icom
istituto per la competitività

ICT a prova di cybersicurezza. Evoluzione dei requisiti e impatto sulle aziende

N. 1/2022 Policy Brief – Area Digitale

AUTORI

Silvia Compagnucci, Thomas Osborn, Lorenzo Principali, Domenico Salerno

Abstract

Con l'aumentare della quantità e del valore dei dati trasmessi e conservati nelle reti di telecomunicazione, uniti al conseguente incremento nel numero di attacchi cibernetici registrati, la sicurezza è diventata un tema sempre più centrale per offrire garanzie tanto ai fornitori quanto agli utilizzatori di servizi digitali, un perimetro che la digital transformation sta allargando e continuerà ad allargare sempre più nel prossimo futuro.

L'incremento degli attacchi, che in taluni casi vede l'Italia tra i Paesi più colpiti, ad esempio per ciò che concerne i ransomware, va di pari passo con la crescita dei relativi danni economici, dovuti sia alla perdita o al furto dei dati, sia alla perdita di fiducia da parte di aziende e utilizzatori finali.

Per quanto concerne le reti, si sta passando da una condizione in cui le certificazioni relative alla sicurezza erano volontarie ad una nuova condizione in cui le richieste aumentano o diventano obbligatorie. Gli strumenti disponibili, tuttavia, per quanto efficaci, non risultano scevri da limiti, soprattutto in termini di tempi, costi e procedure.

Per tali ragioni, risulta essenziale trovare un bilanciamento tra i necessari standard di sicurezza e gli effetti che regolamentazioni e controlli provocano sugli equilibri di mercato. A fronte di un incremento nella diffusione di schemi e controlli a livello nazionale, è opinione diffusa che l'ipotesi di certificazioni condivise a livello europeo favorirebbe uniformità e consentirebbe maggiore efficienza e costi minori anche per il raggiungimento dei requisiti di sicurezza richiesti. In questa direzione trova riscontro anche l'attività dell'UE e delle agenzie comunitarie, come l'ENISA, che, attraverso la promozione di iniziative comuni, puntano a sviluppare un ecosistema sicuro all'interno di un quadro che non limiti le opportunità di crescita e di sviluppo del settore.

Tra gli Stati membri, l'Italia si è dimostrata consapevole dell'importanza di collaborare a livello internazionale e della necessità, ormai impellente, di garantire la sicurezza, sebbene appaia necessaria un'azione maggiormente decisa in termini di bilanciamento e semplificazione per un settore la cui importanza, sia in termini strategici che economici, sta assumendo un valore sempre maggiore.

Introduzione

La crescente centralità assunta dal cyberspazio per lo svolgimento delle attività socio-economiche pone all'attenzione delle istituzioni l'esigenza, ormai davvero improcrastinabile, di mettere in campo iniziative ed azioni in grado di assicurare un ecosistema digitale quanto più possibile sicuro. Caratterizzandosi il cyberspazio per essere un mondo dai confini evanescenti, che inevitabilmente coinvolge tutti gli Stati chiamati a dettarne le regole mediante esercizio della propria sovranità, la messa in campo di azioni congiunte a livello internazionale, la spinta verso l'interoperabilità e la standardizzazione rappresentano alcune delle principali chiavi per il successo. L'Italia, in particolare, è ben consapevole dell'importanza della collaborazione a livello internazionale e della necessità che ciascuno Stato agisca per impedire che il proprio territorio o le proprie infrastrutture Ict siano usate per condurre attività cybercriminali da parte di attori governativi o non governativi. Si tratta di posizioni recentemente espresse all'interno di un **position paper[1] sull'applicabilità del diritto internazionale alla cybersicurezza realizzato dal Ministero degli Affari esteri e della cooperazione internazionale** nel quale, partendo dalla constatazione delle difficoltà di individuare gli autori di illeciti nel cyberspazio e di apprestare contromisure adeguate all'attacco cibernetico, si sottolinea il valore della legge internazionale e la necessità di garantire la tutela dei diritti umani includendola nell'ambito degli obblighi di due diligence gravanti sugli Stati e nelle aree di responsabilità del settore privato.

1. CYBER-CRIME E INCIDENTI INFORMATICI. LO STATO DELL'ARTE

1.1. Rischio informatico e incidenza degli attacchi per PA, imprese e infrastrutture in Italia

La trasformazione digitale è un fenomeno che sta generando un impatto dirompente sia sulle abitudini dei cittadini, che sempre più riconoscono nella rete la sede privilegiata dove trasferire la

[1] Italian position paper on "International Law and Cyberspace (2021), disponibile al seguente link https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

maggior parte delle attività tradizionalmente compiute offline, sia per le organizzazioni, le quali trovano nel canale digitale nuovo slancio e continue opportunità di sviluppo. Il mutato contesto socio-economico, oltre alle innumerevoli esternalità positive, ha portato alla nascita di nuove minacce come il cyber-crime.

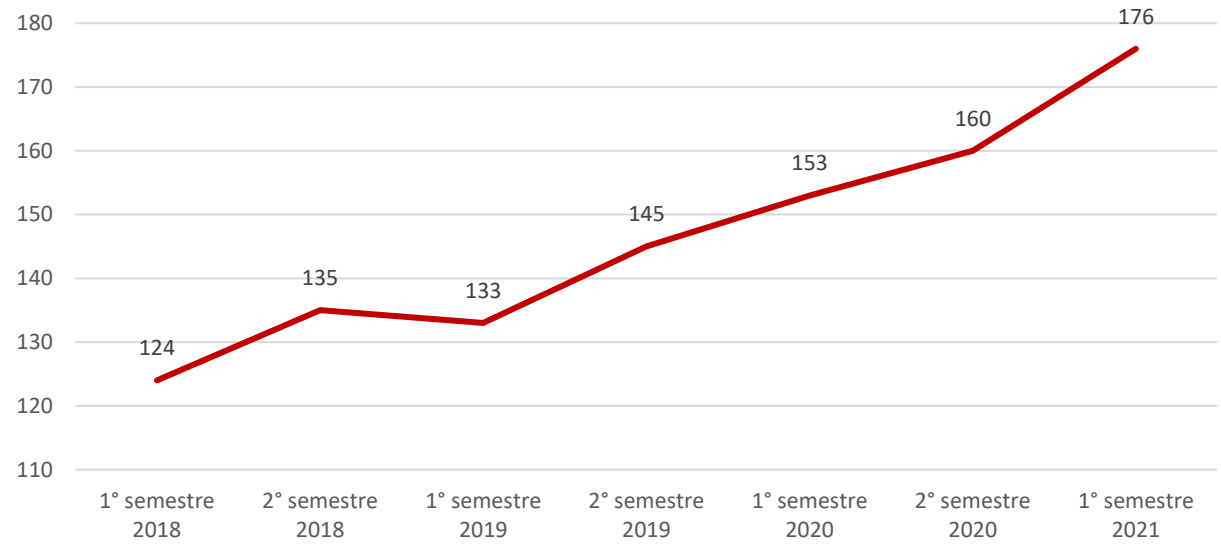
Date le dimensioni che tale problematica ha assunto, il Consiglio Europeo ha inserito gli attacchi informatici tra le principali priorità da affrontare nel ciclo programmatico per la criminalità internazionale organizzata e grave dell'EMPACT[2] per il triennio 2022-2025. La diffusione di azioni malevole online, come emerge dai dati contenuti nell'ultima versione del resoconto riassuntivo "Europol in Brief", sta diventando un serio rischio per la sicurezza dell'Unione. L'Agenzia europea che supporta e coordina le autorità nazionali dei diversi Stati membri nel contrasto alle gravi forme di criminalità transnazionale nel 2019 ha incentrato il 20,1% delle proprie operazioni nella lotta al cybercrime. Da ciò si evince che un crimine grave su cinque all'interno dell'UE è di carattere informatico.

Secondo l'ultimo rapporto pubblicato nel mese di ottobre 2021 dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT), che ogni anno censisce gli attacchi cibernetici classificati come gravi a livello globale[3], nel **primo semestre 2021 il numero di eventi malevoli gravi si è attestato a quota 1.053**, in notevole crescita rispetto allo stesso periodo dell'anno precedente, in cui si erano fermati a 917. In generale, osservando la media mensile di attacchi per semestre è possibile notare come la crescita dirompente del crimine informatico vada avanti ormai già da alcuni anni. Tra il primo semestre del 2018 e lo stesso periodo dell'anno in corso la media dei cyberattacchi gravi che si sono verificati nel mondo è infatti aumentata di oltre il 41% (Fig.1).

[2] La European Multidisciplinary Platform Against Criminal Threats è una piattaforma condivisa che mira ad affrontare le minacce più importanti poste all'Unione europea in modo coerente e metodologico migliorando e rafforzando la cooperazione tra i servizi competenti degli Stati membri, le istituzioni UE, i paesi terzi e il settore privato

[3] Vengono considerati attacchi gravi le azioni malevole di portata tale da diventare di dominio pubblico, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica.

Fig.1: Media mensile attacchi per semestre (2018 - 2021)



Fonte: Clusit - Rapporto sulla Sicurezza ICT in Italia (edizione ottobre 2021)

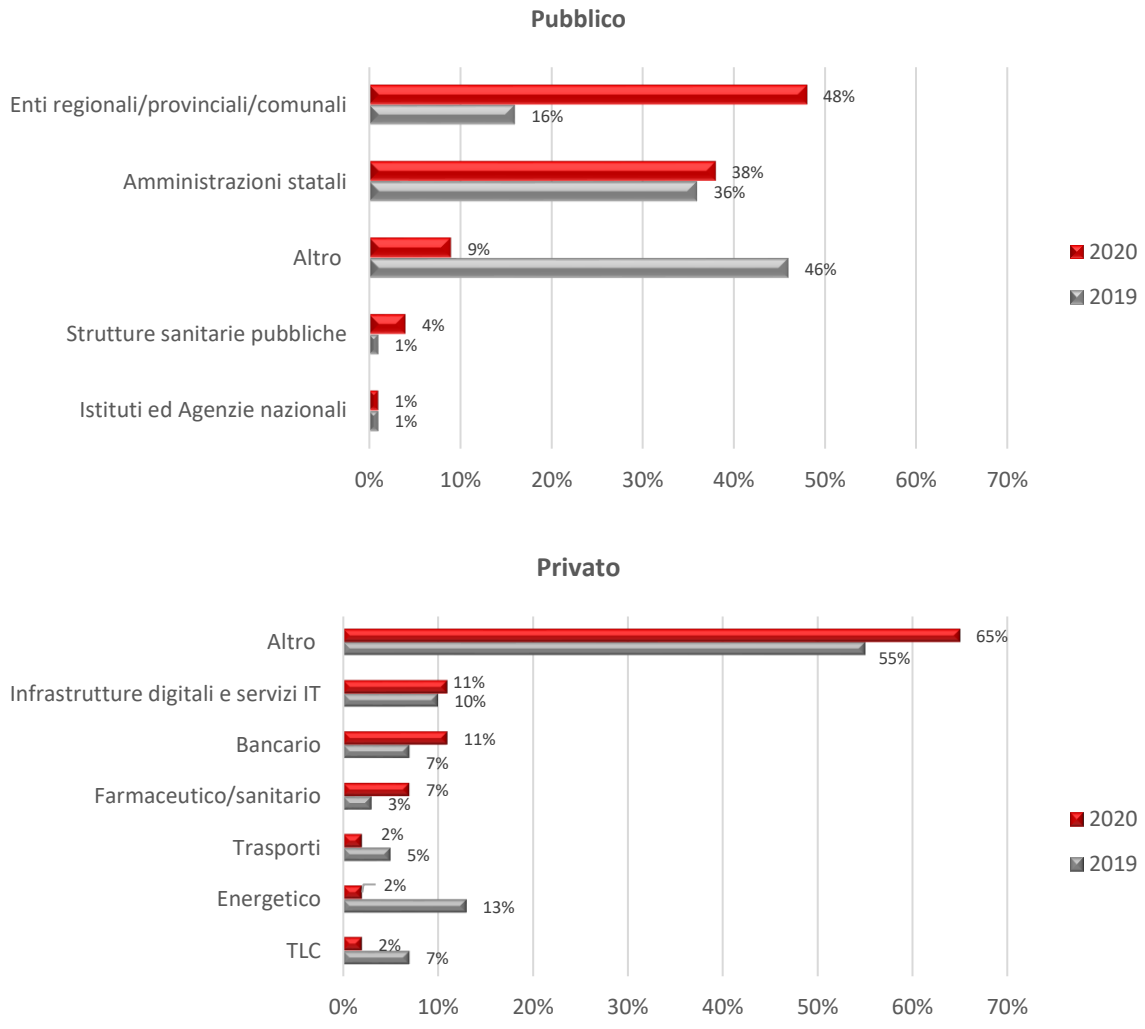
Concentrando l'attenzione sul panorama italiano, l'ultima "Relazione sulla politica dell'informazione per la sicurezza"[4] mostra come, anche per il nostro Paese, il crimine informatico costituisca un problema estremamente serio. Il numero di attacchi cibernetici verso organizzazioni pubbliche e private nazionali è cresciuto infatti del 20% tra il 2019 e il 2020. Le amministrazioni pubbliche sono risultate nel 2020 l'obiettivo privilegiato dei cybercriminali, attirando l'83% delle azioni ostili, ovvero il 10% in più rispetto all'anno precedente. Tra le PA più bersagliate (Fig.2) ci sono gli enti locali (48%), seguiti dalle amministrazioni centrali (38%). Un trend particolarmente allarmante, che si ricollega a quanto accaduto a luglio 2021 nella Regione Lazio[5], è quello riguardante riguarda gli attacchi a strutture sanitarie pubbliche, passati dall'1% del 2019 al 4% del 2020.

Riguardo al settore privato, i soggetti che hanno subito il maggior numero di azioni ostili fanno capo al settore bancario e ai servizi IT (entrambi a quota 11% degli attacchi complessivi), seguiti a breve distanza dal comparto farmaceutico/sanitario (7%). Si è notevolmente ridotta, invece, la quota degli

[4] Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza 2019", 1° marzo 2021.
[5] Nel mese di luglio 2021 un attacco informatico ha interessato il Centro elaborazione dati (CED) della Regione Lazio paralizzando per giorni tutte le attività sanitarie regionali e ostacolando notevolmente sia le normali attività che la campagna di vaccinazione anti covid-19.

attacchi rivolti alle TLC (dal 7% al 2% degli attacchi totali) e alle aziende del settore energetico (passati dal 13% al 2% del totale). Il settore delle telecomunicazioni risulterebbe quindi, paradossalmente, meno esposto di molti altri, probabilmente anche per la maggiore dimestichezza delle imprese che lo compongono con le tematiche relative alla cybersecurity.

Fig. 2: Attacchi informatici critici avvenuti in Italia per tipologia di Target



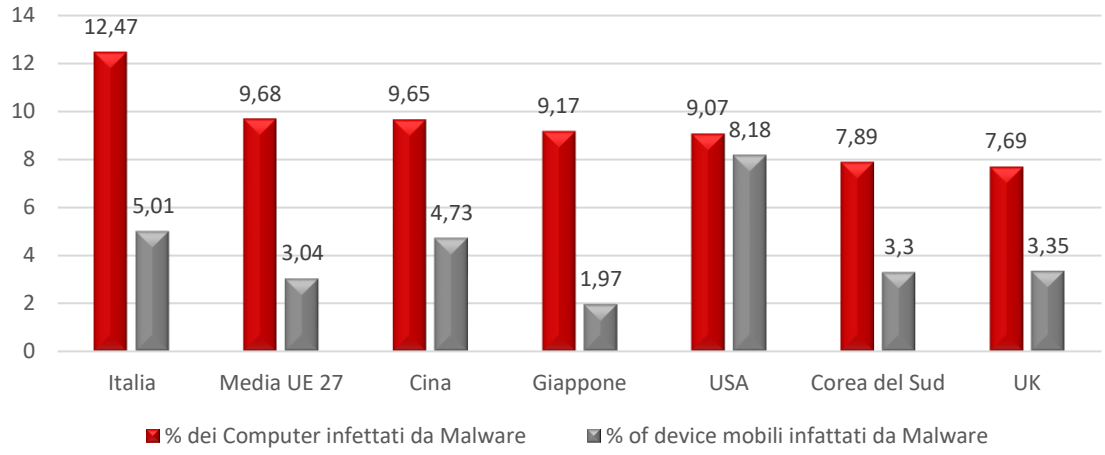
Fonte: Relazione sulla politica dell'informazione per la sicurezza 2020 – Presidenza del Consiglio dei Ministri

Le azioni ostili non interessano però solo le aziende e le pubbliche amministrazioni, ma sono un problema che può interessare tutti gli utilizzatori di dispositivi elettronici. Che il problema della cybersecurity sia diffuso capillarmente risulta palese dalla osservazione dei dati pubblicati da

Comparitech nello studio “Which countries have the worst (and best) cybersecurity?”. Secondo l’organizzazione circa il 10% dei computer e il 3% dei dispositivi mobili utilizzati all’interno dell’Unione Europea sono stati infettati da malware[6].

Analizzando i dati delle principali economie mondiali è possibile notare inoltre come l’Italia si posizioni al primo posto in termini di computer compromessi con software malevoli (12,47%), davanti a Cina, Giappone, USA, Corea del Sud e Regno Unito. Per quanto riguarda i dispositivi mobili, invece, il dato sulle infezioni fatto registrare dall’Italia (5,01%) tra le aree geografiche considerate è secondo solo a quello degli USA (8,18%) ed è circa il 2% più elevato della media UE27 (Fig.3).

Fig.3: Percentuale di devices che hanno subito attacchi informatici per area geografica (2019)



Fonte: Which countries have the worst (and best) cybersecurity? - Comparitech, 2020

1.2. Impatto economico e prospettive di miglioramento della cybersecurity presso PA e aziende

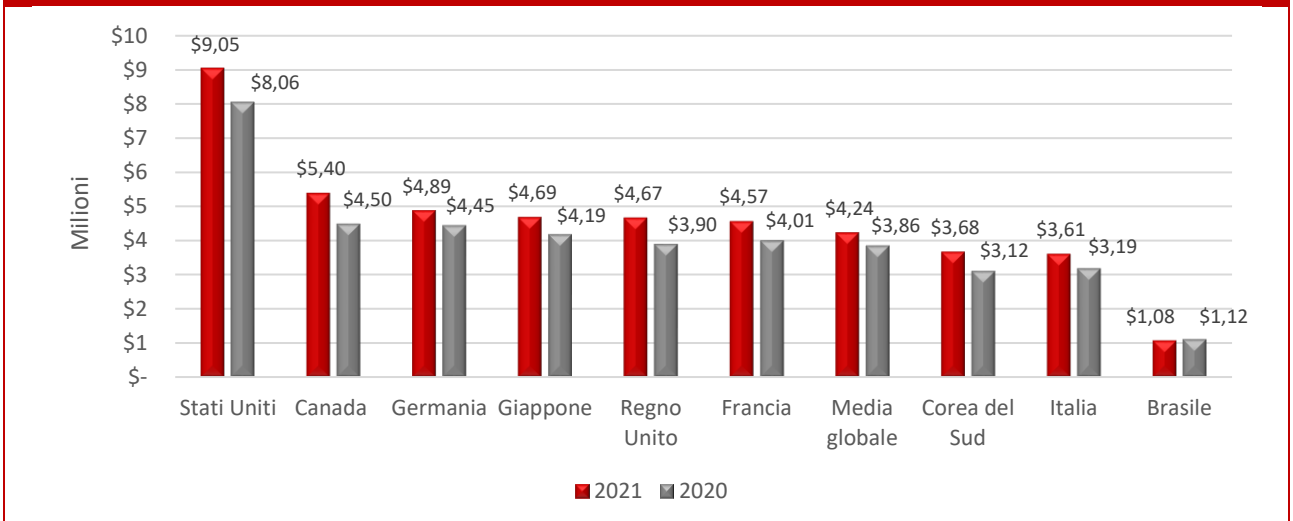
L'utilizzo di Internet e dei dispositivi connessi offre nuove opportunità a persone, aziende e istituzioni ma, allo stesso tempo, apre la porta a nuovi rischi. La vastità ed il continuo allargamento

[6] “Il Malware, abbreviazione di malicious software (software dannoso o malevolo), è un software creato per danneggiare dispositivi e sistemi informatici, agendo contro l'interesse degli utenti. Oltre al computer o al dispositivo infetto, il malware può colpire anche tutti i dispositivi con cui comunica il sistema contenente il virus” (Red Hat).

del perimetro delle attività comprese nell'ambito digitale, oltre ad abilitare l'accesso a molteplici benefici, se non adeguatamente tutelate, rischiano di costituire anche terreno fertile per azioni criminali che possono essere allo stesso tempo indiscriminate o mirate, rivolte a grandi e piccole organizzazioni sia del settore pubblico che privato.

Da punto di vista delle organizzazioni, subire un attacco informatico che comporta la perdita di dati genera un impatto negativo di estrema rilevanza sia dal punto di vista economico che su quello della perdita di fiducia da parte degli utenti. L'ultima versione dello studio "Cost of a Data Breach Report", condotto da IBM, ha cercato di stimare il costo medio di un data breach che ricade sulle imprese che ne sono vittima. Nel corso dell'analisi, condotta intervistando 3500 rappresentanti delle organizzazioni coinvolte, sono state prese in esame 537 violazioni avvenute in 17 Paesi differenti. Dallo studio è emerso che il costo medio delle violazioni a livello globale è stimabile nel 2021 intorno a quota $ 4,2 milioni. Osservando l'andamento temporale è possibile notare come le ripercussioni economiche sulle aziende colpite siano cresciute del 15% tra il 2017 (anno in cui si attestavano a quota $ 3,62 milioni) e il 2021, di cui del 9% solo nell'ultimo anno.

Fig.4: Costo medio di un data breach per paese (2020 – 2021)



Fonte: IBM Security 2021

In questo scenario, fortunatamente, l'Italia risulta essere tra i Paesi danneggiati in misura minore dalle azioni ostili dei cybercriminali. Analizzando i dati diffusi da IBM emerge infatti che il costo medio dei data breach di cui sono state vittime le aziende italiane nel 2021 si è attestato a quota $

3,61 milioni. Un dato che, sebbene in crescita del 13,6% rispetto al 2020, risulta inferiore sia alla media globale che a quello fatto registrare dalle altre principali economie europee e mondiali (Fig.4).

Una delle tipologie di attacchi informatici più diffusi a danno delle imprese è il ransomware, ovvero un particolare tipo di malware che, una volta penetrato in una rete, cripta le informazioni contenute al suo interno richiedendo all'azienda malcapitata un riscatto per ottenere nuovamente l'accesso ai dati. Secondo uno studio condotto da Sophos tra gennaio e febbraio 2021, intervistando 5.400 specialisti IT provenienti da 30 paesi differenti, è emerso che il 37% delle aziende intervistate aveva subito un attacco ransomware nel 2020. Nel 54% dei casi l'attacco ricevuto è riuscito a penetrare le difese informatiche aziendali e a criptarne i dati e il 65% dei soggetti che si sono trovati in questa situazione è stato costretto a pagare il riscatto per rientrarne in possesso. In generale, dalle interviste raccolte da Sophos è emerso che l'impatto economico medio derivante da un attacco ransomware a livello globale nel 2021 si è attestato a quota $ 1,85 milioni, facendo registrare una crescita del 59% rispetto all'anno precedente, in cui aveva raggiunto in media quota $ 760 mila (Fig.5).

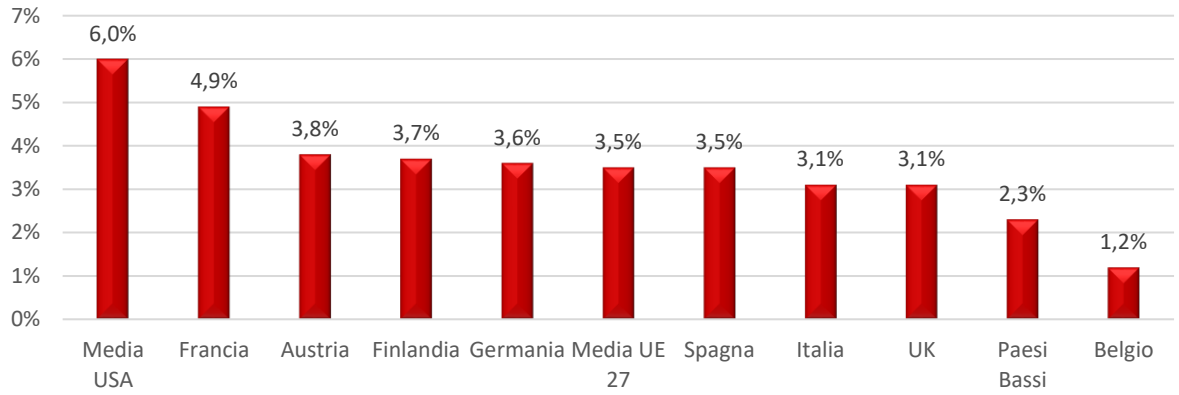
Fig.5: Impatto economico medio derivante da un attacco con ransomware ($)

Fonte: Sophos

Dai dati sopracitati risulta quindi evidente come sia necessario potenziare gli strumenti di sicurezza informatica a disposizione di aziende e amministrazioni per ridurre gli effetti negativi derivanti da potenziali attacchi. Disporre di un sistema di sicurezza all'avanguardia riduce infatti sia la possibilità che una rete venga penetrata sia, in caso avverso, il tempo che i criminali informatici hanno a

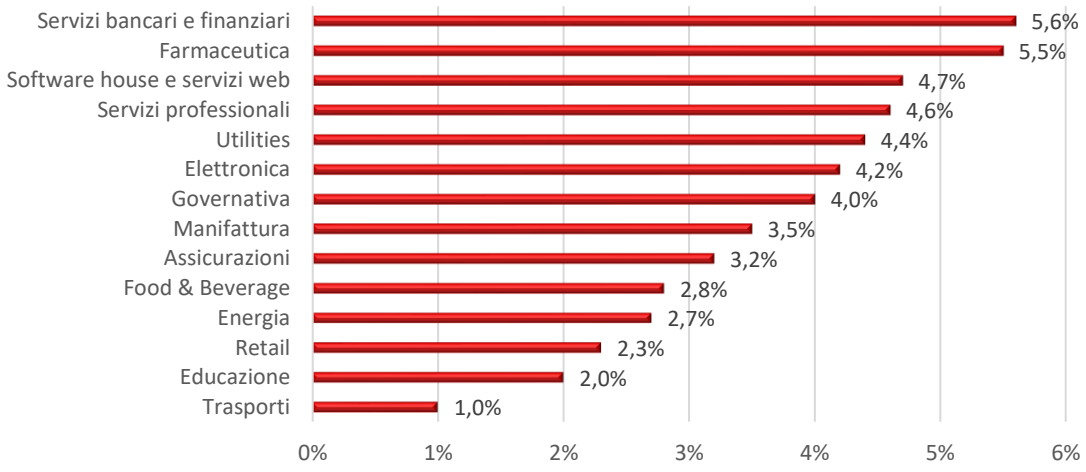
disposizione prima di essere scoperti ed estromessi. Purtroppo, secondo il rapporto "NIS Investments" pubblicato dall'ENISA nel dicembre 2020, la spesa media per la sicurezza IT delle organizzazioni Italiane (in relazione al budget IT) è inferiore sia alla media USA che a quella dell'UE27 (Fig.6). Infatti, in media le organizzazioni USA investono il 6% del proprio budget IT in sicurezza, quelle europee il 3,5% e quelle italiane il 3,1%.

Fig.6: % della spesa in sicurezza informatica delle organizzazioni rispetto al budget IT per area geografica (2020)



Fonte: ENISA, 2020

Fig.7: % della spesa in sicurezza informatica delle organizzazioni rispetto al budget IT per area settore (2020)



Fonte: ENISA, 2020

Osservando nel dettaglio le tipologie di organizzazioni analizzate dall'ENISA emerge che i settori in cui viene investita in sicurezza la quota maggiore del budget in IT (Fig.7) sono i servizi bancari e finanziari (5,6%), il farmaceutico (5,5%) lo sviluppo di software e servizi Internet (4,7%). **Le pubbliche amministrazioni, che per propria natura detengono le informazioni sensibili di tutti i cittadini di un Paese, allocano alla sicurezza solo il 4% del budget IT**.

2. LA CYBERSECURITY NELLE TELECOMUNICAZIONI

2.1. Evoluzione e funzionalità degli standard di sicurezza

Il crescente utilizzo di strumenti informatici negli ambiti più disparati della società, dalla professionalità individuale all'intrattenimento fino a questioni di interesse pubblico nazionale, ha portato allo sviluppo di elaborate infrastrutture a supporto del settore delle telecomunicazioni, la cui sicurezza è essenziale per lo svolgimento di tali attività. Sin dagli anni '80 le autorità nazionali e sovranazionali si sono adoperate per elaborare un **sistema di valutazione della sicurezza** per prodotti e sistemi ICT che fosse affidabile e condiviso, sia per l'importanza strategica dell'architettura cibernetica, sia per la sua rilevanza come elemento abilitante fondamentale per lo sviluppo economico.

Tra i primi tentativi di strutturazione di uno standard di valutazione di sicurezza c'è la creazione del *Trusted Computer System Evaluation Criteria* – **TCSEC**, sviluppato nel 1983 da parte del Dipartimento di Difesa degli Stati Uniti. Più comunemente conosciuta come *Orange Book*, dal colore della copertina, questa pubblicazione identificava i requisiti fondamentali per la definizione dell'efficacia dei controlli di sicurezza di un sistema informatico, ponendo enfasi particolare sul trattamento di informazioni sensibili e classificate. La risposta europea all'iniziativa americana si è concretizzata nella redazione, nel 1990, dell'*Information Technology Security Evaluation Criteria* – **ITSEC** – uno standard che però non è riuscito a diffondersi a livello mondiale. Successivamente, sulla base dell'ITSEC sono stati sviluppati i **Common Criteria** (1996), divenuti nel 1999 **standard ISO/IEC 15408**, che si sono affermati come punto di riferimento globale per la valutazione della sicurezza informatica.

A livello tecnico, per ottenere la certificazione dello standard ISO/IEC 15408 (Common Criteria), è necessario identificare tre elementi fondamentali in relazione all'oggetto della valutazione (**Target of Evaluation**): gli **obiettivi di sicurezza**, **l'ambiente di sicurezza** e i **requisiti funzionali**. Il primo elemento definisce l'intenzione per cui si intende operare la valutazione (contrastare una minaccia, assicurare il rispetto delle leggi, ovvero "sicuro per cosa"); il secondo elemento definisce il contesto in cui l'oggetto della valutazione deve espletare le sue funzioni e viene definito attraverso l'uso che

dovrà farsi del prodotto/sistema in oggetto, l'ambiente di utilizzo e le minacce da contrastare ("sicuro in quale contesto"); l'ultimo elemento identifica le verifiche di sicurezza e il corrispondente livello di assurance garantito da queste ("sicuro a fronte di quali verifiche").

I Common Criteria sono strutturati in modo da rispettare criteri qualitativi tali da garantire alla documentazione prodotta un elevato livello di fiducia, efficacia e correttezza. In particolare, l'ente che esegue le verifiche non deve avere interessi economici legati al risultato della valutazione (**imparzialità**), la ripetizione della procedura deve restituire lo stesso risultato (**ripetibilità**), lo stesso risultato deve poter essere raggiunto da un terzo ente valutante (**riproducibilità**) e il risultato non deve comprendere stime di carattere soggettivo (**obiettività**).

Fig. 8: I Common Criteria: elementi di valutazione e criteri qualitativi

Fonte: elaborazioni I-Com su varie, 2021

Attualmente, in Italia vige dal 1995 uno **Schema Nazionale** per la certificazione della sicurezza di prodotti e sistemi ICT nell'ambito dei *dati classificati*, cui si è aggiunto più recentemente un **Secondo Schema Nazionale**[7] per la fornitura di servizi di certificazioni nel contesto della Pubblica Amministrazione e negli ambiti non ricompresi nella Sicurezza Nazionale.

[7] DPCM 30 ottobre 2003

La struttura di entrambi gli schemi è modellata sulla base degli standard internazionali di riferimento (ITSEC e Common Criteria), così da permettere l'adozione del principio del **mutuo riconoscimento** a livello europeo, per cui gli stati europei riconoscono le certificazioni erogate da altri Stati europei.

Tra gli enti operanti dello Schema Nazionale, cruciale importanza è rivestita dagli **organismi di certificazione** e **laboratori preposti alla valutazione**. I primi si occupano di coordinare il funzionamento dello Schema, indirizzare e verificare i processi di certificazione e di accreditare i laboratori, mentre i secondi operano la valutazione di sicurezza e producono la documentazione che dovrà essere successivamente validata dall'ente certificatore.

L'accreditamento di un laboratorio è di importanza critica dal momento che questo consiste nell'atto con cui l'autorità di riferimento riconosce all'ente indipendenza, affidabilità e competenza tecnica.

In particolare, in Italia l'architettura relativa alla valutazione della componentistica ICT si sviluppa su **tre livelli** (Fig. 9).

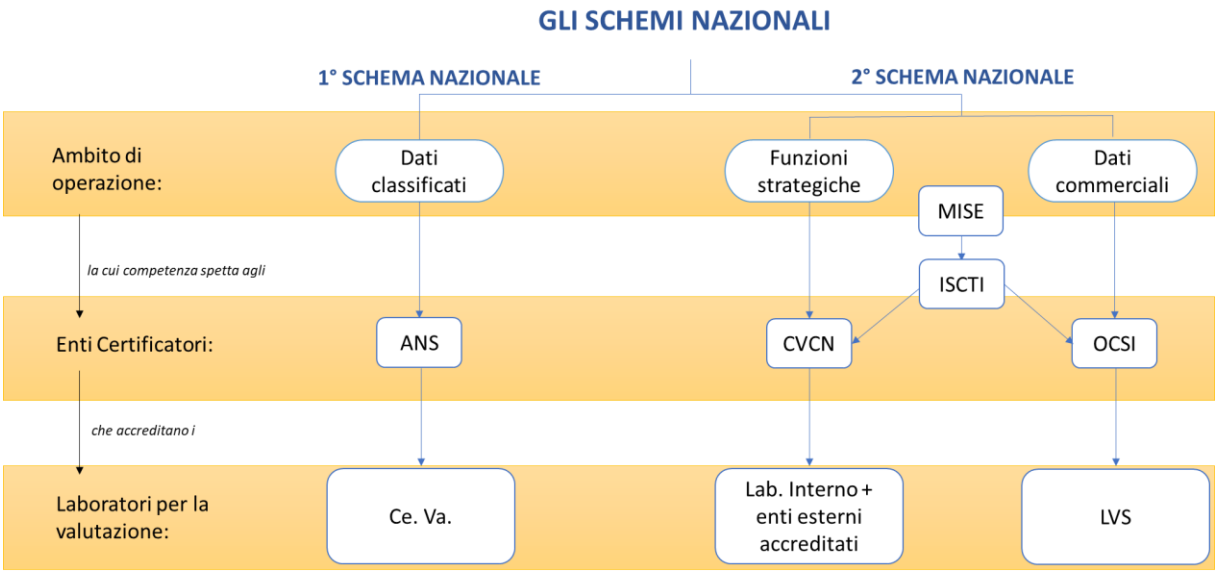
1) Il primo livello riguarda la valutazione tecnica di prodotti che trattano di **dati classificati**; in questo caso è l'Autorità Nazionale per la Sicurezza (ANS), l'ente di certificazione di riferimento che si occupa dell'accreditamento dei laboratori - i Centri di Valutazione (Ce. Va.) - che devono occuparsi della valutazione vera e propria secondo gli standard ITSEC e Common Criteria.

2) Il secondo livello inerisce invece i soggetti titolari di **funzioni critiche o strategiche** e fa riferimento al Centro Valutazione e Certificazione Nazionale (CVCN[8]) che si serve sia di un laboratorio interno che di enti esterni accreditati.

[8] Il CVCN è stato istituito presso l'ISCTI con il DPCM del 24/01/2013.

3) Per quanto riguarda invece i prodotti e sistemi ICT **commerciali**, l'autorità di certificazione è l'Organismo di Certificazione della Sicurezza Informatica (OCSI)[9] che si occupa di accreditare gli apposti Laboratori per la Valutazione della Sicurezza (LVS).

Fig.9: Gli schemi nazionali: ambiti operativi ed enti interessati



Fonte: elaborazioni I-Com su varie, 2021

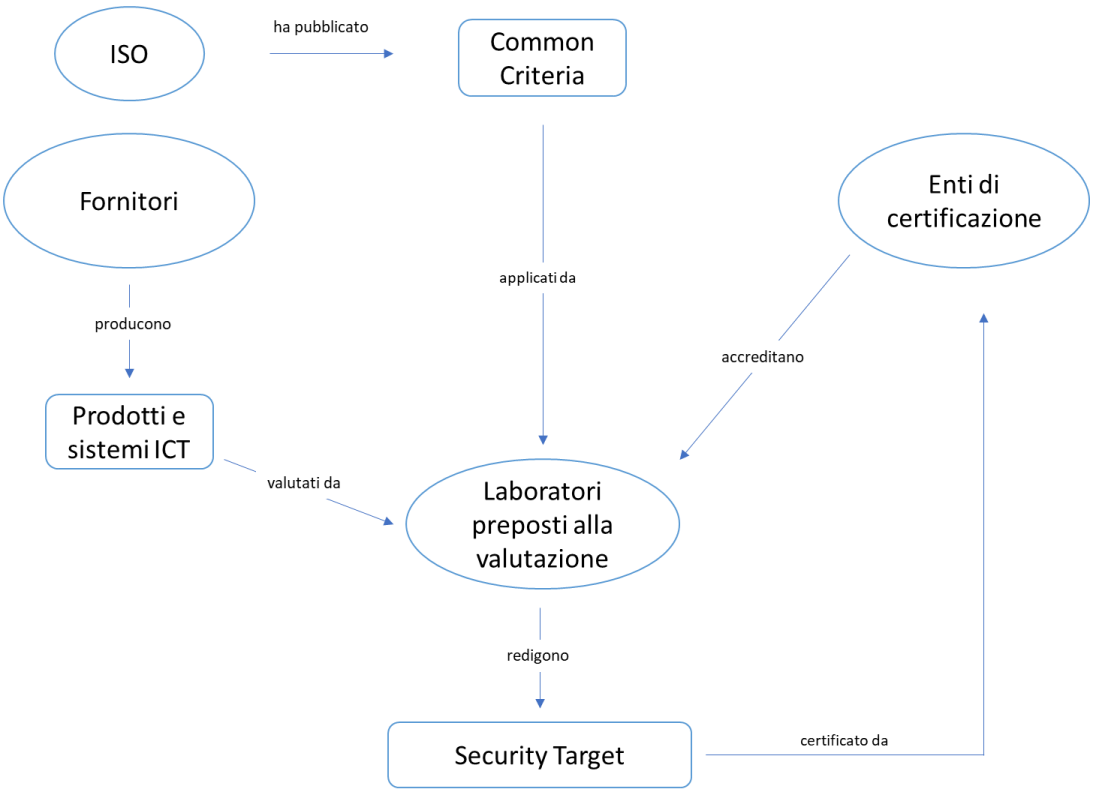
A livello operativo, i laboratori valutano il codice sorgente ed eseguono **Vulnerability Assessment** per poi produrre il Report della valutazione complessiva che l'ente di certificazione dovrà valutare al fine di rilasciare il certificato. Il processo di certificazione dettato dai Common Criteria poggia su due documenti critici: il **Protection Profile** e il **Security Target**.

Il **Protection Profile** è un documento che descrive per una certa categoria di prodotto/sistema ICT, in modo indipendente dalla sua realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente e i requisiti funzionali e di garanzia. Le specifiche del Protection Profile non descrivono il particolare prodotto oggetto della valutazione (funzione del Security Target), ma piuttosto identificano i **requisiti di sicurezza** che questo deve rispettare al fine di soddisfare uno scopo o espletare una funzione. Il Protection Profile, fungendo template di riferimento per la stesura del Security Target,

[9] L'OCSI è stato istituito presso l'ISCTI con il DPCM del 30/10/2003.

conferisce allo standard dei Common Criteria un elemento di distanza rispetto allo standard ITSEC, che invece prevede che sia il committente a scegliere gli elementi che qualificano la valutazione.

Fig.10 : Il funzionamento degli schemi nazionali



Fonte: elaborazioni I-Com su varie, 2021

Il **Security Target** è il documento che **descrive** il **prodotto oggetto della valutazione** (il TOE) e costituisce di fatto il prodotto finale del processo di valutazione. Gli elementi che strutturano il contenuto del documento sono:

- Descrizione del Target of Evaluation
- Conformità in relazione al Protection Profile
- Definizione del problema di sicurezza
- Obiettivi di sicurezza del TOE
- Definizione di componenti estese

- Requisiti di sicurezza e garanzia
- TOE summary specification.

I requisiti di sicurezza, ovvero i **Security Functional Requirements** (SFR), specificano funzionalità di sicurezza individuali che un prodotto o un sistema possono fornire. I Common Criteria ne presentano il catalogo in cui le funzioni vengono suddivise in famiglie[10]. Per esempio, un SFR può definire come eseguire l'autenticazione dell'utente. La lista dei SFR varia a seconda della valutazione, anche se i TOE sono prodotti dello stesso tipo[11].

I requisiti di garanzia, **Security Assurance Requirements** (SAR), descrivono le misure prese durante lo sviluppo e la valutazione del prodotto in modo da garantire l'aderenza con i SFR. Ad esempio, una valutazione può richiedere che tutto il codice sorgente sia conservato in un sistema di gestione delle modifiche. Il catalogo dei SAR comprende 8 famiglie[12], ma la specifica dei SAR cambia di valutazione in valutazione.

Per misurare numericamente il grado di sicurezza del TOE, si ricorre agli **Evaluation Assurance Level** (EAL), **7 livelli di sicurezza**, **ciascuno dei quali corrisponde ad un pacchetto di requisiti (SFR e SAR)**. Il primo, EAL1 (TOE testato funzionalmente) è applicato quando è richiesto un livello di fiducia minimo in presenza di minacce poco rilevanti; seguono l'EAL2 (TOE testato strutturalmente), EAL3 (testato e verificato metodicamente), EAL4 (progettato, testato e riveduto metodicamente), EAL5 (progettato e testato in modo semi-formale), EAL6 (verifica del progetto e testing semi-formali) ed EAL7 (verifica del progetto e testing formali). **Tuttavia, l'EAL4 è probabilmente il livello più alto raggiungibile da prodotti e sistemi che non siano stati progettati appositamente per rispondere ai**

[10] 12 categorie: Security Audit, Communication, Cryptograpgic Support, User Data Protection, Identification and Authentication, Security Management, Privacy, Protection of the TSF, Resource Utilization, TOE access, Trusted Path/Channels.

[11] Lo standard non impone l'inclusione di nessun particolare SFR all'interno del Security Target, ma vengono identificati i legami di dipendenza tra la corretta operatività di una funzione ed un'altra (così come, l'abilità del sistema di negare l'accesso di un utente non autorizzato sulla base del suo ruolo è dipendente dall'abilità del sistema di identificare il ruolo dell'utente).

[12] Protection Profile Evaluation, Security Target Evaluation, Development, Guidance Documents, Life-Cycle Support, Test, Vulnerability Assessment, Composition.

Common Criteria, è indicato nei casi di minaccia medio-alta ed è il livello più richiesto dai committenti.

In termini generali, l'ottenimento della certificazione si traduce spesso in **vantaggi** reali per il fornitore del prodotto ICT. In primo luogo, vi è un vantaggio di **competitività** sul mercato, dal momento che un prodotto certificato venderà di più di un prodotto non certificato. Inoltre, una certificazione può garantire l'accesso ad un **mercato chiuso o specializzato** che necessita di requisiti minimi di sicurezza per i suoi prodotti, come ad esempio il mercato bancario. In presenza di uno standard comune di valutazione, gli utilizzatori possono facilmente operare **confronti tra i prodotti**, riponendo maggiore fiducia nei fornitori che hanno ottenuto certificazioni e che hanno dunque ricevuto un riconoscimento ufficiale per le loro competenze. In più, i Common Criteria offrono al **governo** uno strumento per garantire che i sistemi IT utilizzati nel Paese siano sicuri e quindi contrastare rischi sistemici.

Tuttavia, lo standard ISO/IEC 15408 non è esente da **critiche**. Una prima debolezza della certificazione inerisce i **tempi di esecuzione** della valutazione e del rilascio della certificazione. Al crescere del livello di assurance crescono le verifiche a cui il TOE deve essere sottoposto e dunque le tempistiche si dilatano. Fatta eccezione per i livelli EAL1 e EAL2 che possono richiedere anche "solo" poche settimane, **i livelli dal terzo in poi, possono coprire un orizzonte temporale di vari mesi**, il che espone il prodotto/sistema al **rischio di essere divenuto obsoleto nel momento del rilascio della certificazione**, specialmente se si considera il dinamismo che caratterizza il settore digitale. In questo senso, una maggiore agilità e rapidità sembrerebbe poter essere garantita dal **Nesas**[13], lo standard sviluppato da 3GPP e GSMA che semplifica notevolmente i Common Criteria con procedure di accreditamento e tempi di valutazione brevi, a basso costo, e capaci di soddisfare le esigenze di sviluppo delle nuove tecnologie digitali. A livello di tempistiche, mentre le verifiche condotte con i Common Criteria per assicurare un livello superiore all'EAL4 comportano procedure

[13] Differentemente dai Common Criteria, NESAS non valuta e certifica i prodotti da testare rispetto a particolari livelli di sicurezza. Al contrario, si considera che l'intero set di requisiti di sicurezza, ipotesi sull'ambiente operativo e modello dell'attaccante raggiunga un livello ritenuto rilevante da 3gpp per un prodotto di rete rispetto alla security baseline. L'intento finale è che ogni prodotto di rete abbia la propria security baseline.

complesse e potrebbero richiedere circa 12-18 mesi, l'utilizzo del Nesas comporta procedure semplificate che consentirebbero il time-to-market dei prodotti da testare in circa 3-6 mesi.

Per i Common Criteria, inoltre, la quantità di **documentazione richiesta** aumenta progressivamente con il livello di valutazione, **aumentandone anche i costi oltre alle tempistiche**. In generale, i **costi** del processo sono **elevati** dal momento che la valutazione richiede l'utilizzo di risorse specializzate, motivo per cui la certificazione viene principalmente utilizzata in contesti di sicurezza nazionale o per prodotti e sistemi che ne giustificano l'investimento. Inoltre, una debolezza dello schema è la **rigidità** dello stesso **per il mantenimento della certificazione**. Il sistema, che prevede la perdita della certificazione non appena ci si discosta dalla configurazione verificata, **non contempla la possibilità di installare nuove patch senza una nuova certificazione.** Solo in taluni casi, ovvero quando si sia verificato che l'aggiornamento software non può compromettere il funzionamento delle parti critiche del sistema, un'integrazione della documentazione di valutazione può bastare.

È importante inoltre considerare, infine, che i **costi della valutazione sono a carico del fornitore**. Attualmente **le certificazioni sono volontarie ma le Autorità Nazionali potranno definire eventuali obbligatorietà**. La tematica dell'obbligatorietà delle certificazioni è particolarmente sensibile se si considerano prodotti già operativi: se infatti per i prodotti ancora da realizzare è possibile progettare il design in modo da rispettare gli standard, la richiesta della certificazione per prodotti e sistemi già attivi potrebbe comportare oneri enormi per alcuni fornitori e spostare equilibri di mercato.

2.2. Il bisogno di interoperabilità e standardizzazione

Per le reti mobili, la tendenza verso l'interoperabilità e la standardizzazione in Europa ha origini profonde. L'idea è nata con la progettazione della prima rete mobile GSM, che mirava a consentire il roaming e quindi la possibilità per i consumatori europei di poter portare il proprio dispositivo mobile in un altro paese continentale, utilizzare una rete mobile straniera e usufruire dei servizi in loco, fatturati però dal proprio operatore domestico. Già negli '80 si era osservato come sviluppare uno standard aperto, evitando di utilizzare soluzioni nazionali proprietarie, avrebbe consentito di creare economie di scala molto più significative a livello comunitario, favorendo l'innovazione. Per

raggiungere questo risultato, tra la fine degli anni '80 e l'inizio degli '90, è stato necessario implementare una collaborazione piuttosto intensa tra le diverse parti interessate, tra cui gli Stati, che si sono accordati per riservare specifiche bande di frequenza a tale utilizzo, e alcuni operatori di rete, che hanno contribuito a sviluppare lo standard, divenuto operativo a partire dal 1992. Con il passare del tempo, la responsabilità ed il controllo dello standard GSM è stato trasferito **all'European Telecommunications Standards Institute (ETSI)**, ed anche i vendor delle apparecchiature di rete hanno cominciato a partecipare alle attività di standardizzazione**. Il successo del GSM ha poi attratto sempre più operatori di rete anche al di fuori dell'Europa, trasformando la rete operante in GSM nella prima vera rete mobile mondiale e mostrando l'importanza e i vantaggi di una standardizzazione internazionale collaborativa**. Anche lo standard successivo, chiamato 3G (a livello tecnico UMTS e WCDMA), è stato progettato attraverso un'iniziativa congiunta, in questo caso con portata globale, ovvero il **3GPP** (3rd Generation Partnership Project). Fondato nel 1998 e tutt'ora attivo, comprende operatori di rete e vendor di tutto il mondo e si occupa di coordinare i lavori per definire le funzioni e i protocolli delle reti mobili. Poiché ogni nuova generazione costituisce un'evoluzione rispetto allo standard precedente, le attività partite con il 3G sono proseguite con lo standard 4G e ora sono concentrate sul 5G. **Con il passare degli anni, il 3GPP ha progressivamente rilevato le attività di gestione delle specifiche GSM dall'ETSI e, allo stato attuale, tutti gli standard concordati e approvati dal 3GPP sono automaticamente riconosciuti e ratificati dagli organismi di standardizzazione nazionali o internazionali**. Questi ultimi sono costituiti, tra gli altri, dallo stesso ETSI in Europa, da ATIS (Alliance for Telecommunications Industry Solutions) negli Stati Uniti e dal TTC (Telecommunication Technology Committee) in Giappone. Attualmente il 3GPP consiste in una partnership mondiale di organismi di standardizzazione per le telecomunicazioni di tutto il mondo e definisce gli standard normativi ufficialmente riconosciuti pressoché in tutti i Paesi del globo. Gli operatori di rete, per operare nei vari Paesi, sviluppano e gestiscono tecnologie standardizzate dal 3GPP, utilizzando le tecniche di trasmissione definite da tali standard e le stesse frequenze da esso individuate a livello internazionale, che vengono peraltro recepite dai regolatori nazionali dei singoli Paesi. Come per ogni caso di successo o insuccesso relativo alla diffusione e all'accettazione degli standard, queste sono generalmente dovute alla numerosità dei partecipanti e al peso dei membri, ovvero alla sua massa critica. Nel caso del 3GPP,

la partecipazione è aperta ad ogni soggetto dell'industria della telefonia mobile che sia membro di uno degli enti di regolamentazione menzionati, inclusi i vendor di apparecchiature, i produttori di device mobili, gli operatori di rete, le autorità di regolazione e altri tipi di organizzazioni e gruppi di interesse. Di conseguenza, tale vasta adesione fa sì che gli standard emanati dal 3GPP siano generalmente accettati dalla maggioranza degli operatori e dei Paesi.

Il funzionamento delle procedure è basato su proposte di contributi e meccanismi di approvazione: per far sì che un nuovo principio o una nuova idea vengano implementati in uno standard, questi devono essere portati all'attenzione dei membri per l'approvazione. L'ente è organizzato in vari Technical Specification Groups (TSG) suddivisi per temi (ad es. funzioni e protocolli di rete, crittografia, autenticazione e sicurezza) e sottogruppi (Working Groups). Il gruppo SA3, in particolare, è responsabile per gli aspetti relativi alla sicurezza, ed ha il compito di analizzare ogni nuova caratteristica sviluppata all'interno del 3GPP specificandone i requisiti ed i meccanismi per garantirne la protezione.

L'obiettivo finale delle operazioni del 3GPP consiste nell'assicurare una completa interoperabilità tra le reti dei diversi operatori e nei diversi Paesi, in modo che potenzialmente tutti i device mobili funzionino su tutti i network. Inoltre, per ogni generazione di standard è presente un numero piuttosto consistente di release delle specifiche tecniche, che vengono implementate nelle apparecchiature di rete dei vendor e nelle infrastrutture degli operatori di reti.

2.3. ENISA e i benefici della standardizzazione

Come sottolineato dall' ENISA (European Union Agency for Security)[14], i vantaggi della standardizzazione nella sicurezza informatica sono chiari e ben noti. Tra questi, l'Agenzia elenca l'interoperabilità, la riusabilità, l'aumento della qualità di conoscenza e consapevolezza dell'importanza della cibersicurezza, l'armonizzazione della terminologia, la coerenza tra diversi

[14] ENISA, *Standardisation in Support of the Cybersecurity Certification. Recommendations for European standardisation in relation to the Cybersecurity Act*, December 2019.

produttori, fornitori e utenti, la ripetibilità, il controllo delle prestazioni ed una migliore valutazione della sicurezza e dell'integrità della supply chain.

Inoltre, per la valutazione della **sicurezza informatica**, la **standardizzazione** è ritenuta **necessaria** per una serie di attività quali la **valutazione del rischio, dei criteri e dei metodi di valutazione,** così come dei profili di protezione, **e per il mantenimento dei certificati di sicurezza informatica lungo il loro ciclo di vita**. Anche la coerenza tra le valutazioni eseguite da diversi enti e laboratori è una questione chiave. A tal fine, gli standard dovrebbero essere sviluppati per supportare revisioni incrociate (peer review) e controlli sugli stessi valutatori. Scopo finale di queste operazioni è garantire la massima sicurezza possibile in un contesto in cui le procedure relative alla sicurezza informatica siano coerenti in tutta Europa e potenzialmente in tutto il mondo. A livello europeo, in particolare, l'obiettivo è garantire che qualsiasi valutazione della sicurezza informatica effettuata in uno degli Stati membri dell'UE sia efficace e accettata da tutti gli altri Stati, senza che sia necessario effettuare valutazioni multiple[15].

Un altro punto importante sottolineato dall'ENISA consiste nell'introduzione di **nuovi requisiti relativi a differenti livelli di garanzia** (da distinguere ad esempio tra livelli di base, sostanziali e elevati) per coprire diverse analisi dei rischi, in modo da **mantenere l'equilibrio tra una certificazione in grado di mitigare le possibili minacce**, **tenendo allo stesso tempo conto delle esigenze del mercato**, relative a costi, tempi e prestazioni da raggiungere. Una tale distinzione è opportuna anche per **differenziare i costi delle certificazioni, che dovrebbero essere distinti in base all'importanza dei target.** Ad esempio, il costo per testare apparati della difesa non dovrebbe avvicinarsi a quello per testare apparecchiature ad uso civile ad esempio utilizzate per raccogliere i dati climatici, mentre dovrebbe essere commisurato al target e ai possibili impatti di eventuali attacchi.

Anche in questa direzione, secondo l'ENISA, la standardizzazione di criteri e i metodi di valutazione della sicurezza informatica è centrale. Allo stato attuale, inoltre, la natura trasversale della sicurezza

[15] Ibidem, pag. 10

informatica fa sì che la standardizzazione abbracci settori molto diversi (ad es. automobilistico, sanitario, infrastruttura cloud, IoT, 5G, energia), allo stesso tempo evitando che diversi verticali creino proprie soluzioni di sicurezza settoriali. In questo senso, la coerenza tra i settori verticali può garantire requisiti minimi realizzabili per la sicurezza informatica, sostenendo una maggiore diffusione e adozione.

2.4. Strumenti per valutare l'impatto delle certificazioni sul mercato

La sicurezza delle reti TLC, insieme agli effetti derivanti dalla mancanza di essa in termini economici e di competitività del mercato, costituiscono temi centrali nel lavoro dell'Unione Europea e degli Stati Membri. Già con l'adozione del quadro unico di certificazione stabilito nell'ambito del **Cybersecurity Act (CSA)** era stato introdotto uno strumento che mirasse a stabilire livelli condivisi di sicurezza nei prodotti, nei servizi, e nei processi derivanti da tecnologie ICT, nonché a mantenere la fiducia in essi. L'elaborazione di schemi di certificazione della cybersecurity a livello comunitario mira, dunque, a fornire **criteri armonizzati per effettuare valutazioni di conformità e per stabilire il grado di aderenza di prodotti, servizi e processi rispetto a requisiti specifici, predefiniti e condivisi tra gli Stati**.

Sul piano economico, tali sistemi sono ideati con l'intento non solo di intervenire in quelle **dinamiche di mercato** che comportano risultati subottimali e non efficienti, ma anche per affrontare **aspetti socioeconomici** quali la fiducia degli utenti finali, l'obbligo di diligenza dei produttori e fornitori, e la reputazione del mercato stesso. I fattori determinanti per le certificazioni di cybersecurity nell'UE vanno dunque oltre i requisiti di cybersecurity, e impattano in modo continuo e dinamico anche in termini di concorrenza e di fiducia dei consumatori.

Sebbene questa ampia varietà di fattori non sia sempre stata considerata nei processi normativi e di assegnazione di tali certificazioni da parte delle istituzioni UE, la necessità di tenere conto del legame tra i temi strettamente relativi alla sicurezza e gli effetti economici da essi influenzati ha recentemente portato alla pubblicazione di un'**analisi, condotta dall'ENISA**, in cui viene proposta una **nuova e più comprensiva metodologia per l'analisi degli impatti di tali certificazioni condivise**

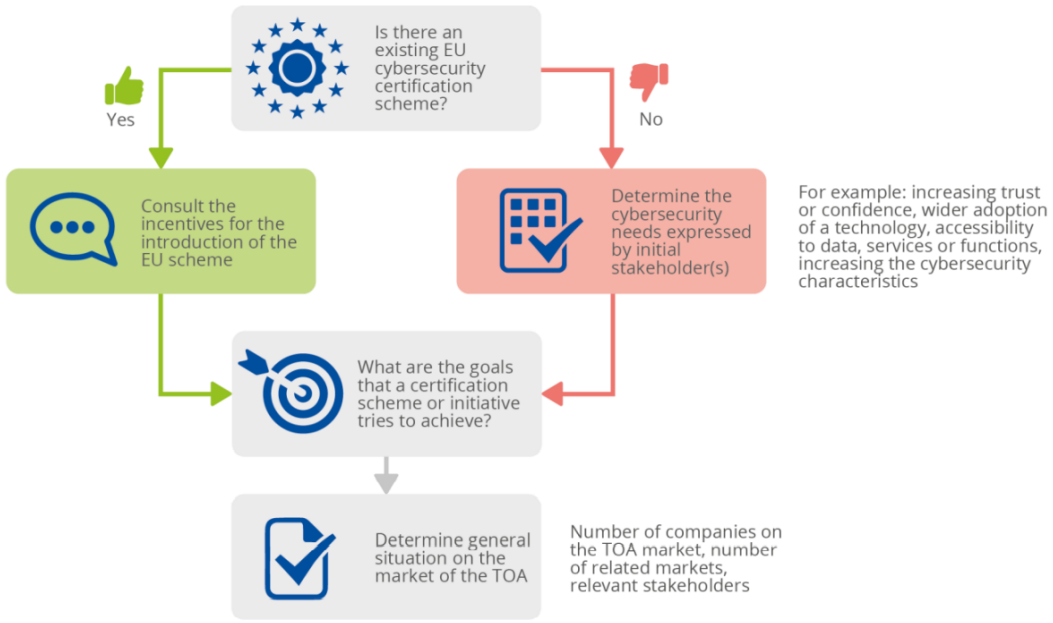
sul mercato. La stessa agenzia ha dichiarato che una gestione di questo tipo nel campo delle certificazioni per la cybersecurity sarebbe di grande beneficio per la Commissione sia in termini economici che di regolamentazione e concorrenza[16].

Proprio in considerazione di tale importanza, la nuova procedura di analisi proposta dall'ENISA nasce con l'intento di fornire un metodo dotato di maggiore chiarezza e di processi di valutazione applicabili tanto alle certificazioni già in uso quanto a nuove soluzioni, la metodologia proposta si incentra sull'importanza di definire un chiaro **target di analisi (TOA)**. Intorno ad esso vengono sviluppati quattro livelli di indagine ovvero la descrizione del contesto di mercato, l'individuazione dell'ambito del TOA, la valutazione dell'impatto delle iniziative di certificazione della cybersecurity relative al TOA in questione, e l'identificazione di eventuali alternative più efficienti. L'obiettivo preposto dall'ENISA è quello di fornire uno **strumento metodologico in grado di identificare le necessità di certificazione** e **le incongruenze attuali** senza tuttavia basarsi esclusivamente sui diretti input delle parti interessate, ma piuttosto su prove derivanti sia dal lato dell'offerta che della domanda **in modo da tenere conto degli aspetti sociali ed economici**.

All'interno di questo processo, sono proposte due possibili tipologie di analisi in base al contesto di regolamentazione e di mercato. La prima, ovvero l'**analisi di mercato**, viene condotta in **settori in cui non esiste attualmente alcuna iniziativa di certificazione da parte dell'UE**, fornendo quindi gli strumenti per determinare se c'è una giustificazione per l'UE a considerare nuove iniziative da sviluppare e se un intervento di questo tipo è necessario, specialmente nei mercati emergenti. La seconda, ovvero l'**analisi d'impatto**, si applica invece a **settori in cui il framework europeo per le certificazioni sulla cybersecurity è già in uso**, **fornendo supporto nella valutazione degli effetti della certificazione stessa.** In questo caso l'analisi serve per determinare i risultati derivanti da un **meccanismo di sicurezza** e per capire se tale strategia è effettivamente costruttiva per le **performance del mercato** in termini di **concorrenza** e di **rafforzamento della fiducia** da parte dei consumatori.

[16] "This broader understanding and oversight would be beneficial to the policy and regulatory certification activities of the European Commission", ENISA Cybersecurity Certification Market Study - aprile 2021.

Fig.11: Rappresentazione schematica del primo passaggio della metodologia proposta dall'ENISA per l'analisi degli impatti delle certificazioni condivise sul mercato



Fonte: ENISA Cybersecurity Certification Market Study. Aprile 2021

Di conseguenza, la metodologia ENISA prevede l'esecuzione di una **valutazione preliminare dell'impatto dell'iniziativa di certificazione**, sia nel caso in cui questa fosse già applicata e in atto (analisi d'impatto), sia nel caso di una possibile introduzione di una nuova certificazione in campi ad oggi non inclusi in nessuna regolamentazione (analisi di mercato). In entrambi i casi, viene suggerita **un'analisi costi-benefici** comprendente non solo le spese tipicamente sostenute dagli stakeholder (imprese, governo/pubbliche amministrazioni, cittadini) (Tabella 1), ma anche le valutazioni su fenomeni di mercato (scenari *"business as usual"*, il numero di soggetti interessati e affetti, ecc.). Le difficoltà maggiori in questo caso riguardano la possibilità di accedere a dati adatti a identificare e quantificare non solo i **costi e i benefici finanziari**, ma anche i **costi e benefici socio-economici e di mercato**. Questo risulta particolarmente complicato nei casi in cui valutazioni monetarie possono essere assegnate a costi diretti e altri costi e benefici tangibili (costi amministrativi), ma non ad altri tipi di fattori considerati, per i quali, invece, è possibile unicamente una valutazione qualitativa.

Tab.1: Costi e benefici che potrebbero essere associati ad una possibile iniziativa di certificazione condivisa nel campo della cybersecurity

Tipo di costo	Categoria specifica
Costi diretti	Costi amministrativi
	Costi di adeguamento
	Spese, tasse, ecc.
	Amministrazione e attuazione
Costi indiretti	Costi derivanti da mercati collegati o registrati da operatori che non sono direttamente oggetto della certificazione
	Costi indiretti di adeguamento
	Impatti negativi sul mercato

Tipo di beneficio	Categoria specifica	Descrizione	Beneficiario principale
Miglioramenti nell'efficienza del mercato	Stesse categorie riportate nella tabella dei costi	Migliore distribuzione delle risorse, rimozione di fallimenti normativi o di mercato, risparmi sui costi generati dal (nuovo) schema di certificazione.	- L'intero sistema economico
	Maggiore disponibilità di pagamento (willingness to pay) per prodotti certificati	Rafforzamento della reputazione delle imprese che producono il prodotto/servizio/processo certificato. Maggiore fiducia dei consumatori.	- Le imprese produttrici del prodotto/servizio/processo certificato
Benefici indiretti derivanti dall'adeguamento		Effetti spill-over associati alla conformità di terzi con lo schema di certificazione.	- Le imprese nei mercati associati - Clienti nei mercati associati
Effetti indiretti sul contesto macroeconomico		Crescita del PIL, maggiore concorrenza nel mercato, incremento della produttività	- L'intero sistema economico

Altri benefici socio-economici		Maggiore protezione di diritti fondamentali, coesione sociale, stabilità internazionale. Maggiore sicurezza cibernetica	- L'intero sistema economico

Fonte: ENISA Cybersecurity Certification Market Study. Aprile 2021

La terza parte della metodologia riguarda la **comparazione tra le opzioni di intervento** nella ricerca della **soluzione dagli esiti migliori sia per gli stakeholder che per il mercato nel suo insieme**. L'obiettivo di questa fase è determinare quali soluzioni a livello Comunitario, o a livello nazionale, possano essere intraprese e in quale forma (mezzi normativi e non normativi). Nel caso di analisi di mercato, questo serve a determinare le opzioni o le modalità di un possibile schema di certificazione, sia nel caso in cui fosse necessaria una nuova certificazione sia nel caso in cui risultasse possibile allargare il campo di applicabilità di certificazioni già esistenti. Nel caso in cui si applicasse un'analisi d'impatto, invece, il confronto avviene con l'elaborazione di uno scenario controfattuale, vale a dire la situazione che sarebbe potuta accadere nel caso in cui le certificazioni esistenti non fossero state applicate.

Nella quarta e ultima fase del processo, l'ENISA fornisce una serie di domande per individuare le soluzioni migliori tra quelle messe a confronto in termini di massimizzazione dei benefici netti comprensivi sia di valutazioni finanziarie che socioeconomiche.

Nel complesso, la proposta di procedura elaborata dall'ENISA dimostra **il considerevole grado di coscienza diffusa sulla centralità dei temi legati alla sicurezza e all'importanza di trovare modalità di gestione uniformi ed efficienti** per la gestione dei modi in cui la cybersecurity interagisce con il funzionamento dei mercati e i fenomeni socioeconomici in senso lato. In questo senso, la divisione – e, talvolta, anche la sovrapposizione - tra sistemi di certificazioni stabiliti a livelli nazionali e Comunitari è per molti aspetti **dispersiva e poco efficiente**. Si evidenzia dunque **l'esigenza di un intervento uniformatore** che vada a superare tali contraddizioni attraverso valutazioni condivise sull'impatto in termini di effettivo miglioramento della sicurezza e di conseguenza sul funzionamento dei mercati.

2.5. Verso una certificazione europea?

Allo stato attuale, su mandato dell'Unione Europea (tramite il già citato Cybersecurity Act), l'impegno di Enisa si è concretizzato nella pubblicazione del Security Toolbox per supportare la sicurezza nelle reti 5G. Infatti, sebbene sia stato assegnato ad ENISA il compito di promuovere lo sviluppo di uno schema di certificazione della sicurezza informatica per le reti coinvolgendo tutte le parti interessate (tra cui lo European Cybersecurity Certification Group, il NIS Cooperation Group e enti di standardizzazione per il 5G) [17], al momento una delle misure centrali, ovvero l'assessment del profilo di rischio dei fornitori e l'applicazione di restrizioni per quelli ritenuti ad alto rischio (i c.d. High-risk vendors, HRV), manca di una definizione chiara di high-risk vendors. Di conseguenza, sembrerebbe profilarsi l'applicazione di una baseline comune del risk assessment per tutti i vendor anche perché, allo stato attuale, non è stato definito un quadro comune per valutare il profilo di rischio dei singoli fornitori. A tal proposito, la progettazione e l'implementazione di un terreno comune per una valutazione trasparente e uniforme da utilizzare in tutta l'UE costituirebbe uno step fondamentale.

Di fatto, allo stato attuale esiste un duplice range di azioni che coinvolgono sia i vendor (che siano classificati o meno come HRV), sia gli operatori di rete. Questi ultimi devono non solo rafforzare i propri requisiti relativi alla sicurezza e al monitoraggio, ma anche effettuare l'assessment del profilo di rischio dei propri fornitori, e applicare un approccio *risk-based* tanto per la rete core quanto per le funzioni di accesso e gestione di rete. In particolare, in una prospettiva di ecosistema, gli operatori di rete devono mettere in atto strategie multi-vendor per evitare o minimizzare la dipendenza da singoli vendor e assicurare un adeguato bilanciamento a livello nazionale.

A livello di mercato, appare quindi opportuna l'implementazione di uno standard di valutazione e certificazione della sicurezza unificato, in cui venga rafforzato sia il ruolo dell'UE, sia quello delle autorità nazionali, creando le condizioni affinché la valutazione dei fornitori venga effettuata tramite criteri oggettive, secondo principi coerenti e misurabili, così da generare un ambiente

[17] Nel quadro della definizione delle minacce e dell'approccio al risk management – in cui alcune misure sono state redatte dal gruppo di cooperazione NIS nell'ambito del Toolbox UE, a sostegno dell'obiettivo generale di standardizzare l'approccio alla sicurezza informatica –

sufficientemente competitivo, equo e affidabile, tale da garantire la diffusione delle migliori tecnologie, con i relativi benefici economici e sociali.

Un indirizzo di respiro europeo è da tenere in considerazione **anche in Italia,** sia per l'importanza di implementare una certificazione che sia in qualche modo convergente – anche nell'ottica di rendere le certificazioni rilasciate in Italia valide anche negli altri Paesi europei - sia in merito agli **specifici strumenti** da far convergere nell'iniziativa di certificazione.

Per quanto concerne il primo aspetto, si osserva come le ristrette dimensioni del mercato fornitori, composto interamente da provider operanti a livello internazionale, rischino di rallentare sensibilmente lo sviluppo delle reti, qualora i fornitori si trovino a fronteggiare tante diverse procedure quanti sono i Paesi europei in cui operano.

In secondo luogo, è importante valutare con attenzione gli strumenti da utilizzare per le certificazioni a livello nazionale. Ad esempio, l'eventuale utilizzo dei Common Criteria per la verifica della sicurezza della componentistica di rete, se da un lato potrebbe tradursi in **vantaggi in termini di competitività** (maggior livello di fiducia verso un prodotto/sistema certificato), allo stesso modo, come per ogni altra forma di certificazione (Tab. 1), presenta anche una serie di **costi** – sia per l'azienda stessa, sia per il contesto socioeconomico. Infatti, riprendendo le osservazioni dell'ENISA, i Common Criteria presentano anche **criticità** in termini di **tempi di esecuzione delle verifiche**, eccessivamente lunghi e inadatti al dinamismo e la velocità di evoluzione del settore digitale, e di **mancata flessibilità di analisi in termini di costi-benefici sugli impatti in ciascun mercato**, in quanto, ad esempio, non viene permesso a priori il **mantenimento della certificazione per il prodotto/sistema** su cui vengono installate nuove patch per l'aggiornamento.

In conclusione, si evidenzia, da un lato, l'opportunità di valutare la possibilità di effettuare un'analisi dell'impatto sul mercato delle certificazioni e delle iniziative di armonizzazione in chiave europea anche nel contesto italiano, sia a livello di ricerca, sia a livello di dibattito, rispetto alle performance tanto in termini di concorrenza quanto in termini di rafforzamento della fiducia da parte degli utilizzatori e dell'intero sistema; dall'altro si sottolinea come l'implementazione di un approccio standardizzato a livello europeo potrebbe creare una base comune per una valutazione fondata sulle minacce e su controlli di mitigazione misurabili, in cui far competere i principali fornitori di

telecomunicazioni secondo regole uniformi, nell'ottica di creare un ecosistema capace di generare fiducia tra i diversi mercati e Paesi coinvolti.

3. L'EVOLUZIONE DELL'ECOSISTEMA NAZIONALE DELLA CYBERSICUREZZA E IL NUOVO ASSETTO DELLE COMPETENZE IN MATERIA

3.1. Dall'istituzione alla piena operatività del perimetro di sicurezza nazionale cibernetica

La necessità di garantire un ecosistema quanto più possibile sicuro ha determinato, da un lato, la graduale estensione dell'ambito di applicazione della disciplina sul golden power, introdotta con il D.L. 15 marzo 2012 n. 21 (convertito con modificazioni con la legge n. 56 del 2012) che negli ultimi anni, attraverso una serie di modifiche normative[18], è stata caratterizzata da un'incessante evoluzione sempre nella direzione del rafforzamento e dell'estensione dei poteri attribuiti all'esecutivo e, dall'altro, ha spinto all'adozione del **D.L. 21 settembre 2019, n. 105**, convertito dalla L. 18 novembre 2019, n. 133 con il quale è stato istituito il **perimetro di sicurezza nazionale cibernetica** 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 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.

Tale decreto, in particolare, ha tracciato un percorso attuativo frazionato con scadenze temporali diversificate, che si snoda attraverso cinque decreti del Presidente del Consiglio dei ministri ed un regolamento governativo di esecuzione: 1) un DPCM che definisca le **modalità e i criteri procedurali di individuazione dei soggetti** (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge e declini i **criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti**, dei sistemi informativi e dei servizi

[18] Il decreto legge n. 148/2017, convertito con legge n. 172/2017, è intervenuto estendendo l'esercizio dei poteri speciali applicabili nei settori dell'energia, delle comunicazioni e dei trasporti agli asset "ad alta intensità tecnologica", mentre due anni dopo, con il D.L. 25 marzo 2019, n. 22 (c.d. Decreto Brexit), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41 sono stati inclusi, nelle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica; 2) un DPCM di natura provvedimentale di definizione dell'elenco dei soggetti individuati; 3) un DPCM che disciplini i termini e le modalità attuative delle procedure secondo cui i soggetti rientranti nel perimetro notificano al Gruppo di intervento per la sicurezza informatica (CSIRT) gli **incidenti** aventi impatto su reti, sistemi informativi e servizi informatici e stabilisca le **misure di sicurezza** da adottare (**DPCM n. 81 del 14 aprile 2021,** pubblicato sulla G.U. dell'11 giugno 2021); 4) un regolamento governativo per la disciplina delle **procedure, delle modalità e dei termini con cui i soggetti danno comunicazione al CVCN** delle procedure per l'affidamento di forniture di beni, sistemi e servizi ICT e i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici assicurano la propria collaborazione per l'effettuazione delle attività di test di sicurezza (**DPR n. 54 del 5 febbraio 2021** pubblicato sulla G.U. del 23 aprile 2021); 5) un DPCM per **l'individuazione, sulla base di criteri di natura tecnica, delle categorie di forniture di beni, sistemi e servizi ICT** destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici assoggettati all'obbligo di comunicazione; 6) un DPCM per la definizione dei **criteri per l'accreditamento**, da parte del CVCN, dei laboratori di cui lo stesso CVCN può avvalersi per lo svolgimento dei suoi compiti di verifica (ancora in corso di definizione).

Seppur in ritardo rispetto alla tabella di marcia che prevedeva l'adozione del primo DPCM entro 4 mesi dall'entrata in vigore della legge di conversione del decreto istitutivo del perimetro, complice, certamente, anche l'emergenza sanitaria ancora in atto, lo scorso 21 ottobre è stato pubblicato sulla Gazzetta Ufficiale il **DPCM 30 luglio 2020, n. 131** che ha formalmente dato avvio all'articolata e complessa procedura di attuazione della disciplina del perimetro di sicurezza cibernetica. Si tratta del primo atto cui è affidato il compito, da un lato, di definire le **modalità e i criteri procedurali di individuazione dei soggetti** (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge e, dall'altro, declinare i **criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici** di rispettiva pertinenza, comprensivo della relativa architettura e componentistica.

In particolare, tale decreto: 1) include nel concetto di **funzione essenziale** le attività tese 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 e la funzionalità dei sistemi economico e finanziario, e dei trasporti mentre riconduce al concetto di **servizio essenziale**, i soggetti che svolgono attività: a) strumentali all'esercizio di funzioni essenziali dello Stato; b) necessarie per l'esercizio e il godimento dei diritti fondamentali; c) necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; d) ricerca e attività 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; 2) individua i seguenti **settori di attività**: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche; l) enti previdenziali/lavoro; 3) fissa le modalità ed i criteri di individuazione dei soggetti inclusi nel perimetro di sicurezza cibernetica; 4) prescrive alle amministrazioni l'individuazione delle funzioni o servizi essenziali per i quali "il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime" e la predisposizione di un **elenco** di tali soggetti che viene trasmesso al CISR e al CSIR tecnico e poi formalizzato in un atto amministrativo, adottato e periodicamente aggiornato dal Presidente del Consiglio dei ministri, su proposta del CISR. È compito del Dipartimento delle informazioni per la sicurezza (DIS) darne comunicazione alle amministrazioni interessate; 5) istituisce un **Tavolo interministeriale** per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR, presieduto da un vice direttore del DIS, composto da due rappresentanti di ciascuna amministrazione CISR, un rappresentante per ciascuna delle due agenzie di informazioni (Agenzia informazioni e sicurezza esterna – AISE e Agenzia informazioni e sicurezza interna – AISI) e due rappresentanti dei ministeri di volta in volta interessati che sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare di cui almeno uno in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, che si riunisca periodicamente, e comunque almeno una volta ogni 6 mesi (senza alcun gettone di presenza, compenso o rimborso spese o altri emolumenti per la partecipazione alle riunioni); 6) detta i **criteri per la predisposizione e**

l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici prescrivendo ai soggetti inclusi nel perimetro di individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale valutando, nello specifico, l'impatto di un incidente sul bene ICT e la dipendenza con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione e predisporre ed aggiornare, con cadenza almeno annuale, l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono; 7) fissa in sei mesi dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco il termine per procedere alla **trasmissione degli elenchi** appena descritti alla Presidenza del Consiglio o al Ministero dello sviluppo economico.

In attuazione di quanto previsto dal DPCM appena descritto, con **decreto del 25 novembre** scorso è stata definita la lista segreta degli oltre 100 soggetti pubblici e privati inclusi nel perimetro.

Il **23 aprile 2021** è stato invece pubblicato il **DPR n. 54 del 5 febbraio 2021**, terzo atto di attuazione della legge sul perimetro. Il decreto su CV e CVCN, in particolare, disciplina le procedure e i termini per le valutazioni da parte del CVCN e dei CV su prodotti in acquisizione da parte dei soggetti inclusi nel perimetro e si compone di 4 Capi che definiscono con puntualità le tipologie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN, le modalità ed i contenuti delle comunicazioni da effettuare in favore di CVCN o CV da parte dei soggetti inclusi nel perimetro, le tipologie di valutazioni, test e verifiche realizzabili, nonché le attività di verifica ed ispezione cui possono essere sottoposti i soggetti inclusi nel perimetro.

Con **DPCM n. 81 del 14 aprile 2021, pubblicato sulla G.U. dell'11 giugno 2021** sono state regolamentate le **notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici**. Si tratta di un decreto che si compone di 11 articoli suddivisi in quattro Capi che: a) disciplinano le notifiche da incidente con particolare riguardo agli incidenti aventi impatto su beni ICT, alla notifica volontaria degli incidenti, alla trasmissione delle notifiche e ad incidenti attinenti alla gestione delle informazioni classificate; b) classificano gli incidenti aventi impatto sui beni ICT a seconda della gravità degli incidenti anche tenuto conto della tempistica necessaria per una risposta efficace; c) ricollega al verificarsi di uno degli incidenti avente impatto su un bene ICT l'obbligo di

notifica al CSIRT italiano (intendendo per impatto una limitazione dell'operatività del bene ITC ovvero una compromissione della disponibilità, integrità o riservatezza dei dati e delle informazioni da esso trattati ai fini dello svolgimento della funzione o del servizio essenziali); d) disciplinano la notifica volontaria degli incidenti; e) disciplina le modalità e i termini di adozione delle misure di sicurezza; f) individua le misure minime di sicurezza di natura tecnica e organizzativa che sono volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT e agli elementi delle notifiche di incidente.

Con **DPCM 15 giugno 2021 pubblicato sulla G.U. del 19 agosto 2021** è stato stilato l'elenco dei prodotti da sottoporre al Technology screening mentre è ancora atteso l'ultimo DPCM che fisserà le regole di accreditamento per quanto riguarda i laboratori accreditati di prova che potranno effettuare screening di tecnologie.

3.2. L'istituzione dell'Agenzia per la cybersicurezza nazionale

Se è in fase di ultimazione la complessa ed articolata procedura di definizione del quadro normativo che consentirà la piena operatività del perimetro di sicurezza nazionale, con la **legge n. 109 del 4 agosto 2021** di conversione del D.L. n. 82/2021 è stata istituita l'**Agenzia per la cybersicurezza nazionale**.

Si tratta di un intervento straordinariamente rilevante che, partendo dalla constatazione della crescente centralità assunta dalla cybersecurity e della frammentarietà del quadro normativo che assegnava a numerose autorità specifiche competenze in materia creando un sistema altamente complesso ed incerto, ha riunito in capo ad unico soggetto – l'Agenzia – tutte le competenze in materia di cybersicurezza, segnando una svolta epocale per il nostro ordinamento.

La normativa in esame, in particolare, dopo aver attribuito in via esclusiva (e dunque con impossibilità di delega) al Presidente del Consiglio l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, l'adozione della strategia nazionale di cybersicurezza (sentito il Comitato interministeriale per la cybersicurezza - CIC) istituito dall'art. 4, la nomina e la revoca, previa deliberazione del Consiglio dei Ministri e con successiva comunicazione al COPASIR (secondo le

modifiche introdotte in sede di conversione), del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale istituita dall'art. 5, istituisce, per l'appunto l'Agenzia.

La nuova Agenzia per la cybersicurezza nazionale che opererà sotto la responsabilità del Presidente del Consiglio dei ministri e dell'Autorità delegata per la sicurezza della Repubblica e in stretto raccordo con il Sistema di informazione per la sicurezza della Repubblica, sarà l'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, predisporrà la strategia nazionale di cybersicurezza, assicurerà, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale, promuoverà 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 pubbliche amministrazioni, opererà come Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi per le finalità di cui al decreto legislativo NIS e come Autorità nazionale di certificazione della cybersicurezza, accrediterà le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, assumerà tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale (comprese le attività di ispezione e verifica e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative), acquisirà le competenze attribuite al DIS dal decreto-legge perimetro e dai relativi provvedimenti attuativi, quelle relative alla sicurezza e all'integrità delle comunicazioni elettroniche di cui al D.Lgs. n. 259/03 e svolgerà tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, nonché tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti.

A tali funzioni e competenze, in sede di conversione del decreto ne sono state aggiunte ulteriori ed, in particolare, l'assunzione di iniziative idonee a valorizzare la crittografia come strumento di

cybersicurezza (anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui sopra), l'adozione di ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali, la qualificazione dei servizi cloud per la pubblica amministrazione, la promozione, nell'ambito delle funzioni di raccordo con le altre amministrazioni competenti in materia di cybersicurezza, di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché di studi di fattibilità ed analisi valutative finalizzati a tale scopo. Rispetto al tema formazione ed al compito dell'Agenzia di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, invece, la legge ha riconosciuto la possibilità, per l'Agenzia stessa, di avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati nonché di predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni.

Si segnala, inoltre, l'istituzione, disposta sempre in sede di conversione, di un **Comitato tecnico-scientifico,** presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri (per la cui partecipazione è espressamente esclusa la corresponsione di gettoni di presenza, compensi o rimborsi di spese), la cui composizione ed organizzazione è rimessa al regolamento di cui si dirà *infra.*

La legge attribuisce all'Agenzia personalità giuridica di diritto pubblico e le riconosce autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. La stessa legge fissa poi alcuni elementi organizzativi dell'Agenzia, disponendo che l'organizzazione e il funzionamento della medesima siano definiti da un apposito regolamento (da adottare, con DPCM, entro 120 gg. dall'entrata in vigore della legge di conversione del decreto stesso previo parere delle

Commissioni parlamentari competenti) che ne preveda, in particolare, l'articolazione fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse disponibili e fissando in 4 anni (rinnovabili per altri 4 anni una sola volta) la durata degli incarichi del direttore generale e del vice direttore generale. La disciplina in esame dispone, inoltre, che con DPCM (su proposta del direttore generale) da adottarsi entro 120 gg. dall'entrata in vigore della legge di conversione dello stesso, sia previsto il regolamento sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia mentre con ulteriore regolamento, da adottare sempre nello stesso termine, previo parere delle Commissioni parlamentari competenti, sia dettata la disciplina del contingente di personale addetto all'Agenzia che in sede di prima applicazione viene individuato in 300 unità (fatta salva la possibilità con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, di rideterminare la dotazione organica nei limiti delle risorse finanziarie destinate alle spese per il personale).

Se l'Acn sarà dunque la principale autorità preposta a livello nazionale ed internazionale alla salvaguardia della cybersicurezza, la nuova disciplina, nel ripensare il quadro delle competenze in materia, all'art. 4 istituisce il **Comitato interministeriale per la cybersicurezza (CIC)**, attivo presso la Presidenza del Consiglio con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Il Comitato, in particolare, è chiamato a proporre al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale, esercitare l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza, promuovere 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 e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza ed infine esprimere il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza. nazionale.

Presso l'Agenzia è poi costituito il **Nucleo per la cybersicurezza**, a supporto del Presidente del Consiglio, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento, presieduto dal direttore della stessa Acn e composto dal consigliere militare del premier, da un rappresentante, rispettivamente, del Dis, dell'Aise, dell'Aisi e di ciascuno dei ministeri rappresentati nel comitato interministeriale per la sicurezza della repubblica (Cisr) oltre che da un rappresentante del ministero dell'Università, il ministro delegato per l'innovazione tecnologica e la transizione digitale e un rappresentante del dipartimento della protezione civile di Palazzo Chigi - che, nelle situazioni di crisi, assicura supporto al premier e al CISR. Il Nucleo, in particolare, può formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia, 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, in raccordo con le pianificazioni di difesa civile e di protezione civile, promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese, valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi, riceve, per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi e valuta se gli eventi assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale.

Ebbene, in attuazione di quanto previsto dalla normativa primaria e nel rispetto della roadmap dalla stessa tracciata, il 4 novembre scorso è stato presentato alle Camere, per il rilascio dei rispettivi pareri (previsto entro il 10 dicembre 2021), lo **Schema di decreto del Presidente del Consiglio dei ministri recante regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale.** Si tratta di uno schema composto da 18 articoli che, a livello di impostazione generale, come espressamente riconosciuto nella relazione illustrativa, segue il

modello della Banca d'Italia e, dunque, linee operative e gestionali tese al risultato e la valorizzazione dei seguenti principi: autonomia e responsabilizzazione, efficienza e razionale impiego delle risorse disponibili, ottimale valorizzazione del capitale umano, contrasto delle situazioni di conflitto d'interesse, dei fenomeni di corruzione e infiltrazione della criminalità organizzata, flessibilità e innovazione tecnologica a supporto dei processi gestionali, semplificazione dei processi di lavoro ed essenzialità dei percorsi amministrativi, sviluppo dei sistemi informativi a supporto delle decisioni e pieno utilizzo delle potenzialità delle tecnologie digitali. Dopo aver disciplinato gli organi dell'agenzia – il Direttore Generale, il Vicedirettore Generale e il Collegio dei revisori dei conti –, il regolamento istituisce **7 Servizi**[19] (all'interno dei quali operano specifiche Divisioni, nel numero massimo di 30) direttamente correlati alle funzioni e alle politiche generali dell'Agenzia che sono posti alle dipendenze del Direttore generale ed operano sulla base degli indirizzi dallo stesso forniti.
La dotazione organica dell'agenzia, in sede di prima applicazione, è stabilita in un massimo di 300 unità.

L'art. 8 si occupa dell'**Organismo Indipendente di Valutazione** (OIV) rimettendo al provvedimento di nomina del Direttore generale la scelta sulla composizione monocratica o collegiate dello stesso. Le decisioni strategiche, nonché quelle relative alla struttura ed al funzionamento dell'agenzia, sono affidate al Comitato di Vertice, presieduto dal Presidente del Consiglio dei ministri o dall'Autorità delegata, ove istituita e composto dai vertici dell'Agenzia, ossia il Direttore generale e il Vice Direttore generale.

A garanzia dell'unitarietà di azione e dell'allineamento informativo tra i Servizi in merito agli indirizzi e le decisioni strategiche concernenti l'organizzazione, il funzionamento e le attività dell'Agenzia, è istituito un **Comitato di coordinamento e programmazione** costituito dal Direttore generale, dal Vice Direttore generale e dai Capi dei Servizi o da loro delegati.

[19] Gabinetto, Autorità e sanzioni, Certificazione e vigilanza, Operazioni, Programmi industriali, tecnologici, di ricerca e formazione, Risorse umane e strumentali e Strategie e cooperazione.

Per lo svolgimento delle funzioni di raccordo e collaborazione con università, istituti di ricerca, strutture private anche di altri Paesi, progetti dell'Unione europea, il regolamento ha previsto l'istituzione del **Comitato tecnicoscientifico (CTS)** i cui componenti devono possedere indiscussa competenza, a livello nazionale e internazionale, negli ambiti di attività dell'Agenzia, in particolare nel contesto della definizione e dell'attuazione di progetti di ricerca e sviluppo tecnologico, industriale e scientifico, della formazione e qualificazione delle risorse umane, della promozione e diffusione della cultura della cibersicurezza, nonché riscontrabili requisiti di onorabilità. È esclusa la percezione di qualsiasi compenso durante il periodo di carica di 2 anni (con possibilità di rinnovo per un ulteriore anno).

Lo stesso regolamento prevede l'adozione di un codice etico dell'Agenzia, con provvedimento del Direttore generale, che individui i principi guida del comportamento dei dipendenti di ruolo e di tutti coloro che operino, a qualsiasi titolo, presso l'Agenzia e l'istituzione di un garante del codice etico che vigili sull'osservanza del codice.

Parimenti al vaglio delle Camere per il rilascio dei rispettivi pareri è lo schema di **regolamento del personale dell'Agenzia** che definisce l'ordinamento e il reclutamento del personale e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale dell'Agenzia un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia.

Mentre sono in fase di adozione i regolamenti organizzativi dell'Agenzia, con **DPCM del 16 settembre 2021 pubblicato sulla G.U. del 30 ottobre 2021**, sono stati definiti i termini e delle modalità del trasferimento di funzioni, beni strumentali e documentazione dal Dipartimento delle informazioni per la sicurezza all'Agenzia per la cybersicurezza nazionale. Il provvedimento, in particolare, individua i termini e le modalità per assicurare, mediante opportune intese, la prima operatività dell'Agenzia attraverso l'individuazione di appositi spazi, in via transitoria e per un periodo massimo di ventiquattro mesi, e, nel rispetto delle specifiche norme riguardanti l'organizzazione e il funzionamento del Dis, per il trasferimento delle funzioni, dei beni strumentali e della documentazione, anche classificata, per l'attuazione delle disposizioni del decreto-legge e la corrispondente riduzione di risorse finanziarie ed umane da parte del Dis.

Il passaggio di consegne è improntato a gradualità: il decreto, infatti, prevede che il Dis debba assicurare "con intesa, la prosecuzione, non oltre il 31 marzo 2022, dell'erogazione dei servizi informatici necessari alla prima operatività dell'Agenzia, tra cui quelli per garantire la continuità del servizio del Csirt Italia e del perimetro di sicurezza nazionale cibernetica, assicurandone la fruibilità dalla sede dell'Agenzia".

Conclusioni

La sicurezza delle comunicazioni elettroniche è ora più che mai tema di grande attualità e interesse tanto tra stakeholder e operatore del settore, quanto tra policy maker e regolatori a livello nazionale ed internazionale. La trasformazione digitale, che ha subito un'ulteriore improvvisa accelerazione a seguito della pandemia, è un fenomeno che sta generando un impatto dirompente sia sulle abitudini dei cittadini, che sempre più riconoscono nella rete la sede privilegiata dove trasferire la maggior parte delle attività tradizionalmente compiute offline, sia per le organizzazioni, le quali trovano nel canale digitale nuovo slancio e continue opportunità di sviluppo.

Il mutato contesto socioeconomico, unito alle innumerevoli esternalità positive in termini di efficienza, ha tuttavia portato anche alla crescita di nuove minacce come il cyber-crime. Sebbene ci sia una diffusa opinione per la quale il recente aumento nel numero di atti illeciti, in particolare in Europa, sia dovuto principalmente ad una maggiore disponibilità a denunciare il fenomeno da parte dei soggetti coinvolti, l'imponente incremento in termini di danni economici causati da essi colloca il tema della cybersecurity al centro del dibattito sia dal punto di vista economico sia da quello regolatorio. L'utilizzo di Internet e dei dispositivi connessi offre infatti nuove opportunità a persone, aziende e istituzioni ma, allo stesso tempo, soprattutto nelle fasi iniziali di tali processi, apre la porta a nuovi rischi. La vastità ed il continuo allargamento del perimetro delle attività comprese nell'ambito digitale, se non adeguatamente tutelate, possono infatti costituire terreno fertile per azioni criminali capaci di provocare danni per diversi milioni di euro non solo ai grandi player del settore e alle organizzazioni pubbliche e private, ma anche alle PMI, che ad oggi risultano poco preparate a contrastare tali fenomeni, e quindi di riflesso anche ai consumatori finali. Sul punto, rispetto al nostro sistema fondato prevalentemente su piccole e medie imprese, non può essere

sottovalutata la netta correlazione esistente tra numero di azioni criminali subite ed entità degli investimenti compiuti in sicurezza informatica.

Insieme alla necessità di una più diffusa alfabetizzazione digitale non solo di impiegati nel settore ma anche dei cittadini che spesso rappresentano l'anello debole ed il canale di accesso per gli attacchi informatici, è molto avvertita, a livello generale, l'esigenza di perseguire un **approccio internazionale** nell'affrontare temi relativi alla gestione dei dati e alla sicurezza degli stessi al fine di pervenire ad una **standardizzazione europea che assicuri procedimenti replicabili in tutta l'UE**. In questo contesto, grande attenzione a livello nazionale ed internazionale è data all'utilizzo di **sistemi di valutazione che garantiscano livelli adeguati di sicurezza delle reti**. Se fino a qualche tempo fa le certificazioni erano considerate in qualche modo un plus, nell'ultimo periodo sempre più istituzioni, sia a livello europeo che nazionale, stanno convergendo verso la promozione (vedi Enisa) o la richiesta obbligatoria (Stati nazionali) di qualche forma di **certificazione**.

Sebbene gli schemi più diffusi, in particolare i **Common Criteria**, garantiscono standard ampiamente riconosciuti come strumenti validi nel mercato, la **complessità delle procedure e le relative tempistiche di implementazione** rendono necessario trovare un equilibrio tra i requisiti di sicurezza e gli effetti che le regolamentazioni e i controlli determinano sul mercato. Ad esempio, schemi di certificazione promossi direttamente dagli operatori di mercato - come il **Nesas** - hanno il vantaggio di semplificare notevolmente le procedure di accreditamento e tempi di valutazione (che si riducono da 12-18 mesi necessari con i CC a soli 3-6 mesi), diminuiscono notevolmente i costi e sono capaci di soddisfare le esigenze di sviluppo delle nuove tecnologie digitali.

Rispetto al **tema dei costi**, in particolare, si osserva come alcuni degli stessi enti che erogano le certificazioni abbiano manifestato la necessità di rendere il modello maggiormente sostenibile, e quindi più snello, veloce e fruibile poiché, allo stato attuale, il numero di certificazioni che devono essere effettuate rischia di generare un aumento dei costi non proporzionato nemmeno per il "modello di business" degli erogatori, a fronte di un numero di risorse che necessariamente non può espandersi all'infinito.

In questo senso è ormai opinione condivisa la necessità di **aumentare il livello di interoperabilità, semplicità ed efficacia**, così da migliorarne l'efficienza e l'applicabilità. Nelle discussioni intorno allo sviluppo di nuove e più efficaci forme di certificazione risulta pertanto fondamentale tenere conto di tali elementi, evitando di creare sovrapposizioni con gli standard già in uso in modo da eludere inefficienza, maggiori spese, e mancanza di fiducia da parte del tessuto imprenditoriale. In questa direzione sembra essere diretta anche l'attività dell'UE e delle agenzie comunitarie, quali l'ENISA, che, attraverso normative nazionali e condivise, puntano a sviluppare un ecosistema sicuro che al contempo non limiti le opportunità di crescita e di sviluppo del settore. Appare quindi opportuna **l'implementazione di standard di valutazione e certificazione della sicurezza unificati**, in cui vengano rafforzati sia il ruolo dell'UE, sia quello delle autorità nazionali, creando le condizioni affinché la valutazione dei fornitori venga effettuata tramite criteri oggettivi, secondo principi coerenti e misurabili, così da generare un ambiente sufficientemente competitivo, equo e affidabile, tale da garantire la diffusione delle migliori tecnologie, con i relativi benefici economici e sociali.

Un indirizzo di respiro europeo è da tenere in considerazione **anche in Italia,** sia per l'importanza di implementare una certificazione che sia in qualche modo convergente – anche nell'ottica di rendere le certificazioni rilasciate nel nostro Paese valide anche negli altri Stati membri della UE - sia in merito agli **specifici strumenti** da far convergere nell'iniziativa di certificazione. A tale riguardo, rispetto al modello nazionale che vede coesistere la disciplina sul golden power ed il perimetro di sicurezza nazionale cibernetica, è indispensabile che nella costruzione di nuovi strumenti di certificazione siano chiariti i confini tra le due discipline e sia garantita la standardizzazione nei test e nelle analisi del rischio, al fine di scongiurare il rischio che si crei confusione procedurale e disomogeneità.

Un ulteriore elemento largamente considerato come determinante riguarda **le tempistiche di tali processi di certificazione, anche per ciò che concerne gli aggiornamenti**. Per favorire efficienza e apertura di mercato è infatti necessario garantire tempi rapidi in modo da consentire lo sviluppo di servizi adeguati e sicuri per gli utilizzatori finali, così come uscire dal circolo vizioso per il quale un aggiornamento determinerebbe la necessità di ripetere il processo per intero. È difatti diffuso tra gli operatori del settore il timore che si determini un sistema in cui tali procedure di certificazione

vengano ripetute analogamente più volte, determinando inevitabilmente danni in termini di *time-to-market* e di blocco dell'innovazione senza alcuna produzione di valore aggiunto. In questo senso il **concetto di *patching continuo*** può risultare fondamentale, anche per garantire un aggiornamento continuo di tali sistemi di sicurezza e per colmare lacune e vulnerabilità, piuttosto che soffermarsi sul rigido bisogno di attraversare nuovamente il processo di certificazione ad ogni cambio di configurazione del prodotto.

La garanzia di processi di sicurezza efficaci e il più possibile standardizzati deve inoltre essere accompagnata con finanziamenti strutturali, nonché da un intervento mirato a favorire una maggiore consapevolezza diffusa su questi temi. È noto, a tale riguardo, che il nostro Paese registra una mancanza di insegnamenti specifici nella maggior parte degli atenei italiani che si traduce in una carenza di professionisti per le industrie stesse e che è necessario un **ripensamento complessivo della formazione**, non solo di livello universitario. L'obiettivo di un ecosistema sicuro non può infatti prescindere da un intervento che punti a colmare il ritardo italiano relativo, in particolare, ad una insufficiente preparazione di capitale umano in questi temi di frontiera. A tal proposito, il PNRR si configura come un'occasione irripetibile per favorire un consistente intervento finalizzato a **rilanciare gli ITS** e ad **ammodernare l'offerta formativa degli atenei italiani** su questi temi.