma europeo per la protezione delle infrastrutture critiche (EPCIP) definisce il quadro generale delle attività volte a migliorare la protezione delle infrastrutture critiche in tutti gli Stati dell'Unione europea e in tutti i settori pertinenti dell'attività economica. L'EPCIP cerca di fornire un approccio inter-settoriale per tutti i tipi di rischio summenzionati, attraverso scambi regolari di informazioni tra gli Stati membri nel quadro delle riunioni dei punti di contatto. Un

---

[53] Europa Atlantica, «La sicurezza delle infrastrutture critiche tra nuove regole e strategie europee», Formiche.net, 31 luglio 2019, https://formiche.net/2019/07/regole-strategie-europee-sicurezza-infrastrutture-critiche/.

[54] «Infrastrutture Critiche», https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en.

[55] Ad esempio, impianti per l'energia elettrica oppure oleodotti per il trasporto del petrolio; di quest'ultima classificazione si può prendere in esame il terminal marittimo di Voltri, a Genova, attraverso il quale transitano gigantesche quantità di merci, che vengono poi distribuite nell'intera Europa. Alla stessa categoria può appartenere l'autostrada del Brennero, attraverso la quale transitano merci e persone, che si spostano successivamente nell'intera Europa. *PuntoSicuro, «Infrastrutture critiche: cosa sono e come vanno protette -...», https://www.puntosicuro.it/security-C-125/una-norma-fondamentale-per-la-protezione-delle-infrastrutture-critiche-AR-20199/.*

pilastro fondamentale di questo programma è la direttiva 2008/114/CE, dell'8 dicembre 2008, sulle infrastrutture critiche europee (ECI), la quale stabilisce una procedura per la loro individuazione e designazione, ed un approccio comune per valutare la necessità di migliorarne la protezione in ambito di cybersecurity[56]. La disciplina in esame ha un campo di applicazione settoriale in quanto si applica solo agli ambiti dell'energia e dei trasporti[57], sottolineando che "vi sono nella comunità infrastrutture critiche, la cui distruzione o il cui danneggiamento avrebbe un significativo impatto transfrontaliero", per cui è "opportuno che le ECI siano individuate e designate come tali attraverso una comune procedura". Altresì, prevede che "la responsabilità principale e definitiva della protezione delle ECI ricade sugli Stati membri e sui proprietari/operatori di tali infrastrutture". La direttiva comunitaria fornisce quindi le definizioni di *infrastruttura critica* e di *infrastruttura critica europea*[58] e stabilisce che gli Stati membri devono assicurare che tutte le ECI designate dispongano di un piano di sicurezza per gli operatori (PSO) e di un Security Liaison Officer (SLO)[59].

La procedura dedicata alle ECI comporta, in primo luogo, l'individuazione degli elementi che definiscono un'infrastruttura; in secondo luogo, viene effettuata un'analisi dei rischi basata sulle minacce più gravi, sulla vulnerabilità di ogni elemento e sull'impatto potenziale di questi a danno della ECI; infine, vengono individuate, selezionate e attribuite le priorità delle

---

[56] «EUR-Lex - Jl0013 - EN - EUR-Lex», https://eur-lex.europa.eu/IT/legal-content/summary/protecting-critical-infrastructure.html.

[57] «Infrastrutture Critiche», https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en.

[58] L'infrastruttura critica è, secondo la direttiva 2008/114/CE, "un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni". Invece, l'infrastruttura critica europea è, sempre per la direttiva 2008/114/CE, "un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture".

[59] Tale figura professionale corrisponde ad un soggetto dotato di conoscenze, abilità e competenze nel campo della security tali da garantire la gestione complessiva dei processi di security. È chiamata a gestire le attività di valutazione, governo e mitigazione delle criticità di natura prevalentemente criminosa, che possono compromettere le risorse materiali, immateriali, organizzative e umane di cui un'organizzazione dispone o di cui necessita per garantirsi nel tempo un'adeguata capacità produttiva e concorrenziale. Il SLO agisce come punto di contatto fra il proprietario/l'operatore della ECI e l'autorità competente dello Stato membro, al fine di scambiare informazioni utili relative ai rischi e alle minacce individuati, riguardo alla ECI interessata. *Redazione InSic, «Security manager, chi è e cosa fa», InSic (blog), 5 gennaio 2022, https://www.insic.it/privacy-e-sicurezza/security-articoli/security-manager-chi-e-e-cosa-fa/.*

contromisure e delle procedure stesse. A questo proposito è necessario operare una distinzione fra le misure graduali di sicurezza, che possono essere attivate in funzione dei diversi livelli di rischio e di minaccia, e quelle permanenti di sicurezza, che individuano gli investimenti e gli strumenti indispensabili in materia di sicurezza che si prestano ad essere utilizzati in ogni momento; rientrano sotto quest'ultima voce le informazioni riguardanti le misure di tipo generale, quali quelle tecniche (inclusa l'installazione di strumenti di rilevazione, controllo degli accessi, protezione e prevenzione), organizzative (comprese le procedure di allarme e gestione delle crisi), di controllo e verifica, le comunicazioni, la crescita della consapevolezza e l'addestramento e la sicurezza dei sistemi informativi.

La presente normativa costituisce il primo passo di approccio graduale all'individuazione delle ECI, ma è possibile ritenere che debba essere rivista al fine di valutarne l'impatto e di esaminare la necessità di includere nel suo campo di applicazione altri settori, oltre a quelli già citati; tra questi, quello delle tecnologie dell'informazione e della comunicazione (ICT) in quanto costituisce un servizio trasversale rispetto ai vari settori ed è capace, se in crisi, di avviare un effetto domino immediato con effetti devastanti[60]. Prendendo in considerazione l'aspetto della valutazione dell'impatto in modo indipendente dalla minaccia che ha indotto il disservizio, la direttiva del 2008 delinea un approccio *all hazard*[61]; in questo senso tutti i tipi di minacce, da quelle naturali, a quelle legate alle attività antropiche, dagli incidenti occasionali agli attacchi terroristici deliberati, sono potenzialmente considerabili causa del disservizio e di avvio della crisi dell'infrastruttura critica sotto osservazione. La direttiva stabilisce una serie di azioni e di procedure volte ad individuare e proteggere le infrastrutture critiche europee, indicando le parti coinvolte e attribuendo loro specifiche responsabilità e, in particolare, prevedendo l'applicazione di una procedura in più fasi affinché un'infrastruttura sia riconosciuta come ECI. La normativa indica inoltre i criteri relativi ai singoli settori e quelli intersettoriali per

[60] «Le infrastrutture critiche: un punto di vista normativo», S News S.r.l., 13 luglio 2015, https://www.snewsonline.com/le-infrastrutture-critiche-un-punto-di-vista-normativo/.

[61] La Commissione Europea è stata la prima a evidenziare l'opportunità e l'urgenza di un approccio all-hazard, come evidenziato nella comunicazione 2006/786 che istituisce l'European Programm on Critical Infrastructure Protection (Epcip*). Europa Atlantica, «La sicurezza delle infrastrutture critiche tra nuove regole e strategie europee», Formiche.net, 31 luglio 2019, https://formiche.net/2019/07/regole-strategie-europee-sicurezza-infrastrutture-critiche/.*

selezionare quelle infrastrutture la cui rilevanza a livello comunitario è tale da ritenerle di interesse europeo; spetta a ogni Stato membro la designazione finale dell'infrastruttura critica come ECI, mediante comunicazione alla Commissione. In altre parole, ogni Stato membro dovrà interagire con gli altri Stati dell'Unione mediante un organismo nazionale competente per la protezione delle infrastrutture critiche; infatti, i paesi dell'UE effettuano una valutazione delle minacce relative alle ECI entro un anno dalla designazione di infrastruttura critica e comunicano alla Commissione i dati generali sulle tipologie di rischi, minacce e vulnerabilità ogni due anni. Infine, per garantire il coordinamento delle attività ogni Stato membro deve nominare un Punto di contatto unico. Agli Stati è altresì richiesto di svolgere una valutazione dei rischi, delle minacce e delle vulnerabilità con costante regolarità, analizzando in particolare i sottosettori individuati all'interno delle ECI.

Per quanto riguarda la collaborazione con il settore privato, ogni proprietario/operatore di infrastruttura designata come ECI dovrà predisporre di un piano di sicurezza dell'operatore (PSO). La direttiva fornisce un'indicazione dei contenuti minimi che dovranno essere trattati nel PSO: il piano dovrà identificare tutti i beni della infrastruttura critica e le soluzioni in atto o in corso di implementazione per la loro protezione. Ogni proprietario/operatore della ECI dovrà nominare un funzionario di collegamento in materia di sicurezza che agisca come punto di contatto per le questioni di sicurezza fra l'ECI e l'organismo nazionale competente per la protezione delle infrastrutture critiche[62]; il funzionario serve da punto di contatto fra il proprietario/l'operatore dell'ECI e l'autorità del paese dell'UE interessata.

Tenendo conto degli sviluppi successivi all'adozione della comunicazione dell'EPCIP del 2006, si è reso necessario un approccio aggiornato alla politica dell'Unione in materia di infrastrutture critiche. L'articolo 11 della direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee fa riferimento a uno specifico processo di revisione della direttiva e pertanto, nel corso del 2012, è stata condotta una revisione globale in

[62] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), La disciplina giuridica del settore a seguito della direttiva comunitaria in materia di protezione delle infrastrutture critiche, pag. 32-35.

stretta collaborazione con gli Stati membri e le parti interessate. I risultati preliminari di tale riesame sono stati sintetizzati in un documento di lavoro dei servizi della Commissione del 2013 su un nuovo approccio al programma europeo per la protezione delle infrastrutture critiche che stabilisce un'attuazione riveduta e più pratica delle attività nell'ambito dei tre principali filoni di lavoro: prevenzione, preparazione e risposta. Il nuovo approccio mira a creare strumenti e gestione comuni alla protezione e alla resilienza delle infrastrutture critiche, tenendo maggiormente conto delle interdipendenze[63]. Tali aspetti vengono superati nella successiva Direttiva NIS (che si occupa della sicurezza cyber degli Operatori di Servizi Essenziali), rendendo il dettato della normativa più efficiente[64]. È già in corso l'iter per superare la direttiva 2008/114/CE con una nuova disciplina che, sull'esperienza di questi anni, riesca a fornire una cornice giuridica all'interno della quale sviluppare con maggiore efficacia ed efficienza la dinamica della protezione delle infrastrutture critiche. È infatti evidente come sia sempre più necessaria una visione *all hazard* al fine di cogliere le problematiche legate tanto ad eventi di origine naturale che quelli indotti da fattori antropici (siano essi accidentali o dolosi) ma anche a problematiche di natura geopolitica e di sicurezza nazionale. Sicuramente la nuova direttiva dovrà ampliare il suo campo di azione estendendosi ai settori idrico e sanitario, tenendo conto delle possibilità di operare in sinergia con la normativa NIS per quel che riguarda gli aspetti di cybersecurity.

[63] «Infrastrutture Critiche», https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en.

[64] Europa Atlantica, «La sicurezza delle infrastrutture critiche tra nuove regole e strategie europee», Formiche.net, 31 luglio 2019, https://formiche.net/2019/07/regole-strategie-europee-sicurezza-infrastrutture-critiche/.

2. La Direttiva NIS

La direttiva NIS n. 2016/1148[65], entrata in vigore il 16 luglio 2016, è stata il primo atto legislativo dell'Unione europea in materia di cybersicurezza[66], il cui specifico obiettivo è il suo miglioramento in ambito europeo, armonizzando le relative capacità nazionali in materia, la collaborazione transfrontaliera e la supervisione dei settori critici in tutta l'UE[67]. Altrimenti detto, la direttiva NIS[68] è cardine della strategia per la cybersicurezza e auspica al rafforzamento della cooperazione tra gli Stati membri, il settore pubblico e quello privato[69], imponendo nel contempo alle imprese dei settori critici di segnalare gli incidenti gravi alle autorità nazionali e di adottare pratiche di gestione del rischio per garantire un ambiente digitale sicuro e affidabile in tutta l'Unione. Successivamente all'adozione della direttiva NIS, ogni Stato membro dell'UE ha iniziato ad adottare la legislazione nazionale che segue o recepisce la direttiva in oggetto: i paesi dell'Unione europea godono di un certo livello di flessibilità per tenere conto delle circostanze nazionali, ad esempio per riutilizzare le strutture organizzative esistenti o per allinearsi alla legislazione nazionale esistente[70]. Più specificamente, la NIS rappresenta il primo tentativo di rafforzare il livello globale di cybersicurezza tra gli Stati membri e di determinare una base di garanzie destinate a sviluppare un ecosistema di fiducia che attribuisce un ruolo primario agli Operatori dei Servizi Essenziali (OSE), ossia quelle aziende che forniscono un

[65] La Direttiva NIS è stata riformata ad opera del Regolamento (UE) 2021/87.

[66] Il 6 luglio 2016 a Bruxelles il vicepresidente della Commissione europea Andrus Ansip, responsabile per il mercato unico digitale, e il commissario Günther H. Oettinger, responsabile per l'Economia e la società digitali, hanno accolto con favore il voto espresso dalla plenaria del Parlamento europeo per adottare la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS). La direttiva in oggetto è stata la principale proposta legislativa nell'ambito della strategia dell'Unione europea per la cybersicurezza del 2013 e stabilisce, tra le altre misure, l'obbligo per tutti gli Stati membri dell'UE di adottare una strategia nazionale sulla sicurezza delle reti e dei sistemi informativi. *«National Cybersecurity Strategies (NCSSs) Map», Topic, ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.*

[67] «NIS Directive Tool», NIS Visual Tool, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool.

[68] L'acronimo "NIS" sta per Security of Network and Information systems: la direttiva (UE) 2016/1148 si occupa infatti della sicurezza delle reti e dei sistemi informativi.

[69] Si fa riferimento alle aziende internet e agli operatori di infrastrutture principali quali le piattaforme del commercio elettronico, le reti sociali e i servizi in materia di trasporti, banche e assistenza sanitaria.

[70] «NIS Directive», Topic, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

servizio fondamentale, la cui eventuale interruzione avrebbe un impatto significativo sull'andamento dell'economia o della società in termini di rischi[71].

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. Altresì, la direttiva NIS consente agli Stati membri di estendere l'ambito di applicazione delle proprie disposizioni anche a settori diversi da quelli elencati nella stessa[72]. Al fine di garantire la più ampia cooperazione tra i Paesi dell'Unione europea in materia di cybersicurezza, la direttiva NIS istituisce due organi che hanno il ruolo primario di promuovere la fiducia a livello unionale: il primo di questi è il Gruppo di Cooperazione, che appoggia e facilita la cooperazione strategica e lo scambio di informazioni tra Stati membri; il secondo, invece, consiste in una rete di gruppi di intervento per la sicurezza informatica in caso di incidente, denominati CSIRT, che garantiscono una risposta operativa rapida ed efficace. Inoltre, per far sì che tale cooperazione avvenga, è necessario che ciascun Stato membro adotti una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi per la determinazione degli obiettivi strategici e le opportune misure attuative. Sugli Stati incombe anche l'obbligo di designare Punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi creando così un meccanismo di cooperazione, e il dovere di nominare autorità nazionali competenti dotate dei poteri necessari per valutare la conformità degli operatori di servizi essenziali e dei fornitori di servizi digitali agli obblighi loro imposti e con risorse adeguate per prevenire, gestire e rispondere a rischi e/o incidenti di sicurezza delle reti e dell'informazione. Il dettato della NIS non pregiudica le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, specie la tutela della sicurezza nazionale, comprese le misure volte al mantenimento dell'ordine pubblico e alla tutela di informazioni la cui divulgazione sia considerata dagli Stati contraria agli interessi essenziali

[71] La definizione degli OSE è quella fornita dall'Anssi (National Cybersecurity Agency of France).

[72] «Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto», Agenda Digitale, 15 gennaio 2021, https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.

della loro sicurezza. Inoltre, gli Stati membri possono adottare o mantenere in vigore disposizioni atte a conseguire un livello più elevato di sicurezza della rete e dei sistemi informativi, e per far fronte alle minacce attuali ed emergenti devono sviluppare e adattare costantemente le proprie strategie di cybersicurezza (NCSS[73]), stabilendo i principi strategici, le linee guida, gli obiettivi e, in alcuni casi, le misure specifiche al fine di mitigare i rischi associati alla sicurezza informatica[74].

Le strategie nazionali, che ogni Paese dell'Unione deve adottare per il conseguimento e il mantenimento di un livello elevato di sicurezza, disciplinano un quadro di governance per conseguire gli obiettivi e le priorità della strategia, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; devono essere indicate le misure di preparazione, risposta e recupero scelte dagli Stati, inclusa la collaborazione tra settore pubblico e settore privato, ed i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi. Ancora, è necessario che gli Stati individuino piani di ricerca e sviluppo relativi alla strategia da adottare, che sia elaborato un piano di valutazione dei rischi, e che sia previsto un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale. A tali scopi, gli Stati membri possono richiedere l'assistenza dell'ENISA nello sviluppo delle strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi. Dal 2012, infatti, l'ENISA sostiene gli Stati nello sviluppo, nell'attuazione e nella valutazione delle loro strategie nazionali in materia di cybersicurezza. La mappa delle NCSS dell'ENISA[75] elenca tutti i documenti delle strategie nazionali di

[73] L'acronimo NCSS sta per National Cybersecurity Strategies.

[74] Al fine di rafforzare le infrastrutture critiche contro varie minacce e di mantenere la fiducia dei cittadini, la Commissione europea ha proposto, nel 2013, la direttiva in oggetto sulla sicurezza delle reti e dell'informazione. Nel dicembre 2015 il Parlamento europeo e il Consiglio hanno raggiunto un accordo sulla proposta della Commissione ed il Parlamento europeo ha adottato la direttiva finale nel luglio 2016, entrando in vigore nell'agosto dello stesso anno. L'ENISA sostiene gli sforzi degli Stati membri dell'Unione dal 2012 fornendo orientamenti su come sviluppare, attuare e aggiornare le NCSS, analizzando le strategie esistenti e delineando le buone pratiche. *«National Cybersecurity Strategies Guidelines & Tools», Topic, ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools.*

[75] L'ENISA sostiene gli sforzi volti a migliorare il livello generale di cybersicurezza negli Stati membri sia a livello nazionale che unionale. Gli Stati membri stanno affrontando l'innovazione come priorità strategica nell'ambito delle strategie nazionali di cybersicurezza (NCSS). L'analisi è strutturata attorno a diversi aspetti dell'innovazione quali: priorità di innovazione, industrializzazione e collaborazione e mercato e politica. Ognuno di questi aspetti è allo stesso

cybersicurezza nell'Unione europea, i relativi obiettivi strategici e buoni esempi di attuazione. Informazioni più specifiche sugli obiettivi e sulle buone pratiche si basano sulla guida alle buone pratiche NCSS pubblicata dall'ENISA nel 2016[76]. Ogni Stato deve designare una o più autorità nazionali competenti in materia di cybersicurezza (le quali controllano l'applicazione della presente direttiva a livello nazionale) e nel farlo possono affidare questo ruolo anche a una o più autorità già esistenti. Inoltre, gli Stati designano un Punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi, e, come nel caso summenzionato, il compito può essere affidato ad un'autorità esistente. Quest'organo svolge una funzione di collegamento per garantire la cooperazione transfrontaliera ed una collaborazione effettiva, efficiente e sicura delle autorità dei vari Stati membri con il Gruppo di cooperazione e con la rete di CSIRT; ove opportuno e conformemente al diritto nazionale, le autorità competenti e il Punto di contatto unico consultano le autorità di contrasto e le autorità per la protezione dei dati nazionali competenti e collaborano con esse. La direttiva NIS lascia liberi gli Stati membri di decidere come implementare la disciplina relativa alle autorità competenti e al Punto di contatto unico all'interno della propria nazione: possono adottare o mantenere in vigore disposizioni atte a conseguire un livello di sicurezza più elevato della rete dei sistemi informativi; la NIS impone infatti un livello minimo di sicurezza per le tecnologie, le reti e i servizi digitali in tutti gli Stati membri e, introducendo misure di gestione del rischio più coerenti e la segnalazione sistematica degli incidenti, dovrebbe aiutare i settori che dipendono dai sistemi ICT ad essere più affidabili e stabili. Al fine di contribuire allo sviluppo della fiducia fra gli Stati membri e di promuovere una cooperazione operativa rapida ed efficace, è istituita una rete di CSIRT. Le reti, i sistemi ed i servizi informativi svolgono un ruolo vitale nella società, per cui è essenziale che essi siano

tempo diviso in due dimensioni: le priorità dell'innovazione possono essere suddivise in innovazione nelle tecnologie e nei servizi e in incentivi economici e investimenti; l'industrializzazione e la collaborazione possono essere ripartite in processi e attività di industrializzazione e collaborazione delle parti interessate; infine, mercato e politica possono essere articolati in allineamento del mercato e della tecnologia e regolamentazione del mercato. Ogni dimensione può essere supportata da diverse attività e meccanismi. *«Good Practices in Innovation on Cybersecurity under the NCSS», Report/Study, ENISA, https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.*

[76] «National Cybersecurity Strategies (NCSSs) Map», Topic, ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

affidabili e sicuri per le attività economiche, sociali ed in particolare ai fini del funzionamento del mercato interno. Gli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei servizi informativi; per una risposta efficace è necessario un approccio globale a livello di Unione, che contempli disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali[77].

Ogni Stato membro si occupa della designazione di uno o più CSIRT: essi hanno il compito di trattare gli incidenti e i rischi secondo una procedura ben definita e possono essere creati all'interno dell'autorità competente. Gli Stati garantiscono la collaborazione effettiva, efficiente e sicura dei propri CSIRT nella rete europea e possono chiedere l'assistenza dell'ENISA nello sviluppo della rete nazionale. La rete di CSIRT assolve a molteplici funzioni, prime fra tutte quelle di permettere lo scambio di informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione degli stessi, e, su base volontaria, l'offerta di dati non riservati su singoli incidenti. Su richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, la rete europea discute delle informazioni non sensibili sul piano commerciale connesse a tale incidente e dei rischi associati; tuttavia, lo stesso CSIRT può rifiutare di contribuire a tale discussione se ciò rischia di compromettere l'indagine sull'incidente. In aggiunta, sempre su richiesta di un rappresentante, la rete discute e, ove possibile, individua un intervento coordinato per un incidente rilevato nella giurisdizione di quello stesso Stato membro. La rete fornisce inoltre, sulla base dell'assistenza reciproca volontaria, sostegno agli Stati membri nel far fronte a incidenti transfrontalieri; analizza gli insegnamenti appresi dalle esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA; infine, formula orientamenti volti ad agevolare la cooperazione operativa attraverso l'individuazione di nuove forme, anche in relazione alle categorie di rischi e di incidenti, ai preallarmi, all'assistenza reciproca e ai principi e alle modalità di coordinamento in caso di incidenti transfrontalieri. Di quest'ultima

[77] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), pag. 31-32.

attività, la rete di CSIRT deve informare il Gruppo di cooperazione al fine di chiedere orientamenti in merito[78].

Grazie al dettato della NIS, l'ENISA ha visto accresciuto il proprio ruolo di assistenza agli Stati membri e al Gruppo di cooperazione nei loro compiti: infatti, questa, oltre ad aiutare i Paesi dell'Unione ad affrontare le questioni comuni di cybersicurezza e a concordare gli approcci e le procedure comuni da seguire, individua le buone pratiche negli Stati membri per quanto riguarda l'attuazione della direttiva NIS e sostiene il processo di segnalazione a livello unionale per gli incidenti di cybersicurezza, sviluppando soglie, modelli e strumenti atti allo scopo[79]. Altra novità apportata dalla direttiva, riguarda il Gruppo di cooperazione per le reti e i sistemi

---

[78] L'articolo 12 Dir. UE 2016/1148, dedicato alla "Rete di CSIRT " disciplina: "1. Al fine di contribuire allo sviluppo della fiducia fra gli Stati membri e di promuovere una cooperazione operativa rapida ed efficace, è istituita una rete di CSIRT.
2. La rete di CSIRT è composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE. La Commissione partecipa alla rete dei CSIRT in qualità di osservatore. L'ENISA assicura il segretariato e sostiene attivamente la cooperazione fra i CSIRT.
3. La rete di CSIRT ha i seguenti compiti:
a) scambiare informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT;
b) su richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente e i rischi associati; tuttavia, qualsiasi CSIRT di uno Stato membro può rifiutare di contribuire a tale discussione se ciò rischia di compromettere l'indagine sull'incidente;
c) scambiare e mettere a disposizione su base volontaria informazioni non riservate su singoli incidenti;
d) su richiesta di un rappresentante di un CSIRT di uno Stato membro, discutere e, ove possibile, individuare un intervento coordinato per un incidente rilevato nella giurisdizione di quello stesso Stato membro;
e) fornire sostegno agli Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria;
f) discutere, esaminare e individuare ulteriori forme di cooperazione operativa, anche in relazione a:
(i) categorie di rischi e di incidenti; (ii) preallarmi; (iii) assistenza reciproca; (iv) principi e modalità di coordinamento, quando gli Stati membri intervengono a proposito di rischi e incidenti transfrontalieri;
g) informare il gruppo di cooperazione in merito alle proprie attività e a ulteriori forme di cooperazione operativa discusse sulla scorta della lettera f) e chiedere orientamenti in merito;
h) discutere gli insegnamenti appresi dalle esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA;
i) discutere, su richiesta di un singolo CSIRT, le capacità e lo stato di preparazione di tale CSIRT;
j) formulare orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.
4. Ai fini del riesame di cui all'articolo 23 ed entro il 9 agosto 2018 e, successivamente, ogni 18 mesi, la rete di CSIRT elabora una relazione in cui valuta l'esperienza acquisita riguardo alla cooperazione operativa, comprese conclusioni e raccomandazioni, realizzata ai sensi del presente articolo. Tale relazione è trasmessa anche al gruppo di cooperazione.
5. La rete di CSIRT definisce il proprio regolamento interno". *CyberLaws, «Articolo 12 - Direttiva NIS (EU-2016/1148)», CyberLaws (blog), 1° gennaio 2018, https://www.cyberlaws.it/2018/articolo-12-direttiva-nis-eu-2016-1148/.*

[79] «National Cybersecurity Strategies (NCSSs) Map», Topic, ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

informativi, istituito per garantire la cooperazione e lo scambio di informazioni tra gli Stati membri; la missione generale del Gruppo è raggiungere un elevato livello comune di sicurezza per le reti e i sistemi informativi nell'Unione europea. Infatti, questo sostiene e facilita la cooperazione strategica e lo scambio di informazioni tra gli Stati membri dell'Unione, ed i suoi compiti sono esplicitamente descritti all'articolo 11 della direttiva NIS.

Dal punto di vista operativo il Gruppo di cooperazione in materia di sicurezza delle reti e dell'informazione è sostenuto dal lavoro della rete di CSIRT, alla quale fornisce orientamenti strategici per lo svolgimento delle sue attività; il Gruppo sta inoltre lavorando a stretto contatto con la rete europea di cooperazione elettorale per contrastare le minacce ai processi elettorali nell'ambito di un nuovo meccanismo operativo congiunto istituito nell'ambito del piano d'azione per la democrazia europea. È composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'Unione per la cybersicurezza (ENISA), e la presidenza è occupata dallo Stato membro che esercita la presidenza del Consiglio dell'Unione europea. I principali risultati del Gruppo di cooperazione riguardano gli orientamenti non vincolanti per consentire un'attuazione efficace e coerente della direttiva NIS in tutta l'Unione e per affrontare questioni più ampie di politica in materia di cybersicurezza[80].

Vista la trasformazione della minaccia, l'evoluzione del testo della direttiva NIS è stata inevitabile, in particolare per ampliare il campo di applicazione e preparare le aziende alle sfide attuali e future della sicurezza delle reti e dei sistemi informativi. Questa constatazione ha portato la Commissione a proporre una revisione della direttiva, sotto il nome di NIS2[81]: in primo luogo, è chiamata a reinterpretare le disposizioni per adeguarsi ai flussi digitali post pandemia covid-19, che hanno visto il considerevole aumento di traffico nella rete e delle

[80] «Gruppo Di Cooperazione NIS | Plasmare Il Futuro Digitale Dell'Europa», https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

[81] 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. *«Direttiva NIS2 approvata: ecco cosa cambia in materia di sicurezza di dati, reti e sistemi», Cyber Security 360 (blog), 17 novembre 2022, https://www.cybersecurity360.it/legal/direttiva-nis2-approvata-ecco-cosa-cambia-in-materia-di-sicurezza-di-dati-reti-e-sistemi/.*

relative superfici di attacco; in secondo luogo, facendo tesoro dei primi anni di dibattito e applicazione della NIS, i nuovi provvedimenti mirano ad ampliare i settori di attività, finendo per coinvolgere un numero e una varietà sempre maggiore di organizzazioni. Tra i capisaldi che verranno implementati nella direttiva NIS2 possono essere citati la rideterminazione e l'ampliamento dell'ambito di applicazione delle norme in materia di sicurezza dei dati; il potenziamento degli organi e delle attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale grazie alla condivisione delle esperienze tra gli Stati membri; infine, la razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria degli incidenti informatici.[82] Un'ulteriore novità prevista è che, nell'ipotesi in cui dovesse verificarsi un incidente di sicurezza informatica, a risponderne non sarà più soltanto l'azienda titolare del servizio, ma anche gli altri *stakeholder*[83] che intervengono lungo la *supply chain*[84].

La direttiva NIS2 detta 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 informatici con un piano e un'attività di monitoraggio continuo e di *incident response*; dotarsi di un piano di continuità di business e gestione delle crisi; testare regolarmente la sicurezza dell'infrastruttura ICT e l'efficacia delle misure di gestione del rischio adottate; e infine, assicurare la sicurezza delle supply chain, controllando che i propri fornitori dispongano di adeguati requisiti in termini di sicurezza. L'obiettivo del legislatore europeo è quello di estendere gli obblighi in materia di sicurezza informatica a tutti gli attori coinvolti, per creare un clima di responsabilità condivisa

---

[82] «Direttiva NIS2 approvata: ecco cosa cambia in materia di sicurezza di dati, reti e sistemi», Cyber Security 360 (blog), 17 novembre 2022, https://www.cybersecurity360.it/legal/direttiva-nis2-approvata-ecco-cosa-cambia-in-materia-di-sicurezza-di-dati-reti-e-sistemi/.

[83] Nel linguaggio economico, per stakeholder si intende il portatore di un interesse, sia con riferimento a un'attività aziendale che a un progetto. Se parliamo di una società, per esempio, gli stakeholder sono i clienti, i fornitori, i creditori, i dipendenti, gli azionisti, i residenti nell'area in cui ha sede la società, le amministrazioni locali e i rappresentanti dei vari gruppi di interessi concreti. *Admin, «Stakeholder – definizione e significato», Dizionario Economico (blog), 15 dicembre 2015, https://dizionarioeconomico.com/stakeholder.*

[84] Per supply chain o catena di approvvigionamento si intende il processo che permette di portare sul mercato un prodotto o servizio, trasferendolo dal fornitore fino al cliente. *Mecalux, «Supply chain: cos'è e come funziona la catena di approvvigionamento», consultato 19 dicembre 2022, https://www.mecalux.it/blog/supply-chain-cos-e.*

nei confronti della gestione del rischio e dell'adozione delle necessarie misure di prevenzione e rimedio agli attacchi informatici[85]. Il panorama delle minacce digitali si è evoluto in modo estremamente rapido negli ultimi anni, anche in considerazione del sempre maggior numero di settori che si affidano alla tecnologia digitale. In questo scenario, la nuova direttiva, cosiddetta NIS2, ha l'obbiettivo di aggiornare quella precedente nell'ottica di migliorare la resilienza europea nel campo del digitale. Come già preannunciato, la recente pandemia di covid-19 ha ulteriormente evidenziato l'importanza e la necessità della tecnologia digitale, soprattutto in merito a determinate aziende e settori: dalla salute alla vendita al dettaglio, dalla produzione all'istruzione; per questo, la Commissione ha ritenuto necessario aggiornare la NIS al fine di fornire risposte adeguate e innovative al nuovo panorama e alle sue sfide, anche per quanto riguarda l'Internet of Things (IoT), il 5G e le reti mobili di futura generazione[86]. Nella NIS2 viene eliminata la distinzione tra fornitori di servizi essenziali e fornitori di servizi digitali, e le aziende vengono classificate in "essenziali" e/o "importanti" a seconda della criticità dei servizi che offrono[87]. Anche l'ambito di applicazione viene ampliato comprendo più servizi, come la produzione di prodotti farmaceutici, dispositivi medici e prodotti chimici, il settore alimentare, la gestione delle acque reflue e dei rifiuti, i servizi postali, nonché la pubblica amministrazione.

Nonostante le novità apportate, è possibile evidenziare la mancanza di un approccio armonizzato, che darebbe luogo ad una significativa frammentazione nel recepimento della

[85] «Direttiva NIS2 approvata: ecco cosa cambia in materia di sicurezza di dati, reti e sistemi», Cyber Security 360 (blog), 17 novembre 2022, https://www.cybersecurity360.it/legal/direttiva-nis2-approvata-ecco-cosa-cambia-in-materia-di-sicurezza-di-dati-reti-e-sistemi/.

[86] «Direttiva NIS 2, gli sviluppi attuali e gli scenari futuri: il punto», Cyber Security 360 (blog), 20 dicembre 2021, https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-gli-sviluppi-attuali-e-gli-scenari-futuri-il-punto/.

[87] Le infrastrutture digitali, come i fornitori di servizi DNS (Domain Name System), i fornitori di punti di scambio Internet (IXP) e i fornitori di cloud e data center, verranno considerati come "essenziali"; mentre i mercati online, i motori di ricerca e fornitori di social network verranno classificati come servizi "importanti". In aggiunta, la nuova direttiva introduce la regola della soglia di dimensione, indicando come tutti i soggetti di medie e grandi dimensioni che operano nei settori o forniscono i servizi contemplati dalla direttiva stessa rientrano nel suo ambito di applicazione: le micro e piccole entità sono escluse dal campo di applicazione della direttiva, almeno che non indichino un ruolo chiave nella fornitura di servizi essenziali all'interno dell'Unione oppure operino in particolari settori o tipi di servizi, come nel caso della pubblica amministrazione, in quanto coperti automaticamente dalla direttiva, indipendentemente dalle loro dimensioni.

nuova direttiva[88], e la previsione di oneri amministrativi aggiunti, i quali dovrebbero essere ridotti al minimo in quanto imporre alle aziende di segnalare ogni incidente di sicurezza informatica rischia di creare oneri eccessivi sia per le imprese che per coloro che analizzano questi dati. Sarebbe dunque necessario specificare le soglie esatte che portano agli obblighi di segnalazione: di fatto i tempi rigorosi di notifica degli incidenti (24 ore) possono rivelarsi molto impegnativi in scenari reali, e soprattutto in quei casi in cui le aziende interessate operano in compartimenti intra ed interstatali. Inoltre, tali tempistiche potrebbero dover essere estese per corrispondere a quelle già in vigore in altre normative come nel GDPR (72 ore). Non è realistico credere che sia possibile raggiungere una sicurezza totale contro gli attacchi informatici, ma una maggiore collaborazione tra i governi e le aziende per meglio contrastare e intraprendere azioni contro i criminali informatici è il primo passo verso un sistema più efficace e sicuro[89].

[88] A titolo esemplificativo, l'Unione europea ha presentato una proposta per una direttiva sulla resilienza dei soggetti critici (CER) e per un regolamento sulla resilienza operativa digitale (DORA), il che richiede un'attenzione particolare per evitare duplicazioni e confusioni giuridiche, considerando anche i requisiti di protezione dei dati stabiliti dal Regolamento generale sulla protezione dei dati (GDPR) e la proposta di Regolamento ePrivacy.

[89] «Direttiva NIS 2, gli sviluppi attuali e gli scenari futuri: il punto», Cyber Security 360 (blog), 20 dicembre 2021, https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-gli-sviluppi-attuali-e-gli-scenari-futuri-il-punto/.

3. Il diritto alla protezione dei dati personali

La tutela dei dati personali è diventata un settore chiave per le aziende del web: il dato personale è il metro di misura di un servizio o di un prodotto, da qui l'esigenza di una regolamentazione a tutela dei diritti dei cittadini[90] e in particolare del diritto alla protezione dei dati (*data protection*)[91]. Il diritto in esame è sancito dall'articolo 8 della Convenzione europea dei diritti dell'uomo del 1950 (CEDU) e dall'articolo 16 del Trattato sul funzionamento dell'Unione europea (TFUE); costituisce un diritto fondamentale dell'individuo, appartiene alle sole persone fisiche e in genere alle persone viventi, ed è un diritto autonomo rispetto al più generale diritto alla riservatezza (*privacy*)[92]. Il diritto alla protezione dei dati personali nasce come corollario del diritto alla riservatezza; quest'ultimo ha un'accezione prevalentemente negativa in termini di *ius excludendi alios* dalla vita privata di ciascun individuo, in quanto è volto a non far rilevare informazioni personali essendo legato alla stessa concezione che è alla base del diritto di proprietà. Non è quindi pensato come un diritto a sé, ma nasce come limite alla libertà di espressione e al diritto all'informazione: altrimenti detto, il diritto alla riservatezza è il diritto a che non vengano diffuse informazioni personali, a mezzo stampa o tramite i media, senza che la persona interessata abbia dato il suo consenso, a meno che la notizia ad essa riferita sia di pubblico interesse[93]. Differentemente, il diritto alla protezione dei dati personali estende la tutela dell'individuo oltre la sfera della vita privata e in particolare nelle relazioni sociali, così

[90] Grazie alle disposizioni del Regolamento (UE) 2016/679, i cittadini sono al centro del sistema in quanto sono loro riconosciuti: il diritto alla portabilità dei dati, il diritto all'oblio (riconosciuto fino ad ora solo a livello giurisprudenziale), il diritto di essere informati in modo trasparente, leale e dinamico sui trattamenti effettuati sui propri dati e il diritto di essere informati sulle violazioni dei propri dati personali. Il Regolamento (UE) 2016/679 riconosce, pertanto, un livello elevato e uniforme di tutela dei dati ed è finalizzato a dare un maggiore controllo ai cittadini sull'utilizzo dei propri dati. *«Regolamento UE 2016/679, ecco tutto ciò che cittadini e PA devono sapere», Agenda Digitale, 27 maggio 2016, https://www.agendadigitale.eu/infrastrutture/nuovo-regolamento-privacy-ue-ecco-tutto-cio-che-cittadini-e-pa-devono-sapere/.*

[91] 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.

[92] Bruno Saetta, «Diritto alla protezione dei dati personali», Protezione dati personali, https://protezionedatipersonali.it/diritto-alla-protezione-dei-dati-personali.

[93] «Diritto alla protezione dei dati personali», Data Protection Law | Privacy e protezione dati personali (blog), https://www.dataprotectionlaw.it/diritto-alla-protezione-dei-dati-personali/.

garantendo l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati (espandendosi nel diritto alla protezione dell'identità personale)[94]. Il diritto in esame è disciplinato nel dettaglio dal Regolamento (UE) 2016/679[95] – ossia dal Regolamento generale sulla protezione dei dati, in sigla GDPR – del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali[96]. La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali; la portata della condivisione e della raccolta di questi è aumentata in modo significativo: sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano[97]. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati ed è attuato allo stesso modo in tutti i Paesi dell'Unione senza margini di libertà nell'adattamento (pur

---

[94] Si tratta, quindi, di garantire la libertà personale come diritto fondamentale, non solo come libertà fisica ma anche contro ogni controllo illegittimo e ogni ingerenza altrui. *Alfonso Contaldo e Davide Mula, Cybersecurity LAw, 2020ª ed. (Pacini Giuridica, s.d.).*

[95] L'articolo 4 Reg. 2016/679, rubricato "Definizioni", detta: "Ai fini del presente regolamento s'intende per:
1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro". *«Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio - del 27 aprile 2016 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/ 46/ CE (regolamento generale sulla protezione dei dati)», s.d.*

[96] Del diritto alla protezione dei dati personali trattano, inoltre, vari altri atti normativi italiani e internazionali e il Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101.

[97] Bruno Saetta, «Regolamento generale per la protezione dei dati», Protezione dati personali, https://protezionedatipersonali.it/regolamento-generale-protezione-dati.

lasciando spazi di manovra ai legislatori nazionali in alcune materie, in particolare quelle che investono in via diretta l'esercizio di pubblici poteri[98]). Il GDPR[99] vincola infatti tutti gli Stati membri e, pur essendo stato emanato nel 2016, dispiega la sua efficacia a partire dal 25 maggio del 2018, lasciando un periodo di due anni di tempo per adeguarsi alle novità legislative[100]. I suoi obiettivi riguardano la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea, lo sviluppo del mercato unico digitale europeo e, infine, la risposta alle nuove sfide derivanti dalle nuove tecnologie digitali[101]. In particolare, il Regolamento (UE) 2016/679 disciplina il trattamento dei dati personali sia indipendentemente dal fatto che questo venga eseguito o meno nell'Unione, sia quando è svolto da titolari o responsabili stabiliti nell'UE o in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (per esempio l'ambasciata o la rappresentanza consolare di uno Stato membro), ed anche quando il titolare o il responsabile non è stabilito nell'Unione europea ma le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi nell'area europea, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure siano relative al monitoraggio del loro comportamento tenuto all'interno dell'Unione[102].

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

---

[98] Vedi il Decreto Legislativo di adeguamento n. 101 del 2018.

[99] L'acronimo GDPR sta per General Data Protection Regulation.

[100] Silvia Rigotto, «Regolamento UE 679: quali sono le finalità e a che punto siamo in Italia?», datapro (blog), 8 settembre 2021, https://dataprogdpr.com/regolamento-ue-679-a-cosa-serve/.

[101] Il considerando (9) del Reg. (UE) 2016/679 recita: "Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE". *«Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio - del 27 aprile 2016 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/ 46/ CE (regolamento generale sulla protezione dei dati)», s.d.*

[102] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), pag. 145.

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 designato nel territorio dello Stato italiano, destinatari), l'esistenza di un processo decisionale automatizzato, compresa la profilazione, ed infine, i diritti previsti dal regolamento. L'obiettivo generale del diritto di accesso è fornire alle persone informazioni sufficienti, trasparenti, agevoli, e quindi accessibili, sul trattamento dei loro dati personali in modo che possano essere consapevoli e verificare la liceità del trattamento e l'esattezza dei dati trattati[103]. Il diritto di accesso, quindi, comprende diverse componenti: la conferma che i dati relativi alla persona siano trattati (o meno), l'accesso ai dati personali e quello alle informazioni sul trattamento, quali le finalità, le categorie di dati e destinatari, la durata del trattamento e i diritti degli interessati[104]. Riassumendo, il Regolamento (UE) 2016/679 costituisce un prezioso tentativo di armonizzazione delle regole privacy dei vari Stati ed è finalizzato a sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e software[105]; inoltre, ha ampliato i diritti riconosciuti all'interessato con riferimento ai dati che lo riguardano, rendendoli maggiormente incisivi in una realtà permeata sempre più dal ricorso alle nuove tecnologie e all'utilizzo della rete[106]. In base alla normativa che regolamenta tale diritto, quindi, ogni individuo può pretendere che i suoi dati personali siano raccolti e trattati da terzi nel rispetto delle regole e dei principi previsti dalle leggi in materia, sia dell'Unione europea che dei suoi singoli Stati membri. Lo scopo della disciplina è quello di attribuire

[103] Il diritto di accesso, ai sensi della legge sulla protezione dei dati, deve essere distinto da diritti analoghi con altri obiettivi, ad esempio il diritto di accesso ai documenti pubblici che mira a garantire trasparenza nel processo decisionale delle autorità pubbliche e buone prassi amministrative. *«Cosa è il diritto alla protezione dei dati personali?*», https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/2003167.*

[104] EDPB - Guidelines 01/2022 on data subject rights - Right of access [https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf]

[105] «Regolamento UE 2016/679, ecco tutto ciò che cittadini e PA devono sapere», Agenda Digitale, 27 maggio 2016, https://www.agendadigitale.eu/infrastrutture/nuovo-regolamento-privacy-ue-ecco-tutto-cio-che-cittadini-e-pa-devono-sapere/.

[106] «Cosa è il diritto alla protezione dei dati personali?*», https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/2003167.

all'interessato il potere di disporre dei propri dati, assicurando all'individuo il controllo su tutte le informazioni riguardanti la propria vita privata, e fornendogli allo stesso tempo gli strumenti per la tutela di queste informazioni[107]. Col regolamento europeo, si passa da una visione proprietaria del dato (in base alla quale non lo si può trattare senza consenso) ad una visione di controllo, che favorisce la libera circolazione del dato rafforzando nel contempo i diritti dell'interessato[108]. I principi che reggono l'elaborazione dei dati sono anzitutto la liceità, la correttezza e la trasparenza nel trattamento dei dati; in secondo luogo, i dati devono essere trattati solo per uno scopo legittimo e specifico, oltre che esplicito, e devono essere adeguati, rilevanti e necessari rispetto alla finalità; infine, devono essere mantenuti aggiornati e completi, conservati solo per il tempo necessario rispetto alla finalità e trattati in modo sicuro e in modo da non subire alterazioni o accessi non autorizzati. Il regolamento pone l'accento sulla responsabilizzazione (o *accountability*) di titolari e responsabili del trattamento, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento[109]: la novità sta nel fatto che viene affidato ai titolari 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 nel regolamento[110]. Il primo fra tali criteri è sintetizzato dall'espressione inglese *data protection by default and by design*, che riguarda la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo, ove il trattamento si colloca, e dei rischi per i diritti e le libertà degli interessati. Il secondo criterio rispetto alla gestione degli obblighi dei titolari, invece, è da intendersi come il rischio di impatti negativi sulle libertà e i diritti degli interessati[111]; tali impatti dovranno essere

---

[107] Bruno Saetta, «Diritto alla protezione dei dati personali», Protezione dati personali, https://protezionedatipersonali.it/diritto-alla-protezione-dei-dati-personali.

[108] «Diritto alla protezione dei dati personali», Data Protection Law | Privacy e protezione dati personali (blog), https://www.dataprotectionlaw.it/diritto-alla-protezione-dei-dati-personali/.

[109] Si vedano gli articoli 23-25, in particolare, e l'intero capo IV del Regolamento (UE) 2016/679.

[110] «Regolamento Ue 2016/679 e stato di attuazione in Italia», 6 luglio 2018, https://www.diritto.it/regolamento-ue-2016-679-lo-del-suo-recepimento/.

[111] Si vedano i considerando (75), (76) e (77) del Reg. (UE) 2016/679.

analizzati attraverso un apposito processo di valutazione[112], tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) o consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di autorizzare il trattamento, bensì quello di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58, che vanno dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento[113]. Dunque, l'intervento delle autorità di controllo si collocherà, in via principale, successivamente alle determinazioni assunte autonomamente dal titolare[114]. La trasparenza è intrinsecamente legata alla correttezza e al nuovo principio di responsabilizzazione ai sensi del regolamento. Dall'articolo 5, paragrafo 2, risulta che il titolare del trattamento dev'essere sempre in grado di dimostrare che i dati personali sono trattati in modo trasparente nei confronti dell'interessato; a questo si aggiunge il fatto che il principio di responsabilizzazione impone la trasparenza delle operazioni di trattamento affinché il titolare sia in grado di dimostrare il rispetto degli obblighi che il regolamento gli impone[115]. Concludendo, alle autorità di controllo, e in particolare al Comitato europeo della protezione dei dati spetta un ruolo fondamentale al fine di garantire uniformità di approccio e di fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre

[112] Si vedano gli articoli 35 e 36 del Reg. (UE) 2016/679.

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

[114] Ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e di effettuazione di valutazioni di impatto in piena autonomia, con l'eventuale successiva consultazione dell'Autorità, tranne alcune specifiche situazioni di trattamento (vedi articolo 36, paragrafo 5 del Regolamento).

[115] «linee guida sulla trasparenza ai sensi del regolamento 2016/679 - wp260 rev.01», https://www.iusprivacy.eu/linee-guida-sulla-trasparenza-ai-sensi-del-regolamento-2016-679-wp260-rev-01-4293989599.htm.

tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati[116].

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

4. Il Cybersecurity Act

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[117]. Allo stesso tempo, nessun prodotto o servizio garantisce completamente la cybersicurezza e bisogna promuovere regole basilari sull'igiene informatica, dando loro la priorità. I moderni prodotti e sistemi ICT spesso integrano e utilizzano una o più tecnologie e componenti terzi quali moduli software, biblioteche o interfacce per programmi applicativi. Tale utilizzo, detto «dipendenza», potrebbe presentare rischi supplementari connessi alla cybersicurezza in quanto le vulnerabilità riscontrate in componenti terzi potrebbero pregiudicare anche la sicurezza dei prodotti, servizi e processi ICT. In molti casi, l'individuazione e la documentazione di tali dipendenze consentono agli utenti finali di migliorare le loro attività di gestione dei rischi in materia di sicurezza delle reti e dei sistemi informativi ottimizzando, ad esempio, le procedure messe in atto per individuare le criticità e porvi rimedio[118]. Il Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019, cosiddetto Cybersecurity Act, entrato in vigore il 27 giugno 2019[119], è, in quanto tale, immediatamente esecutivo in tutti gli Stati membri senza necessità di interventi attuativi da parte dei legislatori nazionali; la normativa

---

[117] 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», Scegliformitore (blog), 14 dicembre 2020, https://sceglifornitore.it/blog/servizi-it-cosa-sono-cose-linformation-technology/.*
L'acronimo "ICT" (Information and Communication Technologies) fa riferimento alle tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni. Rilevanti incentivi economici favoriscono questo processo di integrazione, promuovendo la crescita delle imprese attive nel settore. *«ICT (Information and Communication Technologies) in "Dizionario di Economia e Finanza"», https://www.treccani.it/enciclopedia/ict_(Dizionario-di-Economia-e-Finanza).*

[118] «Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione Europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cybersicurezza)», s.d. In particolare, riferimento ai considerando (10) e (11).

[119] Con l'adozione del Regolamento (UE) 2019/881 l'UE è giunta finalmente alla conclusione di un lungo iter approvativo, iniziato nel 2017 con la presentazione del testo iniziale del Cybersecurity Act da parte della Commissione europea.

individua il sistema di certificazione per la sicurezza informatica europea[120], e tratta principalmente del rafforzamento del mandato dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) [121], la quale assume un ruolo diretto nella prevenzione dei cyber-attacchi, rafforzando la propria posizione, e della definizione del quadro europeo delle certificazioni in ambito sicurezza informatica, attraverso cui vengono tracciati standard – validi in tutto il territorio UE – con cui valutare se prodotti e servizi ICT siano effettivamente sicuri e certificabili[122]; in questo modo, le imprese che operano a livello unionale beneficeranno di dover certificare i propri prodotti, processi e servizi ICT solo una volta e vedere i loro certificati riconosciuti in tutta l'Unione europea[123]. Il Regolamento in esame costituisce una parte fondamentale della nuova strategia per la sicurezza cibernetica dell'Europa, e consente non solo di rafforzare la resilienza dell'Unione agli attacchi informatici, ma anche di creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi[124]. In quest'ottica, dunque, il Cybersecurity Act si affianca all'altra importante normativa in materia introdotta a livello unionale, ossia la Direttiva NIS. Il previsto riconoscimento reciproco, da parte degli Stati membri, delle certificazioni UE ha come principale obiettivo quello di aumentare il coordinamento, anche attraverso l'incremento di un eguale livello di consapevolezza in tutta l'area eurocomunitaria. Inoltre, la coesistenza tra certificazioni pubbliche e le già esistenti certificazioni private (es. ISO) ambisce a creare le

[120] «Cybersecurity Act, pubblicato sulla Gazzetta ufficiale UE il testo definitivo: tutte le novità», Cyber Security 360 (blog), 10 giugno 2019, https://www.cybersecurity360.it/news/cybersecurity-act-approvata-la-legge-europea-per-la-sicurezza-cibernetica-che-ce-da-sapere/.

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

[122] «Cybersecurity Act: cos'è e come aumenta la sicurezza informatica», Worldline (blog), https://www.worldlineitalia.it/cybersecurity-act/.

[123] «Legge dell'UE sulla cybersicurezza | Plasmare il futuro digitale dell'Europa», https://digital-strategy.ec.europa.eu/it/policies/cybersecurity-act.

[124] «Cybersecurity Act, pubblicato sulla Gazzetta ufficiale UE il testo definitivo: tutte le novità», Cyber Security 360 (blog), 10 giugno 2019, https://www.cybersecurity360.it/news/cybersecurity-act-approvata-la-legge-europea-per-la-sicurezza-cibernetica-che-ce-da-sapere/.

conoscenze e le abilità operative necessarie per garantire un appropriato livello di cybersicurezza[125].

La nuova legge sulla sicurezza informatica prevede un mandato permanente e maggiori risorse per l'Agenzia europea per la sicurezza informatica[126], che è chiamata a svolgere un ruolo di primo piano nella gestione del sistema di certificazione introdotto dal Cybersecurity Act; è opportuno che questa sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza, alla qualità delle consulenze e delle informazioni fornite, e alla trasparenza delle procedure e dei metodi operativi. Nello svolgimento dei suoi compiti l'ENISA dovrebbe sostenere attivamente gli sforzi nazionali e contribuire in modo proattivo agli sforzi dell'Unione, collaborando pienamente con le istituzioni, gli organi e gli organismi dell'UE e con gli Stati membri, evitando la duplicazione delle attività e promuovendo le sinergie. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione del settore privato e di altri portatori d'interessi. Dunque, è opportuno stabilire una serie di compiti che definiscano in che modo l'ENISA debba raggiungere i propri obiettivi, lasciandole allo stesso tempo una certa flessibilità di azione[127]. In questo modo, l'Agenzia europea potrà svolgere non solo i suoi consueti compiti di consulenza tecnica, ma anche attività di supporto concreto alla gestione operativa degli incidenti informatici da parte degli Stati membri. L'ENISA avrà un ruolo chiave nell'istituzione e nel mantenimento del quadro europeo di certificazione della cybersicurezza, preparando il terreno tecnico per specifici sistemi di certificazione: è, infatti, incaricata di rafforzare la cooperazione operativa a livello eurounitario, aiutando gli Stati membri che desiderano richiederla a gestire i propri incidenti di cybersicurezza e sostenendo il coordinamento dell'UE

[125] «Norme cybersecurity in Europa, che caos: i nodi da risolvere», Agenda Digitale, 3 gennaio 2020, https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/.

[126] 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".

[127] «Regolamento (UE) 2019/ del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione Europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cybersicurezza)», s.d. In particolare, riferimento al considerando (20).

in caso di crisi e attacchi informatici transfrontalieri su larga scala[128]. Questo compito si basa sul ruolo dell'ENISA di segretariato della rete nazionale delle squadre di risposta agli incidenti in materia di sicurezza informatica (CSIRT), istituita dalla direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)[129]. Altrimenti detto, il Cybersecurity Act ridefinisce completamente il ruolo dell'Agenzia conferendole un compito di spicco nella gestione tecnica e operativa di tutti i potenziali incidenti informatici. Fino a questo momento, infatti, l'ENISA ha svolto principalmente le due funzioni di assistenza e consulenza tecnica nell'attività di elaborazione di politiche in materia di sicurezza informatica per tutti gli Stati membri e di prevenzione di incidenti informatici ed elaborazione di tecniche per contrastarli. L'attività operativa di gestione degli incidenti non era (fino ad ora) svolta dall'Agenzia, ma dai singoli Stati membri; con il nuovo Regolamento europeo, invece, l'ENISA non si limiterà più esclusivamente a ricoprire un ruolo di assistenza tecnica, bensì si occuperà attivamente di fornire supporto nell'attività di gestione operativa degli incidenti informatici[130], oltre allo svolgimento della mansione indispensabile di definizione e gestione delle certificazioni informatiche introdotte dallo stesso Cybersecurity Act[131].

L'Agenzia diventa un vero e proprio centro indipendente con il compito di sensibilizzare e istruire gli Stati membri in ambito cybersecurity[132]. In particolare, l'ENISA contribuisce allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione prestando assistenza e consulenza per lo sviluppo e la revisione delle politiche, della normativa dell'Unione nel campo della cybersicurezza e delle iniziative legislative e politiche settoriali che presentano una correlazione con le questioni relative alla cybersicurezza, in particolare fornendo un parere indipendente, analisi, nonché svolgendo lavori preparatori; inoltre, assiste gli Stati membri nell'attuazione uniforme di tali politiche, in particolare in relazione all'applicazione della

[128] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), pag. 75.

[129] «Legge dell'UE sulla cybersicurezza | Plasmare il futuro digitale dell'Europa», https://digital-strategy.ec.europa.eu/it/policies/cybersecurity-act.

[130] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), pag. 81.

[131] «CSA | Cybersecurity Act», Cyber Security Agency, https://www.csa.gov.sg/legislation/cybersecurity-act.

[132] «Cybersecurity Act: cos'è e come aumenta la sicurezza informatica», Worldline (blog), https://www.worldlineitalia.it/cybersecurity-act/.

direttiva NIS, anche emanando pareri e orientamenti, fornendo consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia; ancora, assiste gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nello sviluppo e nella promozione di politiche sulla cybersicurezza che sostengano la disponibilità generale o l'integrità del carattere fondamentale pubblico di una rete Internet aperta, e contribuisce ai lavori del Gruppo di cooperazione mettendo a disposizione le proprie competenze e fornendo assistenza. Altresì, l'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cybersicurezza dei prodotti, dei servizi e dei processi ICT monitorando continuamente gli sviluppi nei settori di normazione connessi e raccomandando adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cybersicurezza; in secondo luogo, prepara proposte di sistemi europei di certificazione della cybersicurezza per prodotti, servizi e processi ICT, elaborando e pubblicando orientamenti, e sviluppa buone pratiche in merito ai requisiti di cybersicurezza in cooperazione con le autorità nazionali di certificazione; infine, valuta i sistemi europei di certificazione della cybersicurezza adottati e assiste la Commissione nel provvedere alle funzioni di segretariato del Gruppo europeo per la certificazione.

Il secondo tema del Cybersecurity Act[133], come detto, riguarda l'istituzione di un quadro europeo di certificazione della cybersicurezza di prodotti e servizi digitali, con l'obiettivo di facilitare lo scambio e il commercio di tutti prodotti ICT all'interno dell'Unione europea definendo degli standard universali, validi quindi per tutti gli Stati membri: grazie all'istituzione di queste certificazioni, sarà possibile creare un mercato interno all'UE di prodotti e servizi informatici sicuri e certificati[134]. Una volta adottato uno schema europeo di

[133] Viene trattato negli articoli da 46 a 65 del Regolamento (UE) 2019/881.

[134] La costituzione di schemi di certificazione specifici per prodotti e sistemi ICT 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 e delle Tecnologie dell'Informazione (Iscom, operante presso il Ministero dello Sviluppo Economico) già certifica la sicurezza informatica di prodotti e sistemi ICT secondo lo schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione istituito dal DPCM del 30 ottobre 2003. Analoghi schemi di certificazione esistono anche in altri Stati membri. Esempi ne sono la Certification de Sécurité de Premier Niveau des Produits des Technologies de l'Information (CSPN), in Francia; il Commercial Product Assurance

certificazione da parte della Commissione, le aziende interessate potranno presentare domanda di certificazione dei propri prodotti o servizi a specifici organismi accreditati, salvo che lo schema di certificazione in questione non consenta alle aziende di procedere ad una autovalutazione di conformità (solo per prodotti e servizi a basso rischio). L'utilizzo della certificazione rimarrà però volontario, a meno che la certificazione venga espressamente richiesta per determinate categorie di prodotti o servizi da specifiche norme di settore. Inoltre, gli schemi europei di certificazione andranno gradualmente a sostituire gli omologhi schemi di certificazione nazionali, ma i certificati rilasciati sulla base di questi ultimi rimarranno validi siano alla loro scadenza naturale.[135] Nel Cybersecurity Act, all'articolo 51, vengono individuate delle linee guida prioritarie per la definizione dei requisiti che i dispositivi ICT dovrebbero possedere per ottenere la certificazione di sicurezza europea. Per ottenere tale certificazione sarà necessario definire che i sistemi, servizi o processi informatici siano in grado di proteggere i dati dall'accesso non autorizzato e dall'appropriazione indebita durante tutto il proprio ciclo di vita; siano in grado di garantire l'accesso, il trattamento o la modifica di dati esclusivamente a persone, programmi o macchine con gli specifici diritti di accesso; possano proteggere i dati da distruzione, modifica o perdita non autorizzate; ancora, possiedano la funzionalità di ripristinare tempestivamente l'accesso a dati, funzioni e servizi in caso di incidente tecnico o fisico; garantiscano l'individuazione di dipendenze e vulnerabilità note e la registrazione relativa all'accesso ai dati (a quali dati è stato effettuato l'accesso e da chi); siano stati progettati

(CPA), nel Regno Unito; e il Baseline Security Product Assessment (BSPA), in Olanda. Tuttavia, molti degli schemi di certificazione esistenti non vengono riconosciuti all'estero, o almeno non in tutti gli Stati membri. Ciò obbliga le imprese ad espletare vari processi di certificazione per operare a livello transnazionale. Ad esempio, la Commissione europea ha verificato come un fabbricante di contatori intelligenti (i cosiddetti "smart meter") che intenda vendere i propri prodotti in Germania, Francia e Regno Unito debba farli certificare secondo tre schemi differenti. Si noti che, al momento, i costi di certificazione tendono ad essere piuttosto elevati per le imprese; ad esempio, in Germania, i costi per la certificazione dei contatori intelligenti sono superiori a 1 milione di euro, mentre nel Regno Unito e in Francia i costi per ottenere analoga certificazione ammontano a circa 150.000 euro. *«Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT», Agenda Digitale, 7 giugno 2019, https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.*

[135] Alfonso Contaldo e Davide Mula, Cybersecurity Law, 2020ª ed. (Pacini Giuridica, s.d.), pag. 88-89.

secondo i criteri di *security by design*; infine, implementino le impostazioni più sicure e vengano aggiornati costantemente mediante meccanismi protetti e verificati[136].

Partendo dal presupposto che non tutti i prodotti e servizi informatici hanno lo stesso livello di rischio, il Cybersecurity Act definisce tre livelli differenti di certificazione[137], che sono i livelli base, sostanziale e avanzato. Per ottenere il livello di affidabilità di base è sufficiente svolgere un riesame della documentazione tecnica e una valutazione delle possibili attività sostitutive equivalenti; esclusivamente in questo caso il produttore/fornitore dei prodotti o servizi ICT può ricorrere all'autocertificazione. Il livello di affidabilità sostanziale, invece, prevede una valutazione di sicurezza effettuata per ridurre al minimo i rischi di cyber attacchi commessi da soggetti che dispongono di risorse e abilità limitate; per ottenere questa certificazione sarà necessario, in primo luogo, valutare con un test che non ci siano vulnerabilità pubblicamente note, e di seguito un secondo test dovrà garantire che i prodotti/servizi esaminati compiano in modo corretto tutte le necessarie funzionalità di sicurezza. Il livello di sicurezza più approfondito è quello elevato, dove la valutazione di sicurezza viene effettuata per ridurre al minimo il rischio di cyber-attacchi commessi da soggetti che dispongono di risorse e abilità specifiche e significative; in questo caso le valutazioni di sicurezza comprendono tre test: il primo per garantire che non esistano vulnerabilità pubblicamente note, il secondo per dimostrare che i prodotti attuino regolarmente le funzioni avanzate di sicurezza e il terzo per

---

[136] «Cybersecurity Act: cos'è e come aumenta la sicurezza informatica», Worldline (blog), https://www.worldlineitalia.it/cybersecurity-act/.

[137] Il livello di affidabilità di un sistema europeo di certificazione è la base per la fiducia nel fatto che un prodotto, servizio o processo ICT soddisfi i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cybersicurezza. Allo scopo di garantire la coerenza del quadro europeo di certificazione della cybersicurezza, un sistema europeo di certificazione dovrebbe poter specificare i livelli di affidabilità per i certificati europei di cybersicurezza e le dichiarazioni UE di conformità rilasciati nell'ambito di detto sistema. Ciascun certificato europeo potrebbe far riferimento a uno dei livelli di affidabilità: «di base», «sostanziale» o «elevato», mentre la dichiarazione UE di conformità potrebbe far riferimento solo al livello di affidabilità «di base». I livelli di affidabilità fornirebbero il rigore e la specificità corrispondenti della valutazione del prodotto, servizio o processo ICT e sarebbero caratterizzati in riferimento alle specifiche tecniche, norme e procedure correlate, tra cui i controlli tecnici, l'obiettivo delle quali è attenuare o prevenire gli incidenti. Ciascun livello di affidabilità dovrebbe essere coerente nei vari settori in cui la certificazione si applica. *«Regolamento (UE) 2019/ del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione Europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cybersicurezza)», s.d. In particolare, riferimento al considerando (86).*

valutare la resistenza dei prodotti agli attacchi di soggetti qualificati (mediante specifici test di penetrazione)[138].

Conclusivamente una breve riflessione riguardo all'approccio dell'Unione europea in ambito cybersecurity, il quale è definibile lodevole ed incoraggiante in quanto il *risk-base approach*[139], alla base del Cybersecurity Act, se propriamente implementato, potrà diventare uno strumento a vantaggio delle imprese che in Europa decideranno di adottarlo per imporsi a livello internazionale assicurando un livello adeguato in materia di cybersicurezza[140]. Nonostante ciò, occorre fare riferimento alla risoluzione non legislativa adottata dal Parlamento europeo in cui si chiede un'azione decisa contro le minacce alla sicurezza legate alla crescente presenza tecnologica della Cina nell'Unione europea; i deputati, infatti, hanno espresso forte preoccupazione per le recenti affermazioni secondo cui le infrastrutture per le reti 5G potrebbero avere delle *backdoor*[141] incorporate che consentirebbero ai fornitori e alle autorità cinesi di avere un accesso non autorizzato ai dati personali e alle telecomunicazioni nell'UE. Il timore, non celato, è che i fornitori di dispositivi di paesi terzi possano presentare un rischio per la sicurezza informatica eurocomunitaria a causa delle leggi del loro paese che obbligano le imprese a cooperare con lo Stato grazie a una definizione molto ampia della sicurezza nazionale. In particolare, le leggi cinesi sulla sicurezza dello Stato hanno suscitato reazioni

---

[138] «Cybersecurity Act: cos'è e come aumenta la sicurezza informatica», Worldline (blog), https://www.worldlineitalia.it/cybersecurity-act/.

[139] L'approccio basato sul rischio (Risk Based Approach) significa valutare sia il potenziale rischio sia le opportunità. *«Risk Based Approach in ISO\IEC 17025:2017 for testing and calibration laboratories», Alpi Associazione (blog), 24 maggio 2018, https://www.alpiassociazione.it/risk-based-approach-in-isoiec-170252017-for-testing-and-calibration-laboratories/.*

[140] «Norme cybersecurity in Europa, che caos: i nodi da risolvere», Agenda Digitale, 3 gennaio 2020, https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/.

[141] Una backdoor (dal termine inglese per porta di servizio o porta sul retro) è un metodo, spesso segreto, per passare oltre (aggirare, bypassare) la normale autenticazione in un prodotto, un sistema informatico, un crittosistema o un algoritmo. Le backdoor sono spesso scritte in diversi linguaggi di programmazione e hanno la funzione principale di superare le difese imposte da un sistema, come può essere un firewall, al fine di accedere in remoto a un personal computer, ottenendo per mezzo di un sistema di crittografia un'autenticazione che permetta di prendere il completo o parziale possesso del computer vittima. Una backdoor può celarsi segretamente all'interno di un ignaro programma di sistema, di un software separato, o può anche essere un componente hardware malevolo come apparati di rete, sistemi di sorveglianza e alcuni dispositivi di infrastruttura di comunicazione che possono avere celate al loro interno backdoor maligne permettendo l'intrusione di un eventuale criminale informatico. *«Backdoor», in Wikipedia, https://it.wikipedia.org/w/index.php?title=Backdoor&oldid=131990955.*

negative in vari paesi e, per questo motivo, i deputati hanno chiesto alla Commissione e agli Stati membri di fornire soluzioni per affrontare le vulnerabilità informatiche nell'acquisto dei materiali per il 5G. Contestualmente, è stato anche proposto di diversificare gli acquisti con diversi fornitori, introdurre procedure di appalto in più fasi, stabilire una strategia per ridurre la dipendenza dell'Europa dalla tecnologia di sicurezza informatica straniera e, infine, creare un sistema di certificazione per l'introduzione del 5G[142]. Di recente, è stata adottata una raccomandazione della Commissione su 5G e cybersecurity che ha come obiettivo l'implementazione di strumenti legislativi, non a livello europeo ma nazionale, per sviluppare misure atte a mettere in sicurezza l'infrastruttura necessaria all'operatività del 5G, siano essi prodotti, servizi o processi. In aggiunta, viene dato agli Stati membri il potere (Golden Power) di escludere compagnie private per motivi di sicurezza; in tale contesto la recente iniziativa della Commissione europea, ed il consequenziale ritorno a misure basate su strategie nazionali, sembrano essere un passo indietro rispetto agli atti ed iniziative fino ad oggi implementate dall'Unione. L'Italia ha risposto alle sollecitazioni della Commissione con il decreto-legge in ambito di perimetro di sicurezza cibernetica[143].

[142] «Cybersecurity Act, pubblicato sulla Gazzetta ufficiale UE il testo definitivo: tutte le novità», Cyber Security 360 (blog), 10 giugno 2019, https://www.cybersecurity360.it/news/cybersecurity-act-approvata-la-legge-europea-per-la-sicurezza-cibernetica-che-ce-da-sapere/.

[143] «Norme cybersecurity in Europa, che caos: i nodi da risolvere», Agenda Digitale, 3 gennaio 2020, https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/.

Capitolo II: La normativa italiana in materia di cybersicurezza

5. Il Codice dell'Amministrazione Digitale

Il Codice dell'Amministrazione Digitale (CAD)[144] è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese; rappresenta il punto di riferimento normativo per guidare la trasformazione digitale della P.A. in Italia, fornendo utili indicazioni anche a cittadini e provider per la corretta gestione di documenti informatici e processi amministrativi digitalizzati[145]. Secondo il CAD[146] le Pubbliche Amministrazioni, nell'organizzare autonomamente la propria attività, devono utilizzare le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei

[144] Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale. Con l'ultimo intervento normativo il CAD è stato ulteriormente razionalizzato nei suoi contenuti: si è proceduto ad un'azione di deregolamentazione, sia semplificando il linguaggio, sia sostituendo le precedenti regole tecniche con linee guida (a cura di AgID), la cui adozione risulterà più rapida e reattiva rispetto all'evoluzione tecnologica. Inoltre, come evidenziato dalla relazione illustrativa del decreto legislativo n. 217/17, è stata sottolineata con maggior forza la natura di carta di cittadinanza digitale della prima parte del CAD, con disposizioni volte ad attribuire a cittadini e imprese i diritti all'identità e al domicilio digitale, alla fruizione di servizi pubblici online e *mobile oriented*, a partecipare effettivamente al procedimento amministrativo per via elettronica ed a effettuare pagamenti online. È stata promossa l'integrazione e l'interoperabilità tra i servizi pubblici erogati dalle Pubbliche Amministrazioni in modo da garantire a cittadini e imprese il diritto a fruirne in maniera semplice. Altresì, è stata garantita maggiore certezza giuridica alla formazione, gestione e conservazione dei documenti informatici prevedendo che non solo quelli firmati digitalmente – o con altra firma elettronica qualificata – ma anche quelli firmati con firme elettroniche diverse possano, a certe condizioni, produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza prevedere l'intervento di un giudice caso per caso. È stata rafforzata l'applicabilità dei diritti di cittadinanza digitale e promosso l'innalzamento del livello di qualità dei servizi pubblici e fiduciari in digitale, sia istituendo presso l'AgID l'Ufficio del Difensore civico per il digitale, sia aumentando la misura delle sanzioni irrogabili qualora i fornitori di servizi fiduciari violino le norme. Infine, è stato promosso un processo di valorizzazione del patrimonio informativo pubblico riconducendolo tra le finalità istituzionali di ogni amministrazione. Da ultimo, il testo coordinato del Codice dell'Amministrazione Digitale è stato aggiornato con le modifiche apportate dal decreto legge 30 aprile 2022, n. 36, convertito con modificazioni dalla legge 29 giugno 2022, n. 79. *«Codice Amministrazione Digitale|Agenzia per l'Italia digitale», https://www.AgID.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale.*

[145] «Codice amministrazione digitale (CAD) cos'è e punti principali», Agenda Digitale, 16 marzo 2022, https://www.agendadigitale.eu/documenti/codice-dellamministrazione-digitale-cose-e-quali-sono-i-punti-principali-da-conoscere/.

[146] L'equivalente europeo del CAD è il Regolamento (UE) n. 910/2014, cosiddetto eIDAS.

cittadini[147] e delle imprese in conformità agli obiettivi indicati nel Piano triennale per l'informatica nella pubblica amministrazione[148]. Di fatto, le P.A. devono tradurre al loro interno il fondamentale principio del *digital first* predisponendo un modello efficace in grado di mantenere custodito nel tempo il complesso di dati, informazioni e documenti digitali rilevanti per l'ente pubblico, fondendo e coordinando in modalità digitale principi essenziali del diritto e dell'archivistica. In particolare, il CAD definisce che tutti i documenti amministrativi devono nascere informatici e devono essere trattati dalle Pubbliche Amministrazioni in un sistema affidabile di gestione documentale, come specificato nelle regole tecniche (oggi affidate alle Linee Guida di AgID[149]).

---

[147] L'articolo 3 rubricato "diritto all'uso delle tecnologie" del d.lgs. 82/2005, al primo comma, dispone: "Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute. *«Decreto legislativo 7 marzo 2005, n. 82 - Normattiva», https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82.*

[148] L'articolo 5-bis del d.lgs. 82/2005, dedicato alle comunicazioni tra imprese e amministrazioni pubbliche, prevede nel primo comma: "La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese". *«Decreto legislativo 7 marzo 2005, n. 82 - Normattiva», https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82.*

[149] Nel Regolamento per l'adozione di Linee Guida per l'attuazione del Codice dell'Amministrazione Digitale sono da menzionare gli articoli 3 e 4. L'articolo 3, disciplinante le tipologie di linee guida, stabilisce che AgID adotta linee guida di indirizzo contenenti regole generali la cui definizione degli aspetti di dettaglio è demandata alla singola Amministrazione e linee guida contenenti regole tecniche ai sensi degli articoli 14-bis e 71 del CAD o di specifiche disposizioni normative e la definizione degli aspetti di dettaglio, in un apposito Allegato tecnico, costituente parte integrante delle linee guida stesse. Nello svolgimento delle funzioni istituzionali, anche su segnalazione delle amministrazioni e degli uffici, AgID può inoltre adottare linee guida operative. L'articolo 4, invece, disciplina il procedimento per l'adozione delle linee guida che avviene sotto la responsabilità del Referente, designato dal responsabile di struttura AgID competente sulla tematica oggetto linee guida. Il Gruppo di lavoro per la redazione delle linee guida è istituito dal Direttore generale con propria determinazione, su proposta del Referente coadiuvato dalla struttura AgID competente nella tematica oggetto delle linee guida. Del Gruppo di lavoro possono far parte soggetti indicati da AgID o da altre amministrazioni, da associazioni di categoria/professionali o appartenenti al mondo universitario e della ricerca. Il Gruppo di lavoro opera sotto la direzione del Referente che coordina e pianifica le attività di redazione delle linee guida e una volta redatta la bozza finale delle linee guida viene sottoposta a consultazione pubblica ai sensi dall'articolo 71 del CAD, la quale deve effettuarsi con modalità atte a consentire l'accesso a chiunque alla documentazione senza necessità di autenticazione, la formulazione, previa autenticazione, di commenti e la tracciatura degli stessi; ancora, sotto la direzione dal Referente, dovrà valutare i commenti pervenuti decidendo se recepire le indicazioni. A conclusione della consultazione pubblica il Direttore generale con apposita determinazione adotta le linee guida e le trasmette al Servizio per la gestione delle Linee Guida per la pubblicazione ai sensi dell'articolo 71 del CAD. *Regolamento per l'adozione di Linee Guida per l'attuazione del Codice dell'Amministrazione Digitale (ai sensi degli artt. 14-bis e 71 del Codice dell' Amministrazione Digitale - decreto legislativo 7 marzo 2005, n. 82)- https://www.AgID.gov.it/sites/default/files/repository_files/regolamento-adozione-linee-guida-attuazione-cad.pdf -)*

Il Codice dell'Amministrazione Digitale è stato introdotto allo scopo di favorire non solo la digitalizzazione dell'attività amministrativa, ma anche per semplificare le procedure burocratiche e incentivare l'accesso degli utenti a tutta la documentazione ed ai servizi online della Pubblica Amministrazione. Il documento in formato digitale gode della stessa valenza di quello cartaceo ed è più facilmente trasmissibile per via telematica; tale digitalizzazione permette di creare un vero e proprio sistema, ossia un circuito delle Pubbliche Amministrazioni all'interno del quale esse possono facilmente comunicare tra loro ed interagire più rapidamente con gli utenti condividendo materiale ed informazioni[150].

I principali concetti che vengono trattati nel CAD riguardano la Firma Elettronica Avanzata (FEA)[151], lo SPID e il domicilio digitale delle persone fisiche. Il Sistema Pubblico di Identità Digitale (SPID) permette di accedere a tutti i servizi online della Pubblica Amministrazione attraverso un'unica identità digitale costituita da username e password. Grazie a questo unico identificativo è possibile collegarsi sempre, dovunque e con qualsiasi strumento, in quanto la Pubblica Amministrazione dispone di un'unica piattaforma centralizzata ove si possono trovare tutti i servizi che questa offre e che mette a disposizione. Inoltre, per facilitare la comunicazione tra amministrazione e cittadini, ogni individuo deve possedere almeno un domicilio digitale che deve indicare al proprio comune di residenza; questo verrà inserito all'interno della cosiddetta Anagrafe Nazionale della Popolazione Residente (ANPR), comunicato e reso disponibile a tutte le Pubbliche Amministrazioni e a tutti gli enti che erogano servizi di interesse pubblico e di

[150] Sinetqnlap, «Cad: il codice dell'amministrazione digitale, tutti i suoi contenuti», La Legge per Tutti (blog), 28 marzo 2019, https://www.laleggepertutti.it/277731_cad-il-codice-dellamministrazione-digitale-tutti-i-suoi-contenuti.

[151] Il Regolamento eIDAS disciplina tre tipologie di firme elettroniche. La prima è la Firma Elettronica consistente in dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare. La seconda modalità è quella della Firma Elettronica Avanzata (FEA), ossia la firma elettronica che soddisfa i seguenti requisiti: la connessione unicamente al firmatario, l'identificazione del firmatario, la creazione di dati per l'idoneità di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo ed infine il collegamento ai dati sottoscritti in modo da consentire l'identificazione di ogni loro successiva modifica. La terza e ultima tipologia è la Firma Elettronica Qualificata (FEQ) che, in aggiunta a quelle di una firma elettronica avanzata, possiede le caratteristiche della creazione su un dispositivo qualificato per la generazione di una firma elettronica e di un certificato elettronico qualificato che ha effetto giuridico equivalente a quello di una firma autografa. *«Firma digitale verso eIDAS|Agenzia per l'Italia digitale», https://www.AgID.gov.it/it/piattaforme/eIDAS/firma-digitale-verso-eIDAS.*

pubblica utilità[152]. Per quanto riguarda la Firma Elettronica Avanzata, questa viene utilizzata nei casi di interazioni di maggiore sicurezza, come può essere quella con una banca. Tutto il processo inizierà con l'utente che deve aderire al servizio accettandone le condizioni d'utilizzo e, dopo la richiesta della firma elettronica, riceverà la password elettronica monouso tramite sms sul cellulare, in quanto verrà generata automaticamente dal sistema. L'utente firmerà anche un vero e proprio contratto in cui acconsente ad usufruire di tale servizio ed i suoi dati verranno conservati per vent'anni[153]. La Firma Elettronica Avanzata è, quindi, l'equivalente informatico – in quanto soddisfa tutti i requisiti – della firma autografa apposta su un documento cartaceo; "Sigillo" è, invece, il servizio creato dal Ministero dell'Istruzione che si rivolge alle persone che devono firmare documenti digitalizzati: si tratta di una soluzione di Firma Elettronica Avanzata che consente di apporre la firma elettronica sui documenti prodotti dall'amministrazione senza la necessità di utilizzare un certificato di firma digitale emesso da un'autorità di certificazione. L'applicativo Sigillo è sicuro e affidabile in quanto, oltre a garantire l'immodificabilità del documento dopo l'apposizione della firma, abbina indissolubilmente l'oggetto della sottoscrizione con il processo di autenticazione SPID e, dunque, con l'identità del firmatario. Tale garanzia è ancora più forte in quanto viene coinvolto un soggetto esterno riconosciuto affidabile (l'Identity Provider) che è indipendente dal gestore del servizio di Firma Elettronica Avanzata a vantaggio del conseguimento della non ripudiabilità. Per poter accedere a Sigillo i firmatari che devono sottoscrivere un documento devono dotarsi di un'identità digitale SPID di livello 2[154], per ottenere la quale è necessario scegliere un Identity Provider registrandosi sul relativo sito internet[155]. L'identità SPID è

[152] Il CAD, all'articolo 1, comma 1, lettera n-ter, definisce il domicilio digitale come un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato e qualificato valido ai fini delle comunicazioni elettroniche aventi valore legale. Possedere un indirizzo di Posta Elettronica Certificata, in base a quanto stabilito dagli articoli 16 D.L. n. 185/2008, 5 D.L. n. 179/2012 e 37 D.L. 76/2020, è obbligatorio per le Pubbliche amministrazioni, le imprese, le società, le ditte individuali e i liberi professionisti iscritti ad un Albo professionale. *Pietro Rossi, «Domicilio digitale: che cos'è e a cosa serve?», 21 ottobre 2021, https://focus.namirial.it/domicilio-digitale/.*

[153] L'utente potrà scaricare dal sito gratuitamente una copia del documento informatico con la richiesta di accettazione che ha sottoscritto.

[154] «Sigillo - Firma Elettronica Avanzata - Sigillo - Firma Elettronica Avanzata», Mi - Ministero dell'istruzione, https://miur.gov.it/-/sigillo-firma-elettronica-avanzata.

[155] In alternativa, è possibile recarsi presso una delle pubbliche amministrazioni che possono svolgere le procedure di identificazione per il rilascio successivo dello SPID.

rilasciata dai Gestori di Identità digitale, soggetti privati accreditati da AgID che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti. La firma digitale può essere ottenuta anche utilizzando lo SPID come sistema di riconoscimento[156] ed i relativi servizi prevedono l'accesso con credenziali SPID di livello 2 in modo che il cittadino abbia la possibilità di dimostrare con certezza la sua identità e ottenere la firma digitale[157].

Come anticipato, il ruolo di AgID è in continua espansione ed oggi riveste un ruolo fondamentale nell'imposizione di linee guida in materia di amministrazione digitale. Infatti, le norme vigenti conferiscono ad AgID un mandato importante nell'attuazione di iniziative tecniche e organizzative volte sia a migliorare la consapevolezza della Pubblica Amministrazione nei riguardi della minaccia, sia ad aumentarne le capacità di prevenzione, protezione e risposta agli incidenti. In particolare l'edizione del 2017 del Piano Nazionale riassume questo ampio mandato attribuendo ad AgID il compito di "dettare indirizzi, regole

[156] L'articolo 21 del d.lgs. 82/2005, riguardante disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale, stabilisce, al comma 2-bis, che: "Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1bis, primo periodo". Il comma 2-ter prevede: "Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti". Infine, il comma 5: "Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie". *«Art. 21 codice dell'amministrazione digitale - Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale», Brocardi.it, https://www.brocardi.it/codice-dell-amministrazione-digitale/capo-ii/sezione-i/art21.html.*

[157] A seguito del completamento della procedura di notifica dello SPID, a decorrere dal 10 settembre 2019 l'identità digitale SPID potrà essere usata per l'accesso ai servizi in rete di tutte le pubbliche amministrazioni dell'Unione. Questo diritto, introdotto dal regolamento eIDAS, potrà essere anticipato dagli Stati membri che potranno decidere se consentire l'accesso anche ai propri servizi che prevedono l'uso di credenziali di livello 1. Per l'accesso a servizi che prevedono l'uso di credenziali di livello 2 e 3, è prevista l'obbligatorietà di credenziali SPID di pari livello. Tutte le pubbliche amministrazioni che rendono accessibili i propri servizi online con credenziali SPID di livello 2 o 3 (come anche attraverso la carta di identità elettronica), hanno l'obbligo di rendere accessibili detti servizi anche con gli strumenti di autenticazione notificati dagli altri Stati membri. Non rispettare tale obbligo, implica esporsi a una procedura di infrazione per violazione dell'articolo 6 del regolamento eIDAS (n. 910/2014). *«SPID - Sistema Pubblico di Identità Digitale\Agenzia per l'Italia digitale», https://www.AgID.gov.it/it/piattaforme/spid.*

tecniche e linee guida in materia di sicurezza informatica e di omogeneità degli standard, di assicurare la qualità tecnica, la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione e di monitorare i piani ICT delle amministrazioni pubbliche". AgID persegue questo mandato sia direttamente sia mediante il CERT-PA, struttura attiva dal 2013 la quale è stata oggetto, durante il 2017, di uno specifico rafforzamento in termini sia di personale che di strumenti tecnici[158]. In attesa dell'emanazione da parte del Dipartimento della Funzione Pubblica delle Regole tecniche per la sicurezza ICT delle Pubbliche Amministrazioni proposte da AgID, tenuto conto dell'urgenza conseguente all'evoluzione delle minacce cibernetiche sul panorama internazionale, e in particolare nei riguardi della Pubblica Amministrazione, AgID ha sviluppato il documento delle Misure minime per la sicurezza ICT delle Pubbliche amministrazioni che fornisce indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo, obbligatorio per tutti. Tale documento è stato emesso con Circolare n. 2/2017 ed è divenuto quindi obbligatorio riferimento normativo per tutte le amministrazioni, che avrebbero dovuto garantire la propria conformità entro il 31 dicembre dello stesso anno. Nel corso del 2017 AgID, tramite il CERT-PA, ha attivato un progetto per la sperimentazione delle modalità di scambio automatico di informazioni operative (indicatori di compromissione) tra strutture di sicurezza mediante protocolli STIX e TAXII attraverso piattaforme per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce relative all'analisi degli incidenti di sicurezza informatica[159]. Tale sperimentazione, che comprende due Gruppi di lavoro dedicati rispettivamente agli aspetti tecnici e alla definizione di una tassonomia ad hoc, ha lo scopo di produrre le specifiche tecniche organizzative che verranno emanate come standard per la realizzazione di un sistema

[158] Il Piano Triennale, tenendo conto delle indicazioni contenute nel Quadro Strategico e nel Piano Nazionale, ha individuato la razionalizzazione delle risorse ICT descritta nel Capitolo 3 "Infrastrutture" come uno dei principali approcci per aumentare il livello di sicurezza complessivo dell'amministrazione attraverso la riduzione della "superficie" esposta agli attacchi informatici (questo era infatti uno degli aspetti tecnici maggiormente critici tra quelli individuati nel Rapporto "Italian Cybersecurity Report 2014").

[159] «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», Altalex, 4 maggio 2017, https://www.altalex.com/documents/leggi/2017/04/21/direttiva-recante-indirizzi-per-la-protezione-cibernetica-e-la-sicurezza-informatica-nazionali.

nazionale di interscambio automatico di indicatori di compromissione qualificati tra operatori accreditati[160].

Le linee guida di AgID si applicano non solo alle Pubbliche Amministrazioni, ai gestori di servizi pubblici e alle società sottoposte a controllo pubblico, ma anche ai soggetti privati, ove non diversamente previsto dalla legge. Per quanto attiene, invece, l'ambito oggettivo delle linee guida, esse contengono le regole tecniche necessarie all'applicazione degli articoli del CAD che disciplinano – fra le altre cose – la validità e l'efficacia probatoria dei documenti informatici, la sottoscrizione con firma elettronica, le copie informatiche dei documenti analogici, le copie analogiche di documenti informatici, i duplicati e le copie informatiche di documenti informatici, la formazione dei documenti informatici e il relativo protocollo, il fascicolo informatico e la conservazione dei documenti e dei fascicoli informatici[161]. Le linee guida prevedono che la gestione del documento informatico si sostanzia in un processo articolato in tre diverse fasi che sono la formazione[162], la gestione e la conservazione del documento. In primo luogo, sono individuate le quattro modalità attraverso cui deve essere realizzato un documento informatico per essere ritenuto valido, la prima delle quali è la creazione del documento attraverso dei software oppure dei servizi cloud qualificati che siano in grado di garantire l'interoperabilità tra i sistemi; la seconda modalità, invece, consiste

[160] Sempre nel corso del 2017 AgID, tramite il CERT-PA, ha provveduto a sviluppare ulteriormente il National Vulnerability Database gestito tramite la piattaforma Infosec. Quest'ultima è stata potenziata e arricchita di funzionalità nonché messa sperimentalmente a disposizione di tutte le amministrazioni in sola consultazione. Le statistiche di accesso hanno mostrato come Infosec sia rapidamente diventato una piattaforma tecnica di riferimento da parte della comunità nazionale e internazionale di analisti, evidenziando un numero significativo e sempre crescente di accessi dall'estero. Tale sinergia dovrà essere sviluppata anche con una molteplicità di altri attori istituzionali, tra cui il Ministero delle Infrastrutture e dei Trasporti ed il Ministero dell'Istruzione, Università e Ricerca, oltre ad enti pubblici nazionali. Il Piano Nazionale, inoltre, dovrà essere condiviso con stakeholder privati, che costituiscono attori rilevanti nell'ottica di una partnership pubblico-privato e, in quanto tali, rappresentano conditio sine qua non per lo sviluppo di un'efficiente capacità di sicurezza e difesa cibernetica nazionale.

[161] Le linee guida dettano regole in materia di formati di file utilizzabili per la formazione dei documenti informatici ed in tema di metadati relativi a tali documenti. Circa i file utilizzabili, gli allegati individuano i formati digitali che devono avere i documenti fra quelli che sono utilizzati dai vari software oggi conosciuti (quali, per esempio, .doc, .docx, .pdf ecc.). Circa i metadati, gli allegati individuano il set minimo di informazioni relative al file/documento che devono essere associate al file medesimo (quali, per esempio, l'Id, il soggetto produttore, la data, il titolo, l'oggetto ecc.).

[162] Durante la fase di formazione del documento, il soggetto che lo forma deve perseguire obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza rispetto alle regole tecniche relative alla formazione del documento medesimo, bilanciando tale esigenza con i bisogni pratici che il soggetto ha nello svolgimento del proprio lavoro quotidiano.

nell'acquisizione di un documento informatico per via telematica o su un supporto informatico, oppure nella creazione di una copia di un documento analogico attraverso la scansione del medesimo e la successiva acquisizione su un supporto informatico, oppure, ancora, nella diretta acquisizione della copia informatica di un documento analogico. Le restanti modalità di formazione riguardano la memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione di dati attraverso moduli o formulari resi disponibili all'utente; da ultimo, è da menzionare la generazione o il raggruppamento, anche in via automatica, di un insieme di dati o registrazioni, provenienti da una o più banche dati, secondo una struttura logica predeterminata e memorizzata in forma statica.

Una volta che il documento informatico viene formato e identificato univocamente, le linee guida stabiliscono che lo stesso debba essere immodificabile. Per raggiungere tale obiettivo, è stabilito che il documento venga memorizzato su un supporto informatico in formato digitale e che non possa essere alterato nel suo accesso e nella sua gestione e conservazione. Le linee guida, quindi, stabiliscono, per ognuna delle quattro tipologie di formazione di documenti informatici sopra descritte, le operazioni che devono essere compiute per garantire l'immodificabilità e l'integrità del documento informatico nonché la certezza del suo autore. Per quanto riguarda la fase della gestione del documento informatico, ogni Pubblica Amministrazione deve nominare il responsabile della gestione documentale nonché il coordinatore della gestione documentale, che abbiano competenze giuridiche, informatiche e archivistiche. Inoltre, la P.A., attraverso il responsabile della gestione documentale, deve adottare un manuale di gestione documentale che raccoglie le modalità di formazione, gestione-trasmissione, interscambio e accesso ai documenti amministrativi, nonché le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico. Le linee guida si occupano altresì dei requisiti minimi di sicurezza che deve avere il sistema di protocollazione informatica, il quale deve garantire, oltre che l'univoca identificazione ed autenticazione degli utenti e la garanzia di accesso alle risorse esclusivamente agli utenti che sono abilitati e/o a gruppi di utenti secondo la definizione di appositi profili, anche il tracciamento permanente di

qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Ancora, come precedentemente accennato, le linee guida stabiliscono che le Pubbliche Amministrazioni, nella formazione, gestione e conservazione dei documenti informatici, debbano applicare e rispettare le minime misure di sicurezza ICT che sono previste nella circolare n. 2/2017 emanata dall'AgID il 18 aprile 2017[163]. Qualora la tenuta del sistema di gestione informatica dei documenti venga affidata a soggetti esterni, questi ultimi sono individuati come responsabili del trattamento dati[164] e pertanto devono fornire garanzie sufficienti per poter attuare le misure tecniche e organizzative adeguate nel rispetto del GDPR e nella tutela dei dati personali dell'interessato[165]. Nel caso in cui l'Ente si affidi a soggetti esterni che forniscono il servizio di conservazione, questi devono garantire il possesso di requisiti elevati dal punto di vista della qualità e della sicurezza (nel rispetto dello standard

[163] A tal proposito, viene previsto che il coordinatore della gestione documentale e il responsabile della conservazione debbano predisporre un piano di sicurezza del sistema di gestione informatica dei documenti, all'interno del quale devono essere previste delle opportune misure tecniche e organizzative che siano in grado di garantire un livello di sicurezza adeguato rispetto al rischio di violazione della normativa in materia di protezione dei dati personali (tenendo conto anche della tipologia di dati trattati). Il Piano di sicurezza deve contenere anche la descrizione della procedura da adottarsi in caso di violazione dei dati personali, secondo quanto previsto dalle apposite disposizioni del GDPR (cioè il c.d. data breach, di cui agli art. 33 e 34 del citato Regolamento UE).

[164] Le linee guida individuano anche i soggetti che rivestono ruoli nel processo di conservazione. In particolare, vengono individuate le seguenti figure: il titolare dell'oggetto della conservazione; il produttore dei PdV (PdV è l'acronimo di "pacchetto di versamento" ed equivale a un deposito di dati digitali nel sistema di conservazione, da parte della persona addetta alla conservazione, insieme alla documentazione e ai metadati necessari all'archivio per facilitarne la conservazione e la consultazione); l'utente abilitato (che è il soggetto che può richiedere al sistema di conservazione l'accesso ai documenti che vi sono ivi contenuti, per poter acquisire relative le informazioni); il responsabile della conservazione e il conservatore. Nella Pubblica Amministrazione il ruolo di responsabile della conservazione è affidato a un dirigente o funzionario interno individuato dal titolare dell'oggetto della conservazione, che abbia competenze giuridiche, informatiche e archivistiche. Tale figura, però, può essere affidata anche ad un soggetto esterno all'Ente, purchè abbia comunque le competenze di cui si è appena detto e purchè sia soggetto terzo rispetto al Conservatore. Il compito del responsabile della conservazione è quello di definire e attuare le politiche del sistema di conservazione e di gestirlo in autonomia sotto la sua responsabilità: in particolare, egli definisce le politiche di conservazione e i requisiti funzionali che deve avere il sistema di conservazione; gestisce il processo di conservazione e assicura la sua costante conformità alla legge; genera e sottoscrive il rapporto di versamento; effettua il monitoraggio della corretta funzionalità del sistema di conservazione; effettua la verifica periodica, almeno quinquennale, dell'integrità e della leggibilità dei documenti contenuti nel sistema di conservazione; provvede alla duplicazione o copia dei documenti informatici a seconda dell'evolversi del contesto tecnologico; predispone le misure necessarie per garantire la sicurezza fisica e logica del sistema di conservazione.

[165] «Le linee guida dell'AGID sulla formazione e la conservazione dei documenti informatici. | Il portale giuridico online per i professionisti - Diritto.it», 19 maggio 2021, https://www.diritto.it/le-linee-guida-dellagid-sulla-formazione-e-la-conservazione-dei-documenti-informatici/.

ISO/IEC 27001), in modo da assicurare l'autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti[166].

A livello europeo il regolamento eIDAS fornisce una base normativa per le interazioni elettroniche fra cittadini, imprese e Pubbliche Amministrazioni incrementando la sicurezza e l'efficacia dei servizi online e transazioni e-business nell'Unione europea. Il nodo italiano tramite il pulsante Login with eIDAS consente l'interoperabilità transfrontaliera delle identità digitali (eID) e la sua implementazione permette la circolarità delle eID italiane fra gli Stati membri dell'Unione[167]. In altre parole, il nodo eIDAS assicura che le persone e le imprese possano utilizzare l'eID nazionale attraverso schemi di accesso ai servizi pubblici in altri paesi dell'UE con un codice unico e che gli elevati livelli di garanzia dei sistemi eID con login eIDAS riducono il rischio di furto d'identità e uso improprio di informazioni personali[168]. Il progetto FICEP (First Italian Crossborder eIDAS Proxy) è la prima piattaforma italiana di interoperabilità dei sistemi di identità digitale in Europa, ovvero il server transfrontaliero italiano: la sua implementazione consente la circolarità delle identità digitali italiane fra tutti gli Stati membri in forza del Regolamento UE n. 910/2014 sull'identità digitale. Tale progetto ha realizzato un nodo eIDAS nazionale rendendo possibile per cittadini europei, in possesso di identità digitali nazionali riconosciute in ambito eIDAS, l'accesso ai servizi delle Pubbliche

---

[166] Per quanto concerne il processo di conservazione, il trasferimento del documento oggetto di conservazione all'interno del sistema di conservazione avviene generando un PdV nelle modalità e con il formato previsto dal manuale. In particolare, in primo luogo, il sistema di conservazione acquisisce il PdV, il quale viene verificato per riscontrarne la coerenza con le modalità previste dal manuale di conservazione; in secondo luogo, viene generato un rapporto di versamento che sarà identificato in maniera univoca dal sistema di conservazione; infine, viene sottoscritto con la firma digitale o elettronica, da parte del responsabile della conservazione o dal responsabile del servizio di conservazione, il rapporto di versamento e del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente.
Le linee guida dettano anche alcune regole per quanto concerne le infrastrutture utilizzate per il servizio di conservazione. A tal proposito, viene stabilito l'obbligo per il soggetto che fornisce il servizio di conservazione di conservare e rendere disponibili nel territorio italiano le descrizioni del sistema di conservazione. Inoltre, viene stabilito che i conservatori debbono garantire alle amministrazioni di poter accedere in via elettronica in maniera effettiva e tempestiva a tutti i dati conservati, indipendentemente dal territorio dello Stato membro dell'Ue dove i medesimi sono conservati. Viene, inoltre, previsto che tutte le componenti tecnologiche che vengono usate nei sistemi di conservazione, siano esse componenti hardware o software, debbono essere segregate logicamente. Infine, i sistemi di conservazione devono essere realizzati nel rispetto dei principi di integrità e riservatezza dei dati nonché dei principi di privacy by design e privacy by default stabiliti dal GDPR.

[167] «Home | eIDAS - Il progetto FICEP : Il nodo eIDAS italiano», https://www.eid.gov.it/?lang=it.

[168] AgID, in raggruppamento con Infocert S.p.a., Politecnico di Torino, Telecom Italia S.p.a., si è aggiudicata con il bando CEF-Telecom eID 2014 un cofinanziamento per la realizzazione del nodo eIDAS italiano.

Amministrazioni italiane che prevedono il Login eIDAS[169]. Al tempo stesso i cittadini italiani potranno accedere ai servizi online di altri paesi comunitari (ad esempio servizi universitari, bancari, servizi delle pubbliche amministrazioni, altri servizi online) utilizzando le credenziali ottenute nel sistema pubblico di identità digitale SPID. AgID, in base alle norme vigenti, agisce come operatore del nodo eIDAS italiano e si avvale dei partner del Progetto FICEP per le attività di aggiornamento e test delle diverse componenti che costituiscono il nodo eIDAS italiano[170]. L'identità SPID è stata inoltre tra le prime ad essere notificate alla Commissione UE per l'uso transfrontaliero ed è valida per l'accesso ai servizi delle Pubbliche Amministrazioni online in tutti gli Stati membri in forza delle disposizioni del Regolamento UE 2014/910 (cosiddetto eIDAS). Lo SPID ha la particolare caratteristica per cui ogni cittadino può possedere più identità SPID a sé intestate, cosa che lo rende esclusivo in Europa in quanto normalmente le identità digitali sono uniche per ogni intestatario. L'identità SPID non è però la sola identità digitale italiana, infatti il Codice dell'Amministrazione Digitale riconosce altri due sistemi, quali la risalente CNS (Carta Nazionale dei Servizi), che ha valenza solo nazionale, e la CIE (Carta di Identità Elettronica), che è stata notificata, come SPID, alla Commissione UE per poter essere riconosciuta a livello transfrontaliero nell'Unione. La differenza fondamentale tra lo SPID e la CIE è che, pur essendo entrambe identità transfrontaliere, la CIE è prevista solo ed esclusivamente per l'accesso, in Italia e all'estero, ai servizi della Pubblica Amministrazione e gestori di servizi pubblici, mentre non è previsto né consentito un uso verso privati, a differenza di quanto avviene per SPID. Infatti, il CAD prevede che la CIE possa essere utilizzata verso privati solo come strumento per l'effettuazione di pagamenti ma non per l'accesso online ai servizi dei medesimi, come invece avviene per SPID[171]. L'obiettivo che si è prefissata l'Europa nel 2014, ossia quello di dare accesso a tutti i cittadini a servizi fiduciari

[169] Paolo Smiraglia et al., «The FICEP Infrastructure», in E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services, a c. di Sokratis K. Katsikas e Vasilios Zorkadis, Communications in Computer and Information Science (Cham: Springer International Publishing, 2017), p. 196–210, https://doi.org/10.1007/978-3-319-71117-1_14.

[170] «Presentazione del Progetto | eIDAS - Il progetto FICEP : Il nodo eIDAS italiano», https://www.eid.gov.it/presentazione-progetto.

[171] https://www.agendadigitale.eu/giornalista/eugenio-prosperetti, «Un'unica identità digitale per tutti: risolvere il dualismo Spid-Cie», Agenda Digitale, 11 settembre 2019, https://www.agendadigitale.eu/cittadinanza-digitale/ununica-identita-digitale-per-tutti-risolvere-il-dualismo-spid-cie/.

digitali altamente sicuri ma anche a identità digitali da poter spendere in tutta Europa, è stato raggiunto ma in modo molto disomogeneo. Nonostante l'Italia sia tra i paesi "virtuosi", in cui l'identità digitale è più diffusa tra la popolazione, nel resto d'Europa sono solo 14 gli Stati Membri che hanno notificato almeno un sistema di identità digitale alla Commissione, e solo il 59% dei cittadini europei è oggi in possesso di una digital ID[172]. Inoltre, restando sempre in ambito europeo, ad oggi vi è poca interoperabilità sia nei livelli di sicurezza e nella *user experience* [173] delle identità digitali di ogni paese membro, sia nelle modalità di accreditamento ed erogazione dei *Qualified Trust Service Provider*[174], tra cui gli erogatori di firme elettroniche qualificate. Per questo, a giugno 2021, la Commissione ha annunciato la revisione del regolamento eIDAS, la cui novità più discussa e attesa si trova nell'implementazione dell'*European Digital Identity Wallet*[175]. Su larga scala l'obiettivo della revisione eIDAS è

[172] Nel contesto del processo di riesame di cui all'articolo 49 del regolamento eIDAS è stata condotta una valutazione del funzionamento del medesimo regolamento. Secondo i risultati principali della valutazione in relazione all'identità elettronica il regolamento eIDAS non ha realizzato il suo potenziale. È stato notificato soltanto un numero limitato di identità elettroniche, il che limita la copertura dei regimi di identificazione elettronica notificati a circa il 59 % della popolazione dell'UE. Inoltre l'accettazione dei regimi di identificazione elettronica notificati tanto a livello di Stati membri quanto di prestatori di servizi è limitata. Sembra altresì che soltanto alcuni dei servizi accessibili tramite l'identità elettronica nazionale siano collegati all'infrastruttura nazionale eIDAS. Lo studio di valutazione ha inoltre rilevato che attualmente la portata e l'attenzione del regolamento eIDAS, che si concentrano sui regimi di identificazione elettronica notificati dagli Stati membri dell'UE e sull'accesso ai servizi pubblici online, sembrano essere troppo limitate e inadeguate. La maggior parte delle esigenze in materia di identità elettronica e autenticazione a distanza si riscontra nel settore privato, in particolare in settori quali quello bancario, delle telecomunicazioni e degli operatori di piattaforme che sono tenuti per legge a verificare l'identità dei loro clienti. Il valore aggiunto del regolamento eIDAS per quanto concerne l'identità elettronica è limitato a causa dei bassi livelli di copertura, adozione e utilizzo di tale regolamento. I problemi individuati nella presente proposta sono legati alle carenze dell'attuale quadro eIDAS e ai fondamentali mutamenti del contesto riguardanti i mercati e gli sviluppi.

[173] La User experience può essere definita come l'insieme di elementi che riguardano l'interazione di un individuo con un'azienda e i relativi prodotti/servizi o sistemi e, quindi, anche percezioni, atteggiamenti ed emozioni provate prima, durante e dopo l'utilizzo di questi. La user experience (UX) comprende tutte le «percezioni e reazioni che derivano dall'uso o dall'aspettativa di utilizzo di un prodotto, sistema o servizio», secondo la definizione proposta dall'International Organization for Standardization (ISO) secondo cui l'espressione comprende anche «le credenze, le preferenze, le risposte fisiche e psicologiche, i comportamenti e risultati» che derivano dall'utilizzo. *«User experience: cos'è caratteristiche e ottimizzazione», Inside Marketing (blog), https://www.insidemarketing.it/glossario/definizione/user-experience/.*

[174] Un fornitore di servizi fiduciari qualificati (QTSP) è un TSP che fornisce uno o più servizi fiduciari qualificati (QTS) e ottiene lo status qualificato dall'organismo di vigilanza nazionale. La decisione dell'organismo di vigilanza di concedere lo status qualificato si riflette nella corrispondente lista nazionale di fiducia. *«EU Trusted Lists | Shaping Europe's Digital Future», 30 giugno 2023, https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists.*

[175] L'attuale quadro eIDAS non si applica alla fornitura di attributi elettronici, quali i certificati medici o le qualifiche professionali, il che difficile assicurare il riconoscimento giuridico paneuropeo di tali credenziali in forma elettronica; il regolamento eIDAS non consente inoltre agli utenti di limitare la condivisione dei dati di identità a ciò che è strettamente necessario per la prestazione di un servizio. Sebbene dalla valutazione del regolamento eIDAS emerga che il quadro per

molto ampio in quanto, oltre a unificare il panorama delle identità digitali in termini di diffusione, il nuovo regolamento ha anche quello di riportare la sovranità dei dati personali nelle mani dei cittadini – in linea con il GDPR e in contrasto con la gestione delle informazioni da parte delle *big tech* – ma anche garantire parità di condizione nell'utilizzo dei servizi fiduciari all'interno dell'UE: l'Italia infatti è il paese più avanzato per presenza di Qualified Trust Service Provider, ma in altri paesi il numero è molto limitato. Quindi, lo scopo ultimo della revisione di eIDAS è quello di aumentare l'interoperabilità e integrabilità dei servizi fiduciari all'interno dell'UE, facendo un ulteriore passo avanti nell'unificazione dei paesi e porre le basi per creare l'european digital market. Per raggiungere questo obiettivo la revisione eIDAS non comprende solo interventi in ambito di identità digitale, ma aggiunge alcuni servizi fiduciari a quelli già regolamentati nella prima versione (firma elettronica, sigillo elettronico, website authentication certificate)[176]. Il nuovo regolamento, inoltre, obbligherà tutti i paesi europei a mettere a disposizione delle banche dati nazionali informazioni significative sui cittadini, in Italia attualmente carenti o poco attendibili. Ciò che più fa discutere sui tavoli di lavoro della revisione eIDAS, però, è la questione legata ai livelli di sicurezza (il Level of

---

la fornitura di servizi fiduciari ha avuto un discreto successo, fornendo un livello elevato di fiducia e assicurando l'adozione e l'utilizzo della maggior parte dei servizi fiduciari, occorre fare di più per conseguire la piena armonizzazione e accettazione. Per quanto riguarda i certificati qualificati di autenticazione di siti web, i cittadini devono poter fare affidamento su di essi e beneficiare di informazioni sicure e affidabili relative a chi c'è dietro un sito web, riducendo così le frodi. Inoltre, per rispondere alle dinamiche dei mercati e agli sviluppi tecnologici, la nuova proposta espande l'attuale elenco eIDAS di servizi fiduciari aggiungendo tre nuovi servizi fiduciari qualificati, ossia la prestazione di servizi di archiviazione elettronica, i registri elettronici e la gestione di dispositivi per la creazione di firme e sigilli elettronici a distanza. La recente proposta offre altresì un approccio armonizzato alla sicurezza per i cittadini che fanno affidamento su un'identità digitale europea che li rappresenti online e per i prestatori di servizi online che potranno fare pieno affidamento su soluzioni di identità digitale e accettarle indipendentemente dal luogo in cui sono state emesse, ed implica un cambiamento per i soggetti che emettono soluzioni di identità digitale europea in quanto prevede un'architettura tecnica e un quadro di riferimento comuni, nonché norme comuni da sviluppare in collaborazione con gli Stati membri. È necessario un approccio armonizzato per evitare che lo sviluppo di soluzioni di identità digitale nuove negli Stati membri crei un'ulteriore frammentazione causata dall'utilizzo di soluzioni nazionali divergenti. Un approccio armonizzato rafforzerà inoltre il mercato unico in quanto consentirebbe ai cittadini, agli altri residenti e alle imprese di identificarsi online in maniera sicura, pratica e uniforme in tutta l'UE per accedere a servizi pubblici e privati. Gli utenti potrebbero fare affidamento su un ecosistema migliorato per l'identità elettronica e i servizi fiduciari, riconosciuto e accettato ovunque nell'Unione.

[176] I servizi di cui si fa cenno riguardano anzitutto l'electronic archiving, che in Italia è già previsto dal CAD ma si potrà così espandere in tutta Europa, aprendo nuovi mercati per alcuni paesi; ancora, si fa riferimento alla gestione degli apparati di firma e degli HSM, che diventerà un servizio fiduciario a sé stante e alla possibilità di registrazione e storing dei dati su electronic ledger (blockchain), apparsa nella prima versione. Inoltre, i "verificatori" di certificati, firme elettroniche, sigilli e attestazioni diventeranno veri e propri servizi qualificati.

Assurance, LoA) delle identità digitali attualmente in uso nei paesi europei (comprese SPID e CIE) per l'accesso dei cittadini al digital wallet europeo. SPID, infatti, può essere utilizzato con tutti e tre i livelli di sicurezza previsti (Low, Substantial e High), ma la maggior parte degli SPID attualmente in uso in Italia si limita al livello 2 di substantial. Alcuni paesi europei diversi dall'Italia, tuttavia, richiedono che l'accesso al wallet sia limitato alle identità digitali con livello high, già raggiunto invece da CIE. Un recente decreto, inoltre, apporterà delle modifiche alla UX di CIE, rendendola molto più simile a SPID. Insomma, il timore è che con la revisione eIDAS gran parte delle utenze SPID diffuse oggi in Italia non sarebbero accettate per accedere al digital wallet, decisione che potrebbe limitare molto il futuro di SPID e quindi dissipare parte degli investimenti – anche privati – di questi anni. L'EuDI wallet, comunque, si configura già come una grande innovazione nell'ambito delle identità digitali, non solo per i numerosi ambiti e *use case* a cui si potrà applicare, ma anche per l'altissima attenzione alla privacy dei cittadini: il wallet infatti consentirà agli utenti di condividere solo e unicamente le informazioni necessarie per accedere al servizio[177]. La riforma individua nel portafoglio digitale un sistema di identità dotato di portabilità che consenta a tutti i cittadini europei che se ne doteranno di firmare documenti digitali attraverso firme elettroniche qualificate, cioè dotate di attributi certificati e protetti, oltre che di richiedere, ottenere, memorizzare, selezionare, condividere, in modo sicuro, trasparente e tracciabile per l'utente, i propri dati personali di identificazione, nonché l'attestazione elettronica degli attributi per l'autenticazione richiesti da servizi pubblici e privati online. Tutto ciò dovrebbe essere reso possibile dal collegamento fra l'E-Wallet e un nucleo centrale dell'identità personale (PID), cioè l'insieme di dati correlati all'identità di una persona fisica o giuridica, mentre l'attestazione elettronica degli attributi personali (EEA), cioè gli specifici elementi che una persona fisica o giuridica esibisce in un procedimento, dovrebbe essere realizzata da Prestatori di servizi fiduciari (Trust Service Provider), di natura pubblica o privata. A tale proposito, sono inoltre previsti due tipi di attestazione elettronica degli attributi: una che si potrebbe dire semplice ed un'altra che è definita qualificata, anche se non sono

[177] «eIDAS 2.0: facciamo il punto | Intesa, a Kyndryl Company», 2 novembre 2022, https://www.intesa.it/eidas-2-0-facciamo-il-punto/.

ancora ben chiare condizioni e modalità cui dovranno corrispondere i soggetti prestatori di servizi autorizzati a conferire entrambi i tipi di attestazione. Conclusivamente, in una transizione digitale a cui negli ultimi anni, grazie alla pandemia e al PNRR, è stata impressa un'improvvisa quanto provvidenziale accelerazione, l'introduzione del "portafoglio digitale" rappresenta la naturale evoluzione del domicilio digitale già esistente e ulteriormente rafforzato con i decreti semplificazioni 2020 e 2021, come modalità privilegiata delle comunicazioni fra cittadino e Pubblica Amministrazione e come supporto a una maggiore diffusione dei principali strumenti utilizzati per l'attestazione dell'identità personale quali SPID, CIE o l'AppIO[178].

[178] Nicola Testa, https://www.agendadigitale.eu/?post_type=giornalista&p=181703, «eIDAS 2.0: la nuova frontiera dei sistemi di identificazione digitale», Agenda Digitale, 26 giugno 2023, https://www.agendadigitale.eu/cittadinanza-digitale/eidas-2-0-la-nuova-frontiera-dei-sistemi-di-identificazione-digitale/.

6. L'attuale quadro normativo: la Strategia Nazionale di Cybersicurezza e il Perimetro Nazionale di Sicurezza Cibernetica

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[179]. Nel 2021 è stata approvata la Strategia nazionale di cybersicurezza 2022-2026, di durata quinquennale, con annesso Piano di Implementazione, da parte del Comitato Interministeriale 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[180]. Innanzitutto, secondo quanto deciso dalla Strategia, alla lotta contro gli attacchi cibernetici verrà destinato l'1,2% degli investimenti nazionali lordi per il finanziamento di progetti specifici che garantiscano l'autonomia tecnologica in ambito digitale e l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali. Inoltre, la Strategia nazionale messa a punto dal Governo prevede un supporto importante alle aziende private anch'esse prese di mira dal cyber crimine: per loro, saranno previsti sgravi fiscali e aree nazionali a tassazione agevolata[181]. I principali obiettivi che la Strategia 2022-2026 vuole raggiungere consistono nel potenziamento della resilienza nella transizione digitale del Paese, nel raggiungimento dell'autonomia strategica sul piano cibernetico, nell'anticipazione

[179] 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/.

[180] Nella stessa riunione, in merito al Perimetro di sicurezza nazionale cibernetica, è stato approvato lo schema di DPCM ex art. 1 c.7, lett. B) D.L. 105/2019, che indica i criteri che i laboratori devono rispettare per accreditarsi come laboratori di prova per il Centro di valutazione e certificazione nazionale (CVCN) per verificare sicurezza, assenza di vulnerabilità note, contenuti, comunicazione tra il CVCN e i laboratori stessi e tra il CVCN e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa. Si è giunti, così, al completamento dell'attuazione normativa del Perimetro di sicurezza nazionale cibernetica.

[181] Gli investimenti appena menzionati andranno ad aggiungersi ai 623 milioni di euro già previsti dal PNRR e assegnati all'Agenzia cyber in quanto soggetto attuatore del Piano Nazionale di Ripresa e Resilienza.

dell'evoluzione della minaccia cyber, nella gestione delle crisi cibernetiche ed infine nella lotta alla diffusione delle fake news.

Per quanto riguarda i progetti dell'Agenzia per la Cybersicurezza Nazionale, il direttore generale Roberto Baldoni ritiene che servano tecnologie e competenze per gestire il clima di cyberwar derivato dal conflitto russo-ucraino. Sicuramente il rischio cyber non si placherà con la sua fine, anzi bisognerà mantenere l'attenzione alta, dato che la guerra sul campo cyber è iniziata già prima dell'invasione e già era stato registrato un aumento di attacchi cibernetici. I campi maggiormente a rischio sono gli operatori energetici, quelli finanziari e quelli delle telecomunicazioni, inoltre, anche dopo il conflitto, bisognerà tutelare le infrastrutture critiche, tra cui quelle sanitarie in primis. A tal proposito, sono stati avviati due progetti – Intelligenza Artificiale e Incident Response – con l'obiettivo di rafforzare l'azione di analisi, prevenzione e risposta agli attacchi cyber del Paese, che vedranno l'impiego di 300 nuove risorse nel 2023 e 800 nel 2028. È importante rafforzare la difesa del nostro Paese attraverso l'intelligenza artificiale applicata alle nuove tecnologie di analisi e agli strumenti di prevenzione; così, i due progetti menzionati saranno mirati al raggiungimento di questo obiettivo: il primo, sviluppato in collaborazione con l'Unione europea, prevede l'uso di tecnologie dell'Intelligenza Artificiale che permettano di prevedere eventuali attacchi informatici, il secondo, invece, di elaborare una qualifica dell'Incident Response (IR), promuovendo un'analisi degli incidenti capace di individuare le criticità ed evitare che si riproducano in futuro[182].

Con i provvedimenti al vaglio del Comitato Interministeriale per la Cybersecurity presieduto dal Presidente del Consiglio, l'Agenzia per la Cybersecurity Nazionale decolla definitivamente in tutta la sua operatività, fatto salvo l'organico ancora incompleto e in via di reclutamento. Proprio l'anno precedente (il 2020) ha fatto registrare ottimi progressi nel rafforzamento dell'architettura nazionale di sicurezza cibernetica, in primo luogo, in relazione alla

[182] https://www.cybersecurity360.it/giornalista/marco-santarelli, «Ecco la Strategia nazionale di cybersicurezza italiana: competenze e tecnologie per la difesa del Paese», Cyber Security 360 (blog), 18 maggio 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-la-strategia-nazionale-di-cybersicurezza-italiana-competenze-e-tecnologie-per-la-difesa-del-paese/.

promulgazione dei decreti attuativi del Perimetro di sicurezza nazionale cibernetica. È opportuno riportare che il Perimetro è un provvedimento che prevede sia obblighi legali volti al rispetto di stringenti misure di sicurezza e alla notifica degli incidenti, sia specifiche disposizioni in materia di forniture di determinati beni, sistemi e servizi ICT destinati a essere impiegati su reti, sistemi informativi e per l'espletamento dei servizi informatici utilizzati dai soggetti inclusi nel Perimetro stesso per l'esercizio della funzione/servizio essenziale per la sicurezza nazionale. Il provvedimento in questione prevede che siano promulgati una serie di decreti attuativi, quattro DPCM e un DPR. Il primo, il DPCM n. 131 del 30 luglio 2020, ha dettagliato le specifiche e gli ambiti di attività dei soggetti inclusi nel Perimetro di sicurezza cibernetica nonché le modalità di elaborazione, aggiornamento e trasmissione degli elenchi dei beni ICT. La determinazione di tali elementi si configura come passaggio fondamentale per la concreta realizzazione del Perimetro al fine di instaurare una serie di presidi di sicurezza funzionali a garantire un'efficace protezione cibernetica. Il secondo decreto, il DPR n. 54 del 5 febbraio 2021, affronta le procedure e i termini per le valutazioni svolte da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di Valutazione del Ministero degli Affari Interni e della Difesa su prodotti in fase di acquisizione da parte dei soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica. Il terzo decreto, il DPCM n. 81 del 14 aprile 2021, disciplina nel dettaglio le procedure di notifica che devono seguire i soggetti inclusi nel Perimetro in caso di incidenti impattanti su beni ICT, definendone una tassonomia per livelli di gravità, unitamente ad un elenco delle misure di sicurezza, basate su quanto previsto dal Framework Nazionale per la Cybersecurity e la Data Protection, che i soggetti stessi dovranno implementare per ciascun bene ICT di propria pertinenza. Il quarto decreto, il DPCM n. 15 giugno 2021, individua le categorie in relazione alle quali i soggetti inclusi nel Perimetro che intendano procedere, anche per il tramite delle centrali di committenza alle quali sono tenuti a fare ricorso, all'affidamento di forniture di beni, sistemi e servizi ICT, destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, effettuano la comunicazione al CVCN o ai Centri di Valutazione. Le categorie individuate dal decreto in questione riguardano le componenti hardware e software che svolgono funzionalità

e servizi di rete di telecomunicazione o funzionalità per la sicurezza di reti di telecomunicazione e di dati da esse trattati per l'acquisizione dati, il monitoraggio e l'automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali, nonché, riguardano gli applicativi software per l'implementazione di meccanismi di sicurezza. In sintesi, è possibile affermare che il Perimetro di Sicurezza Nazionale Cibernetica, unitamente all'attuazione della Direttiva NIS e delle Misure minime di sicurezza ICT per le PA di AgID, è finalizzato a garantire nel tempo un approccio integrato e univoco dello Stato contro le minacce cibernetiche e consentirà di migliorare la capacità di resilienza di tutto il sistema paese[183]. L'ultimo tassello mancante alla realizzazione del Perimetro di sicurezza nazionale cibernetica è stato colmato con il DPCM che attua l'art. 1 comma 7 lettera B del D.L. 105/2019; il decreto contiene i criteri per l'accreditamento dei Laboratori Accreditati di Prova (LAP) dei quali si potrà avvalere il CVCN, Centro di Valutazione e Certificazione Nazionale, per le valutazioni e le certificazioni di cybersecurity di prodotti dell'Information and Communication Technology, i metodi di comunicazione tra CVCN e LAP e tra CVCN e CV (Centri di Valutazione) di Interno e Difesa. L'Italia, con la creazione del CVCN e col DPCM che norma l'operatività del Centro e l'incorporazione dell'OCSI (Organismo di Certificazione della Sicurezza Informatica) già operante nel MISE, entra a pieno titolo nel novero dei Paesi innovativi in tema di certificazioni e standard, con la possibilità di esprimersi in modo autorevole e universalmente riconosciuto nei consessi sovranazionali durante le discussioni per trovare il modo di standardizzare e organizzare la disciplina della cybersecurity[184].

Relativamente all'istituzione dell'Agenzia per la Cybersicurezza Nazionale (decreto legge 14 giugno 2021, n. 82), seppur creata in ritardo rispetto agli altri Stati europei, si tratta senz'altro di un'iniziativa da accogliere con favore. La nuova Agenzia, come accennato diretta da Roberto

[183] https://www.agendadigitale.eu/giornalista/luisa-franchina e https://www.agendadigitale.eu/giornalista/matteo-taraborelli, «Cyber security, come va la strategia italiana: cosa abbiamo fatto e cosa resta da fare», Agenda Digitale, 2 settembre 2021, https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/.

[184] https://www.agendadigitale.eu/giornalista/luisa-franchina, «Strategia cybersecurity nazionale, siamo alla svolta: ecco i punti chiave per il futuro», Agenda Digitale, 20 maggio 2022, https://www.agendadigitale.eu/sicurezza/strategia-cybersecurity-nazionale-litalia-se-desta-ecco-i-punti-chiave/.

Baldoni, ha sede a Roma, personalità giuridica ed è l'Autorità nazionale per la cybersicurezza per la coordinazione tra i soggetti pubblici coinvolti in materia di cybersecurity a livello nazionale e promuoverà la realizzazione di azioni comuni orientate alla sicurezza e alla resilienza cyber per la digitalizzazione di tutto il sistema Paese. In linea con i modelli francese e tedesco, la nuova Agenzia si porrà al di fuori delle agenzie di intelligence, sottraendo così strutture quali il Computer Security Incident Response Team (CSIRT) italiano o il Nucleo di Sicurezza Cibernetica dal controllo esclusivo del DIS[185]. Nonostante ciò, la nomina di Baldoni, già vicedirettore del DIS con delega alla cybersecurity, è emblematica della continuità necessaria per garantire la sicurezza di un settore di rilevanza strategica. Tale continuità permetterà anche di coordinare al meglio gli sforzi delle autorità competenti NIS nazionali nel porre in sicurezza e contrastare gli attacchi alle Infrastrutture Critiche, anche tenendo conto delle future necessità dovute alle modifiche alla disciplina che verranno introdotte con la revisione della direttiva stessa, la c.d. NIS2[186].

---

[185] L'Agenzia è l'Autorità nazionale competente in materia di sicurezza cibernetica per le finalità di cui al decreto legislativo NIS, ed è l'ente competente per le funzioni ispettive e per le irrogazioni delle sanzioni previste nel decreto attuativo della direttiva europea. L'agenzia diventa altresì l'Ente deputato al rilascio delle certificazioni come previsto dal Regolamento Europeo 2019/881 che prevede l'obbligo per gli Stati membri di nominare l'autorità nazionale di certificazione a cui sono attribuiti una serie di poteri minimi, tra cui quelli istruttori, ispettivi e sanzionatori. Il Decreto, poi, individua l'Agenzia come l'Ente di riferimento in materia di sicurezza cibernetica al quale passano le numerose competenze prima attribuite ad altri organi e in particolare quelle che erano state attribuite al Ministero dello Sviluppo Economico in materia di sicurezza cibernetica, al DIS (Dipartimento delle informazioni per la sicurezza), alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica e all'Agenzia dell'Italia digitale. Tra i compiti affidati alla nuova agenzia rientrano lo sviluppo di politiche di prevenzione, analisi e monitoraggio dei pericoli, la redazione del piano annuale di sicurezza cibernetica nazionale, la promozione di un quadro giuridico e normativo di riferimento, la partecipazione a esercitazioni nazionali e internazionali per testare l'adeguatezza delle misure di sicurezza, lo svolgimento di funzioni consultive, il coordinamento della cooperazione internazionale in funzione di sicurezza cibernetica, la collaborazione con il mondo accademico e della ricerca.

[186] Tra i compiti in materia di cybersecurity nazionale attribuiti alla nuova Agenzia rientrano tutti quelli precedentemente assegnati alla presidenza del Consiglio, al Ministero dello Sviluppo Economico, al DIS e all'Agenzia per l'Italia Digitale così come le competenze in materia di Perimetro di Sicurezza Nazionale Cibernetica. Tra essi rientreranno quindi l'elaborazione della Strategia nazionale di cybersicurezza e il supporto alle attività del Nucleo per la cybersicurezza, rappresentando inoltre l'Autorità nazionale competente e il punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi. Essendo anche Autorità nazionale di certificazione della cybersecurity, l'Agenzia accentrerà tutte le attività di certificazione finora esercitate dal Ministero dello Sviluppo Economico da parte dei competenti organi, quali il CVCN. In aggiunta, l'Agenzia si occuperà della prevenzione, del monitoraggio, del rilevamento, dell'analisi, delle risposte e della gestione di incidenti di sicurezza informatica e gli attacchi cyber. Infine, ma non meno importante, la nuova struttura sarà promotrice del coinvolgimento del sistema universitario e della ricerca, nonché del sistema produttivo nazionale, nel campo della cybersecurity e pertanto avrà il compito di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della sicurezza informatica, anche attraverso l'assegnazione di borse di studio, di dottorato e di assegni di ricerca, favorendo l'attivazione di percorsi.

I quattro pilastri tecnico-operativi su cui si basa l'intera Strategia cyber riguardano la resilienza, la prevenzione ed il contrasto della criminalità informatica, la sicurezza militare del Paese ed infine la ricerca informativa. Tale struttura logica ha finalmente, a differenza di quanto avveniva in passato, consentito di individuare esattamente i ruoli dei soggetti che si occupano della sicurezza del Paese[187]. Durante la conferenza stampa di presentazione della Strategia nazionale di cybersicurezza il direttore dell'Agenzia cyber Baldoni ha esposto le 82 misure di sicurezza incluse nel Piano di implementazione e che verranno applicate al sistema Paese dall'Agenzia stessa in applicazione del documento programmatico. Innanzitutto, la Misura #1 che prevede di rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain e l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati. Contestualmente, nella Misura #2 la strategia cyber si propone di sviluppare le capacità dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza. Sempre in tema di certificazioni di cybersicurezza, da segnalare è la Misura #5 mirata a supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato. Per questo, la Misura #12 prevede di continuare ad accrescere le capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence, rafforzando ulteriormente la *situational awareness* mediante il monitoraggio continuo e l'analisi di minacce, vulnerabilità e attacchi, secondo gli specifici ambiti di competenza. Contestualmente, la Misura #13 prevede di realizzare un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale, al fine di comunicare l'effettivo livello della minaccia, nonché di informare adeguatamente i processi decisionali. Ed è proprio per attuare

[187] «Strategia Nazionale Di Cybersicurezza 2022 – 2026 - Agenzia per la cybersicurezza nazionale», ACN - Agenzia per la cybersicurezza nazionale, https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza/.

un sistema di supporto alle Pubbliche Amministrazioni e a tutto il sistema produttivo italiano che interviene la Misura #33, che si propone di accrescere le capacità di risposta e ripristino a seguito di crisi cibernetiche implementando una rete di CERT settoriali integrata con lo CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati, con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici. Da segnalare, infine, le misure ricomprese nella sezione "Impulso all'innovazione tecnologica e alla digitalizzazione" della strategia cyber che sottolineano l'importanza dei settori Ricerca e Sviluppo di nuove tecnologie. In particolare, la Misura #53 è mirata a promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali. Invece, la Misura #54 è volta a favorire la ricerca e lo sviluppo, specialmente nelle nuove tecnologie, promuovendo l'inclusione dei principi di cybersicurezza e supportando, anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione, progetti di sicurezza cibernetica da parte del settore privato – con particolare riferimento alle startup e alle PMI innovative – e dei Centri di competenza e di ricerca attivi sul territorio nazionale[188].

Occorre adesso soffermarsi più dettagliatamente sulla disciplina del Perimetro di sicurezza nazionale cibernetica, il quale vide una prima luce attraverso la pubblicazione del Decreto del Presidente del Consiglio dei ministri (DPCM) 30 luglio 2020, n. 131, in Gazzetta Ufficiale avvenuta il 21 ottobre dello stesso anno. Il decreto definisce i criteri di individuazione dei soggetti inclusi nel perimetro e gli obblighi imposti agli stessi per salvaguardare la sicurezza nazionale. Se il decreto dà una prima attuazione alla realizzazione del Perimetro cyber, la sua definizione, invece, è stata data dal Decreto Legge 21 settembre 2019, n. 105 che contiene

[188] https://www.cybersecurity360.it/giornalista/paolo-tarsitano, «Strategia nazionale di cybersicurezza, ecco gli obiettivi da raggiungere entro il 2026 per la resilienza del Paese», Cyber Security 360 (blog), 25 maggio 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/strategia-nazionale-di-cybersicurezza-ecco-gli-obiettivi-da-raggiungere-entro-il-2026-per-la-resilienza-del-paese/.

disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. L'art. 1 del D.L., infatti, prevede che "al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica". 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. 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. Invece, un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato laddove ponga in essere 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[189]. 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. 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

[189] Le altre attività oggetto di servizi essenziali sono le attività necessarie per l'esercizio e il godimento dei diritti fondamentali, quelle di ricerca e quelle relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

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.

L'articolo 5 del DPCM prevede che le amministrazioni predispongano una lista dei soggetti che svolgono funzioni e servizi essenziali e che la trasmettano al CISR tecnico (Comitato interministeriale per la sicurezza della Repubblica). La lista è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio e periodicamente aggiornato. Un elemento di novità è introdotto dall'articolo seguente, il quale istituisce il Tavolo interministeriale, presieduto da un vice-direttore generale del DIS e chiamato a supportare il CISR tecnico nell'individuazione dei soggetti da includere nella lista e in ogni altra attività attribuita al CISR o al CISR tecnico dal decreto. Il Tavolo è costituito da due rappresentanti di ciascuna amministrazione CISR, da un rappresentante per ciascuna delle due Agenzie, nonché da due rappresentanti degli altri Ministeri di volta in volta interessati, di cui almeno uno in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica.

Come previsto dal Decreto Legge del settembre 2019, il DPCM n. 131/2020 impone ai soggetti rientranti nel Perimetro una serie di obblighi per garantire un elevato livello di sicurezza. In primis, i soggetti devono predisporre e aggiornare annualmente la lista dei beni ICT di rispettiva pertinenza. Essi devono poi individuare i beni ICT necessari a svolgere la funzione o il servizio essenziale, al fine di valutare l'impatto di un incidente sul bene ICT, in termini di operatività

dello stesso e di compromissione della disponibilità, dell'integrità o riservatezza dei dati (CIA triad), e di valutare le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti. Infine, i soggetti devono individuare i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale. Gli elenchi redatti vengono trasmessi alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico, i quali li inoltrano al Dipartimento delle informazioni per la sicurezza (DIS), al fine di permettere le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica (NSC), dipendente dal DIS. La trasmissione degli elenchi di beni ICT avviene per il tramite di una piattaforma digitale costituita proprio presso il DIS[190]. Il DPCM in questione rappresenta sicuramente un tassello importante nella costruzione del Perimetro di sicurezza nazionale cibernetica e, quindi, un grande passo in avanti per la "messa in sicurezza" dell'infrastruttura ICT. Tuttavia, saranno i prossimi decreti, in particolare il secondo, a dare maggior slancio soprattutto sul piano operativo. Il decreto è la dimostrazione di un crescente interesse del governo italiano per la sicurezza informatica e di una maggiore consapevolezza dei rischi, dall'interruzione della supply chain (da qui la necessità di proteggere le infrastrutture) alla fuga di dati, incrementati a causa della pandemia di Covid-19[191].

Subito dopo la pubblicazione in Gazzetta Ufficiale del secondo DPCM attuativo del Perimetro cibernetico, il Presidente del Consiglio Draghi ha approvato il suo ampliamento aggiornando l'elenco dei soggetti inclusi che dovranno garantire la sicurezza di 223 funzioni essenziali dello Stato[192]. Allo stato attuale, sono stati pubblicati due decreti attuativi riguardanti, da un lato, l'individuazione dei settori interessati dal Perimetro e i criteri per la predisposizione

[190] «Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 - Normattiva», https://www.normattiva.it/eli/stato/DECRETO_DEL_PRESIDENTE_DEL_CONSIGLIO_DEI_MINISTRI/2020/07/30/131/ORIGINAL.

[191] https://www.cybersecurity360.it/giornalista/davide-lo-prete, «Perimetro di sicurezza nazionale cibernetica: regole e criteri di attuazione», Cyber Security 360 (blog), 30 ottobre 2020, https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-di-sicurezza-nazionale-cibernetica-regole-e-criteri-di-attuazione/.

[192] Gabriele Carrer, «Perimetro cyber, c'è la lista. Oltre 100 soggetti protetti», Formiche.net, 3 dicembre 2020, https://formiche.net/2020/12/secondo-dpcm-perimetro-cyber/.

dell'aggiornamento degli elenchi di reti, sistemi informativi e servizi informatici; dall'altro, i processi di notifica degli incidenti che i soggetti inclusi nello stesso sono tenuti a integrare all'interno delle proprie attività e le misure di sicurezza a tutela dei beni ICT. A seguito del citato ampliamento del campo di applicazione, il tema dei settori di interesse del Perimetro torna a rivestire un ruolo centrale nel processo di implementazione dello stesso. Di seguito verranno sintetizzati i principali elementi sul tema alla luce dei recenti sviluppi. I settori di attività inclusi nel Perimetro sono definiti attraverso un criterio di gradualità, in quanto l'ambito di applicazione del Perimetro è circoscritto a soggetti operanti nel settore governativo con riferimento alle attività delle amministrazioni CISR nonché a ulteriori soggetti, pubblici e privati, coinvolti nei seguenti settori (ove non ricompresi in quello governativo): interno; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche; enti previdenziali/lavoro[193]. Per l'identificazione e l'elencazione dei soggetti, pubblici e privati, inclusi nel Perimetro appartenenti ai suddetti settori è prevista l'individuazione di una specifica Amministrazione pubblica competente (es. Ministero dello sviluppo economico; struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione; Ministero dell'economia e delle finanze). Per il settore governativo, tali attività sono invece demandate alle amministrazioni CISR, ciascuna nell'ambito di rispettiva competenza[194].

Come anticipato, è operativo anche l'ultimo tassello del Perimetro di sicurezza nazionale cibernetica, il DPCM del 18 maggio 2022, che rappresenta un passo importante per completare lo scudo cibernetico a difesa delle infrastrutture critiche italiane. In particolare, il quarto DPCM stabilisce le procedure, i requisiti e i termini per l'accreditamento dei laboratori accreditati di prova (i cosiddetti LAP) a supporto del Centro di valutazione e certificazione nazionale

[193] L'elenco delle materie comprese è più ampio di quello racchiuso nella Direttiva NIS dell'Unione europea: interno, difesa, spazio e aerospazio, energia e telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche (quelle ricomprese nel Regolamento Ue 2019/452), enti previdenziali o del lavoro (articolo 3).

[194] https://www.cybersecurity360.it/giornalista/luisa-franchina, https://www.cybersecurity360.it/giornalista/andrea-lucariello, e https://www.cybersecurity360.it/giornalista/francesco-ressa, «Ampliamento del perimetro di sicurezza nazionale cibernetica: ecco i settori di attività», Cyber Security 360 (blog), 18 giugno 2021, https://www.cybersecurity360.it/cybersecurity-nazionale/ampliamento-del-perimetro-di-sicurezza-nazionale-cibernetica-ecco-i-settori-di-attivita/.

(CVCN): da adesso sarà dunque possibile individuare i laboratori che dovranno verificare la sicurezza tecnologica delle aziende e delle pubbliche amministrazioni ritenute essenziali per la sicurezza dello Stato. Di fatto, quindi, come si legge nella nota pubblicata dall'Agenzia per la cybersicurezza nazionale diretta da Roberto Baldoni, il nuovo regolamento rappresenta l'ultimo tassello "per raggiungere gli obiettivi contenuti nella Strategia nazionale di cybersicurezza, volto a innalzare il livello di sicurezza della supply chain di infrastrutture da cui dipende l'erogazione dei servizi essenziali dello Stato". Con questo nuovo regolamento, adottato con il DPCM n. 92 del 18 maggio 2022 e atteso da tempo, si completa dunque il quadro normativo del Perimetro di sicurezza nazionale cibernetica istituito tre anni prima dal governo Conte-bis con l'obiettivo di difendere gli asset strategici nazionali dagli attacchi cyber. Il regolamento definisce, quindi, al Capo I, i compiti del CVCN e le aree di accreditamento. Il Capo II è, invece, dedicato ai requisiti e alle procedure di accreditamento dei laboratori di prova; mentre il Capo III è dedicato all'accreditamento dei centri di valutazione (CV). Ancora, il Capo IV definisce i necessari raccordi del CVCN con i laboratori di prova e con i centri di valutazione. Infine, importante, le procedure di notifica degli incidenti definite dal Capo V del nuovo regolamento. In particolare, il Centro di valutazione e certificazione nazionale, già operativo dal primo luglio 2022, potrà ora accreditare laboratori esterni, sia pubblici sia privati, che costituiranno la rete a supporto dello stesso Centro e dei centri di valutazione (CV) del Ministero della Difesa e del Ministero dell'Interno per le attività di valutazione tecnologica su specifiche categorie di asset ICT impiegati all'interno del perimetro cyber. L'obiettivo è quello di creare, in stretta collaborazione con il mondo dell'industria e dell'accademia, una rete di laboratori accreditati altamente specializzati necessaria al potenziamento delle capacità dell'Italia di valutazione e certificazione e fondamentale per il raggiungimento di un'autonomia tecnologica del nostro Paese. La creazione di una rete strutturata di LAP, che verrà finanziata grazie ad alcuni specifici progetti già inseriti nel Piano nazionale di ripresa e resilienza (PNRR), permetterà dunque di realizzare alcune importanti misure di prevenzione e mitigazione del rischio volte a innalzare la resilienza delle infrastrutture digitali e previste dal piano di implementazione della strategia nazionale di cybersicurezza. Oltremodo, il DPCM in questione

sarà abilitante per la realizzazione di una serie di misure previste dalla Strategia 2022-2026. Innanzitutto, per l'attuazione della Misura #1 che intende rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro e per l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati. In secondo luogo, viene realizzata la Misura #2 il cui intento è quello di sviluppare le capacità dei centri di valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza. Ancora, è attuata la Misura #5 che supporta lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuove l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato. Da ultimo, sono state introdotte norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale e sono state promosse le iniziative utili volte al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali. Dunque, l'ultimo tassello del Perimetro di sicurezza nazionale cibernetica rappresenta un vero e proprio vademecum che consentirà finalmente di individuare i laboratori di prova necessari a verificare la sicurezza tecnologica delle aziende e delle P.A. strategiche per la sicurezza nazionale che fanno parte della lista segreta (stilata da ormai più di un anno) che comprende ministeri, aziende hi-tech e grandi partecipate pubbliche[195].

[195] https://www.cybersecurity360.it/giornalista/paolo-tarsitano, «Perimetro cybersecurity, complete le norme: ecco l'ultimo decreto», Cyber Security 360 (blog), 18 luglio 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-cybersecurity-complete-le-norme-ecco-lultimo-decreto/.

È possibile, quindi, fare il punto sull'attuale disciplina applicabile ai soggetti inclusi nel Perimetro e capire quali possibili modifiche si prospettano alla luce delle ultime novità introdotte dall'Unione europea in ambito cybersecurity. Il Perimetro è stato introdotto con il decreto legge n. 105 del 2019, convertito nella legge n. 133 dello stesso anno ("Decreto"), e mira a regolamentare dal punto di vista della sicurezza delle reti tutti quei soggetti che, per la natura del settore in cui operano, sono maggiormente esposti ad eventuali attacchi, oltre che idonei a creare un maggiore pregiudizio alla sicurezza nazionale. In particolare, il Decreto detta i parametri per individuare i soggetti cui si rivolgono le previsioni del Decreto: il soggetto deve esercitare una funzione essenziale dello Stato, ovvero assicurare un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, e l'esercizio di tale funzione o la prestazione di tale servizio deve dipendere da reti, sistemi informativi e servizi informatici; ancora, l'individuazione deve avvenire sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti. I soggetti così selezionati convogliano in una lista, limitata all'accesso pubblico, adottata con provvedimento del Ministero dello Sviluppo Economico. Non essendo possibile accedere liberamente alla lista di cui sopra, l'eventuale inserimento nella lista verrà comunicato senza indebito ritardo al singolo interessato – come disciplinato dal decreto legge stesso.

Sin dalla istituzione del Perimetro sono stati adottati numerosi atti normativi che hanno introdotto una serie di obblighi in capo ai soggetti inclusi del Perimetro. In particolare, è stato imposto l'obbligo di predisporre l'elenco di beni ICT (Information and Communication Technology) di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono. Ai soggetti rilevanti nel Perimetro è altresì imposto l'obbligo di comunicazione degli affidamenti o dell'acquisto di beni, sistemi e servizi ICT al Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso il Ministero dello sviluppo economico. La comunicazione deve essere effettuata prima dell'avvio delle procedure

di affidamento di forniture di determinate categorie di beni, sistemi e servizi ICT. Deve essere notificato al Computer Security Incident Response Team (CSIRT), entro un termine variabile di un'ora o sei ore, l'incidente avente ad oggetto beni ICT. In particolare, la notifica dovrà avvenire entro sei ore dalla scoperta nei casi di violazione o perdita di confidenzialità o integrità, accesso tramite malware, movimenti laterali o azioni di raccolta e esfiltrazione di dati. Tale finestra di tempo si riduce ad una sola ora dalla scoperta nei casi di inibizione delle funzioni di risposta, compromissione dei processi di controllo, disservizio o violazione dei servizi, sistemi o dati. Infine, è previsto l'obbligo di notifica al CSIRT entro 72 ore in caso di incidenti con oggetto beni diversi da quelli precedentemente elencati, come indicato nella Determina 3 gennaio 2023 dell'Agenzia per la Cybersicurezza Nazionale. Gli incidenti oggetto della notifica, come indicati nella Determina, consistono nell' accesso, esecuzione e installazione non autorizzati, movimenti laterali, esfiltrazione di informazioni e dati che vanno ad impattare su asset che si trovano al di fuori del Perimetro e per questo motivo ritenuti meno a rischio, ma che potrebbero avere un successivo effetto negativo sui beni ICT di asset appartenenti alla medesima supply chain.

La normativa di settore è in continua evoluzione e ci si attendono ulteriori interventi normativi, sia da parte dell'ACN – come previsto dalla Strategia Nazionale di Cybersicurezza (2022-2026) pubblicata a maggio 2022 – sia in termini di implementazione di direttive europee. A questo proposito, riveste particolare rilievo la Direttiva n. 2022/2555 (c.d. Direttiva NIS2) di recente emanazione e destinata, in seguito al suo recepimento previsto entro il 18 ottobre 2024, a integrare se non in alcuni casi superare le norme di legge fino ad ora adottate. Oltre ad ampliare il novero dei soggetti potenzialmente rientranti nel Perimetro, infatti, la Direttiva NIS2 prevede un nuovo e più articolato quadro normativo tra cui spicca un nuovo assetto delle notifiche degli incidenti significativi. In particolare, devono essere trasmessi al CSIRT senza indebito ritardo, e comunque entro 24 ore da quando vi è stata conoscenza dell'incidente, un preallarme che, se opportuno, indichi se l'incidente è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero; inoltre, deve essere trasmessa senza indebito ritardo, e comunque entro 72 ore da quando vi è stata conoscenza dell'incidente, una notifica

dell'incidente che, se opportuno, aggiorni le informazioni fornite in precedenza e indichi una valutazione iniziale dell'incidente, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione. Altresì, dovranno essere trasmesse su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione ed una relazione finale entro un mese dalla trasmissione della notifica dell'incidente. La direttiva NIS2 introduce quindi una nuova e più articolata modalità di notifica degli incidenti, che richiederà un cospicuo dispendio di risorse per la sua integrazione all'interno dell'attuale sistema di notifica degli incidenti previsto dall'ordinamento nazionale. In altre parole, la disciplina nazionale applicata ai soggetti inclusi nel Perimetro è caratterizzata da una stratificazione normativa che pone diverse sfide applicative ed interpretative, che il prossimo recepimento della Direttiva NIS2 potrebbe rendere ancora più articolate. Tuttavia, sembra verosimile ritenere che il legislatore italiano, nel processo di recepimento ed implementazione di tale direttiva, pur dovendo modificare e integrare nuovamente la disciplina ad oggi in vigore, grazie anche al lavoro svolto dall'ACN non sarà colto impreparato, e coglierà anzi quest'occasione per riorganizzare la regolamentazione del Perimetro in modo più organico ed efficace[196].

Conclusivamente, si alza, quindi, ulteriormente il livello di resilienza cibernetica degli attori maggiormente sensibili ai fini della sicurezza nazionale. Dal 24 giugno 2021, il Perimetro di sicurezza nazionale cibernetica è iniziato ad essere operativo nei confronti dei soggetti inseriti il 22 dicembre 2020. Questi ultimi saranno tenuti ad applicare le misure di sicurezza legislativamente previste e a notificare allo CSIRT italiano gli incidenti che si dovessero manifestare. La lista delle misure di sicurezza e la tassonomia degli incidenti per cui il soggetto è tenuto a notificare sono state pubblicate l'11 Giugno 2021, in Gazzetta Ufficiale n. 138.

[196] https://www.agendadigitale.eu/giornalista/andrea-mezzetti e https://www.agendadigitale.eu/giornalista/catyerina-chiari, «Cybersicurezza, le norme in vigore e in arrivo per i soggetti inclusi nel perimetro di sicurezza nazionale», Agenda Digitale, 1 marzo 2023, https://www.agendadigitale.eu/sicurezza/cybersicurezza-le-norme-in-vigore-e-in-arrivo-per-i-soggetti-inclusi-nel-perimetro-di-sicurezza-nazionale-e/.

I. *I soggetti rilevanti per la cybersecurity nazionale: Agenzia per la Cybersicurezza Nazionale, Centro di Valutazione e Certificazione Nazionale e CSIRT*

Inizialmente la disciplina Perimetro nacque senza la previsione di un'agenzia per la sicurezza nazionale, la cui istituzione non era nemmeno in programma; interessante è, quindi, capire come l'Agenzia abbia semplificato la materia impattando sul Perimetro. Di fatti, il decreto legge 14 giugno 2021 n. 82, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", completa la Strategia italiana di cyberresilienza, avviata con la disciplina sul Perimetro cibernetico, e accresce la consapevolezza del settore pubblico, privato e della società civile sui rischi e le minacce cyber. La principale novità del decreto è rappresentata dalla creazione dell'Agenzia per la cybersicurezza nazionale, che opera sotto la responsabilità del Presidente del Consiglio dei ministri e dell'Autorità delegata per la sicurezza della Repubblica, in stretto raccordo con il Sistema di informazione per la sicurezza della Repubblica. L'Agenzia per la cybersicurezza nazionale (ACN) diviene autorità nazionale per la certificazione, in attuazione dell'articolo 58 del Regolamento (UE) n. 881 del 2019 relativo all'attivazione di una strategia di sicurezza informatica negli Stati membri. Inoltre, provvede all'accertamento delle violazioni ed all'irrogazione delle sanzioni[197] e svolge tutte le funzioni già attribuite all'Agenzia per l'Italia digitale (AgID)[198], compresa l'emissione di linee guida con regole tecniche di cybersicurezza. Infatti, un ruolo importante dell'Agenzia riguarda

[197] In altri paesi europei le sanzioni irrogate da un'agenzia vengono incamerate dal Tesoro e successivamente, se appropriato, gli importi relativi vengono, più o meno in parte, ristornati all'agenzia coinvolta. In Italia, invece, è previsto l'incasso diretto delle sanzioni da parte dell'agenzia che le irroga, come ad esempio accade per le sanzioni irrogate dall'Autorità garante per la protezione dei dati personali.

[198] L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. L'AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese, sostenendo l'innovazione digitale e promuovendo la diffusione delle competenze digitali anche in collaborazione con le istituzioni e gli organismi internazionali, nazionali e locali. «*Chi siamo|Agenzia per l'Italia digitale», https://www.AgID.gov.it/it/agenzia/chi-siamo.*

l'obbligo di svolgere attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia. Inoltre, l'ACN promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca[199]. Nel dettaglio, i principali compiti attribuiti all'Agenzia sono quelli di esercitare le funzioni di Autorità nazionale in materia di cybersecurity a tutela degli interessi nazionali e della resilienza dei servizi e delle funzioni essenziali dello Stato da minacce cibernetiche; inoltre, sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione per far fronte agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il Computer Security Incident Response Team (CSIRT) italiano e l'avvio operativo del Centro di Valutazione e Certificazione Nazionale. Altresì, l'Agenzia deve contribuire all'innalzamento della sicurezza dei sistemi di *Information and communications technology* (ICT) dei soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica, delle Pubbliche Amministrazioni, degli Operatori di servizi essenziali (OSE) e dei Fornitori di servizi digitali (FSD) [200]. Si aggiungono gli incarichi di supportare lo sviluppo di competenze industriali, tecnologiche e scientifiche, promuovendo progetti per l'innovazione e lo sviluppo e mirando a stimolare nel contempo la crescita di una solida forza di lavoro nazionale nel campo della cybersecurity in un'ottica di autonomia strategica nazionale nel settore. Infine, spetta all'Agenzia la mansione di assumere le funzioni di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza e attività ispettive negli ambiti del Perimetro di sicurezza nazionale cibernetica, della sicurezza delle reti e dei sistemi informativi (ai sensi della direttiva NIS), e della sicurezza delle reti di comunicazione elettronica.

Presso l'Agenzia è costituito in via permanente il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri, per gli aspetti relativi alla prevenzione e preparazione ad

[199] PuntoSicuro, «Istituita l'agenzia per la cybersicurezza nazionale -...», https://www.puntosicuro.it/security-C-125/istituita-l-agenzia-per-la-cybersicurezza-nazionale-AR-21423/.

[200] «La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021», https://www.federalismi.it/.

eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Per di più, il decreto istituisce il Comitato interministeriale per la cybersicurezza (CIC) con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Tra i compiti del Comitato si annoverano quelli di proporre al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale e di esercitare l'alta sorveglianza sull'attuazione della Strategia nazionale di cybersicurezza[201]. Inoltre, il Comitato promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche[202]. Nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR[203] in materia di gestione delle situazioni di crisi che coinvolgono aspetti di cybersicurezza, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il Direttore generale dell'Agenzia. In tal caso il Nucleo per la cybersicurezza assicura il supporto al CISR e al Presidente del Consiglio dei ministri per gli aspetti relativi alla gestione di situazioni di crisi nonché per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, ivi comprese le attività istruttorie e le procedure di attivazione necessarie[204].

Tutti i prodotti tecnologici e informatici, specialmente quelli utilizzati dalla Pubblica Amministrazione, devono rispondere a standard di sicurezza minimi prima di essere messi sul mercato. Fino ai primi anni duemila la certificazione era limitata ai prodotti utilizzati

---

[201] Francesco Bechis, «L'Agenzia cyber prende forma. Al via il trasloco degli 007», Formiche.net, 2 novembre 2021, https://formiche.net/2021/11/agenzia-cyber-sicurezza-baldoni-draghi/.

[202] «Nasce l'Agenzia per la cybersicurezza nazionale», Altalex, 23 giugno 2021, https://www.altalex.com/documents/news/2021/06/23/nasce-agenzia-per-cybersicurezza-nazionale.

[203] Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza, facente parte del Sistema di informazione per la sicurezza della Repubblica e istituito presso la Presidenza del consiglio. *«CISR - Sistema di informazione per la sicurezza della Repubblica», https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/comitato-interministeriale-per-la-sicurezza-della-repubblica-cisr.html.*

[204] Redazione, «Il d.l. 82/2021 e l'istituzione dell'Agenzia per la cybersicurezza nazionale (Acn)», Piselli & Partners (blog), 15 giugno 2021, https://www.piselliandpartners.com/news-di-settore/agenzia-cybersicurezza-nazionale-acn/.

nell'ambito della sicurezza nazionale e ai sistemi ICT[205] che trattavano informazioni classificate; oggi la digitalizzazione, che ha subìto un progresso esponenziale nei due anni di pandemia e relative restrizioni, ha esteso la superficie di rischio a diverse categorie di prodotti informatici. Grazie al "Perimento cyber" istituito nel 2019 dal governo Conte-bis, ossia alla rete di controlli e verifiche dei CVCN[206] che fa da filtro di sicurezza per aziende e pubbliche amministrazioni, viene certificata la sicurezza degli acquisti *tech* della Pubblica Amministrazione e dei soggetti pubblici e privati che svolgono servizi essenziali[207]. Come anticipato, il decreto Aiuti bis[208] istituisce l'Agenzia per la cybersicurezza come Autorità nazionale di certificazione della cybersicurezza al posto del MiSE[209]. Il bollino di garanzia conferito dall'Agenzia non è una semplice procedura burocratica ma lo standard di riferimento alla base dello screening della sicurezza informatica da parte della pubblica amministrazione; ad esempio, nell'esercizio del Golden Power da parte del governo su acquisti che riguardano la rete 5G, questi può emanare prescrizioni che richiedano al fornitore di turno di adeguarsi a un determinato livello di certificazione, pena l'uso del potere di veto[210]. La scelta del decreto Aiuti bis è quella di adeguare la normativa italiana al regolamento adottato dall'Unione europea nel 2019 per la certificazione cyber di prodotti, servizi e processi ICT; in questo modo l'ACN

[205] L'acronimo ICT (Information and Communication Technologies) si riferisce alle tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni. *«ICT (Information and Communication Technologies) in "Dizionario di Economia e Finanza"», https://www.treccani.it/enciclopedia/ict_(Dizionario-di-Economia-e-Finanza).*

[206] Il CVCN, ossia il Centro di valutazione e certificazione nazionale, è la struttura tecnica che, insieme ad una rete di Laboratori accreditati, si occupa di verificare la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del Perimetro e che rientrano nelle categorie previste dal DPCM 15 giugno 2021, con l'obiettivo di innalzare il livello di cybersicurezza e di resilienza delle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese. Il CVCN ha adottato le metodologie che saranno impiegate nel corso del processo di valutazione, come quella per la predisposizione dell'analisi del rischio, che i soggetti inclusi nel Perimetro adotteranno per redigere la documentazione da allegare alla comunicazione di affidamento. *«CVCN - Agenzia per la Cybersicurezza Nazionale», https://www.acn.gov.it/agenzia/articolazioni/cvcn.*

[207] Francesco Bechis, «Bollino cyber. Il decreto per certificare la sicurezza tech», Formiche.net, 4 maggio 2022, https://formiche.net/2022/05/bollino-cyber-draghi/.

[208] Il decreto legge 9 agosto 2022, n. 115 reca "Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali".

[209] L'acronimo MiSe fa riferimento al Ministero dello Sviluppo economico.

[210] Il potere di veto è stato utilizzato tre volte dal Presidente Draghi nel 2021: precisamente, in due di questi casi, è stato usato per fermare la vendita di tecnologia 5G da parte dell'azienda cinese Huawei perché ritenuta non sicura.

diventa l'ente responsabile di garanzia per mettere al sicuro la pubblica amministrazione da ingerenze esterne che vanno dal 5G cinese ai software russi[211].

La procedura di valutazione potrà prevedere l'esecuzione di test hardware e software sui componenti della fornitura; in questo processo, al CVCN fanno riferimento i Centri di Valutazione presso i Ministeri della Difesa e dell'Interno e potrà avvalersi del supporto di una rete di Laboratori accreditati di prova. Inoltre, il CVCN svolgerà un ruolo di supporto tecnico per le attività connesse all'esercizio dei poteri speciali (Golden Power) in ambito 5G, così come previsto dalle recenti modifiche apportate al decreto legge n. 21/2022 dal cosiddetto "decreto Ucraina"[212]. L'obiettivo è quello, da un lato, di garantire l'immissione nel mercato di prodotti con elementi digitali sicuri, curando tra l'altro la trasparenza delle proprietà di sicurezza, e, dall'altro, di sensibilizzare gli utenti nella scelta e nell'utilizzo di hardware e software sicuri. Per farlo, il legislatore europeo propone di fissare condizioni e requisiti per lo sviluppo di prodotti sicuri, assicurando che questi siano immessi sul mercato con meno vulnerabilità e che i produttori tengano conto della sicurezza durante tutto il ciclo di vita del prodotto[213].

Sul piano nazionale, il legislatore italiano aveva già da tempo ideato un articolato e complesso corpus normativo volto a istituire il cosiddetto "Perimetro di Sicurezza Nazionale Cibernetica". Tale normativa introduce numerosi obblighi legali finalizzati ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici degli operatori nazionali, pubblici e privati, che esercitano una funzione essenziale o che erogano un servizio essenziale dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale[214]. Con il decreto legge 21 marzo 2022 n. 21,

---

[211] I software prodotti nella Federazione russa sono ritenuti, dopo la guerra russa in Ucraina, non più affidabili per il rischio di interferenze delle autorità di Mosca. Una recente circolare dell'Agenzia, ha dato disposizioni ad aziende e pubbliche amministrazioni di rimuovere Kaspersky e i software russi. *Federica De Vincentis, «Draghi allarga il Golden Power. 5G, software russi e le altre novità», Formiche.net, 18 marzo 2022, https://formiche.net/2022/03/draghi-golden-power-5g/.*

[212] Giovanni Salvi, «Dal decreto Aiuti bis una nuova concezione della cybersecurity», Il Sole 24 ORE, 16 agosto 2022, https://www.ilsole24ore.com/art/dal-decreto-aiuti-bis-nuova-concezione-cybersecurity-AEB2dysB.

[213] Gabriele Carrer, «Come cambia la cybersecurity con il dl Aiuti bis? Risponde Iezzi (Swascan)», Formiche.net, 18 settembre 2022, https://formiche.net/2022/09/decreto-aiuti-bis-cyber-iezzi-swascan/.

[214] Stefano Mele, «Cybersecurity Act, la strategia europea e le priorità dell'Italia», Formiche.net, 14 luglio 2018, https://formiche.net/2018/07/cybersecurity-act-la-strategia-europea-e-le-priorita-dellitalia/.

l'Italia, spinta dagli avvenimenti in Ucraina, ha adottato disposizioni d'urgenza in materia di diversificazione delle dotazioni informatiche delle Pubbliche Amministrazioni e di riorganizzazione complessiva dei poteri speciali in materia di comunicazione elettronica a banda larga basati sulla tecnologia 5G. Inoltre, il 4 settembre 2022 è entrato in vigore il decreto legge 3 agosto 2022 n. 123 volto ad adeguare la normativa nazionale al nuovo quadro europeo di certificazione della cybersicurezza, introdotto dal Regolamento (UE) 2019/881[215].

Come detto, altro soggetto che riveste un ruolo di notevole importanza nell'ambito del Perimetro è il CSIRT. Il CSIRT Italia è la struttura tecnica di prevenzione, coordinamento e risposta agli eventi e incidenti informatici con impatto effettivo o potenziale sul territorio nazionale, ed è istituito presso l'Agenzia per la Cybersicurezza Nazionale[216]. È il punto di riferimento per le notifiche di incidente ai danni di tutte le infrastrutture digitali della Pubblica Amministrazione e private, in particolare per le notifiche definite ai sensi di legge per i soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica o per gli operatori di servizi essenziali individuati dalla direttiva NIS. Inoltre, partecipa attivamente alla CSIRT Network, ossia la rete composta dagli CSIRT europei, per contribuire a sviluppare la fiducia tra gli Stati membri dell'Unione e promuovere la cooperazione internazionale. Altrimenti detto, i CSIRT sono centri in grado di coordinare in modo veloce ed efficace la comunicazione fra gli esperti durante le emergenze; gli scopi sono quelli di assistere gli utenti della rete in caso di incidente informatico, prevenire eventuali incidenti futuri e promuovere una cultura a livello internazionale sulla sicurezza informatica[217]. L'evoluzione tecnologica, e con essa la maggior

[215] Gabriele Carrer, «Agenzia cyber. Cosa farà il Cvcn per mettere il 5G al sicuro», Formiche.net, 1 luglio 2022, https://formiche.net/2022/07/agenzia-cyber-cvcn-5g/.

[216] Il decreto legislativo sulla direttiva NIS ha previsto l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team, detto CSIRT italiano, chiamato a svolgere compiti e funzioni che in precedenza erano in capo al CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e al CERT-PA (operante presso l'Agenzia per l'Italia Digitale). *«Articolazioni - Agenzia per la Cybersicurezza Nazionale», https://www.acn.gov.it/agenzia/articolazioni.*

[217] La DARPA (Defence Advanced Research Projects Agency) creò il primo CSIRT (Computer Security Incident Response Team), chiamato CERT/CC (Computer Emergency Response Team Coordination Centre), presso la Carnegie Mellon University di Pittsburgh in Pennsylvania. L'esigenza di strutturare delle squadre in grado di porre rimedio ad incidenti informatici avvenne nel 1988; in tale occasione, si diffuse, riuscendo a contagiare circa il 10% dei computer al mondo, il Morris Worm creato dallo studente della Cornell University Robert Tappan Morris.

consapevolezza dei pericoli e delle esigenze, ha illuminato il percorso da seguire per realizzare un efficientamento delle unità preposte a protezione delle infrastrutture e delle reti informatiche. Questo, tuttavia, ha reso necessaria una trasformazione che ha rigenerato i CERT[218], i quali da squadre incaricate alla gestione delle emergenze informatiche sono evoluti fino a diventare fornitori di servizi di sicurezza completi in grado di svolgere attività di prevenzione quali l'emanazione di bollettini informativi sulla sicurezza ed allarmi, oltre ad erogare attività di formazione e gestione della sicurezza. Per ricomprendere tutte queste nuove mansioni è stato coniato l'acronimo CSIRT[219]. Come si è avuto modo di indicare in precedenza, fra i principali compiti affidati all'ENISA vi è quello di aumentare "il livello delle capacità dei CERT nazionali/governativi e dell'Unione, anche attraverso la promozione del dialogo e dello scambio di informazioni, al fine di assicurare che, tenuto conto dell'evoluzione tecnica, tutti i CERT soddisfino un insieme comune di capacità minime e operino secondo le migliori prassi".

I servizi offerti dai CSIRT sono molteplici; in primo luogo distinguiamo i servizi reattivi, consistenti in misure volte alla gestione e risoluzione degli incidenti, dai servizi proattivi che, al contrario, sono veicolati ad un'attività di prevenzione al fine di scongiurare, o quantomeno circoscrivere, il numero, l'entità e la durata degli incidenti. In secondo luogo, rientrano nei servizi offerti anche la gestione degli artefatti, che consiste nell'analisi – e successiva diffusione – delle informazioni ricavate dai malware affrontati, e la gestione della qualità e della sicurezza, il cui intento è quello di produrre una cooperazione utile allo sviluppo di misure di

---

Nel 1992 la rete di ricerca olandese SURFnet ha lanciato il primo CSIRT europeo, con il nome di SURFnet-CERT. In seguito vennero ad aggiungersi molti nuovi gruppi attualmente elencati nell'Inventario delle attività CERT in Europa dell'ENISA. *Alfonso Contaldo e Flaviano Peluso, La nuova disciplina italiana ed europea alla luce della direttiva NIS, 2018ª ed. (Pacini Giuridica, s.d.).*

[218] L'acronimo CERT sta per Computer Emergency Response Team. I CERT avevano il compito di gestire le emergenze, l'incident response e costruire velocemente un robusto tessuto di consapevolezza all'interno della comunità Internet. Dalla nascita dei CERT la complessità delle infrastrutture è cresciuta ed è diventato più complicato difenderle, mentre gli attaccanti si sono evoluti in gruppi criminali organizzati molto ben finanziati e supportati. Con l'evoluzione delle minacce, dunque, il livello dello scontro si è alzato ed è nata l'esigenza di creare risposte coordinate ed efficaci alle emergenze cibernetiche: sono stati creati i CSIRT per affrontare i nuovi incidenti cibernetici. *«CSIRT, cosa sono e cosa fanno i team di risposta agli incidenti di sicurezza», Cyber Security 360 (blog), 24 settembre 2020, https://www.cybersecurity360.it/soluzioni-aziendali/csirt-cosa-sono-e-cosa-fanno-i-team-di-risposta-agli-incidenti-di-sicurezza/.*

[219] Alfonso Contaldo e Flaviano Peluso, La nuova disciplina italiana ed europea alla luce della direttiva NIS, 2018ª ed. (Pacini Giuridica, s.d.), pag. 67.

immunizzazione dal contagio. In particolare, i servizi reattivi sono soluzioni a breve termine messe in campo per risolvere problematiche già individuate, e sono suddivisibili in una serie di attività: prime fra tutte, gli allarmi e gli avvisi che consentono la divulgazione delle informazioni riguardanti le vulnerabilità della sicurezza; inoltre, attraverso la gestione degli incidenti, i CSIRT possono ripristinare la rete, filtrare il traffico di rete o sviluppare particolari strategie di risposta. Altresì, analizzando gli incidenti, i CSIRT ricavano informazioni riguardanti l'estensione e la gravità degli stessi in modo da comprendere la natura dell'attacco ed elaborare una strategia difensiva; tale analisi si svolge attraverso la raccolta di prove forensi, che devono essere collezionate e conservate seguendo una precisa procedura in modo tale da utilizzarle come prove in tribunale. Una volta individuato l'incidente, la risposta può avvenire in loco attraverso l'assistenza diretta, ossia svolta fisicamente nei luoghi scenario dell'attacco, oppure può essere data un'assistenza a distanza attraverso la fornitura di informazioni e procedure per poter ripristinare il sistema colpito[220]. Invece, i servizi proattivi consistono nell'individuazione e nel monitoraggio dei punti di debolezza e delle modalità utili per penetrare una rete, cercando di risalire anche all'identità dell'intruso (generalmente tale attività presuppone una collaborazione con le forze di polizia o con i fornitori di servizi Internet). Attraverso gli annunci – che consistono principalmente in allarmi di intrusione, avvisi di vulnerabilità e bollettini informativi sulla sicurezza – gli utenti possono rimanere informati su tutte le criticità e malware noti; inoltre, i CSIRT analizzano nuove tecnologie e rischi futuri, attuano previsioni e valutazioni della sicurezza attraverso l'analisi delle infrastrutture delle organizzazioni e forniscono una risposta alle informazioni. Questo servizio è particolarmente impegnativo per le grandi quantità di dati da analizzare e spesso infatti ci si avvale di soggetti più competenti come i Managed Security Service Providers[221]. Con riguardo al servizio di

[220] «Operatori di servizi essenziali (OSE): chi sono e quali obblighi di sicurezza hanno», Cyber Security 360 (blog), 29 gennaio 2021, https://www.cybersecurity360.it/cybersecurity-nazionale/operatori-di-servizi-essenziali-ose-chi-sono-e-quali-obblighi-di-sicurezza-hanno/.

[221] I servizi di sicurezza gestita (MSS – Managed Security Services) sono definiti come il monitoraggio remoto o la gestione delle funzioni di sicurezza IT fornite tramite servizi condivisi dai centri operativi di sicurezza remoti (i cosiddetti SOC – Security Operation Center). Il SOC è un centro dal quale – e attraverso il quale – vengono erogati servizi finalizzati alla sicurezza dei sistemi informativi di un'azienda. Il SOC può essere interno al Data Center aziendale, oppure esterno. In quest'ultimo caso, il SOC è il centro grazie al quale vengono erogati i Managed Security Services (MSS) e l'azienda

gestione degli artefatti, invece, l'attività in oggetto consiste nell'analisi dell'artefatto e nella sua risposta attraverso la determinazione delle azioni più appropriate per rimuovere oppure prevenire l'incidente; in seguito, i CSIRT provvedono alla condivisione dell'analisi o delle strategie di risposta con altri centri, esperti di sicurezza e ricercatori, oppure fanno fronte all'alimentazione di un archivio pubblico o riservato agli utenti di riferimento degli artefatti noti. I CSIRT gestiscono la qualità della sicurezza analizzando i rischi ed elaborando strategie di protezione e risposta; inoltre, vengono svolte attività di continuità operativa e ripristino in caso di disastro, ossia quelle attività necessarie a garantire la continuità delle operazioni. Infine, i CSIRT svolgono consulenze sulla sicurezza e sulle migliori prassi da adottare in base al tipo di utente di riferimento, istruiscono e formano gli utenti grazie a seminari, laboratori, corsi e guide; da ultimo, certificano i prodotti al fine di garantire la sicurezza e valutare se siano conformi agli standard di sicurezza[222].

La legislazione nazionale dettata dal decreto legislativo n. 65/2018[223] stabilisce il quadro generale, l'ambito di applicazione e le misure da attuare in caso di incidenti attraverso la designazione delle autorità nazionali competenti[224], del Punto di contatto unico[225], nonché del Gruppo di intervento per la sicurezza informatica. Inoltre, il CSIRT italiano partecipa alla rete di CSIRT europea al fine di scambiare informazioni e fornire un sostegno agli altri Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria.

---

che eroga tali servizi viene definita Managed Security Service Provider (MSSP). *Alessandro.Achilli, «Managed Security Services: Cosa Sono e le Opportunità per le PMI», IT Impresa, 18 febbraio 2021, https://www.it-impresa.it/blog/mss-managed-security-services-pmi/.*

[222] Alfonso Contaldo e Flaviano Peluso, La nuova disciplina italiana ed europea alla luce della direttiva NIS, 2018ª ed. (Pacini Giuridica, s.d.), pag. 78.

[223] Il d.lgs. 18 maggio 2018 n. 65 attua la legge-delega n. 163 del 2017 recante "delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea – Legge di delegazione europea 2016-2017". La normativa in oggetto prevede il recepimento e l'attuazione della direttiva 2016/1148/UE (c.d. direttiva NIS) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.

[224] Le Autorità che appaiono designate sono il Ministero delle Infrastrutture e dei Trasporti, il Ministero dello Sviluppo Economico, il Ministero dell'Economia e delle Finanze, il Ministero della Salute e il Ministero dell'Ambiente.

[225] Il Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei ministri è designato quale Punto di Contatto Unico in materia di sicurezza informatica e delle reti. Il Punto di Contatto Unico è "l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea" (art. 3 d.lgs. 65/2018).

Parimenti agli operatori di servizi essenziali[226], anche i fornitori di servizi digitali[227] hanno l'obbligo di notificare al CSIRT, e per competenza all'Autorità NIS di settore, "senza ingiustificato ritardo", il verificarsi di incidenti informatici di qualsivoglia natura, descrivendo l'impatto rilevante sui servizi forniti[228]. In particolare, il CSIRT ha il compito di informare le Autorità competenti NIS e il Punto di contatto unico in merito alle notifiche di incidenti trasmesse ai sensi della normativa sul perimetro cibernetico (decreto legge 21 settembre 2019 n. 105). Il ruolo centrale del CERT-EU nello scambio di informazioni tra i CSIRT nazionali viene riaffermato anche nella recente Strategia europea di Sicurezza 2020–2025, dove si parla di "elaborare norme comuni obbligatorie e rigorose per lo scambio sicuro di informazioni e la sicurezza delle infrastrutture e dei sistemi digitali in tutte le istituzioni, gli organismi e le agenzie dell'UE"[229]. L'effetto negativo della normativa è dato dal fatto che diventa particolarmente difficile per le P.A. locali, con esigenze e servizi differenti, riuscire ad ottenere da un unico CSIRT nazionale una forma di supporto che vada oltre la gestione dell'incidente o del *data breach*; infatti, la frammentazione delle funzioni IT non solo aumenta i costi ma ne riduce l'efficienza e la sicurezza rendendo le amministrazioni locali più vulnerabili. Il governo ha provato a fornire una soluzione, delegando i compiti di sicurezza IT per le amministrazioni locali ai CERT regionali, ossia CSIRT attivi in un contesto circoscritto, così da cogliere meglio la dimensione locale dei singoli enti che funzionino come snodo tra CSIRT-IT e amministrazioni locali. I CERT di prossimità si propongono quindi come uno strumento

[226] La lettera g) dell'art. 3 d.lgs. 65/2018 identifica gli operatori di servizi essenziali sulla base di tre criteri: "a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio".

[227] Le lettere h) e i) dell'art. 3 d.lgs. 65/2018, unitamente all'allegato III della disposizione medesima, delineano i fornitori di servizi digitali quali soggetti che operano nel campo dei seguenti servizi: a) mercato online; b) motore di ricerca on line; c) servizi di cloud computing

[228] L'organizzazione ed il funzionamento del CSIRT italiano sono stati successivamente disciplinati nel dettaglio dal DPCM dell'8 agosto 2019. Il CSIRT Italia ha cominciato ad operare il 6 maggio 2020 e contestualmente il CERT Nazionale ed il CERT-PA hanno cessato di esistere come soggetti autonomi. *«Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto», Agenda Digitale, 15 gennaio 2021, https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.*

[229] «CSIRT, cosa sono e cosa fanno i team di risposta agli incidenti di sicurezza», Cyber Security 360 (blog), 24 settembre 2020, https://www.cybersecurity360.it/soluzioni-aziendali/csirt-cosa-sono-e-cosa-fanno-i-team-di-risposta-agli-incidenti-di-sicurezza/.

fondamentale a supporto del CSIRT nazionale, attraverso un controllo più diretto sul territorio, gestendo gli incidenti per i quali non è necessario coinvolgere CSIRT-IT e fornendo alla pubblica amministrazione locale strumenti e aiuti più specifici[230].

[230] La fondazione GCSEC di Poste Italiane è stata la prima in Italia a muoversi nell'ottica di implementare un modello per CERT/CSIRT e ha di recente sviluppato una applicazione Web Based ad uso gratuito per chiunque voglia utilizzarla che estende il concetto di maturità del CERT/CSIRT ai singoli servizi e funzioni aziendali in contesti Cyber. L'applicazione Web Based di riferimento prende il nome di CERTrating Maturity Evaluation Tool e sarà disponibile gratuitamente all'indirizzo https:certrating.it. Rispondendo a semplici domande a risposta multipla CERTrating valuta il livello di maturità del CERT ispirandosi al Maturity Model sviluppato dall'ENISA che offre la postura di un CERT rispetto a quattro livelli di maturità: not basic, basic, medium, advanced.
In particolare la piattaforma valuta il livello di maturità non solo del CERT/CSIRT ma anche di ognuno dei suoi servizi attribuendo ad ognuno il livello di importanza. I servizi sono categorizzati secondo le 14 tipologie definite da ENISA. La piattaforma suggerisce per ognuno degli ambiti Organizzazione, Risorse, Tool e Processi le azioni minime da mettere in campo per raggiungere il livello di maturità successivo. CERTrating offre inoltre una vista grafica semplice ed una reportistica completa della maturità del CERT, dei suoi Servizi e del posizionamento rispetto ad altri CERT italiani misurati, l'andamento della maturità nel tempo rispetto ad obiettivi da raggiungere e le distanze, nonché lo storico di tutte le valutazioni effettuate per il CERT/CSIRT e per i suoi servizi. *«Cert e Csirt questi sconosciuti, tutti i passaggi della cybersecurity italiana», Agenda Digitale, 17 marzo 2020, https://www.agendadigitale.eu/sicurezza/cert-e-csirt-questi-sconosciuti-tutti-i-passaggi-della-cybersecurity-italiana/.*

II. La cybersecurity prima del Perimetro

Il precedente Piano Nazionale, rispetto alla Strategia Nazionale di Cybersicurezza 2022-2026, è stato adottato il 17 febbraio 2017 in linea di continuità con quello relativo al biennio 2014-2015 e alla luce dell'esperienza maturata nel corso dello stesso. Il Piano in questione individua gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre in essere per dare concreta attuazione al Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico (QSN), sulla base degli indirizzi per la protezione cibernetica e la sicurezza informatica indicati dal Presidente del Consiglio dei Ministri nella sua qualità di Organo di vertice dell'architettura nazionale cyber. Traendo spunto dalle riflessioni svolte in occasione delle attività di verifica dell'attuazione del Piano Nazionale del 2013, sono state elaborate alcune misure di revisione dello stesso DPCM del 24 gennaio 2013 che sono state successivamente recepite nell'ambito del DPCM del 17 febbraio 2017[231]. L'attività di revisione ha fatto tesoro sia dell'esperienza maturata nella fase di prima implementazione dell'architettura nazionale, sia delle scelte operate nel settore dai Paesi tecnologicamente più avanzati. In armonia con l'attività svolta nel biennio 2014-2015, il Piano[232] prevede undici indirizzi operativi (IIOO), con obiettivi specifici e conseguenti linee d'azione, così come esplicitato all'articolo 3, comma 1, letter. c), del Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

Prima del 2017 il quadro legislativo era improntato alla distribuzione di funzioni e compiti aventi rilievo per la sicurezza cibernetica tra molteplici soggetti istituzionali, i quali erano competenti nelle diverse fasi della prevenzione degli eventi dannosi nello spazio cibernetico,

[231] La terminologia impiegata nel presente Piano Nazionale è conforme a quella adottata in ambito internazionale (ONU, NATO e UE) in materia, oltre che al glossario, denominato "le parole del cyber", presente in calce al Documento di sicurezza nazionale, annesso quest'ultimo alla relazione annuale al Parlamento ed aggiornato annualmente ai sensi dell'art. 38, co. 1-bis, della legge 124/2007.

[232] Il Piano Nazionale stabilisce la *roadmap* per l'adozione, da parte dei soggetti pubblici e privati, delle misure prioritarie per l'implementazione del Quadro Strategico, sulla base di un dialogo attivo e iterativo 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.

dell'elaborazione di linee guida e standard tecnici di sicurezza, della difesa dello Stato da attacchi nello spazio cibernetico, della prevenzione e repressione dei crimini informatici, della preparazione e della risposta nei confronti di eventi cibernetici. Già il decreto legge 30 ottobre 2015 n. 174, convertito con modificazioni dalla legge n. 198 del 2015, aveva attribuito al CISR funzioni di consulenza, proposta e deliberazione in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale. Si è reso necessario aggiornare, anche nelle more del recepimento della Direttiva (UE) 2016/1148 (cd. NIS), la predetta architettura istituzionale e ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento. L'intenzione che stava alla base del DPCM 2017 era quella di procedere ad una razionalizzazione e semplificazione della predetta architettura istituzionale, prevedendo che le funzioni di coordinamento e raccordo delle attività di prevenzione, preparazione e gestione di eventuali situazioni di crisi di natura cibernetica siano attestate presso strutture che assicurino un più diretto ed efficace collegamento con il Comitato interministeriale per la sicurezza della Repubblica. Il decreto del 2017 definisce, in un contesto unitario e integrato, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione delle vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi. Il modello organizzativo-funzionale delineato con il presente decreto persegue la piena integrazione con le attività di competenza del Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, nonché con quelle espletate dalle strutture del Ministero della difesa dedicate alla protezione delle proprie reti e sistemi nonché alla condotta di operazioni militari nello spazio cibernetico, dalle strutture del Ministero dell'interno, dedicate alla prevenzione e al contrasto del crimine informatico e alla difesa civile, e quelle della protezione civile.

Il DPCM del 2017, e prima ancora quello datato il 24 gennaio 2013, dettò varie regole circa i compiti di ciascun soggetto addetto alla cybersecurity. Innanzitutto, spetta al Presidente del Consiglio dei ministri, quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica, ai fini della tutela della sicurezza nazionale anche nello spazio cibernetico, di convocare il CISR nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale; inoltre, al Premier compete l'adozione su proposta del CISR, curandone l'aggiornamento, del Quadro strategico nazionale per la sicurezza dello spazio cibernetico, contenente l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, e di quelli nazionali operanti al di fuori del territorio del Paese, ed infine l'individuazione degli strumenti e delle procedure con cui perseguire l'accrescimento della capacità del Paese di prevenzione e risposta rispetto ad eventi nello spazio cibernetico, anche in un'ottica di diffusione della cultura della sicurezza. Ancora, il Governo adotta, su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali contenente gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale. Per quanto riguarda il CISR, ossia il Comitato interministeriale per la sicurezza della Repubblica, questi partecipa, in caso di crisi cibernetica, alle determinazioni del Presidente, con funzioni di consulenza e di proposta; il CISR, inoltre, tra le altre cose, esercita l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico e approva linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di best pratices e di misure rivolte all'obiettivo della sicurezza cibernetica. Altresì, il Comitato formula le proposte di intervento normativo ed organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi[233]. È stato previsto un organismo di supporto al CISR chiamato CISR tecnico, il quale è

[233] «Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017», 2017. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

presieduto dal Direttore generale del DIS. Tale organismo collegiale di coordinamento, oltre a svolgere attività preparatoria delle riunioni del CISR dedicate alla materia della sicurezza cibernetica e ad assicurare l'istruttoria per l'adozione degli atti da parte del CISR, espleta le attività necessarie a verificare l'attuazione degli interventi previsti dal Piano Nazionale per la sicurezza dello spazio cibernetico e l'efficacia delle procedure di coordinamento tra i diversi soggetti, pubblici e privati, chiamati ad attuarli. Inoltre, il CISR tecnico coordina, in attuazione degli indirizzi approvati dal CISR e sulla base degli elementi forniti dalle amministrazioni ed enti competenti, dagli organismi di informazione per la sicurezza, dal Nucleo per la sicurezza cibernetica e dagli operatori privati, la formulazione delle indicazioni necessarie allo svolgimento delle attività di individuazione delle minacce alla sicurezza dello spazio cibernetico, al riconoscimento delle vulnerabilità, nonché per l'adozione di best practices e misure di sicurezza[234].

Il Direttore generale del DIS[235] adotta le iniziative idonee a definire le necessarie linee di azione di interesse generale con l'obiettivo di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati ed avanzati supporti tecnologici in funzione della preparazione alle azioni di prevenzione, contrasto e risposta in caso di crisi cibernetica da parte delle amministrazioni ed enti pubblici e degli operatori privati. Il DIS provvede alla trasmissione di informazioni rilevanti ai fini della sicurezza cibernetica alle Pubbliche Amministrazioni e agli altri soggetti, anche privati, interessati all'acquisizione di informazioni, nonché alla condivisione delle stesse informazioni nell'ambito del Nucleo per la sicurezza cibernetica. Altresì, il DIS pone in essere ogni iniziativa

[234] «Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013», 2013. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

[235] Il Dipartimento delle informazioni per la sicurezza (DIS) è l'organo di cui si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata per l'esercizio delle loro funzioni e per assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative di AISE e AISI. Con l'approvazione da parte del Parlamento della legge 133/2012 di iniziativa del COPASIR, approvata all'unanimità dal Parlamento, questo ruolo di coordinamento è stato ulteriormente rafforzato, in particolare per quanto riguarda l'analisi strategica di intelligence e la gestione unitaria delle risorse umane e materiali a disposizione del Comparto, funzioni che sono state espressamente demandate alla responsabilità del Dipartimento. *«DIS - Sistema di informazione per la sicurezza della Repubblica», consultato 30 luglio 2023, https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html.*

volta a promuovere e diffondere la conoscenza e la consapevolezza in merito ai rischi derivanti dalla minaccia cibernetica e sulle misure necessarie a prevenirli[236].

Presso il Dipartimento delle informazioni per la sicurezza è costituito, in via permanente, il Nucleo per la sicurezza cibernetica, a supporto del Presidente e del CISR, nella materia della sicurezza dello spazio cibernetico, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il Nucleo è presieduto dal Vice Direttore generale del DIS, designato dal Direttore generale, ed è composto dal Consigliere militare e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale. Il Nucleo per la sicurezza cibernetica svolge, quindi, funzioni di raccordo tra le diverse componenti dell'architettura istituzionale che intervengono a vario titolo nella materia della sicurezza cibernetica, nel rispetto delle competenze attribuite dalla legge a ciascuna di esse. In particolare, nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi cibernetica, il Nucleo promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale. Ai fini dell'attivazione delle azioni di risposta e ripristino rispetto a situazioni di crisi cibernetica, il Nucleo riceve le segnalazioni di evento cibernetico e dirama gli allarmi alle amministrazioni e agli operatori privati e valuta se l'evento assume dimensioni, intensità o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria. È compito del Nucleo assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica, vengano espletate in maniera coordinata, avvalendosi, per gli aspetti tecnici di risposta sul piano informatico e telematico, del Computer Emergency Response Team (CERT) nazionale, istituito presso il

[236] Presidenza del Consiglio dei Ministri, «Piano nazionale per la protezione cibernetica e la sicurezza informatica», marzo 2017, https://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf.

Ministero dello sviluppo economico, del CERT-PA, istituito presso l'Agenzia per l'Italia digitale, e degli altri CERT istituiti ai sensi della normativa vigente. L'importanza del Nucleo sta nel fatto che esso mantiene costantemente informato il Presidente, per il tramite del Direttore generale del DIS, sulla crisi in atto, predisponendo punti aggiornati di situazione; inoltre, assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente per il superamento della crisi, raccoglie tutti i dati relativi alla stessa elaborando rapporti e fornendo informazioni ai soggetti pubblici e privati interessati. Altresì, il Nucleo assicura i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO, dell'UE o di organizzazioni internazionali di cui l'Italia fa parte[237].

Per quanto riguarda gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di servizi digitali, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, questi hanno il compito di comunicare al Nucleo per la sicurezza cibernetica ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici. Tali soggetti devono collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti. A tal fine, il Ministro dello sviluppo economico promuove l'istituzione di un Centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

Il Piano Nazionale del 2017 è stato rivisitato dai Punti di Contatto cyber dei Dicasteri CISR (Affari Esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico), dell'Agenzia per l'Italia Digitale e del Nucleo per la Sicurezza Cibernetica[238]. Le principali

[237] Giovanni_Nazzaro, «Il piano nazionale per la protezione cibernetica e la sicurezza informatica», Sicurezza e Giustizia (blog), 10 ottobre 2017, https://www.sicurezzaegiustizia.com/il-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/.

[238] Redazione, «La strategia italiana in materia di cyber-security», ICT Security Magazine, 9 febbraio 2016, https://www.ictsecuritymagazine.com/articoli/la-strategia-italiana-in-materia-di-cyber-security/.

direttrici dell'intervento di revisione hanno interessato, in primo luogo, l'indirizzo operativo 5 riguardante l'operatività delle strutture nazionali di *incident prevention, response e remediation*, in cui sono state considerate le esigenze di potenziamento dei CERT, la necessità di costituire le strutture previste dalla Direttiva NIS (CSIRT, Punto unico di contatto nazionale, Autorità nazionale) e le modalità di coordinamento tra i vari attori – attuali e futuri – dell'architettura cibernetica (CERT e CSIRT, Comparto, CNAIPIC, Difesa e AgID), in una prospettiva di progressiva unificazione dei CERT pubblici. In secondo luogo, le principali modifiche del Piano hanno riguardato l'indirizzo operativo 1 dedicato al potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare, che è stato allineato rispetto all'esperienza operativa maturata al fine di potenziare le capacità complessive di risposta integrata ad eventi cibernetici. L'attuazione delle linee d'azione indicate nel presente documento, il cui sviluppo va inteso in un'ottica incrementale, sarà misurata attraverso modalità idonee a consentire, ai sensi dell'articolo 5 comma 3 lit. c) della citata direttiva presidenziale, lo svolgimento delle attività necessarie a "verificare l'attuazione degli interventi previsti dal Piano Nazionale per la sicurezza dello spazio cibernetico e l'efficacia delle procedure di coordinamento tra i diversi soggetti, pubblici e privati, chiamati ad attuarli" [239]. Da ultimo, l'esigenza di consentire un rapido ed efficace salto di qualità dell'architettura nazionale cyber ha reso necessario individuare un nucleo essenziale di iniziative, cui attribuire carattere di priorità ed urgenza, selezionate sulla base delle esigenze che hanno informato l'attività di revisione del QSN e del PN e a motivo dell'evoluzione del quadro normativo interno ed internazionale. Tali misure assumono una particolare valenza sistemica in quanto fanno leva sulle competenze e sulle responsabilità dei diversi attori che costituiscono la struttura portante

[239] Il Piano d'azione 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, cui l'approvazione del citato DPCM 17 febbraio 2017 intende fornire un deciso impulso. Nonostante le iniziative assunte nel corso del biennio 2014-2015, hanno continuato a persistere differenti livelli di efficacia delle misure di protezione di reti e sistemi, che si osservano sia orizzontalmente, tra realtà pubblica e privata, sia verticalmente, all'interno degli stessi ambiti. Occorre, inoltre, considerare che il patrimonio informativo sensibile ai fini della sicurezza nazionale non è pertinenza esclusiva del settore pubblico, ma è integrato anche da quegli asset detenuti da taluni soggetti privati operanti in settori strategici. Ciò rende necessario un approccio di sistema che consenta un'armonica implementazione di standard minimi di sicurezza comuni, specie per i sistemi critici e strategici del Paese. *«Sintesi Strategia - Italia - Strategie Nazionali di Sicurezza Informatica», https://www.sicurezzacibernetica.it/it/db/ncss/Italy/index.php#piano_nazionale.*

del tessuto cyber nazionale, tendendo sia ad implementare il coordinamento e l'interazione tra soggetti pubblici, privati e mondo della ricerca, sia ad accorciare e razionalizzare, rispetto al passato, la "catena di comando" deputata alla gestione delle crisi. A tal fine è attribuito al Direttore generale del DIS un ruolo attivo e centrale nell'architettura nazionale di sicurezza cibernetica[240]. Inoltre, la misura di attuazione più significativa riguarda le attività di approntamento del sistema di difesa cyber, tra cui il perimetro di copertura degli assetti di difesa comuni, per le quali si prevede una stretta ed efficace interazione del CERT Nazionale e del CERT della Pubblica Amministrazione. Ulteriori misure riguardano la certificazione di soluzioni software e hardware, attraverso l'istituzione presso il MiSE di un Centro di valutazione e certificazione nazionale per la verifica dell'affidabilità della componentistica ICT destinata ad infrastrutture critiche e strategiche, oltre che l'identificazione delle funzioni manageriali/professionali critiche e l'obbligo di condivisione degli eventi cibernetici significativi[241]. Il Piano Nazionale del 2017 ha, quindi, quali obiettivi quelli di garantire una semplificazione delle procedure ordinarie e straordinarie della gestione di crisi e del mantenimento delle infrastrutture, di rimodellare gli organi del sistema di protezione cibernetica e di contrarre la catena di comando onde favorire lo sviluppo di più efficienti punti di contatto, così da rendere più rapida la risposta alle emergenze[242]. Infine, occorre rilevare che le indicazioni previste nel Piano in discussione appaiono di non semplice lettura in quanto il documento risente di una struttura istituzionale complessa che si articola nella presenza di una pluralità di soggetti, atti e documenti la cui semplificazione è uno degli obiettivi individuati dal Piano stesso. Altresì, le modalità con cui sono riportati gli indirizzi operativi presenti sono da considerarsi problematiche; infatti, gli undici obiettivi operativi sono decomposti in 34 sotto-obiettivi, a loro volta espansi in 93 classi di attività. Risulta così un elenco molto esteso, senza

[240] «Adottato il nuovo Piano Nazionale per la protezione cibernetica e la sicurezza informatica», Bulgarelli & Partners (blog), 12 giugno 2017, https://bulgarelliandpartners.wordpress.com/2017/06/12/adottato-il-nuovo-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/.

[241] Giovanni_Nazzaro, «Il piano nazionale per la protezione cibernetica e la sicurezza informatica», Sicurezza e Giustizia (blog), 10 ottobre 2017, https://www.sicurezzaegiustizia.com/il-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/.

[242] Dario Centofanti, «Piano Nazionale per La Protezione Cibernetica e La Sicurezza Informatica», Medium, 22 luglio 2017, https://www.popinga.it/piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica-11d8976820d7.

che però sia articolata una struttura per priorità, soggetto competente e tempistica degli stessi. Peraltro, l'assenza nel Piano di qualunque riferimento temporale per l'adozione delle iniziative per il conseguimento dei diversi obiettivi operativi, nonché la mancanza di indicatori atti a qualificare il conseguimento degli stessi unitamente alla sostanziale assenza di indicazioni sulle risorse finanziarie da utilizzare, rappresentano gli elementi di maggior debolezza del Piano[243]. A titolo esemplificativo, occorre menzionare come l'obiettivo operativo 10, seppur intitolato "Risorse", si concentra sull'analisi dei costi senza fornire elementi sulle risorse a disposizione. In questo senso si evidenzia che il Piano, sebbene rappresenti un aggiornamento al mutato contesto di quello adottato nel 2013, si limita, nell'introduzione, a sottolineare che le principali direttrici dell'intervento di revisione hanno riguardato gli indirizzi operativi 1 e 5. A rendere più 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, cui la recente approvazione del citato DPCM 17 febbraio 2017 intende fornire un deciso impulso". Tale piano di azione individua otto obiettivi che, tuttavia, non coincidono in modo puntuale con gli undici obiettivi operativi (né con i loro sotto-obiettivi) andando così a porsi in parte come obiettivi aggiuntivi.

[243] «Cyber security: cos'è e come garantire la sicurezza dei sistemi informatici e delle reti», Cyber Security 360 (blog), 5 settembre 2018, https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-la-guida-definitiva-per-la-corretta-implementazione-in-azienda/.

7. Decreto Aiuti, PNRR e interventi recenti per lo sviluppo informatico

Nella riunione tenuta a Palazzo Chigi l'1 settembre 2022 con i vertici dell'ACN e alcuni ministri, il sottosegretario Franco Gabrielli[244] ha affermato che "la minaccia ibrida ha ormai da tempo preso il sopravvento sulla guerra fisica" e che "la demoralizzazione, la destabilizzazione, cioè la messa in crisi delle istituzioni e di chi le rappresenta è uno degli elementi per consentire un'ingerenza". La riunione nasce come occasione per fare il punto sulle minacce alla sicurezza cibernetica nazionale in seguito agli attacchi informatici di Killnet[245] e, se collegati a Mosca, quelli contro Gse[246] ed Eni[247]. In tale occasione, l'Agenzia per la cybersicurezza nazionale ha lanciato l'allarme sugli attacchi informatici contro le aziende energetiche e la catena di approvvigionamento e di distribuzione dei prodotti o servizi, discutendo dell'insufficienza e dell'inappropriatezza dei principi e delle regole in tema di sicurezza nazionale come conseguenza del mutato scenario tecnologico e geopolitico[248].

Come noto, il governo Draghi ha approvato la Strategia per la cybersicurezza nazionale, un documento di 85 punti che racchiude la *roadmap* per la sicurezza digitale del Paese fino al 2026; insieme, il Consiglio dei ministri ha dato il via libera all'ultimo DPCM del Perimetro cyber, la rete di controlli di sicurezza dei soggetti pubblici e privati che svolgono attività

---

[244] Franco Gabrielli è stato sottosegretario di Stato alla Presidenza del Consiglio con delega alla Sicurezza della Repubblica del governo Draghi.

[245] Killnet è un collettivo hacker russo noto per i suoi attacchi DoS (Denial of Service) e DDoS (Distributed Denial of Service) a diverse istituzioni governative in diversi paesi tra cui l'Italia durante l'invasione russa dell'Ucraina nel 2022 e presumibilmente durante l'Eurovision 2022.

[246] Gestore dei servizi energetici - GSE S.p.A. è una società per azioni italiana nata nel 1999, interamente partecipata dal Ministero dell'economia e delle finanze, alla quale è attribuito l'incarico di promozione e sviluppo delle fonti rinnovabili e dell'efficienza energetica. La Società svolge i propri compiti in conformità con gli indirizzi strategici e operativi definiti dal Ministero dello sviluppo economico e dall'Autorità di Regolazione per Energia Reti e Ambiente ed è assoggettata al controllo della Corte dei Conti. Il GSE ricopre un ruolo centrale nell'incentivazione economica dell'uso delle fonti rinnovabili in Italia, oltre che nella promozione dell'efficienza energetica e della cultura dell'uso sostenibile dell'energia.

[247] Eni S.p.A., originariamente acronimo di Ente Nazionale Idrocarburi, è un'azienda multinazionale creata dallo Stato italiano come ente pubblico nel 1953 sotto la direzione del Presidente Enrico Mattei, convertita in società per azioni nel 1992.

[248] «Cybersecurity, il Consiglio Ue: "Contro gli attacchi rafforzare la cooperazione"», CorCom, 23 maggio 2022, https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-il-consiglio-ue-contro-gli-attacchi-rafforzare-la-cooperazione/.

essenziali per lo Stato gestita dall'Agenzia per la cybersicurezza nazionale[249]. Le priorità della Strategia sono quelle di affrontare una pluralità di sfide come il rafforzamento della resilienza nella transizione digitale del Paese, il conseguimento dell'autonomia strategica nella dimensione cibernetica, l'anticipazione dell'evoluzione della minaccia cyber, la gestione di crisi cibernetiche e il contrasto della disinformazione online[250]. Il decreto legge 9 agosto 2022 n. 115 (il cosiddetto decreto Aiuti bis) recante "Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali", all'articolo 37[251], rubricato "Misure di intelligence di

[249] Con il decreto-legge n. 105 del 2019, convertito nella legge n. 133 dello stesso anno, è stato definito il Perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Come indicato nel DPCM 31 luglio 2020, n. 131, i soggetti pubblici e privati – che forniscono tali servizi o esercitano tali funzioni – sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici – interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro – dalle Amministrazioni competenti nei rispettivi settori.
I soggetti inclusi nel perimetro di sicurezza cibernetica sono tenuti a predisporre annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi essenziali e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT (Computer Security Incident Response Team) attivo presso l'ACN. Le misure di sicurezza, che i soggetti inclusi nel Perimetro sono tenuti ad adottare, e le modalità di notifica degli incidenti sono state definite con il DPCM 14 aprile 2021, n. 81. Inoltre, i soggetti inclusi nel perimetro, ai sensi dell'articolo 1, comma 6, del decreto legge n. 105/2019 – attuato con il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 – sono tenuti a comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN) l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici" e appartenenti a determinate categorie di cui al DPCM 15 giugno 2021.
L'elenco dei soggetti inclusi nel Perimetro nei diversi settori strategici sopra indicati è aggiornato su proposta delle Amministrazioni competenti all'ACN. I settori per i quali il MISE effettua l'istruttoria per l'individuazione dei Soggetti rientranti nel Perimetro di sicurezza cibernetica nazionale sono stabiliti dall'articolo 3, comma 2, lett. e), h) ed i) del DPCM 131/2020 e sono i seguenti: settore telecomunicazioni (lett. e); settore servizi digitali, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione (lett. h); settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca (lett. i*). Corrado Pisano, «Perimetro sicurezza», Ministero delle Imprese e del Made in Italy, https://atc.mise.gov.it/index.php/sicurezza/perimetro-sicurezza.*

[250] Redazione, «Cybersecurity, Draghi approva la strategia nazionale», Formiche.net, 17 maggio 2022, https://formiche.net/2022/05/cyber-strategia-draghi/.

[251] L'Articolo 37, riguardante disposizioni in materia di intelligence in ambito cibernetico, del decreto legge n. 115/2022 modifica il dettato del decreto legge n. 174/2015 stabilendo che: "1. Al decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, dopo l'articolo 7-bis è inserito il seguente:
«Art. 7-ter (Misure di intelligence di contrasto in ambito cibernetico). - 1. Il Presidente del Consiglio dei ministri, acquisito il parere del Comitato interministeriale per la sicurezza della Repubblica e sentito il Comitato parlamentare per la sicurezza della Repubblica, emana, ai sensi dell'articolo 1, comma 3, della legge 3 agosto 2007, n. 124, disposizioni per l'adozione di misure di intelligence di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale. Le disposizioni di cui al primo periodo prevedono la cooperazione del Ministero della difesa e il ricorso alle garanzie funzionali di cui all'articolo 17 della legge 3 agosto 2007, n. 124.

contrasto in ambito cibernetico", attribuisce alla Presidenza del Consiglio poteri di reazione ad attacchi informatici. Invero, il governo Draghi ha inserito, nel decreto Aiuti bis, una norma che consente all'intelligence di attuare una controffensiva in risposta ad un attacco cibernetico subìto: a questo punto, la Presidenza del Consiglio acquisisce il potere di adottare "misure di intelligence di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale"[252]. Le azioni difensive degli Stati sono dunque legittime, a condizione che siano proporzionate all'offesa e rispettose dei principi generali del diritto umanitario internazionale, che si applica non solo alle situazioni di conflitto aperto ma anche a tutte le fasi antecedenti, ivi compreso l'esercizio del diritto di autodifesa. Fino all'adozione del decreto in materia di cybersecurity erano vietate azioni offensive: era solo possibile la commissione di alcuni reati nell'ambito della copertura giuridica offerta dalle garanzie funzionali per poter acquisire informazioni di interesse della Repubblica[253]. Con il decreto Aiuti, invece, operatori qualificati appartenenti all'AISE[254] e

2. Le disposizioni di cui al comma 1 disciplinano il procedimento di autorizzazione, le caratteristiche e i contenuti generali delle misure che possono essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità. L'autorizzazione è disposta sulla base di una valutazione volta ad escludere, alla luce delle più aggiornate cognizioni informatiche, fatti salvi i fattori imprevisti e imprevedibili, la lesione degli interessi di cui all'articolo 17, comma 2, della legge 3 agosto 2007, n. 124.

3. Le misure di contrasto in ambito cibernetico autorizzate ai sensi del comma 2 sono attuate dall'Agenzia informazioni e sicurezza esterna e dall'Agenzia informazioni e sicurezza interna, ferme restando le competenze del Ministero della difesa ai sensi dell'articolo 88 del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66 e le competenze del Ministero dell'interno di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155. Il Dipartimento delle informazioni per la sicurezza assicura il coordinamento di cui all'articolo 4, comma 3, lettera d-bis), della legge n. 124 del 2007.

4. Il Presidente del Consiglio dei ministri informa il Comitato parlamentare per la sicurezza della Repubblica, con le modalità indicate nell'articolo 33, comma 4, della legge n. 124 del 2007, delle misure di intelligence di cui al presente articolo.

5. Al personale delle Forze armate impiegato nell'attuazione delle attività di cui al presente articolo si applicano le disposizioni di cui all'articolo 19 della legge 21 luglio 2016, n. 145, e, ove ne ricorrano i presupposti, all'articolo 17, comma 7, della legge n. 124 del 2007.

6. Il Comitato parlamentare per la sicurezza della Repubblica trascorsi ventiquattro mesi dalla data di entrata in vigore della presente disposizione trasmette alle Camere una relazione sull'efficacia delle norme contenute nel presente articolo»". *«Documentazione Economica e Finanziaria – a cura del CeRDEF – MEF Dipartimento delle Finanze.pdf».*

[252] Prevedere per legge la possibilità di reagire ad attacchi informatici provenienti da altre giurisdizioni allinea l'Italia ad una tendenza già manifestata in altri Paesi dell'Unione e negli USA.

[253] Edoardo C. Raffiotta, «Cybersecurity Regulation in the European Union and the issues of Constitucional Law *», s.d.

[254] L'Agenzia Informazioni e Sicurezza Esterna (AISE) è il servizio segreto italiano per l'estero, facente parte del Sistema di informazione per la sicurezza della Repubblica. Ha compiti e attività di intelligence al di fuori del territorio nazionale.

all'AISI[255] sono autorizzati a compiere atti che costituiscono reati, anche gravi, nella giurisdizione del Paese di destinazione (quello dal quale proviene – presuntivamente – l'attacco); in questo modo, l'interesse nazionale italiano può essere protetto anche violando le prerogative di altri Stati[256]. A tal proposito, la prima criticità che emerge è che l'attribuzione dell'attacco subìto ad uno Stato ostile potrebbe non essere immediata, mentre la reazione italiana potrebbe chiaramente essere addossata alla Repubblica e quindi causare tensioni diplomatiche di non poca rilevanza. L'esperto di cybersecurity Pierguido Iezzi, ceo di Swascan, parte del polo cyber di Tinexta Group ha affermato che "a livello strategico si conferma il ruolo chiave della difesa cyber attiva, mentre sul piano operativo la norma (l'articolo 37 del decreto Aiuti bis) riconosce quanto gli attacchi cyber siano di difficile attribuzione, ampliando lo spettro di azione alle possibili minacce di stampo terroristico, di matrice antagonista, cyber foreign fighter e, più in generale, di natura cybercriminale condotte dalle gang ransomware[257]". La seconda criticità attiene alla necessità di definire normativamente in modo chiaro il perimetro operativo della sicurezza nazionale; per consentire la reazione immediata in caso di attacchi, questo è un passaggio ineliminabile perché solo una volta definita normativamente la sicurezza nazionale è possibile operare il giudizio di bilanciamento, caso per caso, fra interessi dello Stato e diritto di difesa. Inoltre, una norma del genere consentirebbe il coordinamento fra le indagini penali e il coinvolgimento di strutture diverse dalla polizia giudiziaria. Gli attacchi informatici provenienti dall'estero sono reati perseguibili dalle autorità nazionali in base al principio dell'ubiquità dell'azione penale, e, se riguardano impianti di pubblica utilità, sono perseguibili d'ufficio. Di conseguenza, l'attività di reazione immediata dovrebbe prevedere la

[255] L'Agenzia Informazioni e Sicurezza Interna (AISI) è l'organizzazione di investigazione informativa, delegata alla sicurezza interna della Repubblica Italiana; fa parte del Sistema di informazione per la sicurezza della Repubblica, ha compiti di informazione, sicurezza e di controspionaggio all'interno del territorio nazionale.

[256] «Aiuti-bis: dal Copasir provvisorio alla sicurezza nazionale, ecco le nuove misure di cyber intelligence», Cyber Security 360 (blog), 11 ottobre 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/aiuti-bis-dal-copasir-provvisorio-alla-sicurezza-nazionale-ecco-le-nuove-misure-di-cyber-intelligence/.

[257] Le bande di ransomware sono gruppi di individui che lavorano insieme per eseguire attacchi ransomware. Spesso consistono in reti complesse di numerosi criminali informatici con il potere di rubare decine o centinaia di milioni di dollari ogni anno. *Katie Rees, «What Is a Ransomware Gang and How Dangerous Are They?», MUO, 5 aprile 2022, https://www.makeuseof.com/what-is-ransomware-gang/.*

contemporanea informativa al pubblico ministero e la documentazione analitica delle attività svolte, da mettere a disposizione del magistrato[258].

Ulteriori istituti che devono essere rivisti alla luce dell'articolo 37 del decreto Aiuti sono, in primo luogo, il segreto istruttorio nell'ambito del diritto di difesa, che deve garantire la non diffusione di informazioni sugli operanti coinvolti nelle attività e sui metodi adottati; in secondo luogo, viene in rilievo la tutela degli operanti perché nonostante la reazione all'attacco non sia considerata perseguibile in quanto prevista per legge non si riscontra lo stesso automatismo nei confronti degli agenti. Le azioni difensive-offensive (ad esempio la penetrazione o il danneggiamento di sistemi informatici da cui l'attacco è partito) dovranno rispettare i principi di ragionevole certezza dell'attribuzione, di proporzionalità, di rispetto dei diritti fondamentali. L'intrusione nei sistemi da cui arriva la minaccia dovrà garantire la progressività, per l'interruzione degli effetti dannosi e per l'acquisizione degli elementi utili per la corretta attribuzione. Quindi, l'articolo 37 ha una portata innovatrice ma richiede l'integrazione con una serie di provvedimenti normativi e regolamentari che ne consentono l'efficacia operativa e la tenuta giurisdizionale; altrimenti, il pericolo è che i risultati immediati derivanti da una vittoria tattica si traducano in un fallimento e dunque in una sconfitta[259]. Le priorità della trasformazione digitale sul territorio spinte dal Pnrr[260] rischiano di portare importanti investimenti tecnologici non adeguatamente sorretti da pilastri di sicurezza per via della mancanza del *security by design*, ossia la sicurezza dall'inizio dei progetti[261]. L'approccio innovativo territoriale è

[258] Giovanni Salvi, «Dal decreto Aiuti bis una nuova concezione della cybersecurity», Il Sole 24 ORE, 16 agosto 2022, https://www.ilsole24ore.com/art/dal-decreto-aiuti-bis-nuova-concezione-cybersecurity-AEB2dysB.

[259] Andrea Monti, «Come funziona il nuovo potere offensivo del governo nel settore cyber», Formiche.net, 12 agosto 2022, https://formiche.net/2022/08/decreto-aiuti-attacchi-cibernetici/.

[260] Il PNRR è il programma di investimento e intervento, di circa 210 miliardi di euro, con cui l'Italia ha intenzione di dare attuazione all'iniziativa europea Next Generation EU orientata ad offrire una risposta alla crisi economica e sociale determinata dalla pandemia da Covid-19. Tra i principali obiettivi del PNRR sono stati individuati, oltre alla transizione ecologica e all'inclusione sociale, la digitalizzazione e l'innovazione del sistema paese. Un tema fondamentale diventa dunque il potenziamento della cybersecurity a livello nazionale. Come accennato, con l'aumento della digitalizzazione sia in ambito privato che pubblico risulterà necessario potenziare in maniera significativa la capacità di prevenzione, monitoraggio e difesa delle infrastrutture tecnologiche da attacchi e incidenti di tipo cibernetico. L'istituzione dell'Agenzia per la Cybersicurezza Nazionale descritta in precedenza dimostra che l'Italia è pronta a muoversi in questa direzione.

[261] Redazione, «Cybersecurity e digital divide, investiamo anche sul territorio con una regia nazionale», Formiche.net, 2 agosto 2022, https://formiche.net/2022/08/cybersecurity-digital-divide-investiamo-territorio-regia-nazionale/.

sicuramente molto utile e consente di colmare un *digital divide* su molti aspetti ma, al contempo, può comportare delle insidie, ovvero il rischio di aumentare oltremodo questa sorta di nuovo cyber divario digitale. Abbiamo, così, una cybersicurezza a "due marce": una che riguarda le grandi aziende o amministrazioni pubbliche più grandi con investimenti su infrastrutture e strumenti operativi digitali, e un'altra che, invece, coinvolge le piccole e medie realtà produttive territoriali e la maggior parte della Pubblica Amministrazione locale, che rischiano di rimanere indietro perché non adeguatamente supportate sia nell'impiego delle risorse che sulla crescita professionale del personale. La percezione degli addetti ai lavori è che uno degli aspetti problematici – in particolare sul territorio – è la scarsa consapevolezza sui rischi e sulle annesse soluzioni per la mitigazione degli stessi. Forse anche a causa di una sempre più pervasiva spettacolarizzazione degli attacchi sui media, i quali si concentrano sul fenomeno (e quindi sugli effetti) non entrando nel cuore delle cause del problema[262]. Il secondo decreto legge per velocizzare l'attuazione del Pnrr (d.l. n. 36/2022, convertito con modificazioni con legge n. 79/2022) contribuisce al completamento della riforma del pubblico impiego con una fitta rete di novità per le P.A., tra le quali, la previsione di nuovi profili professionali soprattutto per sostenere la transizione digitale ed ecologica delle amministrazioni, una nuova gestione dei concorsi più informatizzata e con sistemi di valutazione volti ad accertare il possesso delle conoscenze e delle capacità logico-tecniche, comportamentali e manageriali. Si stabilisce, inoltre, lo svolgimento di un ciclo di formazione obbligatorio sui temi dell'etica pubblica e del comportamento etico sia a seguito di assunzione, sia in ogni caso di passaggio a ruoli o a funzioni superiori, nonché di trasferimento del personale, le cui durata e intensità sono proporzionate al grado di responsabilità[263]. Inoltre, il Piano nazionale di ripresa e resilienza prescrive l'aggiornamento, entro il 31 dicembre 2022, del Codice di comportamento dei dipendenti pubblici (D.P.R n. 62/2013) con una sezione dedicata al corretto utilizzo delle tecnologie informatiche e dei mezzi di informazione e social media da parte dei dipendenti

[262] Andrea Monti, «L'offensive cybersecurity di Stato richiede un quadro normativo organizzato», Formiche.net, 8 agosto 2022, https://formiche.net/2022/08/cybersecurity-di-stato-quadro-normativo-organizzato/.

[263] «PNRR e nuova Pa: tra consapevolezza privacy, tecnologie informatiche e social network», NT+ Diritto, https://ntplusdiritto.ilsole24ore.com/art/pnrr-e-nuova-pa-consapevolezza-privacy-tecnologie-informatiche-e-social-network-AE1oV81B.

pubblici, anche al fine di tutelare l'immagine della Pubblica Amministrazione. La guerra in Ucraina ha ridisegnato i modelli di sovranità, anche digitale, e ha costretto gli Stati a ridefinire il perimetro della sicurezza nazionale, ovviamente anche con uno specifico focus alle minacce provenienti dal cyberspazio. Gli Stati e le organizzazioni sovranazionali sono stati bruscamente ricondotti a una riconfigurazione della propria strategia difensiva nella quale oggi gioca un ruolo strategico e irrinunciabile la cybersecurity. Anche il Governo italiano si è mosso in questa direzione, con il decreto legge n. 21 del 21 marzo 2022, che prevede alcune misure urgenti per contrastare gli effetti economici e umanitari della crisi in Ucraina. Tra le numerose azioni previste, il legislatore si è concentrato su un ulteriore rafforzamento dei presidi per la sicurezza, la difesa nazionale e per le reti di comunicazione elettronica, nonché sulla revisione della normativa in materia di "Golden Power"[264]. La novità normativa è di grande impatto: richiede che le imprese, prima di procedere all'acquisizione, a qualsiasi titolo, anche attraverso contratti o accordi, di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di rilevanza strategica, ovvero componenti ad alta intensità tecnologica funzionali alla realizzazione o gestione di attività di rilevanza strategica, notifichino alla Presidenza del Consiglio dei ministri un articolato e complesso "piano annuale", il cui contenuto è minuziosamente dettagliato nel decreto legge e comporta, tra gli altri, anche l'obbligo di specificare la lista dei fornitori attuali e potenziali. Ricevuto il piano annuale, inoltre, la Presidenza del Consiglio dei ministri lo approva entro trenta giorni dalla notifica, prorogabili per due volte di altri venti giorni laddove sia necessario svolgere approfondimenti riguardanti aspetti tecnici, oppure impone specifiche prescrizioni o condizioni

[264] Il legislatore ha infatti previsto una riorganizzazione complessiva dei poteri speciali in materia di comunicazione elettronica a banda larga basati sulla tecnologia 5G, riscrivendo completamente e ampliando il contenuto dell'articolo 1-bis del decreto legge n. 21 del 15 marzo 2012. In questo specifico settore, infatti, il nuovo decreto legge, da un lato, conferma, come attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, dall'altro – ed è qui la prima importante novità – apre anche a tutti gli ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud, che saranno individuati, di concerto con gli altri Ministri competenti, con uno o più decreti successivi del Presidente del Consiglio dei ministri. Dunque si estende, potenzialmente, l'ambito dei servizi digitali strategici, per il momento definiti con una formula generale che dovrà essere oggetto di successiva specificazione (come si è detto sopra: «servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud»).

ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. O ancora la Presidenza del Consiglio approva, in tutto o in parte, il piano per un periodo temporale, anche limitato, indicando un termine per l'eventuale sostituzione di determinati beni o servizi, o infine esercita il potere di veto. Il mancato rispetto delle prescrizioni impartite dalla Presidenza del Consiglio dei ministri in fase di verifica del piano annuale comporta anche l'attivazione di un complesso sistema sanzionatorio, che, in caso di omissione della notifica o di mancata osservanza delle prescrizioni, dà luogo all'applicazione di sanzioni amministrative che possono arrivare fino al 3% del fatturato dell'impresa. Inoltre, sono considerati nulli i contratti o gli accordi compresi nella notifica se eseguiti prima che sia decorso il termine per l'approvazione del piano o in violazione dello stesso. In tali casi, il Governo può ingiungere all'impresa di ripristinare a sue spese la situazione anteriore all'esecuzione, stabilendo il relativo termine, con l'applicazione di ulteriori sanzioni amministrative in caso di ritardi[265]. Per di più, un'ulteriore novità di rilievo è costituita dall'introduzione di un sistema di monitoraggio finalizzato a controllare l'osservanza delle prescrizioni e delle condizioni impartite dal Governo nell'esercizio dei poteri speciali, a verificare la loro adeguatezza e ad appurare l'adozione delle misure attuative, anche tecnologiche, imposte[266]. Le attività di monitoraggio sono svolte da uno specifico comitato composto da uno o più rappresentanti della Presidenza del Consiglio dei ministri e dei Ministeri rilevanti, oltre che dall'Agenzia per la cybersicurezza nazionale, e, se ritenuto necessario, dal Centro di valutazione e certificazione nazionale e dalle articolazioni tecniche dei Ministeri dell'Interno e della Difesa[267]. Peraltro, per agevolare le attività di monitoraggio, le imprese dovranno comunicare – con la periodicità indicata con il provvedimento di esercizio dei poteri

[265] «Ora anche il Cyber Resilience Act a tutela del mercato unico digitale europeo: il punto della situazione in materia di cybersicurezza», NT+ Diritto, https://ntplusdiritto.ilsole24ore.com/art/ora-anche-cyber-resilience-act-tutela-mercato-unico-digitale-europeo-punto-situazione-materia-cybersicurezza-AEWSBR2B.

[266] «La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021», Federico Serini, https://www.federalismi.it.

[267] Il Comitato di monitoraggio dispone della facoltà di svolgere ispezioni e verifiche tecniche, relativamente ai beni e alle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione dei servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché ad altri possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi, oggetto del provvedimento di esercizio dei poteri speciali.

speciali – ogni attività esecutiva posta in essere, fornendo i dettagli tecnici ed evidenziando le ragioni idonee ad assicurare la conformità al piano, nonché inviare una relazione periodica semestrale sulle attività eseguite[268].

[268] Stefano Mele et al., «Sicurezza, settori strategici e banda larga: come cambia la protezione dei dati», Il Sole 24 ORE, 7 aprile 2022, https://www.ilsole24ore.com/art/sicurezza-settori-strategici-e-banda-larga-come-cambia-protezione-dati-AEMjmYPB.

8. Il Golden Power e la disciplina sullo standard 5G nello spettro radio

Il Golden Power è un istituto di matrice britannica introdotto nel nostro ordinamento con il decreto legge 15 marzo 2012 n. 21 per conferire al Governo la facoltà di porre condizioni o veti in caso di tentativi di acquisto "ostile", da parte di una società estera, di un'azienda italiana strategica o attiva in un settore ritenuto fondamentale. L'obiettivo dei poteri speciali è impedire a società estere di approfittare di periodi di crisi per acquistare a prezzi di saldo aziende italiane in forte difficoltà e fare così la propria scalata nel mercato. In linea di massima, i settori interessati sono quelli della difesa, della sicurezza nazionale, dell'energia, dei trasporti e delle comunicazioni. Nel testo del cosiddetto Decreto Liquidità, il Governo ha previsto un'estensione dei Golden Power anche ad altri settori ad oggi considerati di importanza strategica per l'Italia; nello specifico, si tratta dei settori alimentare, assicurativo, sanitario e finanziario[269]. Il Governo, però, non vuole tutelare solo le grandi aziende o i grandi gruppi industriali, ma anche le migliaia di piccole e medie imprese che costituiscono la maggior parte del nostro tessuto produttivo e che, di conseguenza, sono ritenute strategiche e fondamentali al pari delle grandi organizzazioni italiane[270]. Dunque, grazie ai Golden Power, l'esecutivo ha la facoltà di opporsi all'acquisto di determinate partecipazioni, o comunque di dettare delle specifiche condizioni in merito, e può altresì apporre veti sull'adozione di particolari delibere aziendali; in particolare, attraverso l'esercizio dei cosiddetti poteri speciali Palazzo Chigi può intervenire in una pluralità di operazioni societarie, quali fusioni, acquisizioni, cambi di azionariato e, in alcuni casi, scelta dei fornitori. Come ribadito dalla Commissione europea, l'esercizio di tali prerogative deve sempre avvenire in maniera imparziale, obiettiva, tramite criteri resi pubblici e deve al contempo essere giustificato da motivazioni di interesse generale[271]. Nel decreto legge n. 21/2012 (convertito con modificazioni dalla legge n. 56/2012), il legislatore italiano,

[269] «Cos'è il Golden Power? La guida completa», Money.it, 30 aprile 2021, https://www.money.it/Golden-Power-cos-e-significato-come-funziona.

[270] «Golden Power: che cos'è e perché è importante per le nostre imprese?», https://gruppoitalfinance.it/it/update/golden-power-che-cose-e-perche-e-importante-per-le-nostre-imprese.

[271] «Cos'è il Golden Power? La guida completa», Money.it, 30 aprile 2021, https://www.money.it/Golden-Power-cos-e-significato-come-funziona.

adeguandosi alle direttive giurisprudenziali europee, ha previsto l'impiego dei poteri speciali solo in caso di «minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale» e sempre nel rispetto dei principi di proporzionalità e ragionevolezza. L'esercizio dei Golden Power non appare più, come avveniva in passato, veicolato dai fenomeni di privatizzazione, né sembra orientato a mantenere una forma di controllo indiretto sulle società privatizzate: piuttosto, esso è finalizzato a realizzare un sistema di controllo pubblico degli investimenti (sia interni che esteri), apparentemente ispirato al modello adottato negli Stati Uniti[272]. In particolare, i criteri e i principi che stanno alla base dei poteri speciali

[272] Com'è noto, nei primi anni '90 si aprì in Italia la stagione delle cosiddette "privatizzazioni" che ha visto gran parte delle imprese pubbliche (il cui complesso pesava tra 1/3 e 1/4 dell'intera economia nazionale) o trasformate in società per azioni (cosiddetta privatizzazione "fredda") o cedute, totalmente o parzialmente, a soggetti privati (cosiddetta privatizzazione "calda"). Dunque, in quella fase storica, lo Stato – sia con la sostituzione di un regime di diritto pubblico con uno di diritto privato, che con l'effettiva dismissione del controllo societario – ha parzialmente ripudiato il ruolo di "imprenditore" e diretto produttore di beni e servizi, per assumere quello di "regolatore", al fine di assicurare il perseguimento di finalità sociali (quali, ad esempio, il servizio universale o la garanzia di pari concorrenza tra le imprese), nonché il rispetto dei limiti fissati dall'articolo 41 della Costituzione all'iniziativa economica privata (che non può svolgersi in modo da recare danno alla sicurezza, alla libertà e alla dignità umana). Questa nuova dimensione "regolatrice" si è esplicata mediante due ordini di "poteri". Il primo – che, riprendendo l'espressione che fu di Constant, può essere definito come "neutro" ed è quello più squisitamente di tecnica regolatrice – è proprio delle varie Autorità amministrative indipendenti. Il secondo – che si connota per una maggiore carica di "politicità" – è rimasto di competenza dell'esecutivo, e si è tradotto in una serie di poteri "speciali" di limitazione dell'autonomia privata e di intervento nella vita delle società, anche in assenza di una diretta partecipazione azionaria (cosiddetta golden share), attribuiti al Governo, nella figura dei Ministeri dell'Economia e dello Sviluppo economico.
È dal complesso di questi poteri che è emerso l'attuale Golden Power. Il contenuto dei poteri speciali, che fu definito inizialmente nella l. n. 474/1994, si sostanziava nella possibilità di: i) opposizione all'assunzione di partecipazioni rilevanti (superiori a 1/20 del capitale sociale) con divieto di esercizio del voto in attesa del gradimento; ii) opposizione alla costituzione di patti parasociali in cui venga rappresentata almeno 1/20 del capitale sociale; iii) veto all'adozione di delibera di scioglimento della società, di trasferimento dell'azienda, di fusione, di scissione, di trasferimento della sede sociale all'estero, di cambiamento dell'oggetto sociale; iv) nomina di un amministratore senza diritto di voto. L'esercizio di questi poteri è stato oggetto di una rivisitazione con l'articolo 66 della legge n. 488/1999, con cui si è stabilito che i poteri in parola potessero essere «introdotti esclusivamente per rilevanti e imprescindibili motivi di interesse generale, in particolare con riferimento all'ordine pubblico, alla sicurezza pubblica, alla sanità pubblica e alla difesa» e dovessero assumere «forma e misura idonee e proporzionali alla tutela di detti interessi, anche per quanto riguarda i limiti temporali».
In aggiunta a ciò, il ricorso alla golden share avrebbe dovuto essere compatibile con «il rispetto dei principi dell'ordinamento interno e comunitario, e tra questi in primo luogo del principio di non discriminazione» e coerente «con gli obiettivi in materia di privatizzazioni e di tutela della concorrenza e del mercato». In attuazione di questa norma, fu emanato il D.p.c.m. 11.02.2000, poi sostituito dal decreto 10.06.2004, che ha stabilito che i poteri speciali attribuiti dalla legge n. 474/1994 potessero essere esercitati esclusivamente nel caso di «rilevanti e imprescindibili motivi di interesse generale, in particolare con riferimento all'ordine pubblico». Rispetto a quanto previsto dalla legge n. 474/1994, il decreto in parola ha tentato di circoscrivere ulteriormente l'ambito di estensione dei poteri speciali, al fine di limitare la discrezionalità del governo in ordine al loro utilizzo: si trattò di un intervento resosi necessario a causa della procedura di infrazione aperta dalla Commissione europea nei confronti dell'Italia, accusata di ricorrere alla golden share in ottica protezionistica, di fatto limitando l'ingresso di investitori stranieri nelle società privatizzate.

sono stati espressamente enunciati nella legge e la valutazione della sussistenza delle condizioni per l'esercizio dei Golden Power è assistita dalla garanzia di un sindacato giurisdizionale rigoroso e veloce di fronte al TAR del Lazio. In questo modo, il legislatore italiano sembrava aver aderito al modello di golden power "virtuoso" descritto dalla giurisprudenza europea, ma questo equilibrio non è durato per molto[273]. Con il decreto legge n. 148/2017, convertito con legge n. 172/2017, il legislatore è intervenuto sulla disciplina dettata dal decreto legge n. 21/2012, estendendo l'esercizio dei poteri speciali applicabili nei settori dell'energia, delle comunicazioni e dei trasporti agli asset «ad alta intensità tecnologica». È sufficiente scorrere rapidamente l'elenco esemplificativo della nozione di asset «ad alta intensità tecnologica», per rendersi immediatamente conto di come quest'ultima si caratterizzi per una notevole ampiezza (e vaghezza) rispetto alle scelte adottate dal D.P.R. n. 85/2014 sull'individuazione degli asset nei settori dell'energia, dei trasporti e delle comunicazioni. Infatti, il decreto in parola fa riferimento oltre alle infrastrutture critiche o sensibili, tra cui vi rientra il settore dell'immagazzinamento e di gestione dati delle strutture finanziarie, anche alle tecnologie critiche (compresa l'intelligenza artificiale, la robotica, i semiconduttori, le tecnologie con

---

Ciononostante, anche la nuova disciplina è stata censurata dalla Corte di Giustizia europea (con sentenza 26.03.2009, in causa C-326/07), in quanto accordava alle autorità nazionali un ambito di valutazione discrezionale eccessivo. Si deve evidenziare come il complesso delle sentenze della CGUE in materia di golden share abbia delineato uno «schema logico al quale si dovrebbe rigidamente attenere il legislatore nazionale ogni volta che si ponga l'eventualità di introdurre restrizioni al dispiegamento delle libertà previste dal TFUE».

In una serie di consequenziali pronunce, la Corte ha precisato che il ricorso ai poteri speciali è consentito solo a patto di soddisfare quattro condizioni: i) non deve essere discriminatorio; ii) deve essere giustificato da motivi imperativi di interesse generale, dovendosi in ogni caso escludere qualsiasi giustificazione di ordine economico (Commissione c. Repubblica portoghese, C-367/98, § 52), e fermo restando che una simile deroga alle norme del diritto europeo va sempre interpretata in senso restrittivo (Commissione c. Regno di Spagna, C-463/00, § 34) ed è pertanto ammessa soltanto in presenza di una «minaccia effettiva ed abbastanza grave ad uno degli interessi fondamentali della collettività» (Commissione c. Repubblica francese, C-483/99, § 48); iii) deve essere idoneo e necessario a garantire il conseguimento dell'obiettivo fissato; iv) deve rispettare il principio di proporzionalità e, quindi, non andare oltre quanto strettamente necessario per il raggiungimento dell'obiettivo (Commissione c. Repubblica italiana, C-58/99, § 13). Queste indicazioni, unitamente a quelle contenute nell'importante sentenza Commissione c. Belgio (C-503/ 99), hanno disegnato i contorni di un modello di golden share "virtuoso", che – pertanto – deve prevedere l'esistenza di un chiaro testo normativo che regoli il potere speciale, l'esplicarsi del potere sotto forma di controllo successivo e non di autorizzazione preventiva, la fissazione di un termine preciso per proporre, da parte dell'impresa interessata, opposizione alla decisione di esercizio del potere, ed infine, la previsione di uno specifico obbligo di motivazione per l'atto di esercizio del potere. *Ibl-Istituto Bruno Leoni, «Golden power, 5G e cybersicurezza: "non è tutto oro quel che luccica"», Filodiritto, https://www.filodiritto.com/golden-power-5g-e-cybersicurezza-non-e-tutto-oro-quel-che-luccica.*

[273] Gabriele Carrer, «Agenzia cyber. Cosa farà il Cvcn per mettere il 5G al sicuro», Formiche.net, 1 luglio 2022, https://formiche.net/2022/07/agenzia-cyber-cvcn-5g/.

potenziali applicazioni a doppio uso, la sicurezza in rete, la tecnologia spaziale o nucleare), alla sicurezza dell'approvvigionamento di input critici, ed infine all'accesso a informazioni sensibili, ossia alla capacità di controllare tali dati. Si tratta di un cambio di prospettiva notevole perché, con il decreto legge n. 21/2012 (e successivo D.P.R. n. 85/2014), gli operatori economici ricevevano un adeguato preavviso sulla possibilità di essere soggetti all'esercizio dei poteri speciali da parte del Governo, visto che era sufficiente verificare che la società oggetto di acquisizione operasse nei settori della difesa militare e della sicurezza nazionale o possedesse uno degli asset nei settori dell'energia, dei trasporti e delle comunicazioni. Per contro, con il decreto legge n. 148/2017, gli operatori hanno perso la possibilità di godere di questo preavviso dal momento in cui il catalogo degli asset è troppo vasto e vago: è evidente che, con la riforma del 2017, il legislatore abbia deciso di rendere molto più pervasivo e ordinario il ricorso ai poteri speciali[274].

Altri aspetti di novità apportati dal decreto del 2017 sono che esso trova applicazione principalmente nel caso in cui l'acquisto a qualsiasi titolo di partecipazioni in società che detengono gli asset strategici avvenga da parte di un soggetto esterno all'Unione europea[275]. Inoltre, il Governo può esercitare i poteri speciali non solo quando questo acquisto comporti una minaccia di grave pregiudizio agli interessi essenziali dello Stato (cioè relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti), ma anche quando esso possa costituire un pericolo per la sicurezza o per l'ordine pubblico[276]. Per determinare se un investimento estero possa incidere sulla sicurezza o sull'ordine pubblico, il decreto legge prevede la possibilità di prendere in considerazione la circostanza per cui l'investitore straniero sia controllato dal governo di un paese terzo, non appartenente all'Unione europea (anche attraverso finanziamenti significativi), oppure quella per cui si sospettino la sussistenza di legami fra l'acquirente e paesi terzi che non riconoscano

[274] Ibl-Istituto Bruno Leoni, «Golden power, 5G e cybersicurezza: "non è tutto oro quel che luccica"», Filodiritto, https://www.filodiritto.com/golden-power-5g-e-cybersicurezza-non-e-tutto-oro-quel-che-luccica.

[275] «Decreto cybersicurezza / Golden power più forte», Il Sole 24 ORE, 7 novembre 2019, https://www.ilsole24ore.com/art/decreto-cybersicurezza-golden-power-piu-forte-ACPv4Rx.

[276] Federica De Vincentis, «Draghi allarga il golden power. 5G, software russi e le altre novità», Formiche.net, 18 marzo 2022, https://formiche.net/2022/03/draghi-golden-power-5g/.

i principi di democrazia o dello Stato di diritto, che non rispettino le norme del diritto internazionale o che abbiano assunto comportamenti a rischio nei confronti della comunità internazionale o, ancora, abbiano rapporti con organizzazioni criminali o terroristiche o con soggetti ad esse comunque collegati[277]. Dopo la riforma del 2017, il Governo è nuovamente intervenuto sulla disciplina dei Golden Power; in seguito ad un primo tentativo da parte del Governo Conte di disciplinare il tema della sicurezza informatica nazionale (attraverso il decreto legge n. 64/2019, di cui non è stata promossa la conversione in legge), l'Esecutivo ha approvato il cosiddetto decreto Cybersicurezza[278]. Peraltro, al principio del 2019 il Governo aveva già licenziato il decreto legge n. 22/2019 (cosiddetto decreto Brexit) con il quale ha scelto di assoggettare all'esercizio dei poteri speciali i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, in quanto ritenuti attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Per effetto di questo ultimo intervento normativo, oltre alle attività già considerate dal decreto legge n. 21/2012, vanno notificate al Governo tanto la stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti, quanto l'acquisizione di componenti ad alta intensità tecnologica, quando posti in essere con soggetti esterni all'Unione europea. Su questo impianto si innesta il decreto legge Cybersicurezza, con cui il Governo ha istituito il Perimetro di sicurezza nazionale cibernetica, all'interno del quale verranno fatte confluire una serie di amministrazioni pubbliche, di enti e di operatori nazionali, pubblici e privati, che esercitano una funzione essenziale dello Stato ovvero un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, dalla cui interruzione o dal cui malfunzionamento potrebbe derivare un pregiudizio per la sicurezza nazionale[279]. Questi soggetti, quando intendano procedere all'affidamento di forniture

[277] NIS Cooperation Group, «EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks», 9 ottobre 2019.

[278] Redazione FIRSTonline, «Golden Power e cybersicurezza: la stretta del Governo per cloud della Pa, tlc e difesa», FIRSTonline, 19 marzo 2022, https://www.firstonline.info/golden-power-e-cybersicurezza-la-stretta-del-governo-per-cloud-della-pa-tlc-e-difesa/.

[279] Inoltre, è stata prevista la possibilità per il Governo di ordinare la modificazione o l'integrazione delle condizioni e delle prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati – e attinenti alle reti, ai sistemi informativi e ai servizi informatici gestiti dai soggetti che ricadano nel Perimetro di sicurezza nazionale cibernetica –

di beni, di sistemi e di servizi ICT, devono darne comunicazione al CVCN istituito presso il Ministero dello sviluppo economico, che, sulla base di una valutazione del rischio, può, entro trenta giorni dalla comunicazione, imporre condizioni e test di hardware e software[280]. Infine, occorre tenere in considerazione il problema dei costi che questa ulteriore interferenza governativa comporta: a quelli imposti dai singoli obblighi informativi sulle parti impegnate nelle compravendite si aggiungono i rischi connessi ai tempi di risposta del Governo per il ricorso ai poteri speciali e alla possibilità di un ricorso giurisdizionale al TAR, nel caso in cui la decisione dell'Esecutivo sia opposta dalle imprese. Tali costi possono essere tollerati laddove l'esercizio dei Golden Power sia un evento straordinario nella vita delle imprese, in quanto proprio solo di determinati settori o perché connesso a eventi infrequenti, quale il mutamento degli assetti proprietari. Invece, se il ricorso ai poteri speciali diventa una costante ordinaria, in quanto legato al possesso di singoli asset o ad accadimenti di ricorrente frequenza (quali le

anche imponendo, se ritenuto necessario, la sostituzione di apparati o prodotti giudicati come «gravemente inadeguati sul piano della sicurezza».

[280] Gli ultimi interventi governativi confermano la nuova impostazione dei poteri speciali come parte di un modello di controllo degli investimenti stranieri; dai loro antecedenti storici, come detto, essi si distanziano per l'applicazione speciale nei confronti dei soggetti extra-UE e per l'estensione dell'ambito di esercizio dei poteri in parola. Quanto al primo aspetto, è sufficiente ricordare come uno dei punti di forza della disciplina del Golden Power delineata dal decreto legge n. 21/2012 sia stato proprio quello di escludere una diversità di trattamento degli investimenti nei settori ritenuti strategici in ragione della nazionalità dell'investitore, applicandosi a qualsiasi investitore, fosse esso nazionale, di Stati membri o di Paesi terzi (questi ultimi vincolati a regime di reciprocità e a scrutinio separato in caso di stabilimento, nei settori dell'energia, dei trasporti e delle comunicazioni). Di contro, una disciplina pensata ad hoc per i soggetti esterni all'Unione rischia di non superare censure di ingiustificata discriminazione e sospetti di malcelato protezionismo. Quanto al secondo aspetto, è chiaro che – in un'ottica di rispetto delle ordinarie dinamiche di mercato – l'esercizio dei poteri speciali ha senso solo laddove esso sia circoscritto a limitati settori (o, meglio, asset) e sia dipendente dal verificarsi di accadimenti, interni alla vita della società, di un certo rilievo (come sono, per l'appunto, i casi disciplinati dal decreto-legge n. 21/2012: che fanno riferimento, essenzialmente, a modifiche del controllo o della struttura societari). Le modifiche introdotte dalle riforme del 2017-2019 si sono allontanate da questa prospettiva, per abbracciarne una di sempre maggiore estensione del ricorso ai Golden Power, sia – come nel caso del decreto legge n. 148/2017 – concentrandosi sui singoli asset, anziché sui settori, che – come fatto dal decreto Brexit – rendono rilevanti non solo gli eventi straordinari, ma anche quelli ordinari, quali i contratti o gli accordi aventi ad oggetto l'acquisto di beni o servizi relativi perfino alla mera manutenzione e gestione delle reti (in tutta evidenza, il decreto cyber sicurezza si inserisce nella medesima ottica di progressiva estensione dell'impiego dei poteri speciali in parola). In questo modo, il modello di controllo che è stato descritto subisce una chiara torsione verso una maggiore incisività e intromissione nell'iniziativa economica privata. Si guardi, in particolare, agli effetti del decreto Brexit: non è ragionevole ritenere che il mero procurement di componenti per la manutenzione di una rete possa rappresentare un'occasione di rischio per la sicurezza nazionale, come ha dimostrato il caso Fastweb-Samsung. È indubbio che, nei settori strategici, possano ritrovarsi esigenze di tutela di interessi sensibili, ma allora è quantomeno opportuno che il Governo eserciti *cum grano salis* i propri poteri speciali. *«Decreto cybersicurezza / Golden power più forte», Il Sole 24 ORE, 7 novembre 2019, https://www.ilsole24ore.com/art/decreto-cybersicurezza-golden-power-piu-forte-ACPv4Rx.*

attività legate alla manutenzione delle reti), quei costi non sono più un fardello giustificato dalla tutela di interessi superiori, ma si traducono in un ostacolo sulla via della crescita economica. L'impressione è che la valutazione di strategicità di un settore o di un'attività non sia frutto di una considerazione obiettiva, rigorosa e di lungo periodo, ma tradisca un momentaneo interesse dell'esecutivo *pro tempore* a presidiare un determinato comparto economico. Come anticipato, il Governo Conte, con il decreto legge 21 settembre 2019 n. 105 (cosiddetto decreto Cybersicurezza) convertito in legge 18 novembre 2019 n. 139, ha esteso l'ambito di applicazione dei Golden Power alle tecnologie 5G in attuazione delle direttive eurounitarie[281]. In particolare, è stata prevista una riorganizzazione dei poteri speciali per la comunicazione elettronica a banda larga basati sulla tecnologia 5G, confermando questo settore come strategico per la difesa nazionale e, di conseguenza, dando spazio anche ad altri settori che contribuiscono alla sicurezza cibernetica, come quelli legati alla tecnologia cloud[282]. Per garantire il rispetto e la giusta applicazione delle prescrizioni adottate dal Governo nell'esercizio dei poteri speciali è stato istituito un Comitato di monitoraggio e di controllo composto da uno o più rappresentanti della Presidenza del Consiglio dei ministri, del Ministero dello sviluppo economico, del Ministero della difesa, del Ministero per l'innovazione tecnologica e la transizione digitale, dell'Agenzia per la Cybersicurezza nazionale, oltre che, se ritenuto necessario, del Centro di valutazione e certificazione nazionale (CVCN) e delle articolazioni tecniche dei Ministeri dell'Interno e della Difesa. Le imprese devono agevolare quest'azione di controllo comunicando tutte le attività esecutive, evidenziandone i dettagli tecnici, e presentando una relazione semestrale sulle attività eseguite[283]. Il Comitato di monitoraggio può, infine, mettere in atto ispezioni e verifiche tecniche relativamente ai beni e alle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione dei servizi di comunicazione elettronica a banda larga basati

[281] «Cybersicurezza è legge, ampliata la golden power anche su 5G», rainews, https://www.rainews.it/dl/rainews/articoli/Cyber-sicurezza-legga-150b4d7e-a7a8-4a45-a2a0-d30f47311d98.html.

[282] «Come cambia la Golden Power dell'Italia (5G, cloud, cyber)», Cyber Security 360 (blog), 25 marzo 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/come-cambia-la-golden-power-dellitalia-5g-cloud-cyber/.

[283] NIS Cooperation Group, «Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures», gennaio 2020.

sulla tecnologia 5G, nonché ad altri possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi ICT[284].

[284] «Golden Power, la proposta alla luce della guerra in Ucraina: tre linee di intervento rapido», Cyber Security 360 (blog), 21 marzo 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/golden-power-la-proposta-alla-luce-della-guerra-in-ucraina-tre-linee-di-intervento-rapido/.

9. Il Framework Nazionale del CINI e le Linee Guida ISO

Nel 2015 è stato presentato il Framework Nazionale per la Cybersecurity, frutto della collaborazione tra accademia, enti pubblici, e imprese private. Il Framework, ispirato al Cybersecurity Framework ideato dal NIST[285], fornisce uno strumento operativo per organizzare i processi di cybersecurity adatto alle organizzazioni pubbliche e private, di qualunque dimensione. In particolare, supporta le organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. Rispetto alla versione del 2015, quella presentata dal Cyber Security National Lab del CINI[286] nel febbraio del 2019 introduce contributi volti a cogliere gli aspetti fondamentali legati alla protezione dei dati secondo quanto previsto nel Regolamento GDPR. Il Framework Nazionale per la Cybersecurity e la Data Protection aiuta le organizzazioni nel definire un percorso volto alla cybersecurity e alla protezione dei dati riducendo i costi necessari e aumentando l'efficacia delle misure realizzate. Inoltre, per le organizzazioni che già implementano misure coerenti con il Regolamento, il Framework può rappresentare un utile strumento per guidare le necessarie attività di continuo monitoraggio[287]. Si introducono le tre nozioni fondamentali di Framework Core, Profile e Implementation Tier. Il Framework Core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico che organizzativo ed è strutturato gerarchicamente in function, category e subcategory. Il Framework definisce, per ogni function, category e subcategory, le attività abilitanti, quali processi e tecnologie, da realizzare per gestire la singola function. A questo scopo il Framework Core associa ad ogni singola subcategory i riferimenti alle pratiche di sicurezza previste da standard di settore o da regolamentazioni generali vigenti, che sono il punto di partenza per una implementazione corretta e sicura. Il Framework Core presenta inoltre delle informative *reference*, ossia riferimenti che legano la singola subcategory alle pratiche di sicurezza note previste da standard di settore ISO o da

[285] National Institute of Standards and Technology.

[286] Consorzio Interuniversitario Nazionale per l'Informatica.

[287] CINI - Cyber Security National Labs, «Framework Nazionale per la Cybersecurity e la Data Protection», 2019.

regolamentazioni generali vigenti quali il Regolamento GDPR e la Direttiva NIS. Il Profile rappresenta il risultato della selezione di specifiche subcategory del Framework, basata su diversi fattori quali la valutazione del rischio, il contesto di business, l'applicabilità delle varie subcategory all'organizzazione. I Profili possono anche essere utilizzati come opportunità per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale con il profilo desiderato. Infine, gli Implementation Tier forniscono contesto sul livello di integrazione dei processi di gestione del rischio cyber.

La nuova versione del Framework ha integrato i cambiamenti apportati dal NIST al Framework Core, includendo elementi volti a considerare le problematiche di sicurezza delle filiere di approvvigionamento e ad approfondire la sicurezza dei processi di autenticazione e gestione delle identità. La nuova versione include inoltre una serie di nuovi elementi indirizzati a guidare la corretta gestione dei dati personali, con specifico riferimento alla sicurezza degli stessi a fronte di possibili attacchi informatici[288]. L'utilizzo del Framework si realizza attraverso due attività fondamentali che sono la contestualizzazione del Framework ad uno specifico ambito applicativo e l'applicazione dello stesso ad una organizzazione. Contestualizzare il Framework per un ambito applicativo significa specificare il suo core selezionando le function, category e subcategory rilevanti, e definire i livelli di priorità e maturità per le subcategory selezionate. L'illusione che solo le grandi imprese siano bersaglio di attacchi da parte dei cyber criminali lascia spesso le medie, piccole e micro imprese totalmente impreparate ad affrontare la minaccia cyber. Ciò non solo espone le imprese stesse a minacce in grado di minarne la sopravvivenza, ma aumenta il rischio cyber all'interno dell'intera filiera produttiva in cui esse operano. Per tali imprese implementare una gestione del rischio cyber basata sul Framework Nazionale può risultare troppo complesso e oneroso; in quest'ottica nell'Italian Cybersecurity Report del 2016 sono stati proposti 15 Controlli Essenziali di Cybersecurity derivati dal

[288] A tale scopo sono state introdotte nove nuove subcategory e una nuova category che colgono i seguenti aspetti legati alla data protection: i processi di data management, con particolare riferimento a quelli applicabili ai dati personali; le modalità di trattamento dei dati personali; i ruoli e le responsabilità nella gestione dei dati personali; la valutazione di impatto sulla protezione dei dati personali; infine, le modalità di documentazione e comunicazione a seguito di incidenti che si configurino come violazione dei dati personali.

Framework Nazionale attraverso un processo di progressiva semplificazione. La sola implementazione di questi 15 controlli non assicura un livello adeguato di sicurezza, essi rappresentano un insieme minimo di pratiche di sicurezza che non possono essere ignorate. I quindici controlli essenziali sono organizzati in otto tematiche di cybersecurity riguardanti l'inventario di dispositivi e software, la governance, la protezione da maleware, la gestione password e account, la formazione e consapevolezza, la protezione dei dati e delle reti e, infine, la prevenzione e mitigazione[289]. Dunque, lo scopo del Framework nazionale è quello di fornire una guida agli operatori del settore e fissare quelle che sono, a livello astratto, le attività principali da eseguire al fine di intraprendere un efficace programma di miglioramento della sicurezza di un'infrastruttura informatica. A fini esemplificativi, tali funzioni potrebbero essere paragonate alle attività di identificazione, raccolta, acquisizione e conservazione delle evidenze digitali descritte nello standard ISO/IEC 27037 relativo all'ambito della digital forensics. Come nello Standard, infatti, vengono indicate le varie fasi attraverso le quali un operatore forense si dovrebbe muovere al fine di trattare correttamente le possibili fonti di prova digitali, in modo similare nel framework si cerca di guidare l'operatore di fase in fase in un processo ciclico che dovrà essere periodicamente applicato. La prima funzione indicata nel Framework è quella di identificazione (*identify function*); occorre mettere a fuoco quello che è il contesto organizzativo comprendendo elementi quali l'ambito applicativo dell'organizzazione, l'ambiente esterno e gli asset da tutelare. La seconda funzione dettata nel Framework è quella di protezione (*protect function*), fase in cui si vanno a identificare quelle soluzioni che hanno il ruolo di impedire il verificarsi di un incidente di sicurezza informatico o, quantomeno, di mitigarne gli effetti negativi. La terza funzione è quella di rilevamento (*detect function*), nella quale vengono indicate delle metodologie volte a rilevare e identificare degli eventi potenzialmente configurabili come incidenti informatici. Altra funzione è quella di risposta (*respond function*), che riguarda quell'insieme di attività che dovrebbero essere intraprese al verificarsi di un incidente di sicurezza. Obiettivo di queste attività è, dunque, ridurre il più

[289] «Framework Nazionale per la Cybersecurity e la Data Protection | Framework Nazionale per la Cyber Security e la Data Protection», https://www.cybersecurityframework.it/framework2.

possibile l'impatto che, con i relativi effettivi negativi, l'incidente ha provocato all'interno dell'infrastruttura organizzativa. Infine, l'ultima funzione è quella di ripristino (*recover function*) in quanto una volta che l'incidente è stato rilevato e gestito bisognerà ripristinare lo stato dell'infrastruttura a una situazione di normalità[290].

All'interno del Framework nazionale, è necessario fare menzione di due importanti linee guida ISO[291]. La nuova ISO/IEC 27001:2022[292], datata il 25 ottobre 2022, è la norma di riferimento sui Sistemi di gestione della sicurezza delle informazioni che prevede requisiti e controlli per garantire il rispetto dello standard. Il suo obiettivo è quello di fornire alle organizzazioni gli strumenti di base per proteggere il patrimonio delle informazioni, compresi i dati personali, al fine di riflettere l'evoluzione digitale e le nuove pratiche aziendali che diventano sempre più cloud e interconnesse. I princìpi che hanno guidato la nuova revisione della norma sono orientati a garantire, oltre alla disponibilità, riservatezza dei dati e all'approccio dinamico basato sull'individuazione delle minacce e delle vulnerabilità, anche la protezione delle informazioni, l'aumento della resilienza agli attacchi informatici e l'eliminazione di misure che si dimostrano inefficaci[293]. Rispetto alla precedente versione del 2013, la disciplina dei controlli ha subìto modifiche rilevanti passando da 114 a 93 (alcuni controlli sono stati accorpati) riorganizzati in quattro sezioni (organizzativa, personale, fisica e tecnologica) invece delle precedenti quattordici ed introducendo 11 nuovi controlli[294]. Nella nuova ISO è introdotto il concetto di attributi, i quali sono suddivisi in cinque gruppi riguardanti il tipo di controllo, la proprietà di sicurezza delle informazioni, i concetti di cybersecurity, le capacità operative e i domini di sicurezza. La ISO 2700/1 è, quindi, uno standard di conformità che presenta molti

---

[290] https://www.agendadigitale.eu/giornalista/alessandro-cortina e https://www.agendadigitale.eu/giornalista/simone-bonavita, «NIST Cybersecurity Framework: una roadmap per la sicurezza delle infrastrutture», Agenda Digitale, 30 settembre 2021, https://www.agendadigitale.eu/sicurezza/nist-cybersecurity-framework-una-roadmap-per-la-sicurezza-delle-infrastrutture/.

[291] L'Organizzazione internazionale per la normazione (in inglese International Organization for Standardization, abbreviazione ISO) è la più importante organizzazione a livello mondiale per la definizione di norme tecniche.

[292] È intitolata "Information security, cybersecurity and privacy protection – Information security management systems – Requirements".

[293] «La nuova ISO/IEC 27001:2022», https://officialblog.7consulting.net/post/2022/11/08/La-nuova-ISOIEC-270012022.aspx.

[294] «La ISO/IEC 27001: le novità dell'edizione 2022», 27 ottobre 2022, https://www.newcert.it/nuova-iso-iec-27001-2022.

elementi in comune con il Regolamento GDPR, in quanto si tratta di uno dei più dettagliati standard di best practice e può essere utilizzata come elemento dimostrativo della conformità al GDPR in merito all'adesione ai codici di condotta e alle certificazioni approvate. La ISO 2700/1 fornisce i requisiti per l'implementazione, il mantenimento e il miglioramento di un sistema di gestione della sicurezza delle informazioni (ISMS)[295]. La ISO 2700/1 attua diversi standard stabiliti nel GDPR, primo fra tutti quello della riservatezza, della confidenzialità e dell'integrità dei dati. Infatti, nel GDPR sono specificati i principi generali per l'elaborazione dei dati, come la protezione contro l'elaborazione non autorizzata o non conforme alla legge, la perdita, la distruzione o danni accidentali; vengono inoltre date linee guida più dettagliate che specificano che le organizzazioni sono tenute ad attuare, operare e mantenere misure tecniche e organizzative per assicurare la sicurezza dei dati, come la crittografia, la resilienza dei sistemi e dei servizi di elaborazione, la capacità di ripristinare la disponibilità dei dati personali tempestivamente e molto altro. Allo stesso modo, molti controlli nella ISO 2700/1 mirano ad aiutare le organizzazioni a garantire la riservatezza, la disponibilità e l'integrità dei dati. Partendo dalla clausola 4, la ISO 2700/1 richiede alle organizzazioni di identificare i problemi interni ed esterni che potrebbero avere impatto sui programmi di sicurezza; la clausola 6 richiede loro di determinare i propri obiettivi di sicurezza IT e di creare un programma di sicurezza che li aiuti a raggiungere tali obiettivi; ancora, la clausola 8 stabilisce gli standard per la manutenzione continua del programma di sicurezza e richiede all'organizzazione di documentare lo stesso programma per dimostrarne la conformità normativa. Riguardo alla valutazione del rischio, sia la ISO 2700/1 sia il GDPR richiedono un approccio alla sicurezza dei dati basato sul rischio; il GDPR richiede alle aziende di eseguire delle valutazioni dell'impatto sulla protezione dei dati per valutare ed identificare i rischi per i dati delle persone. Queste valutazioni sono obbligatorie prima di intraprendere dei processi ad alto rischio, come il monitoraggio sistematico dei dati estremamente sensibili. La ISO 2700/1 consiglia a tutte le organizzazioni di condurre delle valutazioni accurate del rischio per identificare minacce e

[295] Un ISMS è una struttura di politiche e procedure che include i controlli legali, tecnici e fisici coinvolti nei processi di gestione dei rischi IT di un'azienda. I fattori che influenzano l'implementazione dell'ISMS includono gli obiettivi dell'organizzazione, i requisiti di sicurezza, le dimensioni e la struttura.

vulnerabilità che potrebbero influire sulle attività, e per selezionare delle appropriate misure di sicurezza delle informazioni basate sui risultati della valutazione del rischio. Ancora, secondo il GDPR le aziende devono notificare le autorità entro 72 ore dalla scoperta di una violazione dei dati personali; anche gli interessati devono essere informati senza indebito ritardo, ma solo se i dati rappresentano un alto rischio per i diritti e la libertà delle persone interessate. Così, la ISO 2700/1, che affronta i controlli di gestione delle informazioni sulla sicurezza degli incidenti, non specifica un lasso di tempo esatto per la notifica di violazione dei dati, ma afferma che le organizzazioni devono segnalare tempestivamente gli incidenti sulla sicurezza e comunicare questi eventi in modo da consentire che tempestivamente si avviino azioni correttive. Infine, per quanto riguarda la conservazione dei registri, il GDPR richiede alle organizzazioni di conservare dei registri delle loro attività di trattamento, comprese le categorie di dati, le finalità del trattamento e una descrizione generale delle misure tecniche e organizzative rilevanti per la sicurezza. Allo stesso modo, la ISO 2700/1 afferma che le organizzazioni devono documentare i loro processi di sicurezza, nonché i risultati delle loro valutazioni del rischio di sicurezza e del trattamento del rischio; le attività di informazione devono essere inventariate e classificate, i proprietari di attività devono essere assegnati e le procedure per l'utilizzo di dati accettabili devono essere definite. Nonostante quanto appena illustrato, ci sono molte differenze tra i due standard in quanto il GDPR è uno standard completo che fornisce una visione strategica di come le organizzazioni devono garantire la riservatezza dei dati, mentre la ISO 2700/1 è un insieme di best practice con un'attenzione particolare alla sicurezza delle informazioni e fornisce consigli pratici su come proteggere le informazioni stesse e ridurre le minacce informatiche. In particolare, la ISO 2700/1 non copre direttamente gli aspetti associati alla privacy dei dati, che sono delineati invece nel GDPR. Quest'ultimo si concentra sulla privacy dei dati e sulla protezione delle informazioni personali in maniera organica e completa, richiede alle organizzazioni maggiori sforzi per ottenere il consenso esplicito per la raccolta dei dati e garantire che tutti i dati siano trattati in modo lecito. Tuttavia, manca di dettagli tecnici organizzati a sistema su come mantenere un livello appropriato di sicurezza dei dati o attenuare le minacce interne ed esterne. A questo proposito si integra molto

bene con la ISO 27001 che traduce in pratica alcuni principi fondamentali del GDPR. Fornisce, infatti, informazioni pratiche su come sviluppare politiche chiare e complete per ridurre al minimo i rischi per la sicurezza che potrebbero portare a incidenti di sicurezza[296].

L'altra ISO che merita essere menzionata è la nuova versione della ISO/IEC 2700/5[297], pubblicata a ottobre 2022, sulla valutazione del rischio relativo alla sicurezza delle informazioni, la quale introduce alcuni cambiamenti significativi, ma le difficoltà riscontrate nel corso della lunga gestazione della norma si manifestano in molti passaggi incoerenti e imprecisi. I cambiamenti più significativi sono riportati nell'introduzione e riguardano l'allineamento del testo con la ISO/IEC 2700/1. Sono stati altresì introdotti concetti relativi agli scenari di rischio e, per quanto riguarda l'identificazione del rischio, si descrive l'approccio basato sugli eventi in alternativa a quello basato sugli asset[298]. La norma riporta l'approccio di valutazione del rischio già presente nelle precedenti versioni, il quale prevede che i rischi vengano identificati e valutati attraverso un'ispezione degli asset, delle minacce e delle vulnerabilità. Nella ISO/IEC 2700/5 l'approccio basato sugli eventi prevede di identificare scenari strategici attraverso una considerazione delle sorgenti di minaccia e di come esse possono usare o impattare parti interessate per soddisfare gli obiettivi di rischio desiderati. I rischi possono essere identificati e valutati attraverso una valutazione di eventi e conseguenze, i quali possono essere spesso determinati dalla scoperta delle preoccupazioni dell'alta direzione, dei proprietari di rischi e dei requisiti identificati nella determinazione del contesto dell'organizzazione[299]. In conclusione, la ISO/IEC 2700/5 promuove un approccio alla valutazione del rischio ritenuto troppo rigido e non sempre consigliabile in quanto basato su

[296] https://www.cybersecurity360.it/giornalista/giuliano-mandotti, «ISO 27001 e GDPR, linee guida per mettere al sicuro i dati aziendali», Cyber Security 360 (blog), 6 febbraio 2019, https://www.cybersecurity360.it/legal/privacy-dati-personali/iso-27001-e-gdpr-linee-guida-per-mettere-al-sicuro-i-dati-aziendali/.

[297] Il titolo attuale è "Information security, cybersecurity and privacy protection – Guidance on managing information security risks".

[298]Cesare Gallotti, «Nuova edizione della ISO/IEC 27005 "Information security risk management"», ICT Security Magazine, 2 novembre 2018, https://www.ictsecuritymagazine.com/articoli/nuova-edizione-della-iso-iec-27005-information-security-risk-management/.

[299] https://www.agendadigitale.eu/giornalista/cesare-gallotti, «Sicurezza delle informazioni, la nuova ISO/IEC 27005 sulla valutazione del rischio», Agenda Digitale, 24 aprile 2023, https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-la-nuova-iso-iec-27005-sulla-valutazione-del-rischio/.

metodi obsoleti, utilizzati quando la sicurezza delle informazioni era decisamente diversa da quella attuale[300].

Con la pubblicazione del DPCM n. 81/2021 il processo di attuazione della normativa sul Perimetro di Sicurezza Nazionale Cibernetica entra nel suo vivo. Questo regolamento, infatti, da un lato definisce gli obblighi di notifica degli incidenti aventi un impatto sulle reti, i sistemi informativi e i servizi informatici deputati allo svolgimento di una funzione essenziale per gli interessi dello Stato o all'erogazione di un servizio essenziale, dall'altro obbliga gli operatori pubblici e privati inclusi in questa normativa all'adozione di una fitta trama di misure di sicurezza basate principalmente sul Cybersecurity Framework del National Institute of Standards and Technology (Nist) americano. Importante novità riguarda, anzitutto, la previsione dell'obbligo di condivisione degli incidenti solo nel caso in cui l'autorità giudiziaria non abbia comunicato la sussistenza di specifiche esigenze di segretezza investigativa. Inoltre, i dati digitali trattati mediante l'impiego di beni ICT, ivi compresi quelli relativi alla descrizione degli stessi beni, la cui compromissione sotto il profilo della disponibilità, integrità e riservatezza può avere un impatto sullo svolgimento delle funzioni o dei servizi essenziali per i quali il soggetto è stato incluso nel Perimetro, devono essere conservati, elaborati ovvero estratti esclusivamente mediante l'impiego di infrastrutture fisiche e tecnologiche, anche se esternalizzate (ad esempio, tramite cloud computing), localizzate sul territorio nazionale[301]. Qualora opportunamente cifrati, i dati digitali di backup, anche se esternalizzati, possono essere conservati al di fuori del territorio nazionale, ma non al di fuori del territorio dell'Unione europea e le chiavi di cifratura devono essere comunque custodite all'interno del territorio nazionale. Le operazioni di cifratura e decifratura devono comunque essere eseguite mediante infrastrutture localizzate sul territorio nazionale. Complessivamente, quindi, seppure sia senz'altro apprezzabile lo sforzo fatto dal legislatore per aprire in alcuni casi a soluzioni entro i confini dell'Unione europea, appaiono persistere ancora alcuni dubbi sulle richieste prodotte,

[300] «ISO 27001: Come effettuare una valutazione dei rischi in 5 fasi – IT Governance Blog IT», https://www.itgovernance.eu/blog/it/iso-27001-come-effettuare-una-valutazione-dei-rischi-in-5-fasi.

[301] Stefano Mele, «Cosa c'è nel nuovo Dpcm del perimetro cyber. L'analisi di Mele», Formiche.net, 14 giugno 2021, https://formiche.net/2021/06/cosa-ce-nel-nuovo-dpcm-del-perimetro-cyber-lanalisi-di-mele/.

che continuano a soffrire di alcune forzature che male sembrano sposarsi con un mercato tecnologico che si muove in senso diametralmente opposto e con la mancanza di soluzioni nazionali al passo con quelle prospettate dai principali attori internazionali[302].

[302] https://www.cybersecurity360.it/giornalista/francesco-cerciello, «Nuovi obblighi di notifica degli incidenti: quali conseguenze per i soggetti inclusi nel PSNC», Cyber Security 360 (blog), 29 settembre 2022, https://www.cybersecurity360.it/cybersecurity-nazionale/nuovi-obblighi-di-notifica-degli-incidenti-quali-conseguenze-per-i-soggetti-inclusi-nel-psnc/.

Capitolo III: La disciplina spagnola relativa alla cybersicurezza

10. Il Regime di Sicurezza Nazionale

Il Regio Decreto 3/2010, dell'8 gennaio, che regola il Regime nazionale di sicurezza nell'ambito dell'Amministrazione Digitale (di seguito, ENS[303]) aveva l'obiettivo di determinare la politica di sicurezza nell'uso dei mezzi elettronici degli enti che rientrano nel suo ambito di applicazione, essendo costituito dai principi fondamentali e dai requisiti minimi che hanno garantito adeguatamente la sicurezza delle informazioni trattate e dei servizi forniti da questi enti. L'ENS, il cui campo di applicazione comprendeva tutti gli enti della Pubblica Amministrazione, mirava a creare fiducia nel fatto che i sistemi informativi fornissero correttamente i loro servizi e salvaguardassero le informazioni senza interruzioni o modifiche incontrollate, e che le informazioni non potessero raggiungere persone non autorizzate, stabilendo misure per garantire la sicurezza dei sistemi, dei dati, delle comunicazioni e dei servizi elettronici, in modo da agevolare i cittadini e le Pubbliche Amministrazioni nell'esercizio dei loro diritti e nell'adempimento dei loro obblighi attraverso i mezzi elettronici[304]. Dal 2010 sono avvenuti cambiamenti significativi in Spagna e nell'Unione europea, tra cui la progressiva trasformazione digitale della società, il nuovo scenario della cybersecurity e l'avanzamento delle tecnologie applicative. È diventato inoltre evidente che i sistemi informativi sono sempre più esposti alla materializzazione di minacce provenienti dal cyberspazio, con un notevole aumento degli attacchi informatici, sia in termini di volume e frequenza che di sofisticazione, con agenti e attori dotati di maggiori capacità tecniche e operative. Tali minacce si verificano in un contesto di forte dipendenza dalle tecnologie dell'informazione e della comunicazione nella nostra società e di elevata interconnessione dei sistemi informativi[305]. Tutto ciò incide in modo significativo su un numero crescente di soggetti

[303] L'acronimo ENS sta per Esquema Nacional de Seguridad.

[304] Directiva de ciberseguridad: un nuevo escenario jurídico y material – Ricard Martínez Martínez – Revista SIC: ciberseguridad, seguridad de la información y privacidad, ISSN 1136-0623, Vol. 25, Nº. 121, 2016, pag. 98-100

[305] «Ciberseguridad En 2023: Principales Tendencias y Desafíos», 30 novembre 2022, https://www.open3s.com/ciberseguridad-en-2023-principales-tendencias-y-desafios-blog/.

pubblici e privati, sulle loro catene di fornitura, sui cittadini e, quindi, sulla cybersecurity nazionale, compromettendo il normale sviluppo sociale ed economico del Paese, nonché l'esercizio dei diritti e delle libertà dei cittadini, come riconosciuto sia dalla Strategia Nazionale di Cybersecurity del 2013 sia, in particolare, da quella del 2019. Il Regio Decreto del 2010 ha stabilito che l'ENS deve essere sviluppato, migliorato e mantenuto costantemente aggiornato in linea con i progressi dei servizi di Amministrazione Digitale, l'evoluzione della tecnologia, i nuovi standard internazionali in materia di sicurezza e il consolidamento delle infrastrutture che lo supportano. A livello normativo, di pari passo con questi cambiamenti e talvolta all'origine di essi, dal 2010 sono stati modificati sia il quadro europeo (con quattro regolamenti e una direttiva) sia quello spagnolo, con riferimento alla sicurezza nazionale, alla regolamentazione del procedimento amministrativo e del regime giuridico del settore pubblico, alla protezione dei dati personali e alla sicurezza delle reti e dei sistemi informativi, e si è inoltre evoluto il quadro strategico della cybersecurity[306]. Pertanto, la legge 36/2015, del 28 settembre, sulla sicurezza nazionale, considera la cybersicurezza un'area di particolare interesse della sicurezza nazionale, come indicato nell'articolo 10, e quindi richiede un'attenzione specifica in quanto è essenziale per preservare i diritti, le libertà ed il benessere dei cittadini, nonché per garantire la fornitura di servizi e risorse essenziali[307]. In conformità con le disposizioni dell'articolo 4.3 della legge 36/2015[308], è stato approvato il Regio Decreto 1008/2017 che approva la Strategia di Sicurezza Nazionale 2017, e successivamente il Regio Decreto

[306] «Ciberseguridad En 2023: Principales Tendencias y Desafíos», 30 novembre 2022, https://www.open3s.com/ciberseguridad-en-2023-principales-tendencias-y-desafios-blog/.

[307] Noticias Jurídicas, «Contenido de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional · Noticias Jurídicas», Text, Noticias Jurídicas (noticias.juridicas.com), Spain, https://noticias.juridicas.com/actualidad/noticias/10529-contenido-de-la-ley-36-2015-de-28-de-septiembre-de-seguridad-nacional/.

[308] La legge 36/2015, del 28 settembre, sulla sicurezza nazionale, definisce la sicurezza nazionale come l'azione dello Stato volta a proteggere la libertà, i diritti e il benessere dei cittadini, a la difesa della Spagna e dei suoi principi e valori costituzionali, nonché a contribuire, insieme agli alleati, alla sicurezza internazionale nell'adempimento degli impegni assunti. Tutto ciò viene realizzato attraverso il coordinamento di tutte le risorse pubbliche e private con l'obiettivo di ripristinare la normalità in un'ampia gamma di situazioni di crisi, elencate come numerus apertus nell'articolo 10 della legge: cybersecurity, sicurezza economica e finanziaria, sicurezza marittima, sicurezza dello spazio aereo e dello spazio esterno, sicurezza energetica, sicurezza sanitaria e ambientale. L'azione di sicurezza nazionale, attraverso la dichiarazione da parte del Presidente del Governo di una situazione di interesse per la sicurezza nazionale, rende possibile l'azione di tutte le risorse disponibili delle Pubbliche Amministrazioni interessate, comprese quelle in mano ai privati, attraverso l'esercizio degli ordinari poteri previsti dall'ordinamento giuridico.

1150/2021 che vara la Strategia di Sicurezza Nazionale 2021, entrambi i quali identificano il cyberspazio come uno spazio comune globale; in particolare, la Strategia 2021 lo descrive come uno spazio di connessione caratterizzato da apertura funzionale, assenza di confini fisici e facile accessibilità, aggiungendo che negli spazi comuni globali risulta difficile l'attribuzione di qualsiasi azione irregolare o criminale, data la loro estensione, la loro debole regolamentazione e l'assenza di sovranità[309].

D'altra parte, la legge 40/2015 sul Regime giuridico del settore pubblico ha esteso l'ambito di applicazione dell'ENS a tutto il settore pubblico, stabilendo all'articolo 3, che disciplina i principi generali, la necessità per le amministrazioni pubbliche di relazionarsi tra loro e con i propri organi, agenzie pubbliche ed enti collegati o dipendenti attraverso strumenti elettronici, di garantire l'interoperabilità e la sicurezza dei sistemi e delle soluzioni adottate da ciascuna di esse e la protezione dei dati personali, nonché di agevolare la fornitura di servizi agli interessati preferibilmente con tali mezzi[310]. Allo stesso modo, la legge 39/2015 sul Procedimento amministrativo comune delle Pubbliche Amministrazioni, tra i diritti degli individui nei rapporti con le P.A. previsti dall'articolo 13, include il diritto alla protezione dei dati personali e, in particolare, il diritto alla sicurezza dei dati contenuti negli archivi, nei sistemi e nelle applicazioni delle Pubbliche Amministrazioni. A sviluppo delle due leggi precedenti, il Regio Decreto 203/2021, che approva il Regolamento di azione e funzionamento del settore pubblico per via elettronica, specifica in diversi precetti l'obbligo di rispettare le misure di sicurezza previste dall'ENS, come quelle che si riferiscono allo scambio elettronico di dati in ambienti di comunicazione chiusi, ai sistemi di chiavi concordate e ad altri sistemi di identificazione delle persone interessate, all'archivio elettronico unico o ai portali Internet, tra gli altri[311].

[309] Santiago Mediano Abogados, «Publicada la Directiva sobre Ciberseguridad», Santiago Mediano Abogados (blog), 21 luglio 2016, https://santiagomediano.com/publicada-la-directiva-sobre-ciberseguridad.

[310] MLuz Dominguez, «10 principales amenazas emergentes de ciberseguridad que surgirán para 2030», CyberSecurity News (blog), 14 novembre 2022, https://cybersecuritynews.es/10-principales-amenazas-emergentes-de-ciberseguridad-que-surgiran-para-2030/.

[311] Parlamento europeo, «Ciberseguridad: amenanzas principales y emergentes», 21 marzo 2023.

In concomitanza con l'approvazione delle tre leggi sopra citate, il Regio Decreto 951/2015, che modifica il Regio Decreto 3/2010 regolarizzante il Regime di Sicurezza Nazionale in materia di Amministrazione Digitale, ha aggiornato l'ENS alla luce dell'esperienza e delle conoscenze nella sua applicazione, dell'attuale situazione della cybersecurity e dell'evoluzione del quadro giuridico, per adattarlo alle disposizioni del Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (noto come Regolamento eIDAS). Per quanto riguarda le misure di sicurezza dell'ENS nel trattamento dei dati personali, la Legge organica 3/2018 sulla protezione dei dati personali e la garanzia dei diritti digitali ha disposto, nella sua prima disposizione aggiuntiva, che tali misure di sicurezza siano attuate in caso di trattamento dei dati personali per impedirne la perdita, l'alterazione o l'accesso non autorizzato, adeguando i criteri di determinazione del rischio nel trattamento dei dati alle disposizioni dell'articolo 32 del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (cosiddetto Regolamento GDPR). D'altra parte, la prima disposizione aggiuntiva prescrive anche l'attuazione delle misure di sicurezza dell'ENS per gli enti del settore pubblico e per quelli del settore privato che collaborano con loro nella fornitura di servizi pubblici che comportano il trattamento di dati personali[312]. Infine, sulla stessa linea, la Legge organica 7/2021, sulla protezione dei dati personali trattati ai fini della prevenzione, dell'accertamento, dell'indagine e del perseguimento dei reati e dell'esecuzione delle sanzioni penali, ha stabilito all'articolo 37 l'obbligo di applicare le misure ENS al trattamento dei dati personali da parte delle autorità pubbliche competenti[313]. Per quanto riguarda la sicurezza delle reti e dei sistemi informativi, dall'entrata in vigore del Regio Decreto 3/2010 sono stati approvati nell'Unione europea due Regolamenti e una Direttiva che hanno stabilito il quadro d'azione nella legislazione nazionale. Questi sono, in primo luogo, il Regolamento (UE) n. 526/2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione

[312] Gómez, Miguel Angel Domínguez. "El Esquema Nacional de Seguridad, al servicio de la ciberseguridad del sector público." (2018).

[313] «PAe - Esquema Nacional de Seguridad - ENS», https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html.

(ENISA); in secondo luogo, il Regolamento (UE) 2019/881 relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione; infine, la Direttiva (UE) 2016/1148 recante misure volte a garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione, nota come Direttiva NIS, che è stata recepita in Spagna con il Regio Decreto Legge 12/2018, del 7 settembre, sulla sicurezza delle reti e dei sistemi informativi, indicando la necessità di tenere conto dell'ENS nell'elaborazione di disposizioni normative, istruzioni e guide, nonché nell'adozione di misure applicabili alle entità che rientrano nel suo ambito di applicazione. Il Regio Decreto Legge 12/2018, a sua volta, è stato attuato dal Regio Decreto 43/2021, del 26 gennaio, per quanto riguarda il quadro strategico e istituzionale per la sicurezza delle reti e dei sistemi informativi, la supervisione dell'adempimento degli obblighi di sicurezza degli operatori di servizi essenziali e dei fornitori di servizi digitali e la gestione degli incidenti di sicurezza[314]. Questo stabilisce, quindi, che le misure per il rispetto degli obblighi di sicurezza degli operatori di servizi essenziali e dei fornitori di servizi digitali prenderanno come riferimento quelle stabilite nell'Allegato II del Regio Decreto 3/2010, dell'8 gennaio.

Come stabilito nella Strategia di sicurezza nazionale del 2017, la Spagna deve garantire un uso sicuro e responsabile delle reti e dei sistemi di informazione e comunicazione, rafforzando le capacità di prevenzione, rilevamento e risposta agli attacchi informatici, potenziando e adottando misure specifiche per contribuire alla promozione di un cyberspazio sicuro e affidabile. A questo proposito, il 12 aprile 2019, il Consiglio di sicurezza nazionale ha approvato la Strategia nazionale di cybersecurity 2019 con l'obiettivo di definire le linee guida generali nel campo della cybersicurezza per raggiungere gli obiettivi stabiliti nella Strategia nazionale di sicurezza 2017. La Strategia Nazionale di Cybersecurity 2019 contiene un obiettivo generale e cinque obiettivi specifici, e per raggiungerli sono proposte sette linee d'azione per un totale di 65 misure. Il primo di questi obiettivi è la sicurezza e la resilienza delle

[314] «¿Qué es la ciberseguridad y su importancia?», 23 ottobre 2021, https://barrazacarlos.com/es/que-es-la-ciberseguridad/.

reti e dei sistemi informativi e di comunicazione del settore pubblico e dei servizi essenziali, e si sviluppa attraverso due linee d'azione e ventiquattro misure specifiche, tra cui la garanzia della piena attuazione dello Schema di sicurezza nazionale. Per sviluppare questa Strategia, il 29 marzo 2022 il Consiglio dei Ministri ha approvato il Piano Nazionale di Cybersecurity, che prevede quasi 150 iniziative, tra azioni e progetti, per i successivi tre anni[315]. Allo stesso modo, la Strategia Nazionale di Cybersecurity 2019 indica tra i suoi obiettivi il consolidamento di un quadro nazionale coerente e integrato che garantisca la protezione delle informazioni e dei dati personali trattati dai sistemi e dalle reti del settore pubblico e dei servizi, siano essi essenziali o meno, affermando che la conformità richiede l'attuazione di misure di sicurezza incentrate sul miglioramento delle capacità di prevenzione, rilevamento e risposta agli incidenti, attraverso lo sviluppo di nuove soluzioni, il rafforzamento del coordinamento e l'adeguamento del sistema giuridico[316].

Nel mondo iperconnesso di oggi l'implementazione della sicurezza nel cyberspazio è diventata una priorità strategica. Tuttavia, il rischio nel cyberspazio è troppo grande perché il settore pubblico o le imprese possano affrontarlo da soli, poiché entrambi hanno un interesse e una responsabilità condivisi per affrontare la sfida insieme. Con l'aumento del ruolo della tecnologia nella società, la sicurezza informatica diventa una sfida sempre più grande[317]. Le tattiche di interferenza, spesso combinate per ottenere un effetto maggiore, assumono, tra le altre, le forme di attacchi informatici, assunzione del controllo di infrastrutture critiche, disinformazione, soppressione delle informazioni, manipolazione delle piattaforme dei social media e dei loro algoritmi, minacce e molestie per accedere alle informazioni sugli elettori e interferire con la legittimità del processo elettorale, false personalità e identità, pressione sui cittadini stranieri

[315] Paloma González, «Estas son las seis principales amenazas en ciberseguridad para 2020 - Füture», https://future.inese.es/ (blog), 23 gennaio 2020, https://future.inese.es/estas-son-las-seis-principales-amenazas-en-ciberseguridad-para-2020/.

[316] «Novedades en materia de ciberseguridad para 2022», Cuatrecasas, https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/eu-cuales-seran-en-2022-los-principales-desarrollos-normativos-en-materia-de-ciberseguridad.

[317] «25 Tipos de ataques informáticos y cómo prevenirlos», CIBERSEGURIDAD .blog, 20 gennaio 2018, https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/.

che vivono nell'Unione, strumentalizzazione dei migranti e spionaggio[318]. Parallelamente al consolidarsi dello scenario sopra descritto, si è diffusa l'implementazione dell'ENS, che ha portato a una maggiore esperienza accumulata nella sua applicazione, nonché a una migliore conoscenza grazie alle successive edizioni della Relazione nazionale sullo stato della sicurezza (INES), alle guide alla sicurezza CCN-STIC ed ai servizi e strumenti forniti dal Centro Crittologico Nazionale (CCN) in relazione alla capacità di risposta agli incidenti di sicurezza informatica[319]. L'approvazione del Regio Decreto 311/2022 rientra nell'attuazione del Piano di Digitalizzazione della Pubblica Amministrazione 2021-2025, uno dei principali strumenti per la realizzazione del Piano di Recupero, Trasformazione e Resilienza e della sua Componente 11 denominata "Modernizzazione delle Pubbliche Amministrazioni", nonché per lo sviluppo degli investimenti e delle riforme previste dall'Agenda Digitale Spagna 2025[320]. Questo Piano di digitalizzazione prevede espressamente, tra le sue riforme, l'aggiornamento dell'ENS al fine di evolvere la politica di sicurezza di tutti gli enti pubblici spagnoli, tenendo conto delle normative dell'Unione europea volte ad aumentare il livello di sicurezza informatica dei sistemi informativi[321]. Questa riforma è completata dalla creazione del Centro operativo di cybersecurity dell'Amministrazione generale dello Stato e dei suoi enti pubblici, che servirà da riferimento per le altre amministrazioni pubbliche e contribuirà a migliorare la conformità all'ENS degli enti nel loro ambito di servizio[322].

---

[318] Aldo Valdez Alvarado, INTRODUCCIÓN A LA CIBERSEGURIDAD, 2019, https://doi.org/10.13140/RG.2.2.33919.36002.

[319] «El nuevo ENS 2022 y sus principales cambios», CIBERSEGURIDAD .blog, 29 maggio 2022, https://ciberseguridad.blog/el-nuevo-ens-2022-y-sus-principales-cambios/.

[320] «Esquema Nacional de Seguridad 2022 - AFS Informática», 4 maggio 2022, https://www.afsinformatica.com/esquema-nacional-de-seguridad-2022/.

[321] «Patrullaje En El Ciberespacio. El Trabajo de La Policía Cibernética», issuu, https://issuu.com/vkentintado/docs/revista_momento_julio_2020/s/10793398.

[322] «BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.», https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191.

Pubblicato per la prima volta il 9 agosto 2016, il Codice di Diritto della Cybersecurity[323] è un'iniziativa congiunta dell'Istituto Nazionale di Cybersecurity (INCIBE[324]) e della Gazzetta Ufficiale dello Stato (BOE) che fornisce a tutti i professionisti del diritto, in un compendio di norme, l'accesso a informazioni e risorse che forniscono loro il livello di conoscenza necessario in ambito giudiziario per la migliore applicazione del quadro giuridico e tecnico associato. Nelle parole del suo autore, Francisco Pérez Bes, lo scopo dell'opera è quello di "stabilire le linee guida generali per l'uso sicuro del cyberspazio, promuovendo una visione integrata che garantisca sicurezza e progresso in Spagna". Il Codice di Diritto della Cybersecurity ha l'obiettivo di raccogliere in un unico documento tutta la legislazione spagnola in materia di cybersecurity, al fine di contribuire a migliorare la conoscenza e facilitare l'applicazione delle norme che riguardano un settore così importante, ma in continua evoluzione. Si tratta, quindi, di uno strumento essenziale per i professionisti del diritto e della gestione normativa della cybersecurity[325]. Complessivamente, sono stati raccolti parzialmente o totalmente 42 testi di legge che fanno riferimento alla sicurezza informatica, raggruppati in nove sezioni: Costituzione spagnola, Regolamenti di sicurezza nazionale, Infrastrutture critiche, Regolamenti di sicurezza, Team di risposta agli incidenti di sicurezza, Telecomunicazioni e utenti, Cybercriminalità, Protezione dei dati e Rapporti con l'amministrazione[326]. In questa compilazione si può trovare sia la normativa strettamente di cybersicurezza sia quella sulla protezione dei dati: la scelta del suo autore si giustifica nel fatto che, come è stato sostenuto in più sedi, la sicurezza digitale e i diritti umani sono complementari, si rafforzano a vicenda e sono interdipendenti. Secondo la Spagna il fulcro della sicurezza digitale risiede nella

[323] Il Codice di Diritto della Cybersecurity non è un testo giuridico in quanto tale, ma è semplicemente una compilazione di alcuni testi che, in misura maggiore o minore, trattano il tema della cybersecurity.

[324] L'INCIBE è un organismo che fa capo alla Segreteria di Stato per l'Avanzamento Digitale del Ministero dell'Economia e delle Imprese; lavora per rafforzare la fiducia digitale, aumentare la sicurezza informatica e la resilienza e contribuire al mercato digitale in modo da promuovere l'uso sicuro del cyberspazio in Spagna. *«INCIBE | INCIBE», https://www.incibe.es/.*

[325] «¿Qué es el Código de Derecho de la Ciberseguridad?», Instituto Europeo Campus Stellae (blog), 8 luglio 2019, https://campus-stellae.com/que-es-el-codigo-de-derecho-de-la-ciberseguridad/.

[326] AU, «Publicado el Código de Derecho de la Ciberseguridad, una recopilación de la normativa en este ámbito», Áudea (blog), 20 ottobre 2016, https://www.audea.com/publicado-codigo-derecho-la-ciberseguridad-una-recopilacion-toda-la-normativa-espanola-este-ambito/.

protezione degli individui e, di conseguenza, dei diritti umani. In tal senso, la definizione sviluppata dal gruppo di lavoro *"A Free and Safe Internet "* della Freedom Online Coalition[327], ritenuta la più rispettosa dei diritti umani, sostiene che la cybersecurity è la salvaguardia, attraverso politiche, tecnologie e formazione, della disponibilità, della riservatezza e dell'integrità delle informazioni e delle infrastrutture sottostanti, al fine di migliorare la sicurezza delle persone sia online che offline[328]. Questa definizione considera inoltre il ruolo dell'innovazione tecnologica come motore per promuovere il libero flusso di informazioni nei media digitali. In questa direzione, la scelta spagnola è stata quella di rafforzare il legame tra sicurezza digitale e diritti umani al fine di promuovere la libertà e la sicurezza. Con l'obiettivo di contribuire agli sforzi dell'Organizzazione degli Stati Americani (OAS[329]) per supportare lo sviluppo di politiche nazionali di sicurezza digitale e di strategie nazionali di sicurezza digitale, nel 2016 un gruppo di organizzazioni ha presentato una dichiarazione di principi sul tema. Lo scopo era quello di offrire linee guida minime da tenere in considerazione in questi processi di costruzione di strategie nazionali di sicurezza digitale. Il testo della dichiarazione propone di allineare qualsiasi strategia di sicurezza digitale con i quadri giuridici dei diritti umani di ciascun Paese, del sistema interamericano e degli standard internazionali (come quelli delineati

[327] La Freedom Online Coalition (FOC) è un gruppo di Paesi profondamente impegnati nei diritti umani e nelle libertà fondamentali proclamati nella Dichiarazione universale dei diritti umani. Essa crede che i diritti umani che le persone hanno offline debbano essere protetti anche online: si impegna a lavorare per sostenere la libertà di Internet e proteggere i diritti umani online in tutto il mondo. La FOC mira ad essere una coalizione proattiva che garantisce che le questioni relative alla libertà di Internet siano nell'agenda politica internazionale come un modo per guidare cambiamenti e risultati politici concreti attraverso il coordinamento diplomatico, la definizione di norme globali e la collaborazione multistakeholder. Una priorità chiave della Freedom Online Coalition è la definizione di norme globali attraverso un'azione congiunta. Per questo, la FOC offre ai suoi membri uno spazio diplomatico informale per condividere informazioni e preoccupazioni sugli attuali sviluppi che minacciano di compromettere la libertà di Internet in tutto il mondo. Reagendo congiuntamente alle questioni emergenti, i membri della coalizione sono in grado di aumentare la visibilità della loro risposta e l'impatto delle loro dichiarazioni. *«Home Page», Freedom Online Coalition, https://freedomonlinecoalition.com/.*

[328] FOC-WG1. (2014). Recommendations for Human Rights Based Approaches to Cybersecurity. Disponible en https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf

[329] L'Organizzazione degli Stati Americani è un'organizzazione internazionale di carattere regionale che comprende i 35 stati indipendenti delle Americhe (l'unico territorio americano sulla terraferma a non far parte dell'OSA è la Guyana francese, in quanto dipartimento d'oltremare francese). L'organizzazione è il principale forum politico per il dialogo multilaterale e per la soluzione di problemi politici locali. Lo scopo dell'organizzazione è di mantenere la pace, rinforzare la democrazia e i diritti dell'uomo, e migliorare le condizioni sociali ed economiche dei paesi dell'America. *OAS, «OAS - Organization of American States: Democracy for Peace, Security, and Development», Text, 1 agosto 2009, https://www.oas.org/en/.*

nei Principi Internazionali sull'Applicazione dei Diritti Umani alla Sicurezza Digitale), dando particolare rilevanza alla protezione e alla garanzia dell'esercizio dei diritti alla libertà di espressione, alla privacy, alla libertà di espressione e di libera associazione. La Spagna ha ritenuto che quest'approccio sia fondamentale per ricordare ai responsabili politici degli Stati che la sicurezza digitale deve tenere conto della sicurezza delle persone e dei diritti umani. Ciò include il miglioramento dei quadri giuridici nazionali per garantire che la sorveglianza delle comunicazioni sia effettuata in conformità con gli standard dei diritti umani, in particolare sulla base dei principi di necessità e proporzionalità, nonché l'adozione e l'attuazione di politiche pubbliche di protezione dei dati, specie nelle iniziative e nei progetti di condivisione delle informazioni tra i Paesi[330].

Ancora, è da menzionare la nuova Strategia di sicurezza nazionale 2021, approvata dal Consiglio dei ministri e di cui si tratterà nel paragrafo che segue, che sostituirà quella approvata quattro anni prima. Sebbene la legge sulla sicurezza nazionale stabilisca che il documento debba essere aggiornato ogni cinque anni, nel 2020 il Consiglio di sicurezza nazionale ha deciso di rinnovarlo per adattarlo alla nuova realtà delle minacce. L'attuale contesto geopolitico, la pandemia Covid-19, le minacce ibride, la trasformazione e la transizione ecologica sono alcune delle sfide che hanno motivato il cambiamento. Gli obiettivi principali di questa strategia, fortemente orientata alla resilienza, sono i progressi nella gestione delle crisi, l'aumento della sicurezza dei settori strategici e il miglioramento delle capacità della Spagna di prevenire, individuare e reagire alle minacce. La Strategia di sicurezza nazionale 2021 prevede diverse iniziative per sviluppare queste capacità: tra queste, lo sviluppo di un catalogo dinamico di risorse in settori strategici da mettere a disposizione delle autorità competenti, l'elaborazione di piani di preparazione e di predisposizione delle risorse, il progetto di un sistema di indicatori

[330] Maricarmen Sequera, Amalia Toledo & Leandro Ucciferri, «Derechos humanos y seguridad digital: una pareja perfecta», Enero 2018.

critici per lo sviluppo di un sistema di allerta precoce e l'adozione di soluzioni di intelligenza artificiale per la valutazione della situazione di sicurezza e il supporto all'analisi strategica[331].

In conclusione, nei paragrafi che seguono verrà analizzato il recepimento della Direttiva NIS nell'ordinamento spagnolo, avvenuto ad opera del Regio Decreto legge 12/2018 e del Regio Decreto 43/2021. Sarà possibile notare come le misure di sicurezza, il sistema di notificazione degli incidenti, nonché la valutazione degli hardware e software non siano il frutto di una spinta nazionale, a differenza che in Italia, ma siano piuttosto il frutto del recepimento della normativa europea in materia di cybersicurezza. Il sistema di cybersicurezza spagnolo si caratterizza, infatti, per l'adeguamento della legislazione preesistente sulla Sicurezza nazionale alla direttiva NIS, ossia alle necessità nate dall'affrontare i problemi legati al cyberspazio, come potrà notarsi con riguardo all'obbligo di notificazione degli incidenti dettato dal Regio Decreto 3/2010 ed in riferimento alla normativa sulle infrastrutture critiche di cui si è occupata dapprima la Legge 8/2001 e successivamente il Regio Decreto 704/2011. Altresì, nel paragrafo dedicato alle infrastrutture critiche spagnole verrà descritta la disciplina intervenuta in seguito alle procedure d'infrazione relativa al Golden Power, la quale si occupa di far fronte ai problemi di neutralità che originano dagli investimenti stranieri sulle infrastrutture critiche per il Paese. Da ultimo, per concludere la ricerca, verranno analizzati, in una prospettiva comparata, i soggetti a cui sono affidati ruoli di prim'ordine nell'ambito della cybersicurezza spagnola operando un raffronto con quelli che operano all'interno del Perimetro di sicurezza nazionale italiano.

[331] Enrique González Herrero, «Aprobada la nueva Estrategia de Seguridad Nacional 2021», Seguritecnia, 28 dicembre 2021,https://www.seguritecnia.es/actualidad/aprobada-la-nueva-estrategia-de-seguridad-nacional-2021_20211228.html.

11. Le Strategie nazionali di cybersicurezza

Come l'Italia, la Spagna ha redatto una strategia nazionale di cybersicurezza ancor prima della richiesta operata dalla Direttiva NIS, consistente nell'obbligo per ciascun Stato membro di redigere strategie nazionali in materia di cybersicurezza in modo che ciascun Paese dell'area eurocomunitaria sia preparato di fronte ai cyber attacchi e ai pericoli che ne derivano affliggendo la nostra società. Infatti, nel 2013 venne approvata la prima Strategia Nazionale di Cybersicurezza in Spagna; il documento fissava le direttive e le linee generali di attuazione per far fronte alla sfida che assume per il Paese la vulnerabilità del cyberspazio. Inoltre, la Strategia disegnava il modello di governance per la cybersicurezza nazionale. Ugualmente, in questi anni, la Spagna ha compiuto ulteriori progressi per contribuire alla promozione di un cyberspazio sicuro e affidabile. Uno dei suoi pilastri, creato nel 2014, è il Consiglio Nazionale di Cybersicurezza[332], organo di appoggio del Consiglio di Sicurezza Nazionale[333]. Sin da subito, il Consiglio Nazionale di Cybersicurezza ha assunto il compito di coordinare gli organismi con competenza in materia a livello nazionale, nonché quello di sviluppare il Piano Nazionale di Cybersicurezza[334]. Il quadro giuridico ha sperimentato un notevole adattamento: infatti, in risposta all'evoluzione e all'esperienza accumulata in questi anni, nel 2015 venne modificato il

[332] Il Consiglio nazionale per la cybersecurity è l'organo collegiale che supporta il Consiglio di sicurezza nazionale nella sua qualità di Commissione delegata del governo per la sicurezza nazionale, nel quadro della legge 50/1997, del 27 novembre, del governo. Il Consiglio, presieduto dal direttore del Segretario di Stato del National Intelligence Center e dal direttore del National Cryptological Center, è stato creato con accordo del Consiglio di sicurezza nazionale del 5 dicembre 2013. Inoltre, quest'organo ha il compito di rafforzare i rapporti di coordinamento, collaborazione e cooperazione tra le diverse Pubbliche Amministrazioni con competenze in materia di cybersecurity, nonché tra il settore pubblico e privato, e facilita il processo decisionale del Consiglio stesso attraverso l'analisi, lo studio e la proposta di iniziative sia a livello nazionale che internazionale. Si riunisce su iniziativa del suo presidente almeno bimestrale o tutte le volte che lo ritiene necessario tenendo conto delle circostanze che riguardano la sicurezza informatica. *«Consiglio nazionale per la cibersicurezza», https://www.ccn.cni.es/index.php/es/menu-ccn-es/consejo-nacional-de-ciberseguridad.*

[333] Il Consiglio di sicurezza nazionale, nella sua qualità di Commissione delegata del governo per la sicurezza nazionale, è l'organo responsabile di assistere il Presidente del Governo nella direzione della politica di sicurezza nazionale e del sistema di sicurezza nazionale, nonché di esercitare le funzioni attribuitegli nella legge sulla sicurezza nazionale e assegnategli dai suoi regolamenti. Su proposta del Primo Ministro, il Consiglio di Sicurezza Nazionale riferisce al Re almeno una volta all'anno. *«Il Consiglio di Sicurezza Nazionale | DSN», https://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional#collapseFive.*

[334] Arturo Gómez Salgado, «Van por órganos no secretos en ciberseguridad: Monreal», Grupo Milenio, 21 novembre 2022, https://www.milenio.com/negocios/van-por-organos-no-secretos-en-ciberseguridad-monreal.

Regime nazionale di sicurezza per garantire la sicurezza dei sistemi del pubblico settore. D'altra parte, l'entrata in vigore del Regio Decreto Legge 12/2018, relativo alla sicurezza delle reti e dei sistemi di informazione, che attua nell'ordinamento giuridico spagnolo la direttiva NIS, è stata un'importante pietra miliare nel miglioramento della cybersecurity per la Spagna, estendendo l'ambito di applicazione di questa direttiva con l'obiettivo di migliorare la cybersicurezza di tutti i settori strategici. La legge 36/2015 sulla Sicurezza nazionale venne promulgata con l'intento di dar impulso a uno dei progetti di maggior responsabilità per un governo, la Sicurezza nazionale. In questo senso, la legge sulla Sicurezza nazionale contempla la cybersecurity come abito di speciale interesse. Si può affermare, senza dubbio, che la cybersicurezza ha modernizzato la Sicurezza nazionale, trattandosi di uno dei settori più avanzati di oggi.

La Strategia nazionale di cybersecurity del 2019 sviluppa le previsioni della Strategia nazionale di sicurezza del 2017 nel campo della cybersecurity, affrontando gli obiettivi generali, l'obiettivo del settore della cybersicurezza e le linee di azione stabilite per raggiungerlo[335]. Tale strategia definisce la posizione della Spagna su una nuova concezione di cybersecurity nel quadro della Politica di Sicurezza Nazionale, strutturandosi in cinque capitoli. In primo luogo, la Strategia identifica il cyberspazio come bene comune globale, presenta le opportunità e le sfide del cyberspazio e delle infrastrutture digitali delineando la natura intrinsecamente internazionale dell'approccio alla sua sicurezza, nonché descrive le caratteristiche principali della nuova concezione della sicurezza informatica in Spagna. In secondo luogo, nel documento vengono esaminate le principali minacce e sfide nel cyberspazio che la Spagna deve affrontare; inoltre, sono stabilite le finalità e i principi che regolano la Strategia stessa, ossia unità d'azione, anticipazione, efficienza e resilienza, nonché gli obiettivi, uno generale e cinque specifici, trasversali a tutte le aree. Quale obiettivo generale, la Spagna si propone di garantire un uso sicuro e affidabile del cyberspazio, proteggendo i diritti e le libertà dei cittadini e promuovendo il progresso socio-economico. Altri obiettivi da menzionare sono quelli che riguardano la

[335] «Estrategia Nacional de Ciberseguridad | Ciberseguridad», https://ciberseguridad.com/normativa/espana/estrategia-nacional/.

sicurezza e resilienza delle reti e dei sistemi di informazione e comunicazione del settore pubblico e dei servizi essenziali, nonché la sicurezza e l'affidabilità del cyberspazio contro l'uso illecito o doloso, ed infine la promozione della cultura e dell'impegno per la sicurezza informatica e per il potenziamento delle capacità umane e tecnologiche. Le linee d'azione volte a raggiungere gli obiettivi dichiarati riguardano il rafforzamento delle capacità di fronte alle minacce provenienti dal cyberspazio, come pure la sicurezza e la resilienza degli asset strategici della Spagna[336]. Le misure da porre in essere includono la piena attuazione del Piano di Sicurezza Nazionale, del Sistema di Protezione delle Infrastrutture Critiche e della conformità e armonizzazione dei regolamenti sulla protezione delle infrastrutture critiche e dei servizi essenziali, con un approccio prioritario basato sul rischio. È necessario, altresì, rafforzare la capacità di indagare e perseguire i crimini informatici per garantire la sicurezza dei cittadini e la protezione dei diritti e delle libertà nel cyberspazio, così come promuovere la sicurezza informatica di cittadini e aziende e l'industria spagnola della cybersecurity al fine di rafforzare l'autonomia digitale. Quindi, per contribuire alla sicurezza del cyberspazio in ambito internazionale è importante promuovere un cyberspazio aperto, plurale, sicuro e affidabile, a sostegno degli interessi nazionali.

La sicurezza nel cyberspazio è diventata un obiettivo prioritario nelle agende dei governi al fine di garantire la loro sicurezza nazionale e di creare una società basata sulla fiducia. Il cyberspazio è considerato come dimensione cardine per la stabilità, la difesa dei valori e principi costituzionali e democratici, quali i diritti fondamentali dei cittadini nel cyberspazio, specialmente per quanto riguarda la protezione dei dati personali, la privacy, la libertà di espressione ed il diritto ad ottenere informazioni vere e di qualità. La natura trasversale della sicurezza informatica richiede che sia affrontata dalla società nel suo complesso; Internet ha permesso a Stati, gruppi organizzati, collettivi e persino individui isolati di raggiungere un livello di potere e influenza impensabile in passato. Gli Stati, direttamente o attraverso intermediari, utilizzano Internet per la disinformazione e la propaganda: l'uso malevolo dei dati

[336] Santos, Daniel Terrón. "Orden pci/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional [boe n.º 103, 30/iv/2019]." (2019).

personali e le campagne di disinformazione hanno un alto potenziale di destabilizzazione della società. Il governo spagnolo precisa, così come stabiliva la Strategia precedente, la necessità di garantire un uso sicuro e responsabile delle reti e dei sistemi di informazione e comunicazione attraverso il rafforzamento delle capacità di prevenzione, detenzione e risposta ai cyber attacchi, potenziando e adottando mezzi specifici per contribuire alla promozione di un cyberspazio sicuro e affidabile. Coerentemente al 2017, la Spagna continua a rafforzare le proprie capacità per garantire la sicurezza del settore pubblico e dei servizi essenziali. In questo senso, la promozione della cultura della cybersicurezza è diventata uno degli asset centrali per contare su una società più cosciente delle minacce e pericoli che l'aspetta. Il diritto ad un uso sicuro e affidabile del cyberspazio contribuisce a che sussista così una responsabilità condivisa[337]. Il Segretario Generale per l'Amministrazione Digitale (SGAD[338]) contribuisce a questo sforzo collettivo, in quanto membro del Consiglio Nazionale per la Cybersecurity, in stretta collaborazione con il CCN (Centro Crittografico Nazionale[339]), nello sviluppo dello Schema nazionale di sicurezza (ENS) e nella promozione di servizi comuni e condivisi, in particolare quello relativo alla sicurezza informatica[340].

Come anticipato, la strategia nazionale di cybersicurezza si ispira ai principi reggenti della sicurezza nazionale: unità di azione, anticipazione, efficienza e resilienza. La risposta agli incidenti nell'ambito della cybersicurezza deve essere coordinata e risolta in maniera rapida ed

---

[337] Sicilia, Carola Cadenas. "La nueva Estrategia Nacional de Ciberseguridad 2019." (2019).

[338] Il SGAD, con rango di Sottosegretariato, e dipendente dal Ministero degli Affari Economici e della Trasformazione Digitale è l'organismo incaricato di promuovere il processo di razionalizzazione delle tecnologie dell'informazione e della comunicazione nel campo dell'Amministrazione Generale dello Stato e dei suoi Enti Pubblici. *«PAe - SGAD», https://administracionelectronica.gob.es/pae_Home/en/pae_Organizacion/SGAD.html.*

[339] Il Centro Nazionale di Crittografia (CCN) è l'organismo responsabile del coordinamento dell'azione delle diverse agenzie dell'Amministrazione che utilizzano mezzi o procedure di crittografia, garantiscono la sicurezza delle tecnologie dell'informazione in questo settore, riferiscono sull'acquisizione coordinata di materiale crittografico e formano il personale dell'Amministrazione specialista in questo campo. Il CCN è stato creato nel 2004, attraverso il regio decreto 421/2004, collegato al National Intelligence Center (CNI). Infatti, la legge 11/2002, del 6 maggio, che regola il CNI, affida al Centro l'esercizio di funzioni relative alla sicurezza delle tecnologie dell'informazione e alla protezione delle informazioni classificate, conferendo al suo Segretario di Stato la responsabilità di dirigere il Centro nazionale di crittografia. Pertanto, il CCN condivide con il CNI mezzi, procedure, regolamenti e risorse. *«Centro Criptológico Nacional (CCN)», https://www.ccn-cert.cni.es/sobre-nosotros/centro-criptologico-nacional.html.*

[340] «PAe - Publicada la nueva Estrategia Nacional de Ciberseguridad 2019», https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Mayo/Noticia-2019-05-03-Publicada-nueva-Estrategia-Nacional-Ciberseguridad-2019.html.

efficace, qualità realizzabili attraverso un'adeguata preparazione e articolazione dell'unità d'azione di Stato. Infatti, una gestione centralizzata delle crisi che affliggono il cyberspazio permette di mantenere una visione completa sulla situazione della minaccia e permette l'occupazione delle risorse disponibili in maniera più rapida, efficiente, coerente e integrale. La specificità del cyberspazio e degli attori implicati richiede che esistano meccanismi di anticipazione organizzati in organismi specializzati, che orientino l'azione dello Stato in situazioni di crisi. Lo scenario attuale caratterizzato dall'austerità economica obbliga ad orientare l'azione dello Stato in termini di ottimizzazione e di efficienza delle risorse disponibili; inoltre, la resilienza è una caratteristica fondamentale che devono possedere i sistemi e le infrastrutture critiche. Lo Stato è obbligato ad assicurare la disponibilità degli elementi che si considerano essenziali per la nazionale, migliorando la loro protezione contro le minacce cyber[341]. La Strategia nazionale di cybersecurity del 2019 è in linea con la più recente la Strategia di sicurezza nazionale del 2021, da considerarsi quale quadro di riferimento della politica di sicurezza nazionale, una politica statale basata su una concezione ampia della sicurezza. L'attuale Strategia, che ha il rapporto favorevole del Consiglio di Sicurezza Nazionale del 18 novembre ed è stata approvata dal Governo con Regio Decreto, sviluppa ulteriormente alcuni dei concetti e delle linee d'azione definiti nel 2017 e avanza nell'adattamento di questa politica e delle risorse statali che la compongono ai nuovi sviluppi di un ambiente di sicurezza in costante evoluzione. Questa nuova strategia descrive l'attuale contesto di sicurezza nel mondo e identifica quattro dinamiche di trasformazione globale: l'aumento della competizione geopolitica; un ambiente socio-economico segnato dalle conseguenze del Covid-19; l'accelerazione del ritmo di trasformazione portato dalla tecnologia; infine, il processo di transizione ecologica. Per quanto riguarda i rischi e le minacce, la Strategia 2021 riflette una maggiore assertività da parte di alcuni attori internazionali: essi ricorrono ad azioni ostili che non equivalgono a conflitti armati, come nel caso delle cosiddette strategie ibride. Inoltre, le campagne di disinformazione appaiono come un fattore di primo piano, in quanto sono ora riconosciute come un importante problema di sicurezza. In termini di obiettivi,

[341] Gobierno de España, Presidencia del Gobierno, «Estrategia nacional de ciberseguridad», 2019.

la Strategia 2021[342] è orientata allo sviluppo del Sistema di Sicurezza Nazionale per la gestione di crisi di natura multiforme con politiche preventive. In questo senso, prevede l'utilizzo di sistemi di allerta precoce basati su dati e indicatori, attraverso l'applicazione di nuove tecnologie. Questa strategia offre una risposta proattiva e di supporto per una Spagna sicura e resiliente di fronte alle principali sfide di un mondo in continua evoluzione, in cui la difesa della democrazia, dei diritti umani e della sicurezza internazionale è un elemento fondamentale. A tal fine, si articola un triplice approccio strategico: proteggere la vita delle persone, i loro diritti e le loro libertà, nonché l'ordine costituzionale; altresì promuovere la prosperità e il benessere dei cittadini e partecipare al mantenimento della pace e della sicurezza internazionale. In questo contesto, fare progressi nella gestione delle crisi, promuovere la dimensione della sicurezza delle capacità tecnologiche e strategiche del settore, sviluppare la capacità della Spagna di prevenzione, deterrenza, individuazione e risposta alle strategie ibride sono obiettivi prioritari per la Spagna nei prossimi anni. Le misure proposte nella presente Strategia di sicurezza nazionale sono allineate con il Piano di ripresa, trasformazione e resilienza e con la strategia Spagna 2050, documenti che definiscono la tabella di marcia con una visione strategica a lungo termine[343].

Sia il Governo spagnolo sia quello italiano hanno redatto Strategie nazionali in materia di cybersicurezza quali espressione delle visioni nazionali, dei principi e delle priorità che guidano lo Stato nell'avanzamento dei propri interessi nella sfera cyber e in tutti gli ambiti con un'importante componente digitale. Nonostante le strategie italiane e spagnole si pongano obiettivi piuttosto simili, dall'analisi delle strategie elaborate dal Governo spagnolo è possibile confermare la forte attenzione riposta nella garanzia e nella tutela dei diritti inviolabili dell'uomo. L'esercizio di diritti quali la libertà di espressione, il diritto alla privacy o il diritto all'informazione devono essere preservarti non soltanto nel mondo analogico ma anche nel cyberspazio: il legame tra sicurezza digitale e diritti umani deve essere forte per poter

[342] Il processo di elaborazione di questa nuova Strategia è stato di competenza del Consiglio di Sicurezza Nazionale, coordinato dal Dipartimento di Sicurezza Nazionale e nel quale, come novità rispetto alle precedenti edizioni, spicca la partecipazione delle Comunità Autonome.

[343] Gobierno de España, Presidencia del Gobierno, «Estrategia de seguridad nacional», 2021.

promuovere la libertà e la sicurezza dei cittadini. Le strategie sposano l'idea che il fulcro della sicurezza digitale risieda nella protezione degli individui e, di conseguenza, nei diritti umani, confermando in questo modo l'interdipendenza tra essi. Nelle Strategie italiane, nonostante sia implicito il rispetto per i diritti umani nelle scelte relative alla sicurezza informatica, non si riscontra una tale attenzione verso questo tema. Invece, sia la Spagna che l'Italia hanno fissato quale obiettivo quello di promuovere una cultura di cybersicurezza al fine di garantire una sempre maggiore attenzione ai pericoli crescenti nel cyberspazio dovuti all'avanzamento continuo delle tecnologie e delle minacce che colpiscono la nostra sicurezza. Quale ultima riflessione, è bene evidenziare come la Spagna abbia allargato il tema della sicurezza nazionale facendovi rientrare quello della cybersecurity; quest'ultima, infatti, si configura quale speciale branca della sicurezza nazionale ricoprendo un ruolo di particolare importanza. Nei paragrafi che seguono si vedrà come le istituzioni di sicurezza spagnole abbiano visto una riorganizzazione al fine dell'adattamento richiesto dalle esigenza di cybersicurezza. Le Strategie analizzate mettono in luce la visione della Spagna che considera la cybersecurity un tema inscindibile dalla tutela dei diritti umani dei suoi cittadini e, più in generale, dalla sicurezza nazionale.

12. Il recepimento della Direttiva NIS nell'ordinamento giuridico spagnolo

La natura trasversale della cybersicurezza comporta il rischio di perdere efficacia se i requisiti di sicurezza delle informazioni vengono definiti separatamente per ciascuna delle aree settoriali interessate. È quindi opportuno mettere in atto meccanismi che, in una prospettiva olistica, migliorino la protezione contro le minacce alle reti e ai sistemi informativi, facilitando il coordinamento delle azioni in questo settore sia a livello nazionale che internazionale, in particolare all'interno dell'Unione europea. A tal fine, viene emanato il Regio Decreto-Legge 12/2018, che recepisce nell'ordinamento spagnolo la Direttiva (UE) 2016/1148 recante misure volte a garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione. Il Regio Decreto Legge si basa anche sugli standard, sugli strumenti di risposta agli incidenti e sugli organismi di coordinamento statali esistenti in questo settore. Questo, insieme alle ragioni indicate nella sezione I, giustifica il fatto che il suo contenuto trascende l'ambito della direttiva NIS: il decreto in questione si applicherà agli enti che forniscono servizi essenziali alla comunità e che dipendono dalle reti e dai sistemi informativi per lo sviluppo delle loro attività. Il suo campo di applicazione è quindi esteso a settori non espressamente inclusi nella direttiva, al fine di conferire, a questo Regio Decreto Legge, un approccio globale, pur mantenendo la sua legislazione specifica[344]. Inoltre, nel caso delle attività di gestione della rete e di fornitura di servizi di comunicazione elettronica e strutture associate, nonché di servizi elettronici fiduciari, che sono espressamente esclusi dalla direttiva, il decreto si applicherà solo agli operatori critici. Il regio decreto legge si applicherà anche ai fornitori di determinati servizi digitali. La direttiva NIS li sottopone a un regime di armonizzazione massima, equivalente a un regolamento, poiché si ritiene che la loro regolamentazione a livello nazionale non sarebbe efficace in quanto di natura intrinsecamente transnazionale. Il ruolo delle autorità nazionali è quindi limitato alla supervisione della loro applicazione da parte dei fornitori stabiliti nel loro paese e al coordinamento con le autorità nazionali corrispondenti degli altri Paesi dell'UE. A

[344] Millás, Vicente Moret. "Un nuevo escenario jurídico para la ciberseguridad en España: el Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información." (2018).

seguito della suddetta direttiva, il Regio Decreto Legge individua i settori in cui è necessario garantire la protezione delle reti e dei sistemi informativi e stabilisce le procedure per identificare i servizi essenziali offerti in questi settori, nonché i principali operatori che forniscono tali servizi, che sono, in breve, i destinatari dello stesso.

Gli operatori di servizi essenziali e i fornitori di servizi digitali adottano misure adeguate per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi che utilizzano, anche se la loro gestione è esternalizzata. Gli obblighi di sicurezza assunti devono essere proporzionati al livello di rischio che corrono ed essere basati su una valutazione preventiva di tali rischi. I regolamenti attuativi del Regio Decreto Legge in oggetto possono concretizzare gli obblighi di sicurezza richiesti agli operatori dei servizi essenziali, compresi, se del caso, i controlli e le ispezioni da effettuare o la partecipazione ad attività ed esercitazioni di gestione delle crisi. Il decreto legge prevede inoltre che gli operatori di servizi essenziali e i fornitori di servizi digitali notifichino qualsiasi incidente che si verifichi nelle reti e nei servizi informativi che utilizzano per fornire servizi essenziali e digitali, e che abbia un effetto dirompente su di essi, prevedendo anche la segnalazione di eventi o incidenti che possono influire sui servizi essenziali ma che non hanno ancora avuto un effetto negativo effettivo sui servizi essenziali, e delinea altresì le procedure di notifica[345]. Ancora, viene sottolineata la necessità di tenere conto degli standard europei e internazionali, nonché delle raccomandazioni emanate dal Gruppo di cooperazione e dalla rete CSIRT, istituita a livello comunitario dalla direttiva, con l'obiettivo di applicare le migliori pratiche apprese in questi forum e di contribuire alla promozione del mercato interno e alla partecipazione delle imprese nello stesso[346]. Al fine di aumentarne l'efficacia e, allo stesso tempo, di ridurre gli oneri amministrativi ed economici che tali obblighi comportano per gli enti interessati, il presente regio decreto-legge si propone di garantirne la coerenza con quelli

[345] Sono soggetti alla normativa del Regio Decreto Legge 12/2018 i fornitori di servizi digitali che hanno la loro sede legale in Spagna e la loro sede principale nell'Unione europea, nonché quelli che, non essendo stabiliti nell'UE, designano una stabile organizzazione in Spagna. Sono altresì soggetti gli operatori di servizi essenziali stabiliti in Spagna. A tal proposito, un operatore di servizi essenziali si intende stabilito in Spagna quando la sua residenza o la sua sede legale si trovano in territorio spagnolo, purché coincidano con il luogo in cui si trova la direzione amministrativa dei suoi affari o delle sue attività.

[346] Benalal, Alexander and María Berlanga Robles. “Ciberseguridad. Introducción al Real Decreto-Ley 12/2018 de seguridad de las redes y sistemas de información.” (2018).

derivanti dall'applicazione di altri regolamenti in materia di sicurezza dell'informazione, sia orizzontali che settoriali, e il coordinamento nella loro applicazione con le autorità di volta in volta competenti. Per quanto riguarda le norme orizzontali, sono degni di nota i collegamenti stabiliti con la legge 8/2011 che stabilisce misure per la protezione delle infrastrutture critiche, la legge 36/2015 sulla sicurezza nazionale, nonché con il regio decreto 3/2010, dell'8 gennaio, che regolamenta il Regime di sicurezza nazionale nel campo dell'Amministrazione Digitale, quale regolamento speciale sulla sicurezza dei sistemi informativi del settore pubblico. In questo modo, l'ambito di applicazione del regio decreto legge si avvicina a quello della legge 8/2011, aggiungendo ai settori previsti dalla Direttiva (UE) 2016/1148 gli ulteriori settori strategici previsti da tale legge; inoltre, si basa sulla legge 8/2011 per definire il concetto di servizio essenziale, e attribuisce ai suoi organi collegiali il compito di determinare i servizi essenziali e gli operatori di servizi essenziali soggetti alla propria normativa. Tenendo conto della legge 36/2015, al Consiglio nazionale di sicurezza è attribuita la funzione di fungere da punto di contatto con gli altri Paesi dell'Unione europea, nonché un ruolo di coordinamento della politica di cybersecurity attraverso la Strategia Nazionale di Cybersecurity.

La Strategia Nazionale di Cybersecurity di cui la Spagna si è dotata dal 2013 stabilisce le priorità, gli obiettivi e le misure appropriate per raggiungere e mantenere un elevato livello di sicurezza delle reti e dei sistemi informativi. La Strategia continuerà a sviluppare il quadro istituzionale per la cybersecurity delineato dal Regio Decreto Legge in questione, che comprende le autorità pubbliche competenti e i CSIRT di riferimento, da un lato, e la cooperazione pubblico-privato dall'altro. Tale regio decreto legge delimita l'ambito funzionale di azione dei CSIRT di riferimento previsti dallo stesso: questi CSIRT sono la porta d'ingresso per le notifiche di incidenti, che consentiranno di organizzare rapidamente la risposta agli stessi, ma il destinatario delle notifiche è la rispettiva autorità competente, che terrà conto di queste informazioni per la supervisione degli operatori. In ogni caso, l'operatore è responsabile della risoluzione degli incidenti e del ripristino del normale funzionamento delle reti e dei sistemi informativi interessati. È previsto l'utilizzo di una piattaforma comune per la segnalazione degli incidenti, in modo che gli operatori non debbano effettuare diverse notifiche a seconda

dell'autorità a cui devono rivolgersi. Questa piattaforma può essere utilizzata anche per la notificazione delle violazioni della sicurezza dei dati personali ai sensi del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

In materia di sicurezza delle reti e dei sistemi informativi sono diverse le autorità competenti. Per gli operatori di servizi essenziali[347], se considerati operatori critici, è competente la Segreteria di Stato di sicurezza, del ministero dell'interno, attraverso il Centro nazionale di protezione delle infrastrutture e cibersicurezza (CNPIC[348]). Se invece non si tratta di operatori critici, la competenza riguarda l'autorità settoriale corrispondente per materia. Per gli operatori di servizi essenziali e i fornitori di servizi digitali che non sono operatori critici e sono inclusi nell'ambito di applicazione della legge 40/2015 sul regime giuridico del settore pubblico, l'autorità competente è il Ministero della Difesa, attraverso il Centro nazionale di crittografia (CCN)[349]. Inoltre, il Consiglio nazionale di sicurezza, attraverso il suo comitato specializzato in materia di cybersicurezza, stabilisce i necessari meccanismi di coordinamento delle azioni delle autorità competenti. Le autorità competenti, tra le altre cose, controllano l'osservanza da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali degli obblighi loro

[347] Secondo la definizione data dalla legge 8/2011, all'articolo 2, per servizio essenziale si intende il servizio necessario per il mantenimento delle funzioni sociali di base, la salute, la sicurezza, il benessere sociale ed economico dei cittadini, o l'efficace funzionamento delle istituzioni statali e delle pubbliche amministrazioni. *«BOE-A-2011-7630 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.», 6 settembre 2023, https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630.*

[348] Il Centro Nazionale per la Protezione delle Infrastrutture Critiche (CNPIC) è l'organo del Ministero dell'Interno preposto alla promozione, al coordinamento e alla supervisione di tutte le attività affidategli dal Segretario di Stato per la Sicurezza in relazione alla Protezione delle Infrastrutture Critiche sul territorio nazionale. *«CNPIC | Inizio», https://cnpic.interior.gob.es/opencms/es/inicio/.*

[349] La legge 40/2015, del 1° ottobre, sul regime giuridico del settore pubblico, delinea il proprio ambito di applicazione soggettivo all'articolo 2: "La presente legge si applica al settore pubblico comprendente: a) l'Amministrazione Generale dello Stato; b) le amministrazioni delle Comunità autonome; c) gli Enti che compongono l'Amministrazione Locale; d) il settore pubblico istituzionale. Il settore pubblico istituzionale è composto da: a) eventuali enti pubblici ed enti di diritto pubblico legati o dipendenti dalle Pubbliche Amministrazioni; b) gli enti di diritto privato legati o dipendenti dalle Pubbliche Amministrazioni che saranno soggetti alle disposizioni delle norme della presente Legge che ad essi specificamente si riferiscono, in particolare ai principi previsti dall'articolo 3, e comunque, quando esercitano poteri amministrativi; c) le università pubbliche che saranno disciplinate dai loro regolamenti specifici e inoltre dalle disposizioni della presente legge. Sono considerate Pubbliche Amministrazioni l'Amministrazione Generale dello Stato, le Amministrazioni delle Comunità Autonome, gli Enti che compongono l'Amministrazione Locale, nonché gli enti pubblici e gli enti di diritto pubblico di cui alla lettera a) della sezione 2". *«BOE-A-2015-10566 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.», https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566.*

impartiti, stabiliscono con questi canali di comunicazione e si coordinano con i CSIRT di riferimento attraverso i protocolli d'azione. Inoltre, le autorità competenti ricevono le notifiche di incidenti presentate loro attraverso i CSIRT di riferimento, dopodiché informano il punto di contatto unico delle notifiche di tali incidenti; informano, se del caso, il pubblico su determinati incidenti quando la diffusione di tali informazioni sia necessaria per prevenire un incidente o per gestirne uno che si è già verificato[350]. Ancora, le autorità competenti in materia di sicurezza digitale collaborano con le autorità competenti in materia di protezione dei dati personali, pubblica sicurezza, sicurezza nazionale, nonché con le autorità settoriali corrispondenti. Da ultimo, esse stabiliscono obblighi specifici per garantire la sicurezza delle reti e dei sistemi informativi e per la segnalazione degli incidenti, nonché emettono istruzioni tecniche e linee guida per dettagliare il contenuto dei predetti obblighi.

Il Regio Decreto Legge 12/2018 individua anche i Computer Security Incident Response Teams (CSIRT) di riferimento per la sicurezza delle reti e dei sistemi informativi. Per quanto riguarda i rapporti con gli operatori dei servizi essenziali, il CCN-CERT del Centro Crittologico Nazionale è responsabile della comunità di riferimento costituita dai soggetti rientranti nell'ambito soggettivo di applicazione della legge 40/2015. Responsabile della comunità di riferimento costituita dalle entità non incluse, invece, è INCIBE-CERT dell'Istituto Nazionale di Cybersecurity spagnolo. L'INCIBE-CERT sarà gestito congiuntamente dall'INCIBE e dal CNPIC per tutto ciò che riguarda la gestione degli incidenti che interessano gli operatori critici. Inoltre, ESPDEF-CERT del Ministero della Difesa è il CSIRT che collabora con il CCN-CERT e l'INCIBE-CERT nelle situazioni in cui si verificano eventi critici, ossia quelle che hanno un impatto sulla difesa nazionale e che sono determinati dalla normativa stessa. L'INCIBE-CERT sarà anche il team di incident response di riferimento per cittadini, enti di diritto privato e altre entità non incluse nella sezione I del regio decreto. I CSIRT di riferimento si coordinano tra

[350] Le autorità competenti possono stabilire, tramite decreto ministeriale, specifici obblighi di notifica per gli operatori di servizi essenziali; possono inoltre emanare istruzioni tecniche e linee guida per dettagliare il contenuto di tali ordini. Nell'elaborazione di regolamenti, istruzioni e linee guida, si tiene conto degli obblighi settoriali, delle linee guida pertinenti da adottare all'interno del gruppo di cooperazione e degli obblighi di segnalazione degli incidenti a cui l'operatore è soggetto in base ad altre normative, come ad esempio la legge 8/2011 e il regio decreto 3/2010 che approvò il Regime di sicurezza nazionale.

loro e con il resto dei CSIRT nazionali e internazionali nella risposta agli incidenti e nella gestione dei rischi per la sicurezza di cui sono responsabili. Quando le loro attività possono in qualche modo influire su un operatore critico, i CSIRT dell'operatore critico ed il CSIRT di riferimento si coordinano con il Ministero dell'Interno, attraverso il CBRN-CERT, ossia l'Ufficio di coordinamento informatico del Centro nazionale per la protezione delle infrastrutture e la sicurezza informatica (CNPIC). I CSIRT devono garantire un elevato livello di disponibilità dei loro servizi di comunicazione, evitando guasti occasionali, e devono disporre di diversi mezzi per essere in grado di rispondere alle richieste del pubblico. Inoltre, i canali di comunicazione devono essere chiaramente specificati e ben noti ai gruppi di utenti e ai partner che collaborano. Le loro strutture devono garantire la continuità delle attività; a tal fine sono dotati di un sistema appropriato per la gestione e la canalizzazione delle richieste, devono disporre di personale sufficiente a garantire la loro disponibilità in qualsiasi momento, inoltre hanno accesso a infrastrutture di comunicazione la cui continuità sia garantita (per ciò, dispongono di sistemi ridondanti e di spazi di lavoro di riserva). Oltre a quanto detto finora, i CSIRT monitorano gli incidenti a livello nazionale, diffondono tempestivamente avvisi, allarmi, consigli e informazioni sui rischi e sugli incidenti alle parti interessate. Altresì, partecipano alla rete di CSIRT, rispondono agli incidenti e conducono un'analisi proattiva dei rischi e degli incidenti mirando alla consapevolezza della situazione. Al fine di facilitare relazioni di cooperazione con il settore privato, i CSIRT incoraggiano l'adozione e l'uso di pratiche comuni o standardizzate delle procedure di gestione degli incidenti e dei rischi, nonché dei sistemi di classificazione e segnalazione degli incidenti stessi. Le notifiche degli operatori di servizi essenziali e dei fornitori di servizi digitali devono riguardare gli incidenti che interessano le reti e i sistemi informativi utilizzati per la fornitura dei servizi indicati, siano essi propri o di fornitori esterni, compresi quelli dei fornitori di servizi digitali soggetti al Regio decreto legge 12/2018[351].

[351] «Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información», https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:72016L1148ESP_262899&qid=1694017167358.

Le autorità competenti e i CSIRT di riferimento utilizzeranno una piattaforma comune per facilitare e automatizzare i processi di notifica, la comunicazione e la segnalazione degli incidenti. Il CCN-CERT in collaborazione con l'INCIBE-CERT e l'ESPDEF-CERT del Comando congiunto per il cyberspazio mette a disposizione di tutti gli attori coinvolti la Piattaforma nazionale di notifica e monitoraggio degli incidenti informatici. La piattaforma consente lo scambio di informazioni e il monitoraggio degli incidenti tra gli operatori di servizi essenziali o i fornitori di servizi digitali, le autorità competenti e i CSIRT di riferimento in modo sicuro e affidabile, fatti salvi i requisiti specifici che si applicano in termini di protezione dei dati personali. Tale piattaforma dovrà inoltre garantire la disponibilità, l'autenticità, l'integrità e la riservatezza delle informazioni e potrà essere utilizzata anche per adempiere all'obbligo di notifica derivante da normative settoriali. Il CCN-CERT, in qualità di CERT del governo nazionale, collabora con tutte le agenzie pubbliche e le aziende di interesse strategico per il paese nel rilevamento, notifica, valutazione, risposta, trattamento e apprendimento di incidenti di sicurezza delle informazioni o incidenti informatici che i loro sistemi possono subire. In questo processo, sempre svolto nella più assoluta riservatezza tra le due parti, il CCN-CERT fornisce supporto tecnico e operativo, sia nelle fasi di rilevazione, sia di reazione, contenimento ed eliminazione. A questo si aggiunge una politica preventiva, in cui un team di esperti lavora per indagare le tecniche utilizzate, le tendenze, le soluzioni e le procedure più appropriate per affrontarle, comprese le metodologie per raccogliere e analizzare dati ed eventi, le procedure per classificare la loro pericolosità e la loro priorità. Funge inoltre da nodo per lo scambio di informazioni sugli incidenti informatici nei sistemi informativi delle pubbliche amministrazioni e da principale coordinatore con gli organi preposti per lo scambio di informazioni. La sua presenza come CERT del governo nazionale in tutti i forum internazionali con organizzazioni simili di altri paesi fornisce informazioni molto preziose per una gestione rapida ed efficace di qualsiasi incidente.

Per continuare l'analisi in merito al recepimento della normativa europea è bene evidenziare il fatto che il governo spagnolo aveva già istituito un obbligo di notificazione degli incidenti ancor prima dell'emanazione della direttiva NIS; infatti, il sistema di notificazione è stato dettato al principio dal Regio Decreto 3/2010. Questo si è occupato di stabilire i principi di base e i requisiti minimi che, in conformità con l'interesse generale, la natura e la complessità della materia regolamentata, consentono un'adeguata protezione delle informazioni e dei servizi, che richiede l'inclusione dell'ambito e della procedura per gestire la sicurezza elettronica dei sistemi che elaborano le informazioni delle pubbliche amministrazioni nell'ambito di applicazione della legge 11/2007 che istituì lo Schema di sicurezza nazionale. Con ciò si ottiene un comune denominatore normativo, la cui regolamentazione non esaurisce tutte le possibilità di normazione, e consente di essere completata, attraverso la regolamentazione degli obiettivi che possono essere decisi dalle politiche legislative territoriali.

Per rispettare quanto sopra, vengono determinate le dimensioni di sicurezza e i loro livelli, la categoria dei sistemi, le misure di sicurezza appropriate e l'audit periodico della sicurezza[352]. La preparazione di un rapporto è attuata per conoscere regolarmente lo stato di sicurezza dei

[352] Con riguardo al tema delle certificazioni, l'auditing aziendale è una parte molto importante, anzi decisiva, dell'intero processo. La parola "audit" origina dal latino e significa "ascolto": essa era usata nell'antica Roma per indicare quei soggetti che controllavano l'amministrazione del denaro pubblico mediante la cosiddetta audizione dei risultati contabili. Questa attività di controllo viene oggi applicata, mutando il contesto, nell'ambito aziendale, coinvolgendo l'integralità del processo necessario per la certificazione di qualità. Dunque per la definizione di audit aziendale occorre riferirsi a tutto il sistema che comporta la definizione di obiettivi e procedure necessarie, individuando criticità e soluzioni, per arrivare in ultimo all'adempimento di obblighi normativi o ad ottenere o mantenere una certificazione dei sistemi di gestione nel momento in cui questi siano stati implementati in azienda. Il cosiddetto audit interno si riferisce a un'attività di consulenza, controllo e verifica delle procedure messe in campo che viene svolta da personale interno all'azienda, che opera in posizione di indipendenza funzionale. In realtà l'audit interno può essere esercitato da professionisti sia interni che esterni all'azienda: la parola "internal" per l'audit si riferisce alla direzione delle informazioni correlate alla valutazione e al miglioramento dell'efficienza dell'organizzazione aziendale, che è appunto sempre l'impresa stessa e non soggetti esterni, come accade invece in altri ambiti attigui come la certificazione di bilanci. Il primo passaggio importante nel processo di audit riguarda la raccolta dei dati e delle informazioni, identificando le aree dell'impresa che devono essere coinvolte, gli strumenti da utilizzare e la pianificazione delle attività di raccolta dati, con una valutazione complessiva di protocolli e parametri. Lo step successivo riguarda la fase di ascolto e acquisizione delle informazioni attraverso interviste a impiegati e organi dirigenziali dell'impresa, a cui si aggiungono ispezioni ed indagini osservative del contesto di lavoro. La terza fase del processo di auditing comporta l'elaborazione delle criticità rilevate, e i suggerimenti circa le migliorie, le azioni e gli obiettivi da raggiungere per implementare il sistema aziendale al fine dell'ottenimento della certificazione. A conclusione del processo di auditing, colui che svolge il ruolo di auditor dovrà procedere alla elaborazione di una relazione scritta, che rappresenterà la base di partenza per arrivare al miglioramento previsto come mission dal sistema aziendale. *«Cos'è un audit? Il processo di auditing, la definizione», 23 ottobre 2019, https://www.bcbcertificazioni.com/blog/cos-e-un-audit.*

sistemi informativi ed il ruolo della capacità di risposta agli incidenti di sicurezza delle informazioni del Centro nazionale di crittografia[353]. In questo regio decreto la sicurezza è concepita come un'attività integrale, in cui non c'è spazio per azioni specifiche o trattamenti circostanziali, perché la debolezza di un sistema è determinata dal suo punto più fragile e, spesso, questo punto è il coordinamento tra misure individualmente adeguate ma mal assemblate. La sicurezza del sistema deve tener conto degli aspetti della prevenzione, dell'individuazione e della correzione, al fine di garantire che le minacce nei suoi confronti non si concretizzino, cioè non pregiudichino gravemente le informazioni che tratta o i servizi forniti. Le misure preventive dovrebbero eliminare o almeno ridurre la possibilità che le minacce si concretizzino a danno del sistema. Tali misure preventive comprendono, tra l'altro, la dissuasione e la riduzione dell'esposizione. Inoltre, le misure di individuazione sono accompagnate da misure di reazione in modo che gli incidenti di sicurezza siano affrontati in tempo. Le misure di recupero, invece, consentono di ripristinare le informazioni e i servizi in modo da poter affrontare le situazioni in cui un incidente di sicurezza disattiva i mezzi abituali. Fatti salvi gli altri principi fondamentali e gli altri requisiti minimi stabiliti, il sistema garantisce che i dati e le informazioni siano conservati in formato elettronico. Allo stesso modo, il sistema manterrà i servizi disponibili durante tutto il ciclo di vita dell'informazione digitale, attraverso una concezione e procedure che sono la base per la conservazione del patrimonio digitale. Il sistema dispone di una strategia di protezione costituita da più livelli di sicurezza, disposti in modo tale che, in caso di guasto di uno dei livelli, consenta sia di guadagnare tempo per una reazione adeguata agli incidenti che non possono essere evitati, sia di ridurre la probabilità che il sistema nel suo complesso venga compromesso, nonché di ridurre al minimo l'impatto finale su di esso.

Gli incidenti di sicurezza che si verificano e le azioni di trattamento seguite sono registrati. Questi registri saranno utilizzati per il miglioramento continuo della sicurezza del sistema. Le notifiche e le pubblicazioni elettroniche delle risoluzioni e degli atti amministrativi sono

[353] Le informazioni trattate nei sistemi elettronici di cui al regio decreto 3/2010 saranno protette tenendo conto dei criteri stabiliti nella legge organica 15/1999, del 13 dicembre.

effettuate in modo tale da soddisfare, quali requisiti tecnici, l'autenticità dell'organismo, l'integrità delle informazioni pubblicate, nonché l'autenticità del destinatario della pubblicazione o della notifica. I sistemi di informazione sono sottoposti a regolare verifica ordinaria, almeno ogni due anni, per verificare la conformità ai requisiti del Regime nazionale di sicurezza. In via straordinaria, tale verifica deve essere effettuata ogniqualvolta vi siano modifiche sostanziali al sistema informativo, che possono avere un impatto sulle misure di sicurezza richieste. Lo svolgimento della revisione straordinaria determinerà la data di calcolo per il calcolo del biennio, stabilita per la realizzazione della successiva revisione ordinaria. L'audit è effettuato sulla base della categoria del sistema e mira ad approfondire i dettagli di questo al livello che ritiene fornisca prove sufficienti e pertinenti, nell'ambito stabilito per l'audit stesso[354]. Inoltre, la relazione di revisione esprime un parere sul grado di conformità al regio decreto stesso, ne individua le carenze e suggerisce le eventuali misure correttive o complementari necessarie, nonché le raccomandazioni ritenute appropriate. Essa comprende altresì i criteri metodologici di audit utilizzati, la portata e l'obiettivo dell'audit, nonché i dati, i fatti e le osservazioni su cui si basano le conclusioni tratte. Le relazioni di audit sono presentate al responsabile del sistema e al responsabile della sicurezza competenti. Tali relazioni saranno analizzate da quest'ultimo che presenterà le sue conclusioni al responsabile del sistema affinché possa adottare le misure correttive appropriate. I responsabili di ciascuna organizzazione competente in materia di sicurezza informatica possono richiedere relazioni di audit. Il CCN articolerà la risposta agli incidenti di sicurezza attorno alla struttura denominata CCN-CERT, che agirà fatte salve le capacità di risposta agli incidenti di sicurezza che ogni pubblica amministrazione può avere e la funzione di coordinamento a livello nazionale e internazionale del CCN.

Per quanto riguarda la fornitura di servizi di risposta agli incidenti di sicurezza alle pubbliche amministrazioni, il CCN-CERT fornisce ad esse supporto e coordinamento per il trattamento delle vulnerabilità e la risoluzione degli incidenti di sicurezza che hanno l'Amministrazione

[354] Nello svolgimento di tale audit sono utilizzati i criteri, i metodi di lavoro e la condotta generalmente riconosciuti e la normazione nazionale e internazionale applicabili a tali audit dei sistemi di informazione.

Generale dello Stato, le Amministrazioni delle comunità autonome, gli enti che compongono l'Amministrazione Locale e gli Enti di Diritto Pubblico, con una propria personalità giuridica, collegati o dipendenti da una qualsiasi delle amministrazioni indicate. Il CCN-CERT, attraverso il proprio servizio di supporto tecnico e coordinamento, agirà nel minor tempo possibile in caso di eventuali aggressioni ricevute nei sistemi informativi delle Pubbliche Amministrazioni[355]. Inoltre, tale organismo fornisce il servizio di ricerca e diffusione delle migliori pratiche in materia di sicurezza delle informazioni tra tutti i membri delle pubbliche amministrazioni. A tal fine, la serie di documenti CCN-STIC[356], preparati dal CCN, offrirà standard, istruzioni, guide e raccomandazioni per applicare il Regime di sicurezza nazionale e per garantire la sicurezza dei sistemi informatici nell'Amministrazione. Da ultimo, il CCN-CERT provvede alla formazione del personale dell'Amministrazione specializzato nel campo della sicurezza informatica, al fine di facilitare l'aggiornamento delle conoscenze del personale dell'amministrazione e di raggiungere la consapevolezza e il miglioramento delle proprie capacità per l'individuazione e la gestione degli incidenti; inoltre, si occupa di fornire alle amministrazioni informazioni su vulnerabilità, allarmi e segnalazioni di nuove minacce ai sistemi informativi, raccolte da varie fonti di riconosciuto prestigio, compresa la propria[357].

[355] Romero, Javier Candau. "CCN-CERT: defensa frente a ataques dirigidos contra la administración y las empresas de interés estratégico." (2014).

[356] La serie CCN-STIC è composta da regolamenti, linee guida, guide e raccomandazioni sviluppate dal CCN al fine di migliorare la sicurezza informatica all'interno delle organizzazioni. Queste guide vengono regolarmente aggiornate e integrate con nuove informazioni, in base alle minacce e alle vulnerabilità rilevate dal CCN-CERT. Il grosso di questa collana è rivolto alla Pubblica Amministrazione e alle aziende e organizzazioni di interesse strategico. Ci sono anche guide aperte a tutti gli utenti; alcune guide sono classificate come Riservate (DL) o Riservate (C), e devono essere richieste al CCN-CERT, con la condizione essenziale di essere registrate nella parte privata del portale. *«Guide alla sicurezza CCN-STIC», https://www.ccn.cni.es/index.php/en/menu-guides-ccn-stic-en.*

[357] Ministerio de la Presidencia, «Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica», Pub. L. No. Real Decreto 3/2010, § 1, BOE-A-2010-1330 8089 (2010), https://www.boe.es/eli/es/rd/2010/01/08/3.

13. Le infrastrutture critiche della Spagna

La disciplina relativa alle infrastrutture critiche è contenuta nella legge 8/2001 e nel Regio decreto 704/2011, adottato al fine di recepire la direttiva europea del 2008, con il quale si approva il regolamento di protezione delle infrastrutture critiche. Gli Stati moderni oggi affrontano sfide diverse, rispetto che in passato, che conferiscono alla sicurezza nazionale un carattere sempre più complesso. Questi nuovi rischi, generati, in larga misura, dalla globalizzazione, e che includono il terrorismo internazionale, la proliferazione delle armi di distruzione di massa o la criminalità organizzata, si aggiungono a quelli esistenti, di cui il terrorismo tradizionale era stato un esponente. In questo contesto, le società sono sempre più dipendenti dal complesso sistema di infrastrutture che sostengono e consentono il normale sviluppo dei settori produttivi, gestionali e della vita civile in generale. Queste infrastrutture sono spesso altamente interdipendenti, motivo per cui i problemi di sicurezza che possono ripercuotersi a cascata attraverso il sistema stesso hanno il potenziale di causare guasti imprevisti e sempre più gravi nei servizi di base per la popolazione. A tal punto che eventuali interruzioni indesiderate – anche di breve durata e dovute a cause naturali o tecniche o ad attacchi deliberati – potrebbero avere gravi conseguenze sui flussi di forniture vitali o sul funzionamento dei servizi essenziali, oltre a causare gravi interruzioni e malfunzionamenti della sicurezza, oggetto di particolare attenzione per il sistema nazionale di gestione delle crisi. Tra le priorità strategiche della sicurezza nazionale ci sono le infrastrutture, che sono esposte a una serie di minacce. Per la loro protezione, è essenziale, da un lato, catalogare l'insieme di quelli che forniscono servizi essenziali alla società e, dall'altro, progettare una pianificazione che contenga efficaci misure di prevenzione e protezione contro possibili minacce a tali infrastrutture, sia nel campo della sicurezza fisica che nella sicurezza delle tecnologie dell'informazione e della comunicazione[358]. In questa direzione sono state intraprese diverse azioni a livello nazionale, come l'approvazione, da parte del Segretario di Stato per la Sicurezza

[358] Morán Espinosa, Licenciada Alejandra. "Ciberseguridad: aprendizaje disruptivo en la protección de infraestructuras críticas y la seguridad nacional." Seguridad, Ciencia & Defensa (2021): pag. 4.

del Ministero dell'Interno, di un primo Piano Nazionale per la Protezione delle Infrastrutture Critiche, del 7 maggio 2007, nonché la predisposizione di un Catalogo Nazionale delle Infrastrutture Strategiche[359]. Allo stesso modo, il 2 novembre 2007, il Consiglio dei ministri ha approvato un accordo sulla protezione delle infrastrutture critiche, attraverso il quale è stato dato un impulso decisivo in questo settore. Lo sviluppo e l'attuazione di questo accordo rappresentano un progresso qualitativo di prim'ordine per garantire la sicurezza dei cittadini e il corretto funzionamento dei servizi essenziali. Allo stesso tempo, vi sono anche una serie di azioni condotte a livello europeo: in seguito ai terribili attentati di Madrid, il Consiglio europeo del giugno 2004 ha invitato la Commissione europea ad elaborare una strategia globale sulla protezione delle infrastrutture critiche. Il 20 ottobre 2004 la Commissione ha adottato una comunicazione sulla protezione delle infrastrutture critiche nella lotta al terrorismo, che contiene proposte volte a migliorare la prevenzione, la preparazione e la risposta dell'Europa agli attacchi terroristici che la riguardano. Successivamente, nel dicembre 2004, il Consiglio ha approvato l'EPCIP (Programma europeo di protezione delle infrastrutture critiche) e ha lanciato una rete di informazione di allarme sulle infrastrutture critiche (ossia il CIWIN[360]).

Attualmente, l'entrata in vigore della direttiva 2008/114/CE del Consiglio, dell'8 dicembre, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla

[359] Il Sistema PIC, incluso nel Titolo II della Legge 8/2011, è costituito da un insieme di agenti, del settore pubblico e privato, con competenze e responsabilità ben definite affinché le infrastrutture critiche dello Stato forniscano servizi essenziali per la società con garanzie sufficienti e senza interruzioni, creando un sistema preventivo in grado di anticipare le situazioni di crisi. Il sistema PIC spagnolo è composto da 12 dipartimenti ministeriali e 10 organi dell'Amministrazione centrale e autonoma e da oltre 250 operatori critici – pubblici e privati – sotto l'autorità del Segretario di Stato per la Sicurezza. Tutto ciò comporta la gestione da parte del CNPIC di una rete di oltre 300 entità e circa 1.200 piani di sicurezza, sia strategici che operativi.

[360] L'istituzione della rete di informazione di allarme sulle infrastrutture critiche (CIWIN) è una delle misure previste per facilitare l'attuazione del programma europeo per la protezione delle infrastrutture critiche (EPCIP). Nell'ottobre 2008 la Commissione europea ha pubblicato una proposta di decisione del Consiglio relativa a una rete di informazione di allarme sulle infrastrutture critiche (CIWIN). La proposta mirava ad aiutare gli Stati membri e la Commissione europea a scambiarsi informazioni sulle minacce condivise, le vulnerabilità e le misure e strategie appropriate per attenuare i rischi a sostegno della protezione delle infrastrutture critiche (CIP). La rete CIWIN è stata sviluppata come sistema pubblico protetto di informazione e comunicazione basato su Internet di proprietà della Commissione, che offre ai membri riconosciuti della comunità CIP dell'UE l'opportunità di scambiare e discutere informazioni, studi e/o buone pratiche relativi al CIP in tutti gli Stati membri dell'UE e in tutti i settori pertinenti dell'attività economica. Il portale CIWIN, dopo le sue fasi di prototipo e pilota, è operativo da metà gennaio 2013. *«Critical Infrastructure Warning Information Network (CIWIN)», https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin_en.*

valutazione della necessità di migliorarne la protezione, costituisce un passo importante nella cooperazione in questo settore all'interno dell'Unione. La presente direttiva stabilisce che la responsabilità primaria e ultima della protezione delle infrastrutture critiche europee spetta agli Stati membri e ai loro operatori, e determina lo sviluppo di una serie di obblighi e azioni da parte di tali Stati che devono essere recepiti nella legislazione nazionale. Le azioni necessarie per ottimizzare la sicurezza delle infrastrutture si inquadrano principalmente nel campo della protezione contro aggressioni deliberate e, soprattutto, contro gli attacchi terroristici, risultando quindi guidati dal Ministero dell'Interno. Tuttavia, la sicurezza delle infrastrutture critiche richiede di contemplare azioni che vadano oltre la mera protezione materiale contro possibili aggressioni o attacchi, motivo per cui è inevitabile coinvolgere altri organi dell'Amministrazione Generale dello Stato, altre Pubbliche Amministrazioni, altri enti pubblici e il settore privato. Queste infrastrutture critiche dipendono sempre più dalle tecnologie dell'informazione, sia per la loro gestione che per il loro collegamento con altri sistemi, per i quali si basano, principalmente, su mezzi di informazione e comunicazione pubblici e aperti. È quindi necessario contare sulla cooperazione di tutti gli attori coinvolti nella regolamentazione, pianificazione e gestione delle diverse infrastrutture che forniscono servizi essenziali per la società, fermo restando il coordinamento che il Ministero dell'Interno eserciterà in collaborazione con le Comunità autonome. Di conseguenza, e data la complessità della materia, il suo impatto sulla sicurezza delle persone e sul funzionamento delle strutture di base nazionali e internazionali, e in conformità con le disposizioni della direttiva 2008/114 / CE, è necessario sviluppare uno standard il cui scopo è, da un lato, regolamentare la protezione delle infrastrutture critiche contro attacchi deliberati di ogni tipo (sia fisici che cibernetici) e, dall'altro, la definizione di un sistema organizzativo per la protezione di queste infrastrutture che riunisca le Pubbliche Amministrazioni e i soggetti privati interessati. Come parte fondamentale di questo sistema, la legge crea il Centro nazionale per la protezione delle infrastrutture critiche come organo per assistere il Segretario di Stato per la sicurezza nell'esecuzione delle funzioni a lui affidate come organismo responsabile del sistema. Lo scopo della legge 8/2011 è, quindi, l'istituzione di misure di protezione delle infrastrutture critiche che

forniscano una base adeguata su cui stabilire un efficace coordinamento delle Pubbliche Amministrazioni e degli enti che gestiscono o possiedono infrastrutture che forniscono servizi essenziali per la società, al fine di ottenere una migliore sicurezza per loro. Su tale base, saranno sostenuti il Catalogo nazionale delle infrastrutture strategiche (conformemente alla comunicazione del Consiglio dell'Unione europea del 20 ottobre 2004, in base alla quale ciascun settore e ciascuno Stato membro devono individuare le infrastrutture critiche nei rispettivi territori) e il Piano nazionale per la protezione delle infrastrutture critiche, come strumenti principali nella gestione della sicurezza delle nostre infrastrutture[361].

La Segreteria di Stato per la sicurezza è l'organo supremo del Ministero dell'interno responsabile del sistema nazionale di protezione delle infrastrutture critiche. Il Centro Nazionale per la Protezione delle Infrastrutture Critiche (CNPIC) è costituito quale organo ministeriale incaricato di promuovere, coordinare e supervisionare tutte le attività affidate al Segretario di Stato per la Sicurezza in relazione alla protezione delle Infrastrutture Critiche nel territorio nazionale. Il CNPIC riferisce organicamente al Segretariato di Stato per la sicurezza ed è responsabile delle registrazioni, delle cancellazioni e delle modifiche delle infrastrutture presenti nel catalogo, nonché della determinazione della criticità delle infrastrutture strategiche ivi incluse. Per ciascun settore strategico è designato almeno un ministero, agenzia, ente o organo dell'amministrazione generale dello Stato integrato nel sistema. Inoltre, i ministeri e le agenzie del Sistema hanno il compito di promuovere, nell'ambito delle loro competenze, le politiche di sicurezza del Governo nei diversi settori strategici nazionali e di assicurarne l'attuazione, fungendo anche da punti di contatto specializzati in materia. A tal fine, collaboreranno con il Ministero dell'Interno attraverso il Segretario di Stato per la Sicurezza. Infine, l'altro soggetto rilevante in materia di infrastrutture critiche è la Commissione nazionale per la protezione delle infrastrutture critiche, istituita come organo collegiale presso il Segretario di Stato per la sicurezza. La Commissione è responsabile dell'approvazione dei

[361] «BOE-A-2011-7630 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.», https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630.

diversi piani strategici settoriali e della designazione degli operatori critici, su proposta del gruppo di lavoro interdipartimentale per la protezione delle infrastrutture critiche.

La legge 8/2011, che stabilisce misure per la protezione delle infrastrutture critiche, autorizza il governo, nella sua quarta disposizione finale, a emanare i regolamenti per l'attuazione dello sviluppo della suddetta legge. In ottemperanza a tale mandato, il Regio Decreto 704/2011, del 20 maggio, è stato approvato, in primo luogo, al fine di sviluppare, specificare e ampliare gli aspetti contemplati nella suddetta legge, soprattutto quando il tenore della stessa segue non solo l'articolazione di un complesso sistema di carattere interdipartimentale per la protezione delle infrastrutture critiche, composto da enti sia della Pubblica Amministrazione che del settore privato, ma la progettazione di una pianificazione complessiva volta a prevenire e proteggere le cosiddette infrastrutture critiche da minacce o atti intenzionali di figure criminali come il terrorismo, potenziate attraverso le tecnologie della comunicazione. In secondo luogo, questo testo normativo non solo è coerente con il quadro giuridico da cui deriva, ma serve anche agli scopi del Sistema nazionale di gestione delle crisi ed è conforme al recepimento obbligatorio della direttiva 2008/114/CE, del Consiglio dell'Unione europea, sull'individuazione e la designazione delle infrastrutture critiche europee e sulla valutazione della necessità di migliorarne la protezione. Ciò è dovuto alle ampie disposizioni che il testo contempla nell'ambito dei diversi Piani che devono essere predisposti sia dalle Pubbliche Amministrazioni – nel caso del Piano Nazionale per la Protezione delle Infrastrutture Critiche, dei Piani Strategici Settoriali e dei Piani Operativi di Supporto – sia da parte di aziende, enti o istituzioni classificate come operatori critici, ai quali la legge attribuisce una serie di obblighi, tra i quali l'elaborazione di due strumenti di pianificazione: i Piani di Sicurezza dell'Operatore e i Piani Specifici di Protezione. Allo stesso modo, la legge prevede che gli operatori critici designino un ufficiale di sicurezza e di collegamento, che deve essere autorizzato come direttore della sicurezza concesso ad approvare il regolamento di sicurezza privata, o qualifica equivalente, secondo il loro regolamento specifico. Allo stesso modo, è prevista la designazione di un Delegato alla sicurezza per ciascuna delle infrastrutture critiche individuate.

Il Titolo I contiene le questioni generali relative al suo scopo e ambito di applicazione, e dedica un articolo alla figura del Catalogo Nazionale delle Infrastrutture Strategiche, quale strumento del Segretario di Stato per la Sicurezza del Ministero dell'Interno, che deve riunire tutti i dati e la valutazione della criticità delle suddette infrastrutture e che servirà come base per pianificare le azioni necessarie in termini di sicurezza e protezione del lo stesso, da nutrire con i contributi degli operatori stessi. Il Titolo II è interamente dedicato al Sistema di Protezione delle Infrastrutture Critiche e sviluppa, tra l'altro, le disposizioni giuridiche relative agli organismi creati dalla Legge, ovvero il Centro Nazionale per la Protezione delle Infrastrutture Critiche (CNPIC), la Commissione Nazionale per la Protezione delle Infrastrutture Critiche e il Gruppo di Lavoro Interdipartimentale per la Protezione delle Infrastrutture Critiche, specificando la composizione, le competenze e il funzionamento di tutti loro. Il Titolo III è responsabile della regolamentazione degli strumenti di pianificazione, concentrandosi su ciascuno dei suddetti Piani, il cui processo di preparazione, approvazione e registrazione, nonché il loro contenuto materiale, regola in modo più dettagliato. Infine, il titolo IV è dedicato alla sicurezza delle comunicazioni e alle figure dell'Ufficiale di collegamento e Delegato alla sicurezza delle infrastrutture critiche. Lo scopo del presente regolamento è quello di sviluppare il quadro previsto dalla legge 8/2011 al fine di specificare le azioni dei diversi organismi che compongono il Sistema di Protezione delle Infrastrutture Critiche, nonché i diversi strumenti di pianificazione dello stesso. Parimenti, il decreto disciplina gli obblighi speciali che devono essere assunti sia dallo Stato che dai gestori di quelle infrastrutture che sono ritenute critiche. Il Catalogo Nazionale delle Infrastrutture Strategiche è il registro amministrativo che contiene informazioni complete, aggiornate e verificate su tutte le infrastrutture strategiche situate nel territorio nazionale, comprese le infrastrutture critiche e quelle classificate come infrastrutture critiche europee che interessano la Spagna, conformemente alla direttiva 2008/114/CE. Lo scopo principale del Catalogo è quello di valutare e gestire i dati disponibili delle diverse infrastrutture, con l'obiettivo di progettare i meccanismi di pianificazione, prevenzione, protezione e reazione a una possibile minaccia nei loro confronti e, se necessario, attivare, in conformità a quanto previsto dal Piano Nazionale per la Protezione delle Infrastrutture Critiche,

una risposta agile, tempestiva e proporzionata, in funzione del livello e delle caratteristiche della minaccia in questione[362]. Il Catalogo sarà alimentato dalle informazioni fornite al Centro Nazionale per la Protezione delle Infrastrutture Critiche (CNPIC) dagli operatori dell'infrastruttura, nonché dal resto dei soggetti responsabili del Sistema elencati nell'articolo 5 della legge 8/2011. Tale Catalogo ha, conformemente alle disposizioni della normativa vigente in materia di segreto d'ufficio, la qualifica di segreto, conferita con accordo del Consiglio dei Ministri del 2 novembre 2007: la classificazione comprende, oltre ai dati contenuti nel Catalogo stesso, le apparecchiature, le applicazioni informatiche e i sistemi di comunicazione ad esso inerenti, nonché il livello di autorizzazione delle persone che possono accedere alle informazioni in esso contenute[363].

Il Ministero dell'interno, tramite la Segreteria di Stato per la sicurezza, è incaricato di classificare un'infrastruttura come infrastruttura strategica e, se del caso, come infrastruttura critica o infrastruttura critica europea e di includerla per la prima volta nel catalogo, dopo aver verificato che soddisfi uno o più dei criteri di criticità orizzontale di cui all'articolo 2; sezione h) della legge 8/2011. Il processo di identificazione di un'infrastruttura come critica è effettuato dal CNPIC, che può chiedere la partecipazione e la consulenza della parte interessata, nonché degli agenti competenti del sistema, ai quali informerà successivamente l'esito di tale processo. Inoltre, la classificazione di un'infrastruttura come critica europea comporta l'obbligo supplementare di comunicarne l'identità ad altri Stati membri che potrebbero esserne significativamente interessati, come previsto dalla direttiva 2008/114/CE. In tal caso, le notifiche, in reciprocità con gli altri Stati membri, saranno effettuate dal CNPIC, conformemente alla corrispondente classificazione di sicurezza secondo le normative vigenti. In caso di modifica significativa che incida sulle infrastrutture registrate e presenti interesse ai fini previsti dal regolamento, gli operatori critici responsabili forniscono, attraverso i mezzi

[362] Il catalogo deve includere, tra gli altri dati, quelli relativi alla descrizione delle infrastrutture, alla loro ubicazione, proprietà e amministrazione, ai servizi che forniscono, ai mezzi di contatto, al livello di sicurezza di cui hanno bisogno in funzione dei rischi valutati nonché alle informazioni ottenute dalle forze e dai corpi di sicurezza.

[363] La custodia, la gestione e la manutenzione del Catalogo Nazionale delle Infrastrutture Strategiche è di competenza del Ministero dell'Interno, tramite il Segretario di Stato per la Sicurezza.

messi a loro disposizione dal Ministero dell'interno, i nuovi dati di tali infrastrutture al CNPIC, che deve convalidarli prima della loro incorporazione nel Catalogo. In ogni caso, l'aggiornamento dei dati disponibili deve essere effettuato annualmente.

Il Segretario di Stato per la Sicurezza è l'organo supremo del Ministero dell'Interno responsabile del Sistema Nazionale di Protezione delle Infrastrutture Critiche, per il quale il suo capo, o l'organismo a cui delega, eserciterà una serie di funzioni. In primo luogo, dovrà progettare e dirigere la Strategia nazionale per la protezione delle infrastrutture critiche ed approvare il Piano nazionale per la protezione delle infrastrutture critiche dirigendone l'attuazione, nonché dichiarando, se del caso, i livelli di sicurezza da stabilire in ogni momento, in conformità con il contenuto di detto Piano e in coordinamento con il Piano di Prevenzione e Protezione Antiterrorismo[364]. Altresì, al Segretario di Stato per la Sicurezza spetta l'approvazione dei Piani di Sicurezza degli Operatori e i loro aggiornamenti su proposta del CNPIC, prendendo come riferimento, se del caso, le azioni dell'organismo o dell'agenzia competente per concedere loro le autorizzazioni corrispondenti ai sensi delle loro normative settoriali; ancora, l'approvazione dei diversi Piani di Protezione Specifica o eventuali proposte per migliorarli su proposta della CNPIC, e quella dei Piani Operativi di Supporto. Infine, tra le altre cose, deve individuare i diversi settori di responsabilità per la protezione delle infrastrutture critiche; analizzare i meccanismi di prevenzione e risposta previsti da ciascuno degli attori coinvolti; da ultimo, emanare istruzioni e protocolli di collaborazione rivolti sia al personale e agli enti esterni al Ministero dell'Interno, sia agli operatori delle infrastrutture strategiche, promuovendo l'adozione di buone pratiche[365].

[364] Enguix, Jorge Revert. "Esquema Nacional de Seguridad: protección de una infraestructura crítica del sector administración." (2019).

[365] Eventuali altre funzioni potrebbero essere concordate dalla Commissione Delegata del Governo per le Situazioni di Crisi.

Il CNPIC del Ministero dell'Interno, organicamente dipendente dalla Segreteria di Stato per la Sicurezza, ha il compito di assistere il Segretario di Stato per la Sicurezza nell'esecuzione delle sue funzioni nel campo della protezione delle infrastrutture critiche, agendo come organo di contatto e coordinamento con gli agenti del Sistema. Inoltre, tale organo esegue e tiene aggiornato il Piano Nazionale per la Protezione delle Infrastrutture Critiche ed il Catalogo, determinando la criticità delle infrastrutture strategiche incluse nello stesso. Il CNPIC dirige e coordina le analisi dei rischi effettuate dalle agenzie specializzate, pubbliche o private, su ciascuno dei settori strategici nell'ambito dei Piani Strategici Settoriali, per il loro studio e deliberazione da parte del Gruppo di Lavoro Interdipartimentale per la Protezione delle Infrastrutture Critiche; stabilisce, altresì, i contenuti minimi dei Piani di Sicurezza degli Operatori, dei Piani Specifici di Protezione e dei Piani di Supporto Operativo e supervisiona il processo di predisposizione degli stessi, raccomandando, se del caso, l'ordine di preferenza delle contromisure e le procedure da adottare per garantirne la protezione contro attacchi intenzionali[366]. Sempre al CNPIC spetta il compito di analizzare i Piani di Protezione Specifici forniti dagli operatori critici rispetto alle diverse infrastrutture critiche o alle infrastrutture critiche europee di loro proprietà; inoltre, deve implementare, in base al principio generale di riservatezza, meccanismi permanenti di informazione, allerta e comunicazione con tutti gli agenti del Sistema. Nel campo della protezione delle infrastrutture critiche, il Centro Nazionale per la Protezione delle Infrastrutture Critiche funge da punto di contatto nazionale con gli organismi internazionali e con la Commissione europea, nonché presenta a quest'ultima, previa consultazione del Centro nazionale di coordinamento antiterrorismo, le relazioni sulla valutazione delle minacce e sui tipi di vulnerabilità e rischi riscontrati in ciascuno dei settori in cui sono state designate le infrastrutture critiche europee[367].

Per quanto riguarda gli operatori critici, provenienti sia dal settore pubblico che da quello privato, questi saranno gli agenti che compongono il Sistema e sono responsabili di fornire

[366] Gómez, Fernando J. Sánchez. “Diez años del CNPIC: pasado, presente y retos de futuro.” (2017).

[367] Iñurrieta, Tomás Martín. “Protección de Infraestructuras Críticas: "El CNPIC siempre ha trabajado fomentando el consenso y la colaboración con los operadores que prestan sus servicios a la ciudadanía".” (2014).

collaborazione tecnica al Segretario di Stato per la Sicurezza, attraverso il CNPIC, nella valutazione delle proprie infrastrutture che concorrono al Catalogo. Pertanto, devono aggiornare i dati disponibili su base annuale e, in ogni caso, su richiesta o dopo la convalida del CNPIC. Gli operatori critici collaborano, se del caso, con il Gruppo di Lavoro, nella preparazione dei Piani Strategici Settoriali e nella realizzazione dell'analisi dei rischi sui settori strategici in cui sono inclusi. Inoltre, hanno il compito di predisporre un Piano di Protezione Specifico per ciascuna delle infrastrutture considerate critiche nel Catalogo, nonché aggiornarlo periodicamente o quando le circostanze lo richiedano, e devono designare un Delegato alla Sicurezza per ciascuna delle infrastrutture considerate critiche o critiche europee dal Segretario di Stato per la Sicurezza. Per la designazione di una società o di un ente come operatore critico, sarà sufficiente che almeno una delle infrastrutture da esso gestite soddisfi la considerazione di infrastruttura critica, in applicazione dei criteri previsti dall'articolo 2, sezione h), della legge 8/2011, del 28 aprile. In tal caso, il CNPIC preparerà una proposta di risoluzione e ne informerà il titolare o l'amministratore. Tale proposta contiene l'intenzione di designare il gestore o il gestore dell'impianto o degli impianti come operatore critico[368].

Il Piano Nazionale per la Protezione delle Infrastrutture Critiche è lo strumento di programmazione statale preparato dal Segretario di Stato per la Sicurezza e volto a mantenere sicure le infrastrutture spagnole che forniscono servizi essenziali alla società. Detto Piano stabilirà i criteri e le linee guida precise per mobilitare le capacità operative delle pubbliche amministrazioni in coordinamento con gli operatori critici, articolando le misure preventive necessarie per garantire la protezione permanente, aggiornata e omogenea del sistema infrastrutturale strategico contro le minacce derivanti da attacchi deliberati nei loro confronti. Il piano prevede inoltre diversi livelli di sicurezza e di intervento di polizia, che sono attivati, in ciascun caso, in funzione dei risultati della valutazione della minaccia e in coordinamento

[368] La parte interessata dispone di un termine di quindici giorni a decorrere dal giorno successivo al ricevimento della notifica per trasmettere alla CNPIC le accuse che ritiene opportune, dopodiché la Commissione, su proposta del gruppo di lavoro, emette la risoluzione designando, se del caso, detto operatore, come critico. Tale decisione può essere impugnata dinanzi al Segretario di Stato per la Sicurezza e, eventualmente successivamente, alla giurisdizione contenzioso-amministrativa, nei termini generali previsti dalla normativa vigente in materia di procedura amministrativa e dall'ordinanza contenzioso-amministrativa giurisdizionale.

con il piano di prevenzione e protezione antiterrorismo in vigore, al quale è adattato[369]. I diversi livelli di sicurezza conterranno l'adozione graduale di dispositivi e misure di protezione in situazioni di maggiore minaccia contro le infrastrutture strategiche nazionali e richiederanno l'assistenza delle Forze e dei Corpi di sicurezza, delle Forze armate, se del caso, e dei responsabili degli organi. Invece, i Piani Strategici Settoriali sono gli strumenti di studio e pianificazione con ambito capillare sul territorio nazionale che permetteranno di conoscere, in ciascuno dei settori contemplati nell'allegato della legge 8/2011, del 28 aprile, quali sono i servizi essenziali erogati alla società, il funzionamento generale di questi, le vulnerabilità del sistema, le potenziali conseguenze della loro inattività e le misure strategiche necessarie per il loro mantenimento. Il gruppo di lavoro, coordinato dalla CNPIC, elabora, con la partecipazione e la consulenza tecnica degli operatori interessati, se del caso, un piano strategico per ciascuno dei settori o sottosettori di attività da determinare. Questi piani strategici settoriali si basano su un'analisi generale dei rischi che copre le potenziali vulnerabilità e minacce, sia fisiche che logiche, che interessano il settore o il sottosettore interessato nell'ambito della protezione delle infrastrutture strategiche[370]. I Piani di Sicurezza per gli Operatori sono i documenti strategici che definiscono le politiche generali degli operatori critici per garantire la sicurezza di tutte le strutture o sistemi posseduti o gestiti; essi stabiliscono una metodologia di analisi dei rischi che garantisce la continuità dei servizi forniti da detto operatore e in cui sono raccolti i criteri per l'applicazione delle diverse misure di sicurezza attuate per far fronte alle minacce fisiche e logiche identificate su ciascun tipo di beni. Infine, il Segretario di Stato per la Sicurezza del Ministero dell'Interno, attraverso il CNPIC, stabilirà, con la collaborazione dei Ministeri del Sistema e delle agenzie dipendenti, i contenuti minimi dei Piani di Sicurezza dell'Operatore, nonché il modello su cui basare la loro preparazione[371].

[369] Sciara, Ángel José, Isabel María Raposo, Pablo Gorbán and Sonia Emma Cafarell. "Las políticas públicas y la formación de agendas. Las infraestructuras estratégicas desde una mirada regional." (2009).

[370] Monte, Alberto Sánchez del and S Jose Rodriguez. "La Guía nacional de notificación y gestión de ciberincidentes." (2019).

[371] «BOE-A-2011-8849 Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.», https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849.

Invece, per quanto riguarda il tema del ricorso al Golden Power per arginare le acquisizioni da parte di entità estere, la Spagna ha recentemente ampliato la normativa interna a tutela degli asset strategici nazionali, introducendo delle restrizioni alle operazioni di investitori extra UE, i quali necessitano ora di una specifica autorizzazione per poter procedere con operazioni che generino una partecipazione all'amministrazione o al controllo di aziende in settori strategici. Inoltre, al fine di arginare in maniera efficace le sovvenzioni straniere che causano distorsioni e danneggiano la parità di condizioni nel mercato, la Commissione Europea ha recentemente presentato una proposta di Regolamento, al fine di promuovere un controllo e contenere il fenomeno degli "investimenti predatori", finalizzati alla mera acquisizione e delocalizzazione di tecnologia strategica. L'obiettivo è senza dubbio quello di proteggere la sicurezza nazionale. Tale esigenza è avvertita e di forte attualità non soltanto in Spagna e a livello comunitario, ma anche in Italia come visto nel capitolo precedente dedicato all'analisi sulla normativa italiana[372]. La Spagna, con il Regio Decreto Legge del 17 marzo 2020 n. 8 ("misure urgenti straordinarie per far fronte all'impatto sociale ed economico del Covid-19"), ha introdotto restrizioni agli investimenti da parte di soggetti di Paesi non facenti parte dell'Unione europea o dell'Associazione europea di libero scambio (EFTA): per questi occorre oggi un'autorizzazione per l'acquisizione di partecipazioni uguali o superiori al 10% del capitale, o in concreto per operazioni che comunque generino la partecipazione alla gestione o al controllo, di aziende in settori strategici (infrastrutture, tecnologia, approvvigionamenti essenziali, informazioni sensibili, media)[373]. In altre parole, il governo spagnolo ha ampliato la normativa a tutela degli asset strategici proprio in coincidenza temporale con l'aggravarsi dei rischi pandemici. Con il Regio Decreto Legge n. 8/2020 è stato infatti emendato quello del 4 luglio 2003 n. 19 che

[372] Il ricorso sempre più frequente agli IDE (Investimenti Diretti Esteri) verso il nostro Paese e l'aumento del numero delle operazioni di M&A (acronimo di Mergers and Acquisitions, sono un insieme di operazioni di fusione e acquisizione tra aziende) ha portato, in Italia, ad una crescita dei casi di esercizio del Golden Power, il quale, in una prima fase è stato per lo più applicato nei confronti delle imprese che operano nei settori individuati come strategici dalla normativa nazionale (difesa, sicurezza, energia, trasporti e comunicazioni), per poi estendersi ai nuovi settori indicati nel Regolamento UE 2019/452, come, ad esempio la tecnologia 5G. Tale trend crescente si è registrato non soltanto a livello nazionale. Infatti, anche gli Stati esteri hanno riscontrato la necessità di dotarsi di una normativa in grado di consentire un controllo sulle operazioni in settori di rilevanza strategica.

[373] Francesco Portolano, «Golden power: il caso spagnolo e l'applicazione anche a soggetti Ue», Il Sole 24 ORE, 5 aprile 2020, https://www.ilsole24ore.com/art/golden-power-caso-spagnolo-e-applicazione-anche-soggetti-ue-AD520LI.

definiva il quadro giuridico per i movimenti di capitale e gli investimenti esteri in Spagna. Il nuovo regime di screening degli investimenti diretti esteri (IDE) resterà in vigore sino a quando il governo spagnolo non deciderà diversamente. Tali nuove norme sono state inoltre adottate anche per adeguare il quadro normativo del Golden Power spagnolo al nuovo sistema di screening degli IDE che – ai sensi del Reg. 452/2019 – è entrato in vigore nei paesi Ue nell'ottobre del 2021. Le nuove misure sul regime degli investimenti esteri si applicano ad operazioni sul capitale di società spagnole nelle quali l'investitore estero, non residente dell'Unione europea o dell'EFTA, detiene una partecipazione pari o superiore al 10% del capitale azionario, acquisisce il diritto di partecipare alla gestione della stessa, oppure ne acquisisce il controllo. Per quanto attiene alla configurazione settoriale delle autorizzazioni preventive, i comparti elencati sono quelli delle infrastrutture critiche, tanto fisiche che virtuali (energia, acqua, trasporti, sanità, comunicazioni, media, archiviazione od elaborazione dati, difesa, aerospaziale, infrastrutture elettorali o finanziarie); quelli relativi alle tecnologie critiche e prodotti *dual use*, tra i quali l'intelligenza artificiale, i semiconduttori, la robotica, la sicurezza informatica, la conservazione dell'energia, le tecnologie quantistiche e nucleari, le nanotecnologie e biotecnologie; inoltre, rilevano i settori della fornitura di materie prime ed energetiche, ivi compresa la sicurezza alimentare, ed i settori con accesso ad informazioni sensibili[374].

Un nuovo decreto del governo spagnolo estende e rafforza lo screening sugli investimenti esteri per prevenire azioni ostili, ma solo quelli sopra i cinque milioni di euro[375]: così, la Spagna blinda le imprese strategiche ancora una volta. Il nuovo meccanismo di screening degli investimenti diretti esteri prevede non solo il divieto per tutti gli investitori extracomunitari di acquistare più del 10% del capitale di un'impresa spagnola, ma anche per tutti gli investitori UE o parte dell'Associazione europea del libero commercio che sono controllati da aziende extracomunitarie. Per rientrare nell'area indicata l'investitore deve controllare direttamente o

[374] Massimo Ortolani, «Come Usa, Spagna e Francia hanno esteso il Golden Power», Startmag, 19 aprile 2020, https://www.startmag.it/economia/il-covid-19-spinge-usa-spagna-e-francia-ad-estendere-il-golden-power/.

[375] Si tratta di una risposta all'appello della Commissione Ue cui sta lavorando anche il governo italiano.

indirettamente una percentuale superiore al 25% del capitale o dei diritti di voto. Tale stretta ha l'obiettivo di impedire a multinazionali e fondi sovrani extracomunitari di aggirare la normativa esistente usando società ausiliarie (o attraverso Special Purpose Vehichles[376]) per prendere il controllo delle aziende spagnole in settori strategici che, al pari di molte altre aziende europee, hanno subito una grave riduzione del loro valore azionario in Borsa a causa della crisi del coronavirus[377]. Nel nuovo provvedimento si legge anche un allentamento del bando imposto il 17 marzo 2020 dal governo di Pedro Sanchez, che aveva di fatto sospeso buona parte degli investimenti diretti esteri, compresi quelli di dimensioni ridotte, richiedendo per tutti la previa autorizzazione del Consiglio dei ministri. Con il nuovo decreto il permesso non sarà più necessario per gli investimenti inferiori alla soglia di un milione di euro, mentre gli investimenti congelati in attesa di autorizzazione e quelli il cui importo rientri fra uno e cinque milioni di euro potranno essere sbloccati con un via libera della Direzione generale del commercio. Invece, rimane invariata la lista di imprese che il governo reputa strategiche, un ventaglio che attraversa i settori più disparati: le infrastrutture critiche fisiche (energia, trasporti, acqua, sanità), ma anche quelle tecnologiche (comunicazioni, trattamento di dati di settori sensibili, come quelli elettorali e finanziari), e ancora i beni immobili utilizzati per queste infrastrutture (ossia, la robotica, l'intelligenza artificiale, le biotecnologie, perfino la sicurezza alimentare). La Commissione europea ha recentemente invitato gli Stati membri a rafforzare i meccanismi di screening esistenti, ravvisando un aumento del rischio potenziale delle industrie strategiche, in particolare, ma non solo, dell'industria della sanità e chiedendo ai rispettivi governi di fare pieno uso dei loro meccanismi di screening per controbilanciare i rischi delle infrastrutture sanitarie critiche e della produzione di prodotti critici[378]. La tendenza al rafforzamento della

[376] Le Special Purpose Vehicle (SPV, in italiano Società Veicolo) sono società, o altro soggetto giuridico diverso dalla banca, costituite per veicolare attività finanziarie cedute da terzi, in particolare con lo scopo di effettuare una o più cartolarizzazioni. L'attività svolta è diretta esclusivamente a veicolare attività finanziarie cedute da terzi. La struttura della società veicolo è volta a isolare le obbligazioni della società stessa da quelle del cedente. *«Glossario», https://economiapertutti.bancaditalia.it/glossario/index.html.*

[377] Per fare degli esempi, la Iag, la holding che unisce le due compagnie aeree britannica e spagnola British Airways e Iberia, ha perso due terzi della capitalizzazione, Repsol il 40%, mentre Telefònica un terzo.

[378] Tale appello è stato fatto proprio anche dal governo italiano, che ha visto assottigliarsi vertiginosamente la capitalizzazione di molte delle sue più grandi aziende. Fra queste c'è anche Eni che recentemente ha perso il 33,4% del suo valore (che oggi ammonta a 33,5 miliardi di euro). Questo crollo ha fatto risuonare un campanello d'allarme al

normativa posta a tutela degli assets strategici sia degli Stati UE che extra UE continuerà a rafforzarsi, magari attraverso la previsione di ulteriori forme e modalità di esercizio del Golden Power, nonché di settori nell'ambito dei quali questo possa essere esercitato. Si tratta di un delicato equilibrio tra la fondamentale tutela degli interessi strategici e l'esigenza di non precludere, invece, investimenti che potrebbero portare valore aggiunto alle società target. È bene pertanto che il rafforzamento dei profili di sicurezza e dei presidi nazionali strategici non abbia come conseguenza di maggior rilievo la perdita di ingenti investimenti per le società di un determinato Paese che, dalla prospettiva dei potenziali stakeholders investitori, non risulterebbero attrattive, stante il rischio di esercizio di poteri di controllo da parte dello Stato ove è ubicata la target[379].

Ministero dell'Economia e delle Finanze dato che fra gli investitori che detengono una quota di Eni molti sono extracomunitari: è il caso della Bank of China, che possiede l'1,014%. Così, la Consob ha deciso di abbassare all'1% la soglia di possesso azionario oltre la quale si rende obbligatoria la comunicazione al mercato.
Palazzo Chigi, sotto la regia del sottosegretario Riccardo Fraccaro, ha lavorato per estendere la normativa del golden power non solo adottando i decreti attuativi per i settori bancario, assicurativo e finanziario ma anche valutando l'inclusione nello scudo protettivo di altri settori strategici come quello biochimico o farmaceutico. In questa direzione va un recente appello del Copasir (Comitato parlamentare per la Sicurezza della Repubblica), infatti il senatore di Fratelli d'Italia e vicepresidente del Copasir Adolfo Urso annunciò in una nota: "La decisione assunta dal governo spagnolo di tutelare con il golden power le proprie aziende pone l'attenzione sull'attività aggressiva dei fondi sovrani che dispongono di risorse illimitate e di strumenti operativi anche interni all'Unione". A tal proposito aggiunse che "i poteri speciali dovrebbero essere estesi anche ai soggetti della stessa Unione europea che possono essere usati come 'teste di ponte' per azioni predatorie nei confronti del nostro patrimonio tecnologico e industriale" *Francesco Bechis, «Golden power, ecco il decreto che blinda la Spagna. In Italia intanto in Eni...», Formiche.net, 1 aprile 2020, https://formiche.net/2020/04/golden-power-decreto-spagna-eni/.*

[379] «Studio Previti Associazione Professionale | Fisionomia ed esercizio del golden power negli ordinamenti esteri: gli esempi di Spagna, Francia, USA e Cina», Studio Previti Associazione Professionale, https://previti.it/fisionomia-ed-esercizio-del-golden-power-negli-ordinamenti-esteri-gli-esempi-di-spagna-francia-usa-e-cina.

14. I soggetti protagonisti della cybersicurezza

Per concludere l'analisi sulla disciplina della cybersicurezza spagnola è bene trattare dei soggetti, e delle relative funzioni loro affidate, protagonisti nel settore cyber. In questa sede sarà possibile evidenziare come la normativa di cybersicurezza spagnola sia prettamente di matrice europea, a differenza del nostro Perimetro Nazionale di Sicurezza Cibernetica che è di spinta nazionale. Questo è dovuto al fatto che la Spagna, in seguito alle richieste operate dalla direttiva NIS consistenti nell'attuazione di misure volte a elevare il livello di sicurezza della rete e dei sistemi informativi nell'ambito di ciascuna nazione, abbia di volta in volta adeguato la propria normativa in materia di Sicurezza nazionale per far fronte alla crescita esponenziale delle minacce che colpiscono il cyberspazio. Per tale motivo i soggetti spagnoli rilevanti in materia di cybersecurity sono oggetto di una normativa risalente nel tempo, che è stata più volte emendata nel corso dell'ultimo decennio proprio per adeguare il Regime di sicurezza nazionale all'attuale scenario geopolitico in cui la sicurezza digitale riveste un ruolo di primo piano.

La Spagna ha attivato il proprio sistema di sicurezza cibernetica nel 2010 con la creazione dell'INCIBE[380], che è parte di un sistema più complesso dove alcune funzioni di difesa/attacco sono demandate alla Difesa che ha costituito un proprio cyber commando. Dal canto suo l'INCIBE ha il vantaggio e la flessibilità di una struttura di diritto che ha la possibilità di interfacciarsi rapidamente con il mondo privato[381]. Inoltre, quest'istituto lavora per costruire la fiducia digitale, migliorare la sicurezza informatica e la resilienza e contribuire al mercato digitale in modo da promuovere l'uso sicuro del cyberspazio in Spagna. L'Istituto Nazionale di Cybersecurity della Spagna (INCIBE), in precedenza Istituto Nazionale delle Tecnologie della Comunicazione[382], è una società che fa capo al Ministero degli Affari Economici e della Trasformazione Digitale attraverso il Segretario di Stato per la Digitalizzazione e l'Intelligenza

[380] INCIBE sta per Instituto Nacional de Ciberseguridad.

[381] Infatti, l'INCIBE è costituito da circa 200 operatori ed ha una complessa ramificazione verso il mondo privato.

[382] INCIBE è stato creato nel 2006 con il nome di Istituto Nazionale di Tecnologie della Comunicazione (INTECO). Nel 2012 ha iniziato a dedicarsi esclusivamente ai temi della cybersecurity, così nel 2014 il suo nome è cambiato in INCIBE.

Artificiale, e si consolida come ente di riferimento per lo sviluppo della cybersecurity e della fiducia digitale per i cittadini, le reti accademiche e di ricerca, i professionisti, le aziende e soprattutto per i settori strategici[383]. Inoltre, ha forti interazioni con il Ministero dell'Interno relativamente alle attività che ricadono in reati cibernetici. Con un'attività basata sulla ricerca, la fornitura di servizi e il coordinamento con gli agenti con competenze nel settore, l'INCIBE contribuisce a costruire la sicurezza informatica a livello nazionale e internazionale[384]. La missione dell'INCIBE è stabilita dal suo Consiglio di amministrazione in conformità con la strategia generale del governo spagnolo e con la legislazione vigente in materia di sicurezza informatica; i suoi compiti sono quelli di migliorare la sicurezza informatica e la fiducia digitale di cittadini, minori e aziende private in Spagna, proteggere e difendere tali soggetti, nonché rafforzare l'industria spagnola della cybersecurity[385]. Inoltre, l'Istituto Nazionale di Cybersicurezza promuove la cosiddetta i+d+i[386] spagnola attraendo e sviluppando

[383] Dal 28 ottobre 2014, l'Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) è stato rinominato S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE), secondo la risoluzione adottata dall'Assemblea generale del 27 ottobre 2014. Con questo cambio di nome e immagine, l'INCIBE proietta un'identità in linea con il suo orientamento strategico e il suo posizionamento come centro nazionale di riferimento per la cybersecurity.

[384] https://www.agendadigitale.eu/giornalista/massimo-artini, «Agenzia Cibernetica Nazionale italiana, confrontiamola con gli altri attori europei», Agenda Digitale, 17 gennaio 2022, https://www.agendadigitale.eu/sicurezza/lagenzia-cibernetica-nazionale-italiana-il-confronto-con-gli-altri-attori-europei/.

[385] Moreno, Alberto Hernández. "Incibe como entidad de referencia para el desarrollo de la ciberseguridad en España." (2018).

[386] La I+D+I, ossia Investigación, Desarrollo e Innovación (in italiano, R+S+I sta per ricerca, sviluppo e innovazione) è un concetto trasversale a molte aree della conoscenza, e quindi prende termini da diversi ambiti. La ricerca deriva dal gergo scientifico, lo sviluppo dall'economia e l'innovazione dalla tecnologia e, insieme, collegano scienza pura e scienza applicata. Il termine è l'evoluzione del concetto di I+D usato in precedenza. L'inclusione dell'innovazione nel concetto riflette l'interesse ad ampliare il processo per garantire che abbia un'applicazione pratica e che le conoscenze acquisite dalla ricerca siano applicate per migliorare le condizioni di vita e far progredire la società. La ricerca è qualsiasi "indagine originale e pianificata volta a scoprire nuove conoscenze e una migliore comprensione nel campo della scienza e della tecnologia". La ricerca non deve necessariamente avere un'applicazione pratica diretta, il suo scopo è più teorico: ampliare la conoscenza. Lo sviluppo è "l'applicazione dei risultati della ricerca o di qualsiasi altro tipo di conoscenza scientifica per la fabbricazione di nuovi materiali o prodotti o per la progettazione di nuovi processi o sistemi di produzione, nonché per il sostanziale miglioramento tecnologico di materiali, prodotti, processi o sistemi preesistenti". Come sottolineato in precedenza, si tratta di un termine che deriva dall'economia e che ha connotazioni di ottimizzazione economica, sempre con l'obiettivo di migliorare la qualità della vita. Infine, l'innovazione tecnologica è l'attività il cui risultato è un avanzamento tecnologico per ottenere nuovi prodotti o processi produttivi o miglioramenti sostanziali di quelli esistenti. Si considerano nuovi prodotti o processi quelli le cui caratteristiche o applicazioni, dal punto di vista tecnologico, differiscono sostanzialmente da quelli esistenti in precedenza". In altre parole, l'innovazione è l'applicazione pratica per migliorare un prodotto o crearne uno nuovo con l'obiettivo di fornire un servizio migliore. *«Descubre qué es la I+D+i y si aplica en tu empresa | Kaudal», 22 marzo 2022, https://www.kaudal.es/imasd/proyectos-idi/que-es-imasd-como-aplicar-empresa/.*

professionisti nel settore della cybersecurity. Nel luglio 2020, il governo spagnolo ha presentato l'Agenda Digitale España 2025, un registro per la trasformazione digitale del Paese per ottimizzare i benefici socio-economici della digitalizzazione riducendo al minimo i rischi associati. Questa agenda digitale si sviluppa attraverso 10 assi strategici, il quarto dei quali è la cybersicurezza. L'INCIBE allinea la sua attività con questa agenda e con gli obiettivi e le finalità che persegue[387].

L'INCIBE, consapevole dei vantaggi offerti dai sistemi di gestione riconosciuti a livello internazionale, nonché della necessità di stabilire quadri che promuovano il miglioramento continuo, dispone di tre certificati attuali corrispondenti alla gestione della sicurezza delle informazioni e alla qualità dei servizi forniti. La strategia dell'INCIBE evidenzia la necessità di rafforzare la sicurezza logica dell'organizzazione, rispettando i requisiti legali e normativi in materia di sicurezza delle informazioni. Così, nell'ottobre 2017, INCIBE ha ottenuto il Certificato di Conformità con il Regime di Sicurezza Nazionale (ENS) di "categoria MEDIUM", rispetto ai requisiti disciplinati nel Regio Decreto 3/2010, dell'8 gennaio. Inoltre, l'INCIBE ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) aziendale, certificato in conformità all'ultima versione dello standard di riferimento UNE-ISO/IEC 27001:2014, che ratifica l'impegno dell'Istituto per la sicurezza delle informazioni e il miglioramento continuo in questo ambito[388]. Altresì, l'INCIBE dispone di un Sistema di Gestione della Qualità (SGQ) certificato in conformità alla norma di applicazione UNE-EN ISO 9001:2015; così, la politica del sistema è in linea con i processi e le attività aziendali e garantisce un monitoraggio continuo degli obiettivi e degli indicatori stabiliti[389].

L'INCIBE-CERT è il centro di risposta agli incidenti di sicurezza di riferimento per i cittadini e gli enti di diritto privato in Spagna, gestito dall'Istituto Nazionale di Cybersecurity, che dipende anch'esso dal Ministero degli Affari Economici e della Trasformazione Digitale

[387] «INCIBE | INCIBE», https://www.incibe.es/.

[388] Moreno, Alberto Hernández. "INCIBE: balance de seguridad 2017 y plan de actividad 2018." (2018).

[389] Inoltre, con questo certificato, INCIBE si assicura il riconoscimento della gestione della qualità dei suoi servizi, sia a livello nazionale che internazionale, poiché AENOR, in quanto membro della Rete IQNET (International Certification Network), rilascia il diploma IQNET insieme al certificato di conformità alla norma UNE-EN ISO 9001:2015.

attraverso il Segretario di Stato per la Digitalizzazione e l'Intelligenza Artificiale. Nel caso di gestione di incidenti che interessano operatori critici del settore privato, l'INCIBE-CERT è gestito congiuntamente dall'INCIBE e dall'OCC, l'Ufficio di coordinamento della sicurezza informatica del Ministero dell'Interno. L'INCIBE-CERT è uno dei team di riferimento per la risposta agli incidenti che si coordina con il resto dei team nazionali e internazionali per migliorare l'efficienza nella lotta contro i crimini che coinvolgono reti e sistemi informativi, riducendone gli effetti sulla sicurezza pubblica[390].

Come stabilisce il Cybersecurity Act, ossia il Regolamento (UE) 2019/881, è necessaria la certificazione delle infrastrutture critiche, comprese le reti energetiche e i sistemi bancari, oltre a prodotti, processi e servizi, per garantire che questi soddisfino gli standard di sicurezza informatica. L'acquisizione di un prodotto di sicurezza ICT che gestirà informazioni nazionali classificate o informazioni sensibili deve essere preceduta da un processo di verifica che i meccanismi di sicurezza implementati nel prodotto siano adeguati a proteggere tali informazioni. In altre parole, la valutazione e la certificazione di un prodotto di sicurezza ICT è l'unico mezzo oggettivo che consente di valutare e accreditare la capacità di un prodotto di gestire le informazioni in sicurezza. In Spagna, questa responsabilità è assegnata al Centro Nazionale di Crittografia (CCN) attraverso il Regio Decreto 421/2004 del 12 marzo. Questo organismo di certificazione, per quanto riguarda la certificazione funzionale della sicurezza informatica, si articola attraverso il Regolamento di Valutazione e Certificazione della Sicurezza delle Tecnologie dell'Informazione, approvato con Decreto PRE/2740/2007, completato da un proprio regolamento interno adeguato ai requisiti necessari per essere riconosciuto sia a livello nazionale che internazionale come organismo di certificazione della sicurezza ICT. Per la certificazione crittografica e per la certificazione TEMPEST[391], l'ente di

[390] «Instituto Nacional de Ciberseguridad de España (INCIBE)», Ciberseguridad (blog), https://ciberseguridad.com/normativa/espana/organismos/incibe/.

[391] La certificazione TEMPEST garantisce protezione dalle intercettazioni per informazioni classificate come segrete. TEMPEST si occupa delle onde elettromagnetiche irradiate dalle apparecchiature (sia radiate che condotte) e valuta il rischio di intercettazione. Tutte le apparecchiature elettriche ed elettroniche generano radiazioni elettromagnetiche. Nelle radiazioni EMC da apparecchiature di elaborazione dati, come computer portatili o cellulari, sono contenute informazioni sensibili che possono essere facilmente intercettate. Un apparecchio ricevitore può interpretare questi segnali in modo

certificazione si basa su propri criteri e metodologie. Inoltre, un audit interno e uno esterno dell'organismo di certificazione sono effettuati annualmente. L'audit interno è svolto da personale CNI[392] (non appartenente al CCN), per verificare che l'attività di certificazione sia svolta nel rispetto delle regole e delle procedure stabilite di volta in volta. Invece, l'audit esterno viene effettuato dall'Ente Nazionale di Accreditamento (ENAC), secondo la corrispondente norma ISO, ed è necessario affinché sia mantenuto l'accreditamento come organismo di certificazione del prodotto[393]. Il Centro Nazionale di Crittografia (CCN) è l'organismo responsabile della redazione del Catalogo dei Prodotti con Certificazione Crittografica che comprende i prodotti in grado di proteggere le informazioni nazionali classificate. È considerato un cifrario nazionale, con certificazione crittografica, quell'apparecchiatura di cifratura che è stata valutata e ha ottenuto detta certificazione dal CCN[394]. I prodotti approvati per la crittografia di informazioni nazionali classificate o che richiedono legalmente la protezione sono inclusi nel catalogo dei prodotti crittograficamente certificati, ossia la Guida CCN-STIC 103, e la procedura per la valutazione dei prodotti crittografici è inclusa nella Guida predefinita CCN-STIC 102. La valutazione crittografica ha il compito di verificare il funzionamento, l'implementazione e l'analisi degli algoritmi utilizzati, i meccanismi di sicurezza e il corretto funzionamento delle apparecchiature, assegnando loro un livello di classificazione delle informazioni per le quali il sistema ICT è autorizzato a trattare in base alla sua forza crittografica[395]. Affinché un prodotto crittografico possa essere incluso nel catalogo dei prodotti con certificazione crittografica, a seconda delle caratteristiche del dispositivo, possono essere necessarie valutazioni funzionali, valutazioni TEMPEST e valutazioni crittografiche. Il termine

inosservato e senza accesso diretto al dispositivo originale. «Lo standard Tempest», 6 dicembre 2022, https://www.avionews.it/item/1248253-lo-standard-tempest.html.

[392] L'acronimo CNI sta per Centro Nacional de Inteligencia.

[393] In Spagna, nell'ambito dello Schema di Sicurezza Nazionale (Regio Decreto 311/2022 e, in precedenza, Regio Decreto 3/2010), è stato creato lo Schema di Valutazione e Certificazione della Conformità con la partecipazione dell'Ente Nazionale di Accreditamento (ENAC), responsabile dell'accreditamento degli Enti di Certificazione che effettuano le valutazioni dell'ENS. Maggiori dettagli sono contenuti nella Delibera del 13 ottobre 2016 della Segreteria di Stato per le Pubbliche Amministrazioni, che approva l'Istruzione Tecnica sulla Sicurezza in conformità al Regime Nazionale di Sicurezza.

[394] Sono disponibili diversi tipi di crittografi: IP (Internet Protocol), dati, coz, fax, PKI (Public Key Infrastructure), generatori di numeri casuali, centri di gestione, ecc.

[395] Fernández, Aníbal Villalba and Juan Manuel Murillo Rodríguez. "Análisis de las ciberamenazas." (2017).

TEMPEST si riferisce alle indagini e agli studi sui rilasci compromettenti relativi a informazioni classificate che vengono trasmesse, ricevute o altrimenti trattate da apparecchiature o sistemi elettronici. Queste emanazioni non intenzionali, una volta rilevate e analizzate, possono portare a ottenere informazioni. Il termine TEMPEST si riferisce anche alle misure applicate per la protezione contro tali fumi compromettenti. Il CCN, in qualità di autorità di certificazione della sicurezza ICT nel campo dell'EMSEC (Security of emanations), ha, tra le altre missioni, lo sviluppo di normative nazionali in questo campo, la valutazione e la certificazione di apparecchiature, sistemi e strutture, nonché la partecipazione e la consulenza in diversi forum, agendo in tutti loro come National TEMPEST Authority (NTA). Lo Standard TEMPEST (CCN-STIC-210) si applica alle informazioni classificate riservate nazionali o superiori. Pertanto, riguarda apparecchiature, sistemi e impianti, sia fissi che mobili, in cui queste informazioni vengono generate o elaborate[396]. Quindi, come detto, l'acquisizione di un prodotto di sicurezza ICT che gestirà informazioni nazionali classificate o informazioni sensibili deve essere preceduta da un processo di verifica dei meccanismi di sicurezza.

Ancora, il Centro Nazionale Crittologico (CCN), che è stato regolato giuridicamente dal Regio Decreto 421/2004, è un'agenzia dello Stato spagnolo collegata al Centro Nazionale di Intelligence (CNI[397]) che si dedica alla crittoanalisi e alla decifrazione con procedure manuali, mezzi elettronici e crittografia, oltre a condurre ricerche tecnologico-crittografiche e formare personale specializzato in crittografia. Il CCN non è un'agenzia indipendente del CNI, ma, seguendo il modello della Germania e della Francia, è integrato nel servizio di intelligence spagnolo. All'interno di esso vi sono due parti integrate, ossia l'organismo di certificazione

[396] París, Domingo Antonio Guerra. "Esquema Nacional de Seguridad y auditoría." (2016).

[397] Il CNI, acronimo di Centro Nacional de Inteligencia, è il servizio segreto del Regno di Spagna creato con la riforma del sistema di intelligence spagnolo del 2002. L'istituzione del C.N.I. avviene con la Legge del 6 maggio 2002 n. 11. Con la stessa legge agli artt. 9 e 10 vengono rispettivamente concessi il rango di Segretario di Stato al Direttore del CNI (equivalente ad un nostro Ministro), e di Sottosegretario di Stato al Segretario Generale del CNI (equivalente ad un nostro Sottosegretario di Stato). Con la Legge Organica del 6 maggio 2002 n. 2, complementare alla L. 11/2002, viene istituito il controllo giudiziario preventivo sul CNI nel caso in cui le attività informative del Servizio ledano i diritti fondamentali riconosciuti dagli artt. 18.2 e 18.3 della Costituzione spagnola. Tutti gli organi informativi appartenenti al Sistema di intelligence spagnolo sono subordinati al CNI, il quale coordina le varie attività di intelligence, ed il suo Direttore è l'unico responsabile incaricato di presentare le relazioni, pertinenti alle attività informative e alle minacce per il Regno, davanti alla Commissione Delegata Governativa per l'Intelligence. *«Centro Nacional de Inteligencia», https://www.ccn.cni.es/index.php/es/menu-ccn-es/centro-nacional-de-inteligencia-menu-es.*

(OC) dello schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione (ENECSTI) ed il National Cryptological Center Computer Emergency Response Team (CCN-CERT). L'ambito di competenza del CCN è definito dalla legge 11/2002, che regola il CNI, dal Regio Decreto 421/2004, che regola e definisce la propria portata e le sue funzioni, nonché, come detto, dall'Ordine della Presidenza del Ministero PRE/2740/2007 che regola lo Schema Nazionale per la Valutazione e la Certificazione della Sicurezza delle Tecnologie dell'Informazione, e che conferisce al CCN la capacità di agire come Organismo di Certificazione (OC) di detto Schema.

Come si è già avuto modo di evidenziare, il CCN-CERT è la capacità di risposta agli incidenti di sicurezza delle informazioni del CCN. Questo servizio è stato creato nel 2006 come CERT del governo nazionale spagnolo e le sue funzioni sono incluse nella legge 11/2002 che regola il Centro nazionale di intelligence, nel Regio Decreto 421/2004 che regola il CCN e nel Regio Decreto 311/2022, del 3 maggio, che regola il Sistema di sicurezza nazionale. La sua missione, quindi, è quella di contribuire al miglioramento della sicurezza informatica spagnola, essendo il centro nazionale di allerta e risposta che coopera e aiuta a rispondere in modo rapido ed efficiente agli attacchi informatici e ad affrontare attivamente le minacce informatiche, compreso il coordinamento a livello pubblico statale delle diverse capacità di risposta agli incidenti o dei centri operativi di sicurezza informatica esistenti. Il tutto, con l'obiettivo finale di realizzare un cyberspazio più sicuro e affidabile, preservando le informazioni classificate e quelle sensibili, difendendo il patrimonio tecnologico spagnolo, formando personale esperto, applicando politiche e procedure di sicurezza, infine utilizzando e sviluppando le tecnologie più appropriate a tale scopo[398]. In conformità con questi regolamenti e la legge 40/2015 sul regime giuridico del settore pubblico, il CCN-CERT è responsabile della gestione degli incidenti informatici che interessano qualsiasi ente pubblico o azienda. Nel caso di operatori critici del settore pubblico, la gestione degli incidenti informatici sarà effettuata dal CCN-CERT in coordinamento con il CNPIC[399]. La Spagna si è dotata di un Forum, denominato

[398] Nacional, Centro Criptológico. "CCN-CERT, primera lína de defensa frente a los ciberataques." (2015).
[399] «Mision y objetivos», https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html.

CSIRT.es, il quale mira a proteggere il cyberspazio spagnolo, scambiando informazioni sugli incidenti di sicurezza informatica per agire rapidamente e in modo coordinato in qualsiasi situazione che possa interessare contemporaneamente diverse entità in Spagna. Questo forum è una piattaforma indipendente di fiducia e senza scopo di lucro composta dai team di risposta agli incidenti di sicurezza CSIRT/CERT, il cui ambito di azione o comunità di utenti in cui opera, è all'interno del territorio spagnolo. I membri del forum CSIRT.es forniscono alle loro comunità di utenti servizi diversi, a seconda delle risorse e delle esigenze di tali comunità. Per far parte del Forum, i CSIRT devono fornire un qualche tipo di servizio relativo all'attenzione degli incidenti di sicurezza: analisi degli incidenti, risposta agli incidenti di sicurezza o risposta agli incidenti in loco, supporto alla risposta agli incidenti o coordinamento della risposta agli incidenti. Così, il Forum CSIRT.es mira a creare una piattaforma indipendente per il coordinamento e la collaborazione di fiducia tra i CSIRT a livello nazionale che consenta di ottimizzare la cooperazione tra loro per agire contro i problemi di sicurezza informatica nelle reti spagnole. Allo stesso tempo, promuove la diffusione di informazioni di interesse e migliora la visibilità dei membri CSIRT del Forum nella comunità spagnola e internazionale[400]. Tra i principali obiettivi del Forum CSIRT.es rientrano la promozione della cooperazione tra CSIRT spagnoli, sia nel campo della risposta agli incidenti che nello sviluppo di progetti congiunti che contribuiscono al miglioramento della sicurezza sia nel loro campo d'azione che nella comunità spagnola; la condivisione di informazioni pertinenti sugli incidenti di sicurezza e qualsiasi altro tipo di informazione di intelligence considerata utile, nonché lo svolgimento di azioni e raccomandazioni coordinate in situazioni che lo richiedono. I membri di CSIRT.es offrono, inoltre, sostegno e orientamento nella creazione di nuovi CSIRT a livello nazionale e collaborano con altri Forum e iniziative simili a livello nazionale e internazionale[401]. Qualsiasi

[400] «Inicio» https://csirt.es/index.php/es/.

[401] Eccezioni a questa regola possono essere fatte nel caso di Centri pubblici, per i quali il loro ingresso potrebbe essere proposto se hanno almeno due membri che approvano il loro ingresso al Forum, o nel caso di Forze e Corpi di Sicurezza dello Stato (FFCCS), in cui hanno accesso diretto. Resta inteso che un singolo gruppo (CSIRT, gruppo di risposta) per NIF o entità sarà ammesso come membro di CSIRT.es.

CSIRT spagnolo che soddisfi la definizione generica offerta da ENISA è considerato un membro candidato del Forum CSIRT.es[402].

Il Centro Nazionale per la Protezione delle Infrastrutture Critiche (CNPIC) è l'organo del Ministero dell'Interno preposto alla promozione, al coordinamento e alla supervisione di tutte le attività affidategli dal Segretario di Stato per la Sicurezza in relazione alla Protezione delle Infrastrutture Critiche sul territorio nazionale[403]. Garantire la sicurezza delle infrastrutture critiche, pubbliche o private, è trascendente per il funzionamento dello Stato, della società e dei cittadini. Questi tipi di strutture sono quelle che forniscono servizi essenziali ai cittadini (ossia servizi necessari per il mantenimento delle funzioni sociali di base, quali la salute, la sicurezza, il benessere sociale ed economico dei cittadini e l'efficace funzionamento delle istituzioni statali e delle pubbliche amministrazioni) e il cui funzionamento è indispensabile e non consente soluzioni alternative. Pertanto, l'interruzione o la distruzione di tali strutture avrebbe un grave impatto sui servizi essenziali. In questo settore sono integrate le organizzazioni che operano in settori quali le telecomunicazioni, l'energia, i trasporti, la finanza. Data l'importanza strategica di queste infrastrutture, spesso diventano obiettivi primari per atti terroristici o azioni criminali. Pertanto, in Spagna, le azioni necessarie per ottimizzare la sicurezza delle infrastrutture critiche sono principalmente inquadrate nel campo della protezione contro le aggressioni deliberate e, in particolare, contro gli attacchi terroristici, con conseguente leadership del Ministero

[402] Per garantire la cooperazione e la fiducia tra i membri del Forum, l'ammissione di nuovi membri sarà sottoposta a voto unanime (il mancato voto sarà considerato come un voto favorevole applicando il principio della "procedura del silenzio") dai membri completi del forum. Nel processo di votazione, possono essere dati voti a favore o contro l'inclusione del candidato nel forum. In quest'ultimo caso è anche di particolare importanza fornire una ragione motivata per cui il candidato non dovrebbe far parte del forum. In caso di veto motivato, il candidato membro ha la possibilità di difendere la sua posizione in una riunione successiva, e procede quindi al voto a maggioranza assoluta dei membri pieni. Se il voto è positivo, i nuovi membri saranno ammessi in prova per un periodo massimo di un anno, prima del quale dovranno partecipare a un incontro presentando i servizi del loro centro. Una volta fatta questa presentazione, saranno considerati membri a pieno titolo. Se nel periodo di un anno non fanno tale presentazione, il loro accesso alle risorse del forum sarà revocato e dovranno ricominciare il processo di registrazione.

[403] Il 2 novembre 2007, mediante un accordo del Consiglio dei ministri, è stata approvata la creazione del Centro nazionale per la protezione delle infrastrutture critiche, un quadro strutturale che consente di dirigere e coordinare alcune azioni per la protezione delle infrastrutture critiche in Spagna. Le sue competenze sono regolate attraverso la legge 8/2011, con la quale sono stabilite misure per la protezione delle infrastrutture critiche, il Regio decreto 704/2011, con il quale viene approvato il regolamento di protezione delle infrastrutture critiche, nonché attraverso il Regio decreto legge 12/2018 sulla sicurezza delle reti e dei sistemi informativi ed il suo decreto di attuazione (ossia il Regio decreto 43/2021).

dell'Interno. La legislazione spagnola sulla protezione delle infrastrutture critiche stabilisce la necessità di garantire l'adeguata fornitura di servizi essenziali, attraverso meccanismi che consentano la sicurezza di questo tipo di infrastrutture, un compito affidato al CNPIC, che assiste il Segretario di Stato per la Sicurezza nelle sue funzioni. A livello internazionale, vengono stabiliti contatti con tutte le istituzioni o gli organismi che operano nello stesso settore del CNPIC. Inoltre, quest'ultimo è il punto di contatto nazionale nel quadro della protezione delle infrastrutture critiche della Spagna con l'Unione europea, nonché con altri organismi simili in paesi terzi. Per fare ciò, mantiene regolarmente relazioni con le organizzazioni internazionali e con le istituzioni governative dei diversi paesi, avendo incontri di lavoro periodici con i paesi vicini, con l'obiettivo di mantenere contatti fluidi che consentano di rafforzare i legami tra i paesi di confine, che è vitale quando si condividono connessioni e interdipendenze in diversi settori strategici.

Conclusioni

In questa sede è opportuno fare un bilancio sul livello di cybersicurezza in Italia e in Spagna, e più in generale in ambito eurounitario, in cui crescono di giorno in giorno la consapevolezza e la sensibilità nei confronti di questi temi. Proprio per far fronte a tale contesto, nonché alle crescenti sfide che caratterizzano il panorama globale in ambito cyber, nel contesto nazionale sono state delineate una serie di normative al fine innalzare il livello di sicurezza dei settori considerati essenziali per il Paese. La disciplina relativa al Perimetro Nazionale di Sicurezza Cibernetica coinvolge soltanto alcuni soggetti; in particolare si tratta di attori, pubblici e privati, che svolgono un servizio o una funzione essenziale per gli interessi dello Stato in determinati settori ritenuti più sensibili e per i quali è necessario prevedere un livello di sicurezza maggiore. Altro elemento importante è il carattere di segretezza di tale perimetro: solo le Pubbliche Amministrazioni e le aziende individuate rientranti all'interno dello stesso ne sono a conoscenza. Dall'esterno, infatti, non è dato sapere quali siano i soggetti presenti nella lista, nonché le relative funzioni o servizi essenziali svolti. In tale contesto, inoltre, acquisisce particolare rilievo l'Agenzia Nazionale per la Cybersicurezza recentemente costituita; la stessa infatti, attraverso il CSIRT (Computer Security Incident Response Team) e l'avvio operativo del CVCN (Centro di Valutazione e Certificazione Nazionale), assume la funzione di interlocutore unico nazionale per i soggetti pubblici e privati in materia di PSNC, confermando così il suo ruolo determinante nella garanzia e salvaguardia della sicurezza nazionale. Il Perimetro di Sicurezza Nazionale Cibernetico, rappresenta per il nostro Paese una innovazione epocale nella normativa di settore ed una opportunità unica per accrescere la competitività delle nostre imprese strategiche. Questo ha ulteriormente alzato il livello di resilienza cibernetica degli attori maggiormente sensibili ai fini della sicurezza nazionale, per questo il Perimetro può definirsi innovativo rispetto alla NIS, la quale ha prescritto obblighi in capo agli Stati membri con la finalità precipua di assicurare un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea. Lo stesso Direttore dell'Agenzia Nazionale per la Cybersicurezza

Roberto Baldoni (ormai ex direttore, nel momento in cui si scrive), in occasione dell'evento "5G Italy", ha sottolineato come il Perimetro abbia suscitato grande interesse a livello internazionale: infatti, molti Stati europei stanno guardando con attenzione al modello italiano. Per quanto riguarda l'esame dei soggetti rilevanti in materia di cybersicurezza, operando una comparazione tra le discipline analizzate in questa tesi, ossia tra il sistema italiano e quello spagnolo, è possibile affermare che negli ultimi anni l'Italia ha intrapreso, rispetto ai partner europei, un nuovo corso nella gestione e organizzazione della sicurezza cibernetica. Infatti, con l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN) è nato un soggetto autonomo che coordina i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del paese, del sistema produttivo e delle P.A., nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. L'Italia, dunque, si è dotata, anche se in ritardo, di un buon strumento per la gestione delle attività di sicurezza cibernetica: da questo ritardo ha tratto il vantaggio di poter sviluppare una struttura normativa e organizzativa molto efficace. A mio modo di vedere tra le varie agenzie europee è quella che ha la catena di comando più snella avendo una diretta dipendenza solo dalla Presidenza del Consiglio; ha ricevuto fondi sufficienti per una prima strutturazione ed è previsto che nei prossimi anni sarà dotata di ulteriori risorse. Inoltre, sono stati approvati alcuni emendamenti che mettono l'ACN in condizione di creare una forte interazione con il mondo privato e dell'innovazione. Altresì, l'Agenzia ha una capacità di emanare direttive come altre agenzie nazionali dipendenti da altri dicasteri, il che la rende decisamente molto operativa e capace di poter essere autonoma nella gestione del futuro della sicurezza cibernetica nazionale[404]. Un unico neo che va ottimizzato nel rapporto tra le varie entità che sono comunque coinvolte nella gestione della sicurezza cibernetica è quello di aver escluso un rapporto organico con le Forze Armate, demandate per costituzione alla difesa del paese. Dovendo

[404] Anche la rapida strutturazione, in continuità con il passato, degli organigrammi apicali è un segno di importante attenzione da parte del governo nazionale al tema della sicurezza cibernetica.

necessariamente ricomprendere il domino cibernetico in quelli che possono essere (anche più facilmente) attaccati da attori esterni (siano essi statuali o meno), non aver previsto un'organica interazione tra la ACN e il COVI/COR[405] potrebbe essere considerato un errore, soprattutto nella fase di avvio dell'Agenzia[406]. In questo, l'ACN si differenzia dall'equivalente agenzia spagnola INCIBE, la quale è una società dipendente del Governo spagnolo. Altre differenze tra le due agenzie attengono al fatto che l'INCIBE è un'autorità risalente, istituita primariamente sotto altro nome, alla quale nel corso dell'ultimo decennio sono state attribuite competenze di cybersicurezza. Invece, la nostra Agenzia per la Cybersicurezza Nazionale è stata creata su iniziativa del Perimetro di sicurezza, per attribuirle tutta una serie di competenze nell'ambito della sicurezza digitale. Come visto, infatti, l'ACN è un'autorità indipendente che, tra le altre cose, promuove la cultura di cybersicurezza in Italia, irroga sanzioni nel caso di violazioni della normativa cyber e si occupa di delineare linee guida per lo svolgimento delle attività affidate ai soggetti competenti in materia. Recentemente, all'Agenzia è stato attribuito il ruolo di autorità di certificazione che svolge attraverso il Centro di Valutazione e Certificazione Nazionale. Il CVCN, in seno all'Agenzia, si occupa di valutare la sicurezza degli asset, dei sistemi e dei servizi ICT distribuiti nel contesto del Perimetro. Tra i suoi compiti, di particolare rilevanza è il supporto tecnico alle attività legate all'esercizio delle competenze speciali Golden Power nel campo del 5G. In particolare, il CVCN opera sia nella fase preliminare, appoggiando il Gruppo di Coordinamento, sia nella fase di monitoraggio, quale organo di cui il Comitato si avvale a tal fine. Il CVCN ha adottato le metodologie da utilizzare nel corso del processo di valutazione, come il processo di analisi dei rischi, che gli enti inclusi nel Perimetro devono adottare per

[405] Il Comando per le operazioni in rete, abbreviato COR, è un comando operativo interforze delle forze armate italiane, dipendente dal Capo di Stato maggiore della difesa, che si occupa della condotta delle operazioni nel dominio cibernetico, nonché della gestione tecnico-operativa in sicurezza di tutti i Sistemi ICT della Difesa. *«Il Comando per le Operazioni in Rete (COR) - Difesa.it», https://www.difesa.it/SMD_/COR/Pagine/default.aspx.*
Invece, il COVI è il Comando di Vertice dell'Area Operativa Interforze e assolve alle funzioni di organismo di staff del Capo di Stato Maggiore della Difesa per la pianificazione, la coordinazione e la direzione delle operazioni e delle esercitazioni militari in ambito nazionale e internazionale condotte nei cinque domini: terra, mare, cielo, spazio e cyber. *«Il Comando Operativo di Vertice Interforze (COVI) - Difesa.it», https://www.difesa.it/SMD_/COVI/Pagine/default.aspx.*

[406] Infatti, l'ACN è fuori dalle agenzie di intelligenze: così il CSIRT e il Nucleo non sono sotto il controllo esclusivo del DIS.

redigere la documentazione da allegare alla notifica di affidamento. Invece, il CCN spagnolo, quale ente di certificazione, non fa parte dell'agenzia spagnola per la cybersicurezza, piuttosto questo è subordinato al CNI, ossia ai servizi segreti del Regno di Spagna. Ciò testimonia quanto già ampiamente discusso, cioè che la materia della cybersicurezza è stata inserita nell'ambito della Sicurezza nazionale spagnola in quanto considerata quale specifico settore della stessa. Gli standard di certificazione per la valutazione degli hardware e software sono così dettati direttamente da prerogative governative, come avveniva in passato in Italia quando l'attività di certificazione era demandata al MiSE; oggi invece è l'ACN l'autorità nazionale di certificazione della cybersicurezza, al posto del MiSE: il bollino di garanzia conferito dall'Agenzia è lo standard di riferimento alla base dello screening della sicurezza informatica. Sempre nell'ambito del Perimetro Nazionale di Sicurezza Cibernetica rileva la figura del CSIRT Italia; questo è la struttura tecnica di prevenzione, coordinamento e risposta agli eventi e incidenti informatici con impatto effettivo o potenziale sul territorio nazionale, ed è istituito anch'esso presso l'Agenzia per la Cybersicurezza Nazionale[407]. È il punto di riferimento per le notifiche di incidente avente ad oggetto beni ICT ai danni di tutte le infrastrutture digitali della Pubblica Amministrazione e private, in particolare per le notifiche definite ai sensi di legge per i soggetti inclusi nel Perimetro o per gli operatori di servizi essenziali individuati dalla direttiva NIS. In Spagna è attiva, nel modello di forum, una piattaforma indipendente di fiducia denominata CSIRT.es e composta dai team di risposta agli incidenti di sicurezza CSIRT/CERT, il cui ambito di azione o comunità di utenti in cui opera è all'interno del territorio spagnolo. All'interno di tale piattaforma collaborano, tra gli altri, l'INCIBE-CERT, centro di risposta agli incidenti di sicurezza di riferimento per i cittadini e gli enti di diritto privato in Spagna, ed il CCN-CERT, responsabile della gestione degli incidenti informatici che interessano qualsiasi ente pubblico o azienda. Questi CSIRT sono la porta d'ingresso per le notifiche di incidenti, che consentiranno di organizzare rapidamente la risposta agli stessi, ma il destinatario delle

[407] Il decreto legislativo sulla direttiva NIS ha previsto l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team, detto CSIRT italiano, chiamato a svolgere compiti e funzioni che in precedenza erano in capo al CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e al CERT-PA (operante presso l'Agenzia per l'Italia Digitale). *«Articolazioni - Agenzia per la Cybersicurezza Nazionale», https://www.acn.gov.it/agenzia/articolazioni.*

notifiche è la rispettiva autorità competente, che terrà conto di queste informazioni per la supervisione degli operatori. In ogni caso, l'operatore è responsabile della risoluzione degli incidenti e del ripristino del normale funzionamento delle reti e dei sistemi informativi interessati. L'utilizzo di una piattaforma comune per la segnalazione degli incidenti è previsto in modo che gli operatori non debbano effettuare diverse notifiche a seconda dell'autorità a cui devono rivolgersi, in conformità con le disposizioni dei regolamenti di recepimento della direttiva NIS. Della procedura di notificazione a seguito di incidenti che colpiscono i sistemi ICT, come detto, si è occupato il Regio Decreto Legge 12/2018, che recepisce nell'ordinamento spagnolo la direttiva NIS recante misure volte a garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione. Per continuare l'analisi in merito al recepimento della normativa europea è bene evidenziare il fatto che il governo spagnolo aveva già istituito un obbligo di notificazione degli incidenti ancor prima dell'emanazione della direttiva NIS; infatti, il sistema di notificazione è stato dettato al principio dal Regio Decreto 3/2010, che regolamenta il Regime di sicurezza nazionale nel campo dell'Amministrazione Digitale quale regolamento speciale sulla sicurezza dei sistemi informativi del settore pubblico, ed è stato recentemente rafforzato con il Regio Decreto 311/2022. Ciò evidenzia come la normativa spagnola in materia di cybersicurezza sia prettamente di matrice europea: infatti, la Spagna ha recepito le richieste operate prima dalla Direttiva NIS, poi dal Cybersecurity Act, attraverso i propri istituti nazionali già esistenti ed esecutivi allargandone il perimetro operativo. Quindi, anche nella normativa spagnola si riscontra la pianificazione di misure di sicurezza, del sistema di notificazione degli incidenti a danno di infrastrutture critiche e servizi essenziali, nonché una procedura di valutazione dei beni ICT da parte di un organo nazionale, ma è bene evidenziare come questi elementi non siano il frutto di una spinta nazionale, contrariamente a quanto visto per l'Italia, ma un mero recepimento della normativa europea al fine di adattare il problema della cybersicurezza al proprio Schema di sicurezza nazionale. In Spagna, oltre all'ENS e ai regolamenti che recepiscono la direttiva NIS, esiste solo un regolamento speciale per i sistemi classificati, ossia i sistemi coperti dalla legge sul segreto ufficiale e che prevedono ulteriori garanzie di sicurezza.

Concludendo, per sviluppare la cyber resilienza italiana il Governo dovrebbe promuovere un approccio più bilanciato che allinei la visione economica nazionale del Paese con le priorità di sicurezza nazionale e che eviti la duplicazione delle iniziative e indentifichi un meccanismo di coordinamento centralizzato per assicurare che siano raggiunte queste priorità. Dovrebbe anche aumentare la consapevolezza pubblica sulle minacce rivolte alle infrastrutture e ai servizi critici italiani e potenziare il ruolo che ognuno svolge nel contrastare le minacce cyber. Inoltre, è importante rafforzare il rapporto di collaborazione pubblico-privato e la risposta della legge per proteggere meglio cittadini, imprese e Pubbliche Amministrazioni, accelerando la cooperazione civile-militare e finanziando adeguatamente i programmi. Non meno importante è la necessità di una svolta nella cultura pubblica: non solo occorre una conoscenza dei rischi e delle opportunità connessi all'innovazione ICT e a Internet, ma è doveroso gestire tali rischi e investire nella sicurezza in modo appropriato. Solo così l'Italia può ottenere appieno i benefici dell'economia digitale e raggiungere gli obiettivi ambiziosi posti nelle sue strategie. Completando tutti questi passi, l'Italia si porrà sul percorso di diventare una nazione cyber-resilient capace di prosperare ed essere sicura nell'era digitale.

Bibliografia

Abogados, Santiago Mediano. «Publicada la Directiva sobre Ciberseguridad». Santiago Mediano Abogados (blog), 21 luglio 2016. https://santiagomediano.com/publicada-la-directiva-sobre-ciberseguridad/.

Achilli, Alessandro. «Managed Security Services: Cosa Sono e le Opportunità per le PMI». IT Impresa, 18 febbraio 2021. https://www.it-impresa.it/blog/mss-managed-security-services-pmi/.

ACN - Agenzia per la cybersicurezza nazionale. «Strategia Nazionale Di Cybersicurezza 2022-2026 - Agenzia per la cybersicurezza nazionale», https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza/.

Admin. «Stakeholder - definizione e significato». Dizionario Economico (blog), 15 dicembre 2015. https://dizionarioeconomico.com/stakeholder.

Agenda Digitale. «Cert e Csirt questi sconosciuti, tutti i passaggi della cybersecurity italiana», 17 marzo 2020. https://www.agendadigitale.eu/sicurezza/cert-e-csirt-questi-sconosciuti-tutti-i-passaggi-della-cybersecurity-italiana/.

Agenda Digitale. «Codice amministrazione digitale (Cad) 2020, il testo coordinato dopo Semplificazioni», 16 luglio 2020. https://www.agendadigitale.eu/cittadinanza-digitale/come-cambia-il-cad-dopo-il-semplificazioni-il-testo-coordinato/.

Agenda Digitale. «Codice amministrazione digitale (CAD) cos'è e punti principali», 16 marzo 2022. https://www.agendadigitale.eu/documenti/codice-dellamministrazione-digitale-cose-e-quali-sono-i-punti-principali-da-conoscere/.

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/.

Agenda Digitale. «Cybersecurity, Commissione europea: “Ecco la nostra risposta coordinata”», 10 gennaio 2022. https://www.agendadigitale.eu/sicurezza/cybersecurity-verso-una-risposta-europea-quadro-delle-minacce-azioni-e-lacune-da-colmare/.

Agenda Digitale. «Direttiva NIS, così è l’attuazione italiana (dopo il recepimento): i punti principali del decreto», 15 gennaio 2021. https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.

Agenda Digitale. «Norme cybersecurity in Europa, che caos: i nodi da risolvere», 3 gennaio 2020. https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/.

Agenda Digitale. «Regolamento (UE) 2016/679, ecco tutto ciò che cittadini e PA devono sapere», 27 maggio 2016. https://www.agendadigitale.eu/infrastrutture/nuovo-regolamento-privacy-ue-ecco-tutto-cio-che-cittadini-e-pa-devono-sapere/.

Agenda Digitale. «Sicurezza delle informazioni: i tre principi per gestire il cyber risk», 21 giugno 2023. https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-i-tre-principi-per-gestire-il-cyber-risk/.

Alpi Associazione. «Risk Based Approach in ISO\IEC 17025:2017 for testing and calibration laboratories», 24 maggio 2018. https://www.alpiassociazione.it/risk-based-approach-in-isoiec-170252017-for-testing-and-calibration-laboratories/.

Alfonso Contaldo e Davide Mula. Cybersecurity Law. 2020ª ed. Pacini Giuridica, s.d.

Alfonso Contaldo e Flaviano Peluso. La nuova disciplina italiana ed europea alla luce della direttiva NIS. 2018ª ed. Pacini Giuridica, s.d.

Altalex. «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», 4 maggio 2017. https://www.altalex.com/documents/leggi/2017/04/21/direttiva-recante-indirizzi-per-la-protezione-cibernetica-e-la-sicurezza-informatica-nazionali/.

Altalex. «Nasce l'Agenzia per la cybersicurezza nazionale», 23 giugno 2021. https://www.altalex.com/documents/news/2021/06/23/nasce-agenzia-per-cybersicurezza-nazionale/.

Artini, Massimo. Agenda Digitale, 17 maggio 2022. «Agenzia Cibernetica Nazionale italiana, confrontiamola con gli altri attori europei», https://www.agendadigitale.eu/sicurezza/lagenzia-cibernetica-nazionale-italiana-il-confronto-con-gli-altri-attori-europei/.

Atlantica, Europa. «La sicurezza delle infrastrutture critiche tra nuove regole e strategie europee», Formiche.net, 31 luglio 2019. https://formiche.net/2019/07/regole-strategie-europee-sicurezza-infrastrutture-critiche/.

AU. «Publicado el Código de Derecho de la Ciberseguridad, una recopilación de la normativa en este ámbito». Áudea (blog), 20 ottobre 2016. https://www.audea.com/publicado-codigo-derecho-la-ciberseguridad-una-recopilacion-toda-la-normativa-espanola-este-ambito/.

Bechis, Francesco. «Bollino cyber. Il decreto per certificare la sicurezza tech». Formiche.net, 4 maggio 2022. https://formiche.net/2022/05/bollino-cyber-draghi/.

Bechis, Francesco. «Golden power, ecco il decreto che blinda la Spagna. In Italia intanto in Eni…» Formiche.net, 1 aprile 2020. https://formiche.net/2020/04/golden-power-decreto-spagna-eni/.

Bechis, Francesco. «L'Agenzia cyber prende forma. Al via il trasloco degli 007». Formiche.net, 2 novembre 2021. https://formiche.net/2021/11/agenzia-cyber-sicurezza-baldoni-draghi/.

Bergonzini Chiara. «Non solo privacy. Pandemia, contact tracing e diritti fondamentali» dirittifondamentali.it (s.d.).

Bonavita, Simone. Agenda Digitale, 30 settembre 2021 «NIST Cybersecurity Framework: una roadmap per la sicurezza delle infrastrutture». https://www.agendadigitale.eu/sicurezza/nist-cybersecurity-framework-una-roadmap-per-la-sicurezza-delle-infrastrutture/.

Brighi, di Raffaella Isella. «La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea», fasc. 21 (s.d.).

Brocardi.it. «Art. 21 codice dell'amministrazione digitale - Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale», https://www.brocardi.it/codice-dell-amministrazione-digitale/capo-ii/sezione-i/art21.html.

Bulgarelli & Partners. «Adottato il nuovo Piano Nazionale per la protezione cibernetica e la sicurezza informatica», https://bulgarelliandpartners.wordpress.com/2017/06/12/adottato-il-nuovo-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/.

Carchidi, Fabio. «Aspetti problematici di inquadramento della giurisdizione e dell'autorità di controllo competente nei trattamenti di dati transfrontalieri.», s.d.

Casella Scudier «Le novità introdotte con l'entrata in vigore del regolamento UE 2019/881».

Carrer, Gabriele. «Agenzia cyber. Cosa farà il Cvcn per mettere il 5G al sicuro». Formiche.net, 1 luglio 2022. https://formiche.net/2022/07/agenzia-cyber-cvcn-5g/.

Carrer, Gabriele. «Come cambia la cybersecurity con il dl Aiuti bis? Risponde Iezzi (Swascan)». Formiche.net, 18 settembre 2022. https://formiche.net/2022/09/decreto-aiuti-bis-cyber-iezzi-swascan/.

Carrer, Gabriele. «Perimetro cyber, c'è la lista. Oltre 100 soggetti protetti». Formiche.net, 3 dicembre 2020. https://formiche.net/2020/12/secondo-dpcm-perimetro-cyber/.

Centofanti, Dario. «Piano Nazionale per La Protezione Cibernetica e La Sicurezza Informatica». Medium, 22 luglio 2017. https://www.popinga.it/piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica-11d8976820d7.

Centro Criptológico Nacional. "CCN-CERT, primera lína de defensa frente a los ciberataques." (2015).

Cerciello, Francesco. «Nuovi obblighi di notifica degli incidenti: quali conseguenze per i soggetti inclusi nel PSNC». Cyber Security 360 (blog), 29 settembre 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/nuovi-obblighi-di-notifica-degli-incidenti-quali-conseguenze-per-i-soggetti-inclusi-nel-psnc/.

Chiari, Caterina. Agenda Digitale. «Cybersicurezza, le norme in vigore e in arrivo per i soggetti inclusi nel perimetro di sicurezza nazionale». 1 marzo 2023. https://www.agendadigitale.eu/sicurezza/cybersicurezza-le-norme-in-vigore-e-in-arrivo-per-i-soggetti-inclusi-nel-perimetro-di-sicurezza-nazionale-e/.

Ciberseguridad.blog. «25 Tipos de ataques informáticos y cómo prevenirlos», 20 gennaio 2018. https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/.

Ciberseguridad.blog. «El nuevo ENS 2022 y sus principales cambios», 29 maggio 2022. https://ciberseguridad.blog/el-nuevo-ens-2022-y-sus-principales-cambios/.

Ciberseguridad. «Instituto Nacional de Ciberseguridad de España (INCIBE)», https://ciberseguridad.com/normativa/espana/organismos/incibe/.

Ciberseguridad. «Normativa de Ciberseguridad en España», https://ciberseguridad.com/normativa/espana/.

CINI - Cyber Security National Labs. «Framework Nazionale per la Cybersecurity e la Data Protection», 2019.

Commissione europea. «Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo al Comitato delle Regioni - Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro», 7 febbraio 2013.

Commissione europea. «Comunicazione congiunta al Parlamento europeo e al Consiglio - La strategia dell'UE in materia di cibersicurezza per il decennio digitale», 16 dicembre 2020.

CorCom. «Cybersecurity, il Consiglio Ue: “Contro gli attacchi rafforzare la cooperazione”», 23 maggio 2022. https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-il-consiglio-ue-contro-gli-attacchi-rafforzare-la-cooperazione/.

Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Pub. L. No. 345, OJ L (2008). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

Council of the European Union. Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, 013 OJ L § (2003). http://data.europa.eu/eli/dec_framw/2004/68/oj/eng.

Council of the European Union and European Parliament. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040/.

Council of the European Union and European Parliament. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (2019). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0452/.

Cuatrecasas. «Novedades en materia de ciberseguridad para 2022». https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/eu-cuales-seran-en-2022-los-principales-desarrollos-normativos-en-materia-de-ciberseguridad/.

CyberLaws. «Articolo 1 - Direttiva NIS (EU-2016/1148)». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-1-direttiva-nis/.

CyberLaws. «Articolo 3 - Direttiva NIS». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-3-direttiva-nis/.

CyberLaws. «Articolo 7 - Direttiva NIS (EU-2016/1148)». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-7-direttiva-nis/.

CyberLaws. «Articolo 8 - Direttiva NIS (EU-2016/1148)». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-8-direttiva-nis/.

CyberLaws. «Articolo 9 - Direttiva NIS (EU-2016/1148)». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-9-direttiva-nis/.

CyberLaws. «Articolo 11 - Direttiva NIS (EU-2016/1148)». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-11-direttiva-nis-eu-2016-1148/.

CyberLaws. «Articolo 12 - Direttiva NIS (EU-2016/1148)». CyberLaws (blog), 1 gennaio 2018. https://www.cyberlaws.it/2018/articolo-12-direttiva-nis-eu-2016-1148/.

Cyber Security 360. «Aiuti-bis: dal Copasir provvisorio alla sicurezza nazionale, ecco le nuove misure di cyber intelligence», 11 ottobre 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/aiuti-bis-dal-copasir-provvisorio-alla-sicurezza-nazionale-ecco-le-nuove-misure-di-cyber-intelligence/.

Cyber Security 360. «Come cambia la Golden Power dell'Italia (5G, cloud, cyber)», 25 marzo 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/come-cambia-la-golden-power-dellitalia-5g-cloud-cyber/.

Cyber Security 360. «CSIRT, cosa sono e cosa fanno i team di risposta agli incidenti di sicurezza», 24 settembre 2020. https://www.cybersecurity360.it/soluzioni-aziendali/csirt-cosa-sono-e-cosa-fanno-i-team-di-risposta-agli-incidenti-di-sicurezza/.

Cyber Security 360. «Cybersecurity Act, pubblicato sulla Gazzetta ufficiale UE il testo definitivo: tutte le novità», https://www.cybersecurity360.it/news/cybersecurity-act-approvata-la-legge-europea-per-la-sicurezza-cibernetica-che-ce-da-sapere/.

Cyber Security 360. «Cyber security: cos'è e come garantire la sicurezza dei sistemi informatici e delle reti», 5 settembre 2018. https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-la-guida-definitiva-per-la-corretta-implementazione-in-azienda/.

Cyber Security 360. «Direttiva NIS2 approvata: ecco cosa cambia in materia di sicurezza di dati, reti e sistemi», 17 novembre 2022. https://www.cybersecurity360.it/legal/direttiva-nis2-approvata-ecco-cosa-cambia-in-materia-di-sicurezza-di-dati-reti-e-sistemi/.

Cyber Security 360. «Direttiva NIS 2, gli sviluppi attuali e gli scenari futuri: il punto», 20 dicembre 2021. https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-gli-sviluppi-attuali-e-gli-scenari-futuri-il-punto/.

Cyber Security 360. «Golden Power, la proposta alla luce della guerra in Ucraina: tre linee di intervento rapido», 21 marzo 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/golden-power-la-proposta-alla-luce-della-guerra-in-ucraina-tre-linee-di-intervento-rapido/.

Cyber Security 360. «La nuova ISO/IEC 27002:2022: cosa cambia e perché è importante per la sicurezza delle informazioni», 8 marzo 2022. https://www.cybersecurity360.it/soluzioni-aziendali/la-nuova-iso-iec-270022022-cosa-cambia-e-perche-e-importante-per-la-sicurezza-delle-informazioni/.

Cyber Security 360. «Nuove minacce alla sicurezza informatica tra malware e attacchi hacker». https://www.cybersecurity360.it/nuove-minacce/.

Cyber Security 360. «Operatori di servizi essenziali (OSE): chi sono e quali obblighi di sicurezza hanno», 29 gennaio 2021. https://www.cybersecurity360.it/cybersecurity-nazionale/operatori-di-servizi-essenziali-ose-chi-sono-e-quali-obblighi-di-sicurezza-hanno/.

Cyber Security Agency. «CSA | Cybersecurity Act», https://www.csa.gov.sg/legislation/cybersecurity-act/.

Data Protection Law | Privacy e protezione dati personali. «Diritto alla protezione dei dati personali». https://www.dataprotectionlaw.it/diritto-alla-protezione-dei-dati-personali/.

Dipartimento per le Politiche Europee. «Cybersecurity». http://www.politicheeuropee.gov.it/it/comunicazione/europarole/cybersecurity/.

Docs Italia. «Piano triennale ICT | 8. Sicurezza informatica», https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/08_sicurezza-informatica.html.

Dominguez, MLuz. «10 principales amenazas emergentes de ciberseguridad que surgirán para 2030». CyberSecurity News (blog), 14 novembre 2022. https://cybersecuritynews.es/10-principales-amenazas-emergentes-de-ciberseguridad-que-surgiran-para-2030/

European Parliament e Council of the European Communities. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 105 OJ L § (2006). http://data.europa.eu/eli/dir/2006/24/oj/eng.

European Parliament e Council of the European Union. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, 335 OJ L § (2011). http://data.europa.eu/eli/dir/2011/93/oj/eng.

European Commission. «Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)», 22 giugno 2012. SWD(2012) 190 final. https://home-affairs.ec.europa.eu/system/files/2020-09/epcip_swd_2012_190_final.pdf.

ENISA. «National Cybersecurity Strategies Guidelines& Tools». Topic. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools.

ENISA. «National Cybersecurity Strategies (NCSSs) Map». Topic. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

ENISA. «Good Practices in Innovation on Cybersecurity under the NCSS». Report/Study. https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

ENISA. «NIS Directive». Topic. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

Enguix, Jorge Revert. "Esquema Nacional de Seguridad: protección de una infraestructura crítica del sector administración." (2019).

Europol. «European Cybercrime Centre - EC3». https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Federalismi.it «Cybersecurity tra legislazioni, interessi nazionali e mercato https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=43404&dpath=document&dfile=12052020211257.pdf&content/.

Federalismi.it. «La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto legge n. 82 del 2021». https://www.federalismi.it/ApplOpenFilePDF/.

Federalismi.it «Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità», https://www.federalismi.it/ApplOpenFilePDF.cfm? 32021001928.pdf&content/.

Fernández, Aníbal Villalba and Juan Manuel Murillo Rodríguez. "Análisis de las ciberamenazas." (2017).

FIRSTonline, Redazione. «Golden Power e cybersicurezza: la stretta del Governo per cloud della Pa, tlc e difesa». 19 marzo 2022. https://www.firstonline.info/golden-power-e-cybersicurezza-la-stretta-del-governo-per-cloud-della-pa-tlc-e-difesa/.

Franchina, Luisa Agenda Digitale «Strategia cybersecurity nazionale, siamo alla svolta: ecco i punti chiave per il futuro» 20 maggio 2022. https://www.agendadigitale.eu/sicurezza/strategia-cybersecurity-nazionale-litalia-se-desta-ecco-i-punti-chiave/.

Gallotti, Cesare. Agenda Digitale. «Sicurezza delle informazioni, la nuova ISO/IEC 27005 sulla valutazione del rischio», 24 aprile 2023. https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-la-nuova-iso-iec-27005-sulla-valutazione-del-rischio/.

Gallotti, Cesare. «Pubblicata la ISO/IEC 27005:2022 sulla gestione del rischio», http://blog.cesaregallotti.it/2022/10/pubblicata-la-isoiec-270052022-sulla.html.

Gallotti, Cesare. «Nuova edizione della ISO/IEC 27005 "Information security risk management"». ICT Security Magazine, 2 novembre 2018. https://www.ictsecuritymagazine.com/articoli/nuova-edizione-della-iso-iec-27005-information-security-risk-management/.

Gaspari, Federico. Federalismi.it «Poteri speciali e regolazione economica tra interesse nazionale e crisi dell'UE», https://www.federalismi.it/ApplOpenFilePDF. artiddocument&dfile/.

Gobierno de España, Presidencia del Gobierno. «Estrategia de seguridad nacional», 2021.

Gobierno de España, Presidencia del Gobierno. «Estrategia nacional de ciberseguridad», 2019.

Gómez, Fernando J. Sánchez. "Diez años del CNPIC: pasado, presente y retos de futuro" (2017).

González, Paloma. «Estas son las seis principales amenazas en ciberseguridad para 2020 - Füture». https://future.inese.es/ (blog), 23 gennaio 2020. https://future.inese.es/estas-son-las-seis-principales-amenazas-en-ciberseguridad-para-2020/.

Herrero, Enrique González. «Aprobada la nueva Estrategia de Seguridad Nacional 2021». Seguritecnia, 28 dicembre 2021. https://www.seguritecnia.es/actualidad/aprobada-la-nueva-estrategia-de-seguridad-nacional-2021_20211228.html/.

Il Sole 24 ORE. «Decreto cybersicurezza / Golden power più forte», 7 novembre 2019. https://www.ilsole24ore.com/art/decreto-cybersicurezza-golden-power-piu-forte-ACPv4Rx.

InfoCertSpA. «Il Cyber Resilience Act: i nuovi requisiti di cybersecurity europei». Futuro Digitale (blog), 21 ottobre 2022. https://futurodigitale.infocert.it/pillole-normative/il-cyber-resilience-act-i-nuovi-requisiti-di-cybersecurity-europei/.

InSic, Redazione. «Tutto quello che devi sapere sulla Cybersecurity». InSic (blog), 5 marzo 2021. https://www.insic.it/privacy-e-sicurezza/security-articoli/cybersecurity-definizione-e-provvedimenti/.

InSic, Redazione. «Security manager, chi è e cosa fa». InSic (blog), 5 gennaio 2022. https://www.insic.it/privacy-e-sicurezza/security-articoli/security-manager-chi-e-e-cosa-fa/.

Instituto Europeo Campus Stellae. «¿Qué es el Código de Derecho de la Ciberseguridad?», 8 luglio 2019. https://campus-stellae.com/que-es-el-codigo-de-derecho-de-la-ciberseguridad/.

Inside Marketing. «User experience: cos'è caratteristiche e ottimizzazione». Consultato 14 luglio 2023. https://www.insidemarketing.it/glossario/definizione/user-experience/.

Iñurrieta, Tomás Martín. "Protección de Infraestructuras Críticas: "El CNPIC siempre ha trabajado fomentando el consenso y la colaboración con los operadores que prestan sus servicios a la ciudadanía"." (2014).

ISO «ISO/IEC 27002 : 2022». https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/.

Jurídicas, Noticias. «Contenido de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Noticias Jurídicas». Text. Noticias Jurídicas. noticias.juridicas.com. Spain. https://noticias.juridicas.com/actualidad/noticias/10529-contenido-de-la-ley-36-2015-de-28-de-septiembre-de-seguridad-nacional/.

Leoni, Ibl-Istituto Bruno. «Golden power, 5G e cybersicurezza: "non è tutto oro quel che luccica"». Filodiritto. https://www.filodiritto.com/golden-power-5g-e-cybersicurezza-non-e-tutto-oro-quel-che-luccica/.

Ley, La. «121/000091 Proyecto de Ley de modificación de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional», 2022.

Lombardi, Gianluca. «Sicurezza informatica: cybersecurity e ISO 27001». Mondo 27001, 23 novembre 2020. https://www.mondo27001.it/sicurezza-informatica-cybersecurity-e-iso-27001/.

Lo Prete, Davide. Cyber Security 360 (blog). «Perimetro di sicurezza nazionale cibernetica: regole e criteri di attuazione». 30 ottobre 2020. https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-di-sicurezza-nazionale-cibernetica-regole-e-criteri-di-attuazione/.

Lovo, Linda. «Convergenza tra Safety, Security e Cybersecurity». Italsicurezza (blog), 1 giugno 2020. https://www.italsicurezza.it/convergenza-tra-safety-security-e-cybersecurity/.

Lucariello Andrea, Ressa Francesco. Cyber Security 360 (blog), 18 giugno 2021. «Ampliamento del perimetro di sicurezza nazionale cibernetica: ecco i settori di attività». https://www.cybersecurity360.it/cybersecurity-nazionale/ampliamento-del-perimetro-di-sicurezza-nazionale-cibernetica-ecco-i-settori-di-attivita/.

Mandotti, Giuliano. «ISO 27001 e GDPR, linee guida per mettere al sicuro i dati aziendali».

Marconi, Federica. Federalismi.it «L'intervento pubblico nell'economia e il mutevole ruolo dello Stato». https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=45870&dpath/.

Maricarmen Sequera, Amalia Toledo & Leandro Ucciferri. «Derechos humanos y seguridad digital: una pareja perfecta», Enero 2018.

Marina Caporale. Federalismi.it «Dalle smart cities alla cittadinanza digitale». https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=40901&dpath=document&dfile/.

Mecalux. «Supply chain: cos'è e come funziona la catena di approvvigionamento». Consultato 19 dicembre 2022. https://www.mecalux.it/blog/supply-chain-cos-e/.

Mele, Stefano. «Cosa c'è nel nuovo Dpcm del perimetro cyber. L'analisi di Mele». Formiche.net, 14 giugno 2021. https://formiche.net/2021/06/cosa-ce-nel-nuovo-dpcm-del-perimetro-cyber-lanalisi-di-mele/.

Mele, Stefano. «Cybersecurity Act, la strategia europea e le priorità dell'Italia». Formiche.net, 14 luglio 2018. https://formiche.net/2018/07/cybersecurity-act-la-strategia-europea-e-le-priorita-dellitalia/.

Mele, Stefano, Oreste Pollicino, Michele Colajanni, e Giusella Finocchiaro. «Sicurezza, settori strategici e banda larga: come cambia la protezione dei dati». Il Sole 24 ORE, 7 aprile 2022. https://www.ilsole24ore.com/art/sicurezza-settori-strategici-e-banda-larga-come-cambia-protezione-dati-AEMjmYPB.

Millás, Vicente Moret. "Un nuevo escenario jurídico para la ciberseguridad en España: el Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información." (2018).

Mi - Ministero dell'istruzione. «Sigillo - Firma Elettronica Avanzata - Sigillo - Firma Elettronica Avanzata», https://miur.gov.it/-/sigillo-firma-elettronica-avanzata.

Ministerio de la Presidencia. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, Pub. L. No.

Mondo 27001. Amministratore. «ISO/IEC 27002: cosa cambia nel nuovo standard»., 7 marzo 2022. https://www.mondo27001.it/iso-iec-27002-cosa-cambia-nel-nuovo-standard/.

Money.it. «Cos'è il Golden Power? La guida completa», 30 aprile 2021. https://www.money.it/Golden-Power-cos-e-significato-come-funziona.

Monte, Alberto Sánchez del and S Jose Rodriguez. "La Guía nacional de notificación y gestión de ciberincidentes." (2019).

Monti, Andrea. «Come funziona il nuovo potere offensivo del governo nel settore cyber». Formiche.net, 12 agosto 2022. https://formiche.net/2022/08/decreto-aiuti-attacchi-cibernetici/.

Monti, Andrea. «L'offensive cybersecurity di Stato richiede un quadro normativo organizzato». Formiche.net, 8 agosto 2022. https://formiche.net/2022/08/cybersecurity-di-stato-quadro-normativo-organizzato/.

Morán Espinosa, Licenciada Alejandra. "Ciberseguridad: aprendizaje disruptivo en la protección de infraestructuras críticas y la seguridad nacional." Seguridad, Ciencia & Defensa (2021): pag. 4.

Moreno, Alberto Hernández. "INCIBE: balance de seguridad 2017 y plan de actividad 2018." (2018).

Moreno, Alberto Hernández. "Incibe como entidad de referencia para el desarrollo de la ciberseguridad en España." (2018).

Nava, Gilberto. «Cybersecurity, al via il processo di certificazione. Come funziona?» Il Sole 24 ORE, 30 giugno 2022. https://www.ilsole24ore.com/art/cybersecurity-via-processo-certificazione-come-funziona--AEK3fOjB.

Nazzaro, Giovanni. «Il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica». Sicurezza e Giustizia (blog), 10 ottobre 2017. https://www.sicurezzaegiustizia.com/il-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/.

NIS Cooperation Group. «Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures», gennaio 2020.

NIS Cooperation Group. «EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks», 9 ottobre 2019.

NIST. «Reliability of UTC(NIST)». 19 novembre 2020. https://www.nist.gov/pml/time-and-frequency-division/time-services/utcnist-time-scale/reliability-utcnist.

NT+ Diritto. «Ora anche il Cyber Resilience Act a tutela del mercato unico digitale europeo: il punto della situazione in materia di cybersicurezza». https://ntplusdiritto.ilsole24ore.com/art/ora-anche-cyber-resilience-act-tutela-mercato-unico-digitale-europeo-punto-situazione-materia-cybersicurezza/.

NT+ Diritto. «PNRR e nuova Pa: tra consapevolezza privacy, tecnologie informatiche e social network». https://ntplusdiritto.ilsole24ore.com/art/pnrr-e-nuova-pa-consapevolezza-privacy-tecnologie-informatiche-e-social-network/.

OAS. «OAS - Organization of American States: Democracy for Peace, Security, and Development». Text, 1 agosto 2009. https://www.oas.org/en/.

Ortolani, Massimo. «Come Usa, Spagna e Francia hanno esteso il Golden Power». Startmag, 19 aprile 2020. https://www.startmag.it/economia/il-covid-19-spinge-usa-spagna-e-francia-ad-estendere-il-golden-power/.

Paolo Smiraglia, Marco De Benedictis, Andrea Atzeni, Antonio Lioy, e Massimiliano Pucciarelli. «The FICEP Infrastructure». In E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services, a cura di Sokratis K. Katsikas e Vasilios Zorkadis, 196–210. Communications in Computer and Information Science. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-71117-1_14.

París, Domingo Antonio Guerra. “Esquema Nacional de Seguridad y auditoría.” (2016).

Parlamento europeo. «Ciberseguridad: amenanzas principales y emergentes», 21 marzo 2023.

Pietro Maccarrone, Pietro. «Poteri speciali e settori strategici: brevi note sulle recenti novità normative», s.d.

Pisano, Corrado. «Perimetro sicurezza». Ministero delle Imprese e del Made in Italy. https://atc.mise.gov.it/index.php/sicurezza/perimetro-sicurezza.

Portolano, Francesco. «Golden power: il caso spagnolo e l'applicazione anche a soggetti Ue». Il Sole 24 Ore, 5 aprile 2020. https://www.ilsole24ore.com/art/golden-power-caso-spagnolo-e-applicazione-anche-soggetti-ue-AD520LI.

Posato, Pietro. «Domicilio digitale: che cos'è e a cosa serve?», 21 ottobre 2021. https://focus.namirial.it/domicilio-digitale/.

Presidenza del Consiglio dei Ministri. «Piano nazionale per la protezione cibernetica e la sicurezza informatica», marzo 2017. https://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf.

Prospetti, Eugenio. Agenda Digitale. «Un'unica identità digitale per tutti: risolvere il dualismo Spid-Cie». 11 settembre 2019. https://www.agendadigitale.eu/cittadinanza-digitale/ununica-identita-digitale-per-tutti-risolvere-il-dualismo-spid-cie/.

PuntoSicuro. «Infrastrutture critiche: cosa sono e come vanno protette», https://www.puntosicuro.it/security-C-125/una-norma-fondamentale-per-la-protezione-delle-infrastrutture-critiche-AR-20199/.

PuntoSicuro. «Istituita l'agenzia per la cybersicurezza nazionale», https://www.puntosicuro.it/security-C-125/istituita-l-agenzia-per-la-cybersicurezza-nazionale-AR-21423/.

Raffiotta, Edoardo C. «Cybersecurity Regulation in the European Union and the issues of Constitutional Law *», s.d.

RaiNews. «Attacco informatico all'Agenzia delle Entrate, la Procura di Roma apre un'inchiesta», https://www.rainews.it/articoli/2022/07/attacco-informatico-allagenzia-delle-entrate-countdown-fissato-a-5gg-0e679af7-e070-46bf-b663-bfbbb4d62783.html/.

Rainews. «Cybersicurezza è legge, ampliata la golden power anche su 5G», https://www.rainews.it/dl/rainews/articoli/Cyber-sicurezza-legga-150b4d7e-a7a8-4a45-a2a0-d30f47311d98.html/.

Razzini, Andrea. «Cyber Resilience Act: requisiti fondamentali e prodotti coinvolti». Cyber Security 360 (blog), 22 settembre 2022. https://www.cybersecurity360.it/legal/cyber-resilience-act-requisiti-fondamentali-e-prodotti-coinvolti/

Real Decreto 3/2010, § 1, BOE-A-2010-1330 8089 (2010). https://www.boe.es/eli/es/rd/2010/01/08/3.

Redazione. «Cybersecurity, Draghi approva la strategia nazionale». Formiche.net, 17 maggio 2022. https://formiche.net/2022/05/cyber-strategia-draghi/.

Redazione. «Cybersecurity e digital divide, investiamo anche sul territorio con una regia nazionale». Formiche.net, 2 agosto 2022. https://formiche.net/2022/08/cybersecurity-digital-divide-investiamo-territorio-regia-nazionale/.

Redazione. «Il d.l. 82/2021 e l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN)». Piselli & Partners (blog), 15 giugno 2021. https://www.piselliandpartners.com/news-di-settore/agenzia-cybersicurezza-nazionale-acn/.

Redazione. «La strategia italiana in materia di cyber-security». ICT Security Magazine, 9 febbraio 2016. https://www.ictsecuritymagazine.com/articoli/la-strategia-italiana-in-materia-di-cyber-security/.

Redazione. «Sicurezza e gestione del rischio online e offline. Cosa devono fare aziende e Pa». Formiche.net, 1 settembre 2022. https://formiche.net/2022/09/rischio-online-offline-cyber-pa/.

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/.

Rees, Katie. «What Is a Ransomware Gang and How Dangerous Are They?» MUO, 5 aprile 2022. https://www.makeuseof.com/what-is-ransomware-gang/.

Rigotto, Silvia. «Regolamento UE 679: quali sono le finalità e a che punto siamo in Italia?» datapro (blog), 8 settembre 2021. https://dataprogdpr.com/regolamento-ue-679-a-cosa-serve/.

Romero, Javier Candau. “CCN-CERT: defensa frente a ataques dirigidos contra la administración y las empresas de interés estratégico.” (2014).

Rossi, Luca. «Che cos’è il software e a cosa serve?» Internetto, 16 settembre 2018. https://www.internetto.it/che-cose-il-software-e-a-cosa-serve/.

Saetta, Bruno. «Diritto alla protezione dei dati personali». Protezione dati personali. https://protezionedatipersonali.it/diritto-alla-protezione-dei-dati-personali.

Saetta, Bruno. «Regolamento generale per la protezione dei dati». Protezione dati personali. https://protezionedatipersonali.it/regolamento-generale-protezione-dati.

Salgado, Arturo Gómez. «Van por órganos no secretos en ciberseguridad: Monreal». Grupo Milenio, 21 novembre 2022. https://www.milenio.com/negocios/van-por-organos-no-secretos-en-ciberseguridad-monreal.

Salvi, Giovanni. «Dal decreto Aiuti bis una nuova concezione della cybersecurity». Il Sole 24 Ore, 16 agosto 2022. https://www.ilsole24ore.com/art/dal-decreto-aiuti-bis-nuova-concezione-cybersecurity-AEB2dysB.

Santarelli, Marco. «Ecco la Strategia nazionale di cybersicurezza italiana: competenze e tecnologie per la difesa del Paese». Cyber Security 360 (blog), 18 maggio 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-la-strategia-nazionale-di-cybersicurezza-italiana-competenze-e-tecnologie-per-la-difesa-del-paese/.

Santos, Daniel Terrón. “Orden pci/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional [boe n.º 103, 30/iv/2019].” (2019).

Savino Nadia. «Che cos’è un server? La spiegazione semplice». Kasa della comunicazione (blog), 15 settembre 2020. https://www.kasadellacomunicazione.it/server/.

Sciara, Ángel José, Isabel María Raposo, Pablo Gorbán and Sonia Emma Cafarell. “Las políticas públicas y la formación de agendas. Las infraestructuras estratégicas desde una mirada regional.” (2009).

Sceglifornitore. «Servizi IT: cosa sono, cos’è l’Information Technology», 14 dicembre 2020. https://sceglifornitore.it/blog/servizi-it-cosa-sono-cose-linformation-technology/.

Serafin, Giulia. «Golden power: vecchi problemi e nuovi temi societari», http://www.rivistaodc.eu/Article/Archive/index_html?ida=206&idn=28&idi=-1&idu=-1.

Sicilia, Carola Cadenas. “La nueva Estrategia Nacional de Ciberseguridad 2019.” (2019).

Sinetqnlap. «Cad: il codice dell’amministrazione digitale, tutti i suoi contenuti». La Legge per Tutti (blog), 28 marzo 2019. https://www.laleggepertutti.it/277731_cad-il-codice-dellamministrazione-digitale-tutti-i-suoi-contenuti.

S.News S.r.l. «Le infrastrutture critiche: un punto di vista normativo», 13 luglio 2015. https://www.snewsonline.com/le-infrastrutture-critiche-un-punto-di-vista-normativo/.

Studio Previti Associazione Professionale. «Studio Previti Associazione Professionale | Fisionomia ed esercizio del golden power negli ordinamenti esteri: gli esempi di Spagna, Francia, USA e Cina», https://previti.it/fisionomia-ed-esercizio-del-golden-power-negli-ordinamenti-esteri-gli-esempi-di-spagna-francia-usa-e-cina.

Tarborelli, Matteo «Cyber security, come va la strategia italiana: cosa abbiamo fatto e cosa resta da fare». Agenda Digitale, 2 settembre 2021. https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/.

Tarsitano, Paolo. «Perimetro cybersecurity, complete le norme: ecco l’ultimo decreto». Cyber Security 360 (blog), 18 luglio 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-cybersecurity-complete-le-norme-ecco-lultimo-decreto/.

Tarsitano, Paolo. «Strategia nazionale di cybersicurezza, ecco gli obiettivi da raggiungere entro il 2026 per la resilienza del Paese». Cyber Security 360 (blog), 25 maggio 2022. https://www.cybersecurity360.it/cybersecurity-nazionale/strategia-nazionale-di-cybersicurezza-ecco-gli-obiettivi-da-raggiungere-entro-il-2026-per-la-resilienza-del-paese/.

Testa, Nicola. «eIDAS 2.0: la nuova frontiera dei sistemi di identificazione digitale». Agenda Digitale, 26 giugno 2023. https://www.agendadigitale.eu/cittadinanza-digitale/eidas-2-0-la-nuova-frontiera-dei-sistemi-di-identificazione-digitale/.

Valdez Alvarado, Aldo. Introducción a la ciberseguridad, 2019, https://doi.org/10.13140/RG.2.2.33919.36002.

Vincentis, Federica De. «Draghi allarga il golden power. 5G, software russi e le altre novità». Formiche.net, 18 marzo 2022. https://formiche.net/2022/03/draghi-golden-power-5g/.

We-learn. «Cosa sono gli Standard ISO». We Learn, 1 ottobre 2021. https://www.we-learn.it/cosa-sono-le-norme-iso/.

Worldline. «Cybersecurity Act: cos'è e come aumenta la sicurezza informatica», https://www.worldlineitalia.it/cybersecurity-act/.

Sitografia

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

«Articolazioni - Agenzia per la Cybersicurezza Nazionale», https://www.acn.gov.it/agenzia/articolazioni.

«BOE-A-2011-7630 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.», https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630.

«BOE-A-2015-10566 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.», https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566.

«BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.», https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191.

«BOE-A-2011-8849 Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.», https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849.

«Centro di intelligence nazionale (CNI)», https://www.ccn.cni.es/index.php/es/menu-ccn-es/centro-nacional-de-inteligencia-menu-es.

«Centro Criptológico Nacional - Home», https://www.ccn.cni.es/index.php/en/.

«Chi siamo|Agenzia per l'Italia digitale», https://www.agid.gov.it/it/agenzia/chi-siamo.

«Ciberseguridad En 2023: Principales Tendencias y Desafíos», 30 novembre 2022. https://www.open3s.com/ciberseguridad-en-2023-principales-tendencias-y-desafios-blog/.

«Cibersicurezza: la risposta dell'UE alle minacce informatiche», https://www.consilium.europa.eu/it/policies/cybersecurity/.

«CISR - Sistema di informazione per la sicurezza della Repubblica», https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/comitato-interministeriale-per-la-sicurezza-della-repubblica-cisr.html.

«CNPIC | Inizio», https://cnpic.interior.gob.es/opencms/es/inicio/.

«Codice Amministrazione Digitale|Agenzia per l'Italia digitale», https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale.

«Conservazione dei dati per combattere la criminalità: il Consiglio adotta conclusioni», https://www.consilium.europa.eu/it/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/.

«Consiglio nazionale per la cibersicurezza», https://www.ccn.cni.es/index.php/es/menu-ccn-es/consejo-nacional-de-ciberseguridad.

«Cosa è il diritto alla protezione dei dati personali?*», https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/2003167.

«Cos'è un audit? Il processo di auditing, la definizione», 23 ottobre 2019. https://www.bcbcertificazioni.com/blog/cos-e-un-audit.

«Critical Infrastructure Warning Information Network (CIWIN)», https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin_en.

«CVCN - Agenzia per la Cybersicurezza Nazionale», https://www.acn.gov.it/agenzia/articolazioni/cvcn.

"Cybersecurity Act" – Casella Scudier», 27 luglio 2019. https://www.casellascudier.it/le-novita-introdotte-con-lentrata-in-vigore-del-regolamento-ue-2019-881-cybersecurity-act/.

«Cybersecurity: Definizione, Significato e Perché Serve | Alteredu», https://www.alteredu.it/cybersecurity-definizione-e-significato/.

«Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 - Normattiva», https://www.normattiva.it/eli/stato/deccreto_del_presidente_del_consiglio_dei_ministri/2020/07/30/131/original.

«Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017», 2017.

«Decreto-legge 14 giugno 2021, n. 82 - Normattiva», https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14;82.

«Decreto legislativo 7 marzo 2005, n. 82 - Normattiva», https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82.

«Descubre qué es la I+D+i y si aplica en tu empresa | Kaudal», 22 marzo 2022. https://www.kaudal.es/imasd/proyectos-idi/que-es-imasd-como-aplicar-empresa/.

«Directiva de ciberseguridad: un nuevo escenario jurídico y material», https://revistasic.es/archivo/seccionesfijas/index21b2.html?directiva-de-ciberseguridad-un-nuevo-escenario-juridico-y-material&catid/.

«DIS - Sistema di informazione per la sicurezza della Repubblica», https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html.

«Documentazione Economica e Finanziaria - Dettaglio Articolo». https://def.finanze.it/DocTribFrontend/getAttoNormativoDetail.do/.

«eIDAS 2.0: facciamo il punto | Intesa, a Kyndryl Company», 2 novembre 2022. https://www.intesa.it/eidas-2-0-facciamo-il-punto/.

«ENISA Overview of Cybersecurity and Related Terminology», settembre 2017.

«Esquema Nacional de Seguridad 2022 - AFS Informática», 4 maggio 2022. https://www.afsinformatica.com/esquema-nacional-de-seguridad-2022/.

«Estrategia Nacional de Ciberseguridad | Ciberseguridad», https://ciberseguridad.com/normativa/espana/estrategia-nacional/.

«EU Trusted Lists | Shaping Europe's Digital Future», 30 giugno 2023. https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists.

«Firma digitale verso eIDAS | Agenzia per l'Italia digitale», https://www.agid.gov.it/it/piattaforme/eidas/firma-digitale-verso-eidas.

«Framework Nazionale per la Cybersecurity e la Data Protection | Framework Nazionale per la Cyber Security e la Data Protection», https://www.cybersecurityframework.it/framework2.

Freedom Online Coalition. «Home Page», https://freedomonlinecoalition.com/.

«Glossario», https://economiapertutti.bancaditalia.it/glossario/index.html.

«Golden Power: che cos'è e perché è importante per le nostre imprese?», https://gruppoitalfinance.it/it/update/golden-power-che-cose-e-perche-e-importante-per-le-nostre-imprese.

«Gruppo Di Cooperazione NIS | Plasmare Il Futuro Digitale Dell'Europa», https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

«Guide alla sicurezza CCN-STIC», https://www.ccn.cni.es/index.php/en/menu-guides-ccn-stic-en.

«Home | eIDAS - Il progetto FICEP : Il nodo eIDAS italiano», https://www.eid.gov.it/?lang=it.

«ICT (Information and Communication Technologies) in "Dizionario di Economia e Finanza"», https://www.treccani.it/enciclopedia/ict_(Dizionario-di-Economia-e-Finanza).

«Il Comando Operativo di Vertice Interforze (COVI) - Difesa.it», https://www.difesa.it/SMD_/COVI/Pagine/default.aspx.

«Il Comando per le Operazioni in Rete (COR) - Difesa.it», https://www.difesa.it/SMD_/COR/Pagine/default.aspx.

«Il Consiglio di Sicurezza Nazionale | DSN», https://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional#collapseFive.

«INCIBE | INCIBE», https://www.incibe.es/.

«Infrastrutture Critiche», https://home-affairs.ec.europa.eu/pages/critical-infrastructure_en.

«Inicio», https://csirt.es/index.php/es/.

«International Standard ISO/IEC 27000», s.d.

«ISO 27001: Come effettuare una valutazione dei rischi in 5 fasi – IT Governance Blog IT», https://www.itgovernance.eu/blog/it/iso-27001-come-effettuare-una-valutazione-dei-rischi-in-5-fasi.

«La ISO/IEC 27001: scopri le novità dell'edizione 2022», 27 ottobre 2022. https://www.newcert.it/nuova-iso-iec-27001-2022.

«La nuova ISO/IEC 27001:2022», https://officialblog.7consulting.net/post/2022/11/08/La-nuova-ISOIEC-270012022.aspx.

«La Strategia Di Cibersicurezza | Plasmare Il Futuro Digitale Dell'Europa», https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

«Legge dell'UE sulla cibersicurezza | Plasmare il futuro digitale dell'Europa», https://digital-strategy.ec.europa.eu/it/policies/cybersecurity-act.

«Le linee guida dell'AGID sulla formazione e la conservazione dei documenti informatici. | Il portale giuridico online per i professionisti - Diritto.it», 19 maggio 2021. https://www.diritto.it/le-linee-guida-dellagid-sulla-formazione-e-la-conservazione-dei-documenti-informatici/.

«Le società veicolo – Special Purpose Vehicle (SPV) | LinkedIn», https://www.linkedin.com/pulse/le-societ%C3%A0-veicolo-special-purpose-vehicle-spv-elisa-rossi/.

«L'Hardware del computer - Okpedia», https://www.okpedia.it/hardware.

«Linee guida sulla trasparenza ai sensi del regolamento 2016/679 - wp260 rev.01», https://www.iusprivacy.eu/linee-guida-sulla-trasparenza-ai-sensi-del-regolamento-2016-679-wp260-rev-01-4293989599.htm.

«Lo standard Tempest e la sfida italiana», https://www.avionews.it/item/1248253-lo-standard-tempest-e-la-sfida-italiana.html.

«Missione e obiettivi», https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html.

«Norme ISO: cosa sono e a cosa servono», 4 giugno 2019, https://www.bcbcertificazioni.com/blog/norme-iso-cosa-sono-e-a-cosa-servono.

«PAe - Esquema Nacional de Seguridad - ENS», https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html.

«PAe - Publicada la nueva Estrategia Nacional de Ciberseguridad 2019», https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias.

«Pae – SGAD», https://administracionelectronica.gob.es/_Home/en/pae_Organizacion/Sgad.

«Patrullaje En El Ciberespacio. El Trabajo de La Policía Cibernética», https://issuu.com/vkentintado/docs/revista_momento_julio_2020/s/10793398.

«Piano nazionale per la protezione cibernetica e la...», https://www.puntosicuro.it/archivio-news-brevi/piano-nazionale-per-la-protezione-cibernetica-la-sicurezza-informatica-iNews/.

«Presentazione del Progetto | eIDAS - Il progetto FICEP : Il nodo eIDAS italiano», https://www.eid.gov.it/presentazione-progetto.

«Quadro strategico nazionale per la sicurezza dello spazio cibernetico», s.d.

«¿Qué es la ciberseguridad y su importancia?», 23 ottobre 2021. https://barrazacarlos.com/es/que-es-la-ciberseguridad/.

«Raccomandazione (UE) 2017/1584 della Commissione – del 13 settembre 2017 – relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala», s.d.

«Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información», https://eur-lex.europa.eu/legalcontent/ES/TXT/PDF/?uri/.

«Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio – del 27 aprile 2016 – relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)», s.d.

«Regolamento (UE) 2019/ del Parlamento europeo e del Consiglio, del 17 aprile 2019, 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)», s.d.

«Regolamento Ue 2016/679 e stato di attuazione in Italia», 6 luglio 2018. https://www.diritto.it/regolamento-ue-2016-679-lo-del-suo-recepimento/.

«Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004Testo rilevante ai fini del SEE», s.d.

«Sintesi Strategia - Italia - Strategie Nazionali di Sicurezza Informatica», https://www.sicurezzacibernetica.it/it/db/ncss/Italy/index.php#piano_nazionale.

«SPID - Sistema Pubblico di Identità Digitale|Agenzia per l'Italia digitale», https://www.agid.gov.it/it/piattaforme/spid.

Ringraziamenti

Arrivata alla fine del mio percorso di scrittura della tesi desidero ringraziare la mia relatrice Professoressa Magarò per avermi proposto un tema di ricerca innovativo, che mi ha appassionata e messa sin da subito alla prova. Ringrazio anche il Professor Fernández Rodríguez, dell'Università di Santiago de Compostela, per l'aiuto che mi ha fornito nella ricerca delle fonti normative spagnole in materia di cybersicurezza. Un importante contributo alla stesura del capitolo sulla normativa spagnola mi è stato dato dal Professor Galán Cordero, esperto in minacce informatiche e cyberintelligence dell'Università Carlos III di Madrid. Il Professore ha fatto parte del comitato di redazione del Regio Decreto 311/2022, che regola il Regime Nazionale di Sicurezza, inoltre ha partecipato all'elaborazione delle Strategie nazionali di cybersicurezza del 2013 e del 2019. Il suo aiuto è stato molto importante per supplire alla carenza di dottrina spagnola in materia.

Infine, un ringraziamento speciale va al Dottor Gaggero per avermi seguito con disponibilità e competenza lungo l'intero percorso di scrittura.