icom
istituto per la competitività

RAPPORTO OSSERVATORIO
SULLA CIBERSICUREZZA

L'ECOSISTEMA ITALIANO DELLA SICUREZZA INFORMATICA TRA REGOLAZIONE, COMPETITIVITÀ E CONSAPEVOLEZZA

FEBBRAIO 2023

icom
istituto per la competitività

RAPPORTO OSSERVATORIO
SULLA CIBERSICUREZZA

L'ECOSISTEMA ITALIANO DELLA SICUREZZA INFORMATICA TRA REGOLAZIONE, COMPETITIVITÀ E CONSAPEVOLEZZA

FEBBRAIO 2023

CURATORI
Silvia Compagnucci
Stefano da Empoli
Lorenzo Principali

AUTORI
Silvia Compagnucci
Thomas Osborn
Lorenzo Principali
Domenico Salerno
Daniela Suarato
Romolo Tokong

Il presente report è aggiornato alla data dell'08 febbraio 2023

I-Com Edizioni

ISBN 9791280680075
Febbraio 2023

INDICE

EXECUTIVE SUMMARY

CAPITOLO 1
Lo stato della cibersicurezza in Europa

La centralità assunta dall'ecosistema digitale nel corso degli ultimi anni ha aperto un mondo di nuove opportunità per le imprese, sia a livello di gestione a distanza dei processi interni, sia per la possibilità di interagire con potenziali consumatori sparsi in ogni parte del globo. Il volume sempre crescente dei flussi monetari che transano attraverso i canali digitali è però direttamente proporzionale all'impegno che gli hacker impiegano nella creazione di software malevoli.

In base agli ultimi dati diffusi dal Clusit, il **numero di attacchi cibernetici gravi** a livello globale nel primo semestre 2021 si è attestato a 1.141, con un aumento del 14,6% rispetto al periodo precedente. La media mensile indica inoltre che le azioni gravi, probabilmente derivanti da gruppi cybercriminali organizzati, sono cresciute costantemente nel corso degli ultimi 5 anni, passando da quota 130 azioni al mese rilevate nel 2018 a 190 al mese registrate nel primo semestre del 2022. A livello geografico l'Europa è la seconda area più colpita (26%) dietro le Americhe (48%), in un contesto emerge anche una quota notevole di azioni ostili attuate su larga scala e quindi non riconducibili ad un singolo continente (26%). Analogamente, dall'analisi delle vittime di attacchi informatici classificate per settore d'appartenenza si osserva come, nel 2022, la maggioranza degli eventi censiti non abbia avuto un singolo destinatario, bensì target multipli. Analizzando invece i singoli comparti si osserva come quello maggiormente colpito sia il settore sanitario, con 252 azioni ostili subite, seguito da Governo e difesa (135) e ICT (126).

I software utilizzati dai cybercriminali per attaccare i sistemi informatici delle proprie vittime sono definiti **"Malware"**, ovvero applicativi creati appositamente per penetrare le difese informatiche e danneggiare i device, agendo contro l'interesse degli utenti. Una delle tipologie di malware più diffuse di recente è il **ransomware** (tecnicamente "software per il riscatto"), ovvero un particolare tipo di software malevolo che, una volta penetrato in una rete, cripta le informazioni contenute al suo interno richiedendo alla vittima di pagare un riscatto per avere nuovamente accesso ai propri dati. Secondo Sophos, il 66% delle aziende intervistate a livello globale – tutte imprese con oltre 100 dipendenti – ha subìto un attacco ransomware nel 2021, una percentuale quasi doppia rispetto a quella registrata nel 2020, che si attestava sul 37%. In ben il 65% dei casi l'attacco ricevuto è riuscito a penetrare le difese informatiche aziendali e a criptarne i dati. Inoltre, il 46% dei soggetti che si sono trovati in questa situazione è stato costretto a pagare il riscatto per rientrarne in possesso, con un **esborso medio** che si è attestato intorno a quota $812 mila. In generale, dalle interviste raccolte è emerso che l'impatto economico medio derivante da un attacco ransomware a livello globale nel 2021 si è attestato a quota $1,4 milioni.

Tali attacchi generano sulle aziende che li subiscono un notevole impatto negativo sia dal punto di vista economico, sia per quanto concerne la perdita di fiducia da parte degli utenti. Un'organizzazione che non appare in grado di tutelare i dati personali della propria utenza, in particolare se si tratta di informazioni sensibili, rischia di trovare molte difficoltà nel tentativo di riabilitare completamente la propria immagine.

A livello europeo, secondo i dati ENISA, tra le organizzazioni di grandi dimensioni censite (Operatori di servizi essenziali e Digital Service Providers), quelle che subiscono i danni più rilevanti sono le **banche**, con una perdita media che si attesta a quota €475 mila, seguite del comparto **energia** (€462 mila) e da quello dei **trasporti** (€450 mila).

Dai dati sopracitati risulta 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.

Il quadro normativo europeo. Dalla strategia sulla cybersecurity alla NIS 2 e al Cyber Resilience Act

Alla crescente digitalizzazione dei processi e dei servizi e, conseguentemente, all'aggravarsi dei rischi legati alla cibersicurezza, si è accompagnata un sempre maggiore impegno delle istituzioni europee nella creazione di un ecosistema normativo quanto più possibile in grado di assicurare elevati standard di sicurezza. Se nel 2016 è stata adottata la **direttiva NIS (direttiva n. 1148/2016)** con la quale sono state adottate per la prima volta misure organiche nel settore della cibersicurezza, nel 2019 è stato varato il **Reg. n. 881/2019** che ha conferito mandato permanente all'Agenzia dell'UE per la sicurezza informatica (ENISA), attribuendole nuovi compiti ed un ruolo centrale nella creazione e nel mantenimento del quadro europeo di certificazione della cibersicurezza. Il 2020 rappresenta un anno particolarmente importante per le politiche sulla cybersecurity che ha visto il lancio, da parte della Commissione europea, del **"Cybersecurity package"**, costituito dalla **"Strategia dell'UE in materia di cibersicurezza per il decennio digitale"**, una nuova proposta di direttiva sulla resilienza delle entità critiche ed una proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista).

La strategia ha declinato proposte concrete di iniziative politiche, di regolamentazione e di investimento attraverso cui perseguire resilienza, sovranità tecnologica e leadership, favorire lo sviluppo di capacità operative di prevenzione, dissuasione e risposta e la promozione di un ciberspazio globale ed aperto.

In attuazione della strategia descritta nel paragrafo precedente, il 20 maggio 2021 è stato adottato il **Regolamento n. 887/2021** che istituisce, per il periodo compreso fra il 28 giugno 2021 e il 31 dicembre 2029 (salvo proroghe), il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento con sede a Bucarest definendone composizione, compiti ed obiettivi.

Il 27 dicembre 2022 è stata pubblicata sulla Gazzetta Ufficiale dell'UE la **Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (Direttiva CER – Resilience of Critical Entities)** che mira ad aumentare la resilienza di soggetti, negli Stati membri, che sono fondamentali per la fornitura di servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno, in una serie di settori che sono alla base del funzionamento di molti altri settori dell'economia dell'Unione. Tale direttiva, in particolare, detta norme armonizzate volte a garantire la fornitura di servizi essenziali nel mercato interno, accrescere la resilienza dei soggetti critici e migliorare la cooperazione transfrontaliera tra le autorità competenti.

Dopo una lunga procedura ed un ampio dibattito, nella medesima data – 27 dicembre 2022 – è stata pubblicata la **Direttiva n. 2555/2022 (NIS 2)**, che è entrata in vigore lo scorso 17 gennaio 2023 e che dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024. Tale direttiva, al fine di superare l'attuale frammentazione normativa e fornire risposte efficaci alle nuove sfide di cibersicurezza poste dalla crescente digitalizzazione, pur confermando gran parte degli obiettivi e degli strumenti della direttiva NIS, ha ampliato la platea di soggetti destinatari della normativa dalla stessa fissata, ha introdotto limiti dimensionali e la distinzione tra soggetti importanti ed essenziali, ha rafforzato gli obblighi sui soggetti destinatari della di-

sciplina aderendo ad un approccio basato sul concetto del c.d. "multirischio", ha potenziato gli strumenti di cooperazione, ha previsto rilevanti misure di vigilanza ed esecuzione e prescritto importanti sanzioni.
Da ultimo, il 15 settembre scorso la Commissione Europea ha pubblicato una **proposta di regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (Cyber Resilience Act- CRA)** che mira a salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o software con una componente digitale attraverso la fissazione di regole armonizzate per l'immissione sul mercato di prodotti o software con una componente digitale, l'individuazione di requisiti di cybersecurity che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, la fissazione di obblighi per ogni fase della catena del valore e la declinazione di un obbligo generale di diligenza per l'intero ciclo di vita di tali prodotti. In Parlamento europeo tale proposta è stata assegnata alla commissione ITRE (rapporteur Nicola Danti). Il Consiglio, invece, nella relazione presentata il 6 dicembre scorso, ha espresso un apprezzamento generale per la proposta della Commissione, ma al contempo ha formulato una richiesta di chiarimento in merito all'applicabilità della disciplina al software as a service, ha proposto di escludere dall'ambito di applicazione della proposta i prodotti destinati esclusivamente a scopi militari ed ha rilevato l'importanza di valutare l'onere della proposta per l'industria, in particolare per le PMI e di approfondire il ruolo dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), oltre a chiarire, a livello generale, le interazioni con altri atti legislativi in materia.
Problematiche specifiche ed azioni specifiche sono state messe in campo rispetto alla sicurezza delle reti 5G. In particolare, il 26 marzo 2019, la Commissione europea ha adottato la **Raccomandazione n. 2019/534 sulla cybersecurity delle reti 5G** con la quale ha evidenziato i rischi di cybersecurity rispetto a tali reti e presentato orientamenti sulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi. Il successivo 9 ottobre 2019 è stata pubblicata dal gruppo di cooperazione NIS, composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA, una relazione sulla valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti di quinta generazione. Il 29 gennaio 2020 è stata invece pubblicata dalla Commissione la **Comunicazione "Dispiegamento del 5G sicuro – Attuazione del pacchetto di strumenti dell'UE" ed il pacchetto di strumenti dell'UE (Toolbox sul 5G)** comprendente misure di attenuazione dei rischi, che tratta tutti i rischi individuati nella relazione coordinata sulla valutazione dei rischi individuando e descrivendo una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia, che possono essere attuate per attenuare i rischi individuati. Da ultimo, l'11 maggio 2022 gli Stati membri dell'UE, con il sostegno della Commissione europea e dell'ENISA, hanno pubblicato una **relazione sulla cibersicurezza di Open RAN**, un nuovo tipo di architettura di rete 5G che, nei prossimi anni, fornirà modalità alternative di realizzazione della parte di accesso radio delle reti 5G basata su interfacce aperte e che evidentemente pone questioni specifiche in termini di sicurezza.

CAPITOLO 2
Lo stato della cibersicurezza in Italia

Il Paese risulta uno dei più bersagliati dai criminali informatici, presentando una quota del 3,26% dei dispositivi mobili e del 10,74% dei pc fissi che sono stati infettati da malware. Questo dato è notevolmente superiore a quello fatto registrare da altre grandi economie europee come Germania, che presenta un

1,63% di infezioni sul mobile e 4,94% da PC, e Francia, 2,56% mobile e 6,71% PC.

L'ultima **"Relazione sulla politica dell'informazione per la sicurezza"** restituisce una fotografia di quali siano le **Pubbliche Amministrazioni** e i **settori industriali** più colpiti. Per quanto concerne le prime, si osserva come queste nel 2021 siano risultate l'obiettivo privilegiato dei cybercriminali, attirando il 69% delle azioni ostili accertate in Italia: un dato che, seppure in calo, rende l'idea dell'importanza di innalzare le difese cibernetiche delle amministrazioni pubbliche. **Gli enti più bersagliati risultano le amministrazioni statali**, divenute il target di più della metà degli attacchi individuati (56%), precedendo gli enti locali (20%). Inoltre, è proseguito anche nel 2021 il preoccupante trend riguardante le azioni malevole dirette a strutture sanitarie pubbliche, passate dal 4% al 10%, cresciute quindi di 6 p.p. dopo una crescita del 3% già registrata nel periodo di osservazione precedente, coincidente con lo scoppio della pandemia di Covid-19.

Riguardo al **settore privato**, i soggetti che hanno subìto il maggior numero di azioni ostili sono quelli del comparto energetico, la cui quota è passata dal 2% del 2020 al 24% del 2021, seguiti dalle TLC che si sono attestate sul 12% (+10 p.p.). A crescere sono anche gli attacchi sferrati verso le organizzazioni appartenenti al settore dei trasporti (+8 p.p.) e al farmaceutico/sanitario (+2 p.p.). Tendenza opposta è invece quella fatta registrare dalle infrastrutture digitali/servizi IT e dal bancario, che passano entrambi dall'11% al 6%.

La situazione appena descritta appare ancor più allarmante se si considera che, secondo gli ultimi dati diffusi da ENISA, le organizzazioni italiane – e in particolare OSE/DSP – appaiono solo al 19° posto nella UE per **quota del budget IT investita in sicurezza dell'informazione**. Infatti, se da un lato le aziende italiane risultano terze per volume di spesa in valore assoluto (€4 milioni), in termini percentuali queste investono solo il 6,6% del proprio budget IT in sicurezza, contro una media UE del 7,2%.

D'altro canto, le ultime previsioni di mercato diffuse da Statista indicano un **notevole aumento dei ricavi del comparto della sicurezza informatica in Italia nei prossimi anni**. Nel dettaglio, dopo un incremento del 7% tra il 2021 e il 2022, i ricavi del settore cybersecurity dovrebbero aumentare di un ulteriore 25% entro i prossimi tre anni, passando dagli €1,75 miliardi del 2022 ai €2,18 miliardi previsti per il 2026.

L'istituzione dell'ACN e la strategia nazionale di cybersicurezza

Il **Piano nazionale di ripresa e resilienza (PNRR)** ha individuato la sicurezza cibernetica come uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione ed ha previsto l'individuazione di un nuovo organismo per la sicurezza informatica nazionale per guidare l'architettura nazionale generale della cybersicurezza. In attuazione di tali previsioni, il 14 giugno 2021 è stato pubblicato il **D.L. n. 82/2021 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" (convertito con la legge 4 agosto 2021, n. 109)** che ha sancito l'inizio di una nuova era per la cybersicurezza a livello nazionale. L'Agenzia in particolare rappresenta l'Autorità nazionale in materia di cybersecurity, chiamata a predisporre la strategia nazionale di cybersicurezza, ad assicurare il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale, promuovere 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, operare come Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi e come Autorità nazionale di certificazione della cybersicurezza, accreditare le strutture specializzate del Ministero della

difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, assumere 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 di cui si dirà nei paragrafi successivi, 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), acquisire 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 svolgere 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.

Nell'esercizio delle proprie funzioni, il 27 maggio scorso l'ACN ha presentato la **strategia nazionale di cybersicurezza 2022-2026** ed il relativo piano di implementazione con cui si mira ad assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione e del tessuto produttivo, al fine di assicurare servizi sicuri ed incentivarne l'utilizzo da parte dei cittadini, anticipare l'evoluzione della minaccia cyber, contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida, gestire le crisi cibernetiche e perseguire l'autonomia strategica nazionale ed europea nel settore del digitale. Se queste sono le sfide, con riferimento, invece, agli obiettivi, la strategia ne individua tre, protezione, risposta e sviluppo, per ciascuno dei quali declina una serie di misure – complessivamente 82 – con relativi attori responsabili, prevedendo inoltre la definizione di metriche e di Key Performance Indicator (KPI), quali strumenti che consentano di misurarne l'effettiva attuazione ed efficacia.

L'evoluzione della disciplina sul Golden Power. Gli ambiti di intervento e le semplificazioni introdotte

La **disciplina Golden Power** trova origine e fondamento nel **D.L. 15 marzo 2012, n. 21** (convertito, con modificazioni, in **legge 11 maggio 2012, n. 56**) che negli anni ha subito numerosissime modifiche ed integrazioni anche su spinta europea. Ed infatti, il **D.L. 25 marzo 2019**, n. 22 (convertito, con modificazioni, dalla **legge n. 41 del 20 maggio 2019**), ha introdotto, nel D.L. n. 21 del 2012, l'articolo 1-bis, che disciplina l'esercizio dei poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G, mentre il **D.L. 21 settembre 2019, n. 105** (convertito, con modificazioni, dalla legge n. 133 del 18 novembre 2019) ha esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori strategici, coordinandolo con l'attuazione del Regolamento 2019/452 in materia di controllo degli investimenti esteri diretti nell'Unione europea. Da ultimo, il **D.L. n. 21/2022** (convertito con **legge 20 maggio 2022, n. 51**), recante "Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina", nel Titolo IV ha dedicato il Capo I al Golden Power, introducendo una serie di importantissime novità che di fatto hanno ridisegnato la disciplina sui poteri speciali. Gli ambiti di intervento del Golden Power sono difesa e sicurezza nazionale, tecnologia 5G, energia, trasporti, comunicazioni e nuovi settori di cui al Reg. 2019/452. In tali ambiti, al Governo è consentito imporre condizioni e prescrizioni finanche esercitare il potere di veto. Rispetto alla tecnologia 5G, in particolare, la disciplina vigente ha superato il riferimento al singolo contratto in favore di una pianificazione annuale che deve contenere una serie di informazioni modificabili con cadenza quadrimestrale.

In attuazione dell'art. 2-quater "Misure di semplificazione dei procedimenti e prenotifica", con **DPCM 1° agosto 2022, n. 133**, pubblicato sulla G.U. del 9 set-

tembre ed entrato in vigore il successivo 24 settembre scorso, è stato adottato il **Regolamento recante disciplina delle attività di coordinamento della Presidenza del Consiglio dei ministri propedeutiche all'esercizio dei poteri speciali** che ha introdotto una serie di importanti novità tra cui la prenotifica e la possibilità per il Gruppo di Coordinamento, al ricorrere di determinate condizioni, di adottare decisioni di non esercizio dei poteri speciali autonomamente senza la necessaria convocazione e delibera del Consiglio dei Ministri.

Da ultimo, nella logica di valutare l'impatto dell'esercizio dei poteri speciali ed apprestare interventi compensativi a sostegno delle imprese destinatarie delle relative misure, con **D.L. 5 dicembre 2022, n. 187**, recante misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici, convertito con **legge 1° febbraio 2023, n. 10**, si è tornati ad occuparsi del Golden Power prevedendo, all'art. 2, "Misure economiche connesse all'esercizio del golden power".

Dal completamento all'implementazione della disciplina sul perimetro di sicurezza cibernetica

Il decreto legge n. 105/2019, convertito con la legge n. 133/2019, ha 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 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. Per raggiungere tale obiettivo, la disciplina istitutiva del perimetro 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 e che, seppur in ritardo, è finalmente giunto a completamento con l'adozione del DPCM 18 maggio 2022, n. 92 (pubblicato sulla G.U. del 15 luglio 2022) con il quale è stato adottato il regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra il CVCN, i laboratori di prova accreditati ed i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa.

Con **provvedimento dell'11 agosto 2022** l'ACN ha approvato le **determinazioni tecniche previste dal Regolamento in materia di accreditamento dei laboratori di prova**, fissando per le varie aree di accreditamento, i requisiti tecnici e logistici, le misure di sicurezza informatica per i LAP, i requisiti di competenza ed esperienza, le modalità di notifica delle limitazioni di operatività superiori a 24 ore e di comunicazione e raccordo tra il CVCN e i LAP.

Nella logica di favorire la compliance a tale complessa disciplina, la stessa ACN ha elaborato un documento che raccoglie i riscontri ai quesiti emersi con maggiore frequenza nelle interlocuzioni con i soggetti e fornisce informazioni di carattere generale attinenti alle finalità e all'ambito di operatività del Perimetro, agli adempimenti e ai termini da rispettare, nonché alle modalità di comunicazione con l'Agenzia.

Esercizio dei poteri speciali e il perimetro di sicurezza cibernetica

I dati pubblicati nella **relazione sull'attività del Governo svolta sulla base dei poteri speciali** confermano la tendenza incrementale delle notifiche ai sensi del decreto-legge 21/2012. Nel 2021, in particolare, il numero totale di informative presentate è stato pari a 496, in aumento di circa il 45% rispetto all'anno precedente. Il trend è crescente per tutti i settori previsti dal decreto-legge n. 21 del 2012: difesa e sicurezza nazionale (articolo 1), tecnologia 5G (articolo 1-bis) ed energia, trasporti, comunicazioni e nuovi settori del Regolamento (UE) 2019/452 (articolo 2).

Per quanto riguarda il comparto difesa e sicurezza nazionale, nel 2021 le notifiche pervenute sono state 51, in crescita di circa il 38% rispetto all'anno precedente,

rappresentando il 10,3% del totale delle notifiche avvenute nell'anno solare. Sul versante della tecnologia 5G, le notifiche ai sensi dell'articolo 1-bis hanno iniziato ad essere presentate a partire dal 2019. Nel 2021, il loro numero è risultato pari a 20, in aumento di una sola unità rispetto all'anno precedente, rappresentando circa il 4% del totale. Infine, rispetto alle altre macrocategorie, si è evidenziato un incremento significativamente maggiore delle notifiche pervenute ai sensi dell'articolo 2 (energia, trasporti e comunicazioni), dovuto principalmente all'ampliamento di tale categoria, la quale comprende, ora, anche i settori indicati nel Reg. (UE) 2019/452. Nel 2021, le notifiche in tale comparto costituiscono l'85,7% del totale, in crescita di circa il 49% rispetto al 2020 e di oltre il 1000% rispetto al 2019.

Per ogni notifica pervenuta, sulla base del settore merceologico coinvolto, viene individuata un'**amministrazione responsabile dell'istruttoria**. Nel 2021, la maggior parte delle notifiche (188 su 496) è stata assegnata al Ministero dello Sviluppo economico. Si osserva anche un notevole coinvolgimento del Ministero della Salute (116 notifiche), che ai sensi del d.P.C.M. 179/2020 è tra le nuove amministrazioni competenti per l'istruttoria della disciplina Golden Power. Seguono il MEF e il Ministero della Difesa, rispettivamente con 71 e 46 notifiche.

All'esito dell'istruttoria, delle 496 notifiche pervenute nel corso del 2021, per 29 di esse sono stati esercitati i poteri speciali, per 183 notifiche non sono stati esercitati e, infine, 277 non sono state ritenute rientranti nella disciplina Golden Power.

Per quanto concerne la **suddivisione settoriale**, a fronte di un esercizio effettivo dei poteri speciali piuttosto simile (rispettivamente 7 casi per la Difesa e la Sicurezza nazionale, 11 per la Tecnologia 5G e 11 per Energia, Trasporti, Comunicazioni e nuovi settori) i differenti ambiti delle tre aree presentino "confini" piuttosto differenti. Infatti, oltre a mostrare dimensioni diverse in termini complessivi, rispettivamente **51 notifiche per Difesa e Sicurezza, 20 per Tecnologia 5G e ben 425 Energia, Trasporti, Comunicazioni e altri settori**, si osserva come le operazioni notificate ma "escluse" dall'ambito dei poteri speciali siano rispettivamente 16 per il primo comparto, 5 per il secondo e ben 256 per il terzo. Allo stesso modo, infine, si rilevano diversi ordini di grandezza anche per quanto concerne le **procedure semplificate**, utilizzate rispettivamente in 7 casi nell'ambito Difesa e Sicurezza e mai nei casi che ricadono nella tecnologia 5G, a fronte di ben 60 casi per quanto concerne Energia, Trasporti, Comunicazioni e altri settori.

CAPITOLO 3
La cibersicurezza per cittadini e imprese: lo stato dell'arte

Se da un lato la trasformazione digitale ha aperto un nuovo mondo di opportunità per individui e imprese, dall'altro ha fatto sì che anche persone senza alcun rudimento riguardo il funzionamento delle nuove tecnologie si affacciassero ai canali digitali, esponendosi a nuove minacce come il cyber-crime. A tal proposito, secondo il Censis **gran parte della popolazione italiana risulta ancora ampiamente impreparata ad affrontare problematiche di sicurezza informatica**. Analizzando i dati diffusi dall'istituto si osserva come solo il 24,3% degli italiani dichiari di avere una buona conoscenza di cosa si intende per cibersicurezza, laddove il 58,6% risulta averne ha un'idea approssimata ed il restante 17,1% è completamente a digiuno riguardo la sicurezza informatica.

D'altra parte, nonostante pochi italiani siano a conoscenza di cosa sia la sicurezza informatica, più della metà degli stessi si è imbattuto in una o più minacce informatiche nel corso della propria vita.

In particolare, il 64,6% dei cittadini italiani è stato bersaglio del cosiddetto fenomeno del **phishing**, la ricezione di mail ingannevoli volte a truffare i malcapitati inducendoli a rivelare informazioni personali sensibili. Un ulteriore 44,9% della popolazione italia-

na ha avuto un **PC o un laptop infettato da un virus informatico**.

Le problematiche appena descritte generano spesso gravi conseguenze, che possono essere riscontrare nelle dichiarazioni fornite al Censis. Infatti, dai dati dell'istituto emerge come il 17,2% degli intervistati ha scoperto pagamenti di acquisti fatti a proprio nome e a proprio carico e il 14,3% degli stessi si è visto clonare la carta di credito o il bancomat.

La mancanza di consapevolezza riguardo la sicurezza informatica risulta piuttosto diffusa anche presso le imprese. Osservando i dati raccolti dal Censis emerge come solo il 39,7% dei lavoratori ha ricevuto una formazione specifica in materia, percentuale che scende al 23,5% per quanto riguarda operai ed esecutivi. Il problema, anche se meno accentuato, è riscontrabile anche tra chi svolge funzioni amministrative: circa un impiegato su due (47,8%) e il 43,2% dei dirigenti non ha ricevuto una formazione sulla sicurezza cibernetica. Se si considera che gran parte delle azioni malevole subìte dalle imprese sono frutto di errori umani compiuti da soggetti che, inconsapevolmente, offrono un punto d'accesso ai cybercriminali nelle reti aziendali, si comprende quanto sia importante che tutti i dipendenti che si interfacciano con i sistemi informatici aziendali ricevano un adeguata formazione in cibersicurezza.

Secondo gli stessi dati Censis , il 19,5% dei lavoratori ha dichiarato che la propria azienda è stata vittima di un attacco informatico. Inoltre, il 14,7% dei dipendenti ha affermato che, a seguito di un attacco informato subìto, si è verificata una perdita di dati. Nel complesso, i dati sopracitati indicano quanto la mancanza di alfabetizzazione digitale resti ad oggi un problema estremamente diffuso anche nei contesti business. Questa tesi è certificata dal "Rapporto sulla situazione e prospettive delle imprese dopo l'emergenza sanitaria covid-19" pubblicato dall'ISTAT a febbraio 2022, che mostra come la **formazione digitale** risulti un aspetto cruciale solo per il 16% delle aziende residenti nel nostro Paese.

Le best practices nell'ambito della formazione digitale e sulla sicurezza informatica

Per ridurre i rischi derivanti dalle minacce informatiche è necessario operare un profondo lavoro sull'aumento del **livello di consapevolezza degli utenti**, poiché il "fattore umano" gioca spesso un ruolo fondamentale negli incidenti di sicurezza informatica. Rendere gli individui consapevoli dei rischi a cui vanno incontro è quindi l'arma principale per incrementare la sicurezza dell'ecosistema informatico.

Secondo gli ultimi dati diffusi da Eurostat, nell'ultimo decennio la quota di italiani che utilizzano internet ha raggiunto nel 2022 l'86,14% della popolazione. Nonostante ciò, **solo il 59,8% dei cittadini della penisola ha competenze almeno basilari sulla sicurezza informatica**. In generale, osservando la scomposizione demografica per età, si osserva come – ad esclusione dei minori di 16 anni – **la quota di persone a digiuno di cibersicurezza cresce in maniera proporzionale all'età anagrafica**: un italiano su quattro tra i 16 e i 54 anni non ha conoscenze di sicurezza informatica di base, quota che sale ad uno su tre se si considera la fascia di età 55-74 e addirittura a due su tre per gli over 75.

Dai dati appena descritti traspare in modo evidente l'importanza di individuare iniziative che riescano a raggiungere l'intera popolazione del nostro Paese, comunicando messaggi chiari che possano essere pienamente appresi da tutti a prescindere dal livello di alfabetizzazione digitale posseduta. In quest'ottica, nel corso degli ultimi anni numerose organizzazioni sia pubbliche che private si sono impegnate per realizzare attività volte a istruire la popolazione su come rispondere ai pericoli digitali. Tra questi, la più importante è certamente la **Polizia Postale**, attiva in decine di iniziative finalizzate a sensibilizzare la popolazione sui pericoli che si celano sulla rete, sia a livello nazionale, sia in collaborazione con i piccoli e grandi comuni italiani, tra cui spicca l'iniziativa ormai pluriennale "Una Vita da Social".

Oltre alle attività svolte su input delle autorità pubbliche, esistono anche importati campagne nate su spunto privato e della cittadinanza attiva. Uno dei principali esempi di questo tipo è l'**associazione Parole O_Stili** nata a Trieste su iniziativa di 300 tra professionisti della comunicazione d'impresa, della comunicazione politica, influencer e blogger che mira a sensibilizzare verso un utilizzo consapevole e non aggressivo del linguaggio su Internet tramite il proprio Manifesto della Comunicazione non Ostile. Sulla stessa lunghezza d'onda è l'iniziativa denominata "Giovani ambasciatori per la cittadinanza digitale" sviluppata dal **Moige**, associazione composta da genitori, insegnanti, educatori nonché membri della cittadinanza che si impegnano per tutelare la salute dei minori. Queste associazioni svolgono oggi un ruolo importante riuscendo da sole in un'attività molto complessa: avere da un lato il sostegno delle Istituzioni pubbliche sui temi fondamentali e coinvolgere al tempo stesso nelle iniziative anche grandi player privati nazionali ed internazionali che sono in grado di portare mettere in campo le esperienze maturate nel mondo.
A livello internazionale, una delle principali iniziative sulla sicurezza informatica è certamente la "*Mobile Malware Awarness Campaign"* sviluppata dallo **European Cybercrime Centre dell'Europol** per aiutare gli individui a proteggere i propri dispositivi mobili dai criminali informatici.

Le funzioni di impulso di ACN e gli obiettivi della strategia nazionale per accrescere l'awareness
All'ACN sono attribuite importantissime funzioni anche rispetto ad **awareness, formazione e ricerca**. Ed infatti, all'agenzia è attribuito il compito di svolgere attività di comunicazione e promozione della consapevolezza in materia di cibersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia, di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cibersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati (con la possibilità di avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno) e predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile.
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 tecnico-scientifico (CTS)**, riunitosi per la prima volta nel luglio scorso.
Rispetto alla **formazione**, classificata tra i fattori abilitanti insieme a promozione della cultura della sicurezza cibernetica e cooperazione, la strategia nazionale di cibersicurezza, nel perseguire il fine di creare una solida forza lavoro nazionale, composta da esperti e giovani talenti, pone in luce la necessità di favorire l'**accesso degli studenti alle tecnologie informatiche e alle carriere tecnico-scientifich**e (anche attraverso il contributo degli ITS) e di assicurare un'**adeguata formazione del personale docente oltre che dei dipendenti di pubbliche amministrazioni e soggetti privati**. A ciò si aggiunge l'importanza, nella logica più generale di promuovere la cultura della sicurezza informatica, di predisporre un programma capillare di educazione digitale.

CAPITOLO 4
L'offerta formativa in materia cibersicurezza

Il **monitoraggio I-Com delle attività di formazione sulla cibersicurezza in ambito universitario** ha evidenziato un interesse decisamente crescente per queste tematiche da parte del mondo accademico, che **a gennaio 2023** presentava **234 tra corsi e inse-**

gnamenti relativi alla cibersicurezza rispetto ai 79 individuati a gennaio 2022.

Nel dettaglio, l'analisi ha individuato 112 insegnamenti singoli all'interno di corsi di laurea magistrale, 56 insegnamenti singoli in lauree triennali e 13 corsi singoli all'interno di dottorati di ricerca, a fronte di 4 lauree triennali, 22 lauree magistrali, 7 dottorati e 18 master (di primo e di secondo livello) interamente incentrate sulla cybersecurity. Pertanto, il totale delle lauree specifiche (triennali e magistrali) sul tema della cibersicurezza ammonta a 26, ben 13 in più rispetto al 2022. La formazione post-laurea presenta numeri piuttosto simili: tra dottorati e master di primo e secondo livello sono stati conteggiati 25 corsi "specializzati". Nel complesso, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 51 corsi di studio interamente dedicati.

Per quanto riguarda la **distribuzione regionale della complessiva offerta formativa**, questa appare piuttosto disomogenea con una forte concentrazione nel Lazio (45 tra corsi e singoli insegnamenti), Piemonte (32), Campania (25) e Lombardia (21). Tuttavia, se si considerano i **dati normalizzati per il numero di Università presenti sul territorio regionale**, la classifica varia mostrando in prima posizione il Piemonte con 8 corsi per Università, seguito da Liguria (4) e Sicilia (2,8). Le regioni che invece non presentano alcun corso formativo sulla cibersicurezza (anche a causa della scarsa offerta di livello universitario) sono la Basilicata e la Valle d'Aosta. In relazione alla distribuzione regionale della offerta formativa "specializzata" (lauree triennali, magistrali, master e dottorati di ricerca), il Lazio si conferma la regione più interessata con 15 corsi complessivi, catalizzando gran parte dell'offerta sia in termini di lauree dedicate (magistrali e triennali), sia per quanto concerne la specializzazione post-laurea (9 master e 1 dottorato). L'elevato numero di master specifici sui temi della cibersicurezza (18) sembra suggerire una elevata domanda di approfondimento post-laurea su questi temi.

Inoltre, l'analisi mostra che **ben 107 dei 234 corsi rilevati sono in lingua inglese**. L'inglese è lievemente predominante per le lauree magistrali specificamente incentrate sui temi della cybersecurity (12 in inglese, 9 in italiano e 1 ibrida) laddove i master sono quasi interamente in italiano (17 su 18), probabilmente a riprova del maggiore legame col mondo aziendale, mentre i dottorati presentano un profilo più internazionale (5 su 7 in inglese).

In questo contesto, il **ruolo degli Istituti Tecnici Superiori (ITS)** consiste nel fungere da anello di congiunzione tra la realtà scolastica e quella lavorativa, offrendo agli studenti gli strumenti utili a rispondere alle competenze richieste dal mercato del lavoro. Secondo l'ultimo rapporto INDIRE nel 2022 risultavano presenti sul territorio nazionale 120 ITS. A **livello regionale**, la Lombardia si colloca in cima alla classifica con 20 unità, seguita dalla Sicilia con 11 e da Calabria, Campania e Toscana con 9. Parametrando il dato sulla diffusione alla popolazione regionale risulta in testa la Calabria (4,9 ITS ogni milione di abitante), la Liguria (4 ogni milione di abitanti) e l'Abruzzo (3,9 per milione di abitanti). In relazione alle **aree strategiche di indirizzo** prevalgono nettamente le "Nuove tecnologie per il made in Italy" con 49 unità, seguite dalla "Mobilità Sostenibile" (20), "Efficienza energetica" (15), "Tecnologie innovative per i beni e le attività culturali" (14), "Le tecnologie dell'informazione e della comunicazione" (14) e le nuove tecnologie della vita (8). Nonostante i profili lavorativi degli ITS siano configurati selezionando le principali competenze richieste sul mercato, il numero dei ragazzi che sceglie questa tipologia di formazione è notevolmente inferiore rispetto a quello delle altre maggiori economie europee. Secondo dati The European House-Ambrosetti, **nel 2022 il numero di studenti italiani iscritti a scuole di istruzione post-secondaria non terziaria ammonta ad appena 19 mila unità, contro le 740 mila della Germania, le 26 mila della Francia e le 25 mila della Spagna**. Questo può spiegare la criticità a

reperire sul mercato del lavoro italiano competenze adeguate per sopperire alle necessità lavorative. Inoltre, secondo una survey effettuata sempre da The European House-Ambrosetti, le competenze degli studenti che terminano il percorso formativo negli ITS risultano inadeguate per il 74% dei rispondenti, il quale ha sottolineato come sia necessario un maggiore allineamento con le esigenze del settore.

La riforma degli ITS

Uno degli interventi senza dubbio più rilevanti, annunciato nella Missione 4 del PNRR, è senza dubbio la **riforma del sistema ITS, varata con la L. n. 99 del 15 luglio 2022**. Gli ITS, in particolare, diventano **Istituti Tecnologici Superiori – ITS Academy** aperti a giovani e adulti in possesso di un diploma di scuola secondaria di secondo grado o di un diploma quadriennale di istruzione e formazione professionale. L'offerta formativa si concentra su transizione ecologica, compresi i trasporti, la mobilità e la logistica, la transizione digitale, le nuove tecnologie per il made in Italy, compreso l'alto artigianato artistico, le nuove tecnologie della vita, i servizi alle imprese e agli enti senza fine di lucro, le tecnologie per i beni e le attività artistiche e culturali e per il turismo, le tecnologie dell'informazione, della comunicazione e dei dati e l'edilizia, mentre viene rafforzato il legame col mondo delle imprese. Ed infatti, è previsto che l'attività formativa sia svolta per almeno il 60% del monte orario complessivo da docenti provenienti dal mondo del lavoro e che gli stage aziendali e i tirocini formativi, obbligatori almeno per il 35% del monte orario complessivo, possano essere svolti anche all'estero con l'adeguato sostegno di borse di studio. Il mondo delle imprese diventa centrale anche rispetto alle nuove regole per l'avvio di un ITS; infatti, la nuova disciplina subordina la possibilità di avviare un nuovo ITS in una Provincia alla presenza, tra l'altro, di almeno una o più imprese legate all'uso delle tecnologie di cui si occuperà l'ITS Academy e consente di diventare soggetti fondatori di un ITS. Si tratta di una riforma assolutamente importante che ad oggi, complice il cambio di Governo, è ancora in attesa dell'adozione dei decreti attuativi, 19, di cui 17 richiedono il previo accordo della Conferenza Stato-Regioni, indispensabili ad assicurare la piena operatività della riforma.

CAPITOLO 5
Le certificazioni

Il cyberspazio è sempre più caratterizzato da confini evanescenti e dinamici, al punto che, negli ultimi anni, sia gli stati nazionali che l'UE nel suo insieme hanno profuso considerevoli sforzi volti al regolamentarne e uniformarne gli usi e le caratteristiche. Questo è particolarmente vero nell'ambito della sicurezza, dove le sinergie tra Stati puntano, da un lato, a esercitare la propria sovranità e, dall'altro, a mettere in campo azioni congiunte a livello internazionale. Lo strumento principale è quello delle **certificazioni di prodotti e sistemi ICT** che, a livello internazionale, trovano la propria origine nel **TCSEC** statunitense, seguito dall'**ITSEC** europeo e successivamente dai **Common Criteria**. A livello tecnico, questi ultimi hanno la funzione di definire dei criteri per rendere misurabili, e quindi comparabili in maniera oggettiva e incondizionata, le proprietà legate alla sicurezza di un prodotto o di un sistema informatico. A tal proposito vengono utilizzati i principi di imparzialità, ripetibilità, riproducibilità e obiettività. La documentazione prodotta in ottemperanza di questi criteri evidenzia gli elementi fondamentali dell'oggetto della valutazione, ovvero del Target of Evaluation (TOE). Per ottenere la certificazione è necessario identificare gli obiettivi di sicurezza, l'ambiente ed i requisiti funzionali. In numerosi paesi UE attualmente esistono schemi nazionali con caratteristiche specifiche modellati sulla base della struttura indicata dai Common Criteria, così da permettere, in attesa di uno standard Comunitario, l'adozione del principio del mutuo riconoscimento a livello europeo. Per misurare numericamente il grado di sicurezza del TOE si ricorre agli Evaluation Assuran-

ce Level (EAL), 7 livelli di sicurezza, ciascuno dei quali corrisponde ad un pacchetto di sicurezza (SFR) e di garanzia (SAR).
Con il diffondersi di una sempre maggiore consapevolezza dei potenziali rischi cibernetici derivanti dall'espansione costante del mercato digitale nel suo insieme, l'apprezzamento per i sistemi condivisi di valutazione è cresciuto costantemente negli anni. Secondo lo studio Jtsec, nel 2021 il numero di certificazioni rilasciate ha raggiunto il valore più alto della storia con 411 certificati rilasciati (+6% sul 2020).
L'ottenimento delle certificazioni migliora la competitività sul mercato, può garantire l'accesso a mercati con requisiti minimi e offre ai governi nazionali uno strumento per garantire che i sistemi IT utilizzati nel Paese siano sicuri, consentendo di contrastare rischi sistemici, in attesa di standard comunitari. Allo stesso tempo, è opportuno considerare alcuni importanti fattori: la documentazione richiesta dai sistemi nazionali aumenta considerevolmente i costi della valutazione, oggi a carico del fornitore; il processo richiede l'utilizzo di risorse specializzate; e i tempi di esecuzione sono piuttosto lunghi, in particolare per i livelli dal terzo in poi. Altro importante elemento riguarda il tempo addizionale che potrebbe essere impiegato dal CVCN e dai laboratori indipendenti per rendere effettive le procedure di valutazione, poiché potrebbe delinearsi una discrepanza tra l'effettiva capacità di assorbimento dei test da parte dei laboratori e il numero di prodotti da certificare, che è proporzionale al numero di aziende coinvolte all'interno del perimetro di sicurezza cibernetica (oltre 300). A tal proposito, i dati rilevati da Jtsec indicano per il 2021 l'avvenuta certificazione di 11 prodotti in Italia. Inoltre, le rigidità alla base dei Criteria non permettono di mantenere la certificazione per prodotti/sistemi su cui vengono installate nuove patch per aggiornamenti.
Un altro modello di certificazione, il **NESAS** è stato sviluppato direttamente dall'associazione degli operatori che compongono la filiera, GSMA. Si basa su specifiche tecniche che, sebbene non siano formalmente ratificate dagli organismi di standardizzazione riconosciuti, risultano di fatto vincolanti per gli operatori di rete, in quanto soggetti a contratti legali e accordi internazionali di roaming. Molto orientato al mercato, il NESAS consente di effettuare la valutazione delle procedure una sola volta, portando così una notevole accelerazione in termini di tempi e riduzione dei costi. Positivi anche i risvolti per i governi e le autorità nazionali, soprattutto in termini di universale applicabilità del sistema di sicurezza e per la possibilità di farlo interfacciare con le certificazioni nazionali, innalzando ulteriormente il livello di sicurezza. Alcuni governi nazionali hanno riconosciuto ufficialmente lo standard NESAS, tra cui Germania e Paesi Bassi.
A livello europeo, comprese le esigenze di far combaciare più agilmente la rinnovata e rafforzata attenzione circa i fenomeni di cybersecurity con i ritmi sempre più dinamici e flessibili dei mercati digitali, **le istituzioni hanno iniziato a sostenere la creazione di un nuovo sistema di certificazioni sulla sicurezza cibernetica uniforme in tutta l'UE già dal 2019, con la pubblicazione del Regolamento (UE) 2019/881**. Per accompagnare questo percorso, l'ENISA ha istituito un gruppo di lavoro specifico con l'obiettivo di sostenere e promuovere la stesura di **Common Criteria Europei, detti EUCC (Common Criteria based European candidate cybersecurity certification scheme)**, sulla base dei Common Criteria esistenti.
La **prima bozza dell'EUCC (la cosiddetta Versione 1.0)** ha impostato il nuovo schema comunitario su un modello che riprende gli schemi ISO/IEC 15408 e ISO/IEC 18045, esplicitando come l'intenzione consista nel sostituire gradualmente gli attuali schemi di certificazione nazionali. Le novità affrontano direttamente le criticità riscontrate, tra cui tempi e costi, ad esempio favorendo il Patch Management ovvero la possibilità di aggiornare, correggere, migliorare un programma, e il "testing once principle". Sebbene i lavori stiamo procedendo, gli step da superare sono

ancora molteplici, tra cui la c.d. Comitology e la stesura e l'approvazione dell'Implementing Act. Pertanto, le certificazioni effettuate con gli EUCC potranno essere emesse soltanto a partire dal 2024.

Dal Cybersecurity Act al D.Lgs. 3 agosto 2022, n. 123: le certificazioni della cibersicurezza nel contesto europeo e nazionale

Il **Regolamento n. 881/2019 del 17 aprile 2019 (noto come "Cybersecurity Act")**, al fine di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cybersicurezza, cyberresilienza e fiducia all'interno dell'Unione, ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA ed **ha delineato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity in grado di garantire un livello adeguato di cybersecurity dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che** al fine di evitare la frammentazione del mercato interno **per quanto riguarda i sistemi di certificazione della cybersecurity** nell'Unione.

Il regolamento, in particolare, fissa il quadro europeo di certificazione della cybersecurity ed assegna alla Commissione il compito di pubblicare un programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza in cui sono individuate le priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza ed è stilato, sulla base di specifiche motivazioni, un elenco di prodotti TIC, servizi TIC e processi TIC o delle relative categorie che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza.

Il Regolamento individua, inoltre, con particolare rigore, un'ampia gamma di obiettivi di sicurezza connessi all'istituzione dei sistemi europei di certificazione e suddivide in tre, sulla base del livello di rischio associato al previsto uso del prodotto, servizio o processo TIC, in termini di probabilità e impatto di un incidente, i livelli di affidabilità dei prodotti, servizi e processi TIC: di base, sostanziale ed elevato.

In attuazione del descritto regolamento, il 4 settembre 2022 è entrato in vigore il **D.Lgs. n. 123/2022, recante, per l'appunto, norme di adeguamento della normativa nazionale alle disposizioni del Titolo III "Quadro di certificazione della cibersicurezza" del Reg. 2019/881**, che ha individuato nell'ACN l'autorità nazionale di certificazione della cibersicurezza in Italia, le modalità di cooperazione con le altre autorità pubbliche nazionali ed europee e con l'Organismo di accreditamento e la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione. Ad ACN, in particolare, è affidato il compito di definire l'organizzazione e le procedure per lo svolgimento dei compiti in materia di certificazione della cibersicurezza alla stessa attribuiti, autorizzare gli organismi di valutazione della conformità e vigilare sulle attività degli organismi di valutazione della conformità pubblici, controllare il mercato in ambito nazionale ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersicurezza, irrogare le sanzioni previste per i casi di violazioni, assistere l'Organismo di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità, rilasciare (ed eventualmente revocare o chiedere di revocare) i certificati di cibersicurezza, di cui il regolamento dichiara espressamente la natura volontaria.

CAPITOLO 1

LA CIBERSICUREZZA IN EUROPA

1.1 Stato della cibersicurezza in Europa

La centralità assunta dall'ecosistema digitale nel corso degli ultimi anni ha aperto un mondo di nuove opportunità per le imprese, sia a livello di gestione a distanza dei processi interni, sia per la possibilità di interagire con potenziali consumatori sparsi in ogni parte del globo. Le nuove opportunità scaturite da questo cambio di paradigma si portano però dietro anche nuove tipologie di minacce come il cybercrime, sempre più pervasivo anche rispetto ad eventi di carattere geopolitico o persino bellico. Il volume sempre crescente dei flussi monetari che transano attraverso i canali digitali sta diventando direttamente proporzionale all'impegno che gli hacker impiegano nella creazione di software malevoli. Sfortunatamente, questi ultimi trovano spesso terreno fertile nella moltitudine di device che gli utenti utilizzano ogni giorno, nella loro impreparazione e/o nella buonafede rispetto a strategie di ingegneria sociale sempre più sofisticate e finalizzate a carpire dati personali e di accesso.

In base ai dati contenuti nell'ultimo rapporto pubblicato ad ottobre 2022 dall'Associazione Italiana per la Sicurezza Informatica (Clusit), che ogni anno censisce gli attacchi cibernetici classificati come gravi a livello globale, nel primo semestre 2022 il numero di eventi malevoli si è attestato a quota 1.141, con un aumento del 14,6% rispetto al periodo precedente (Fig.1.1).

Osservando la media mensile degli attacchi degli ultimi 5 anni è possibile notare inoltre come le azioni gravi, derivanti evidentemente da gruppi di cybercriminali organizzati, siano cresciute costantemente, passando mensilmente dalle 130 del 2018 alle 190 del primo semestre del 2022 (Fig. 1.2).

Fig. 1.1: Attacchi informatici gravi a livello globale per semestre

Fonte: Clusit - Rapporto sulla Sicurezza ICT in Italia, ottobre 2022

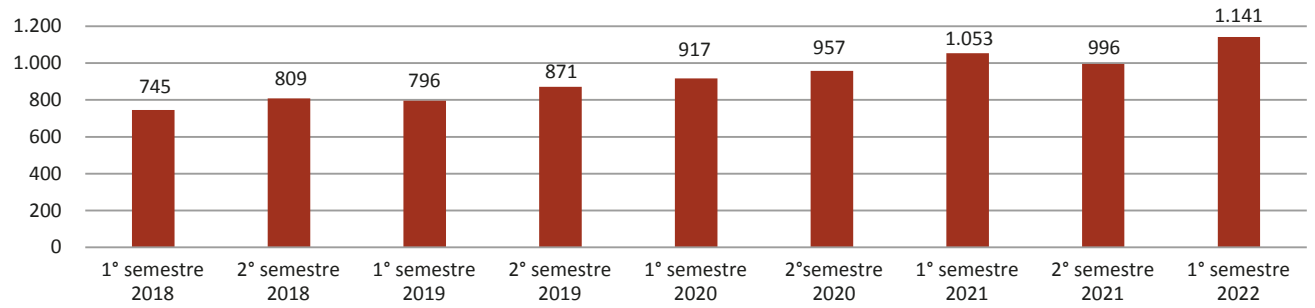


Fig. 1.2: Media mensile degli attacchi informatici gravi a livello globale

Fonte: Clusit - Rapporto sulla Sicurezza ICT in Italia, ottobre 2022

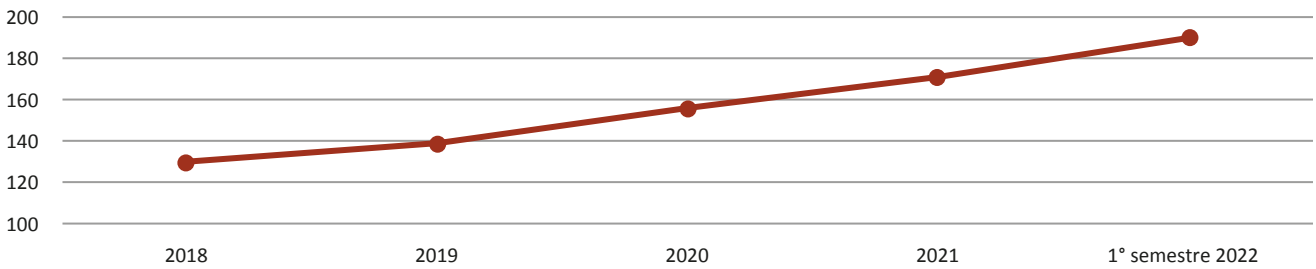
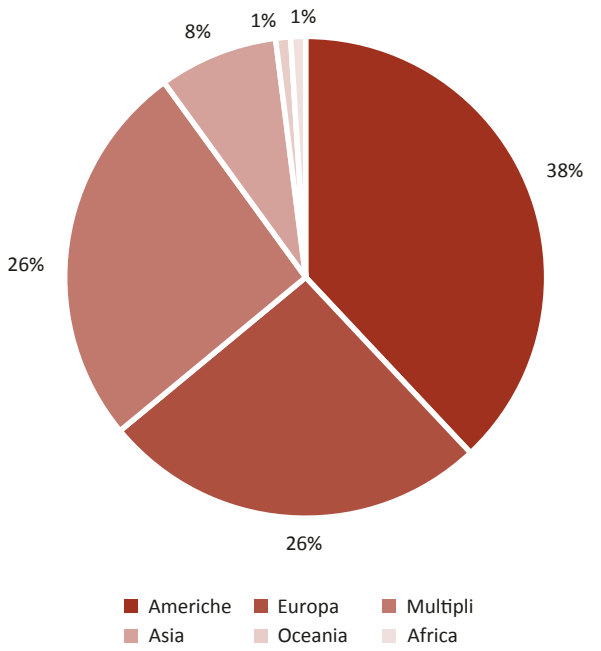


Fig. 1.3: Attacchi informatici gravi a livello globale per area geografica (1S 2022)

Fonte: Clusit - Rapporto sulla Sicurezza ICT in Italia, ottobre 2022



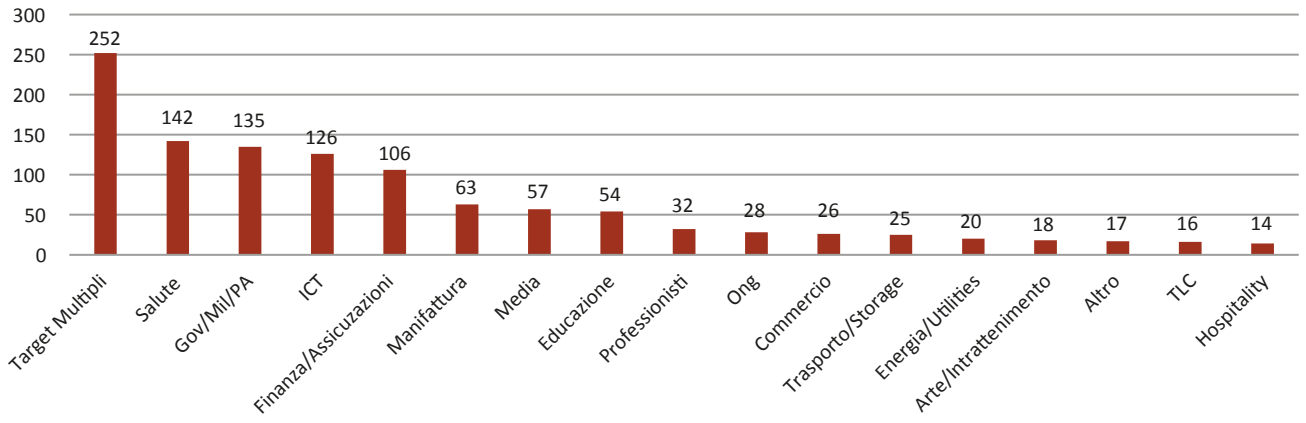
Relativamente alla scomposizione degli **attacchi per area geografica**, si osserva come la percentuale maggiore di eventi malevoli si sia verificata nel continente americano, seguito dall'Europa (26%). È interessante notare inoltre come il 26% delle azioni ostili registrate sia stata attuata **su larga scala**, ovvero interessi organizzazioni residenti in continenti diversi (Fig. 1.3).

Per quanto concerne l'analisi delle vittime di attacchi informatici classificate **per settore d'appartenenza**, secondo i dati raccolti dal Clusit nel 2022 la maggioranza degli eventi censiti non aveva un destinatario specifico, bensì **target multipli** (Fig. 1.4). Analizzando invece i singoli comparti si osserva come quello maggiormente colpito sia il **settore sanitario**, con 252 azioni ostili subite, seguito da **Governo e difesa** (135) e ICT (126).

I software utilizzati dai cybercriminali per attaccare i sistemi informatici delle proprie vittime sono definiti **malware** (abbreviazione di malicious software[1]), ovvero applicativi creati appositamente per penetrare le difese informatiche e danneggiare i device, agendo contro l'interesse degli utenti. Oltre al computer o al dispositivo infetto, il malware può colpire anche tutti i dispositivi

Fig. 1.4: Attacchi informatici gravi a livello globale per settore (1S 2022)

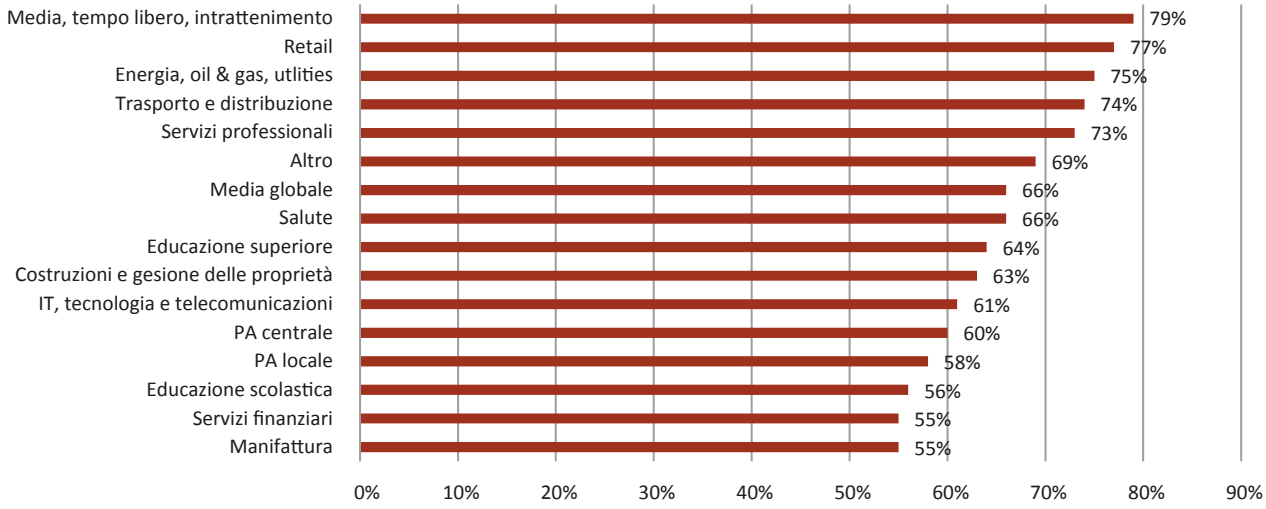
Fonte: Clusit - Rapporto sulla Sicurezza ICT in Italia, ottobre 2022



1 Software dannoso o malevolo.

Fig. 1.5: Percentuale di imprese attaccate con un ransomware per settore (2022)

Fonte: Sophos, The State of Ransomware 2022



con cui comunica il sistema contenente il virus. Una delle tipologie di malware più diffuse di recente è il **ransomware** (tecnicamente "software per il riscatto"), ovvero un particolare tipo di software malevolo che, una volta penetrato in una rete, cripta le informazioni contenute al suo interno richiedendo alla vittima di pagare un riscatto per avere nuovamente accesso ai propri dati. Questo sistema viene spesso utilizzato per colpire grandi amministrazioni pubbliche e private che, pur di non interrompere il servizio e perdere i dati dei propri utenti, sono spinte a cedere al ricatto.

Per comprendere il grado di diffusione di questa minaccia, un dato interessante è fornito da Sophos[2], società specializzata in soluzioni di sicurezza informatica. Dalle interviste condotte tra gennaio e febbraio 2022 su un campione di 5.600 specialisti IT di aziende medio/grandi[3] provenienti da 31[4] paesi differenti ed appartenenti a svariati settori industriali, è emerso che il **66% delle aziende rispondenti ha subìto un attacco ransomware nell'anno precedente, ovvero una percentuale quasi doppia rispetto a quella registrata nel 2020** che si attestava sul 37%. In ben **il 65% dei casi** l'attacco ricevuto è riuscito a penetrare le difese informatiche aziendali e a **criptarne i dati**. Inoltre, il **46% dei soggetti** che si sono trovati in questa situazione è stato **costretto a pagare il riscatto** per rientrarne in possesso, con un esborso medio che si è attestato intorno a quota **$812 mila**. In generale, dalle interviste raccolte è emerso che **l'impatto economico medio derivante da un attacco ransomware a livello globale nel 2021 si è attestato a quota $1,4 milioni.**

Relativamente alla scomposizione dei dati per settore (Fig. 1.5), l'analisi di Sophos mostra che quello maggiormente bersagliato dai ransomware nel 2021 è stato "Media, tempo libero e intrattenimento" (79%), seguito dal "Retail" (77%) e da "Energia, oil & gas e utilities" (75%).

2 https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

3 Per aziende medio/grandi si intendono organizzazioni che hanno tra i 100 e i 5000 dipendenti.

4 Paesi coinvolti nell'analisi: Austria, Australia, Malesia, India, Repubblica Ceca, Polonia, Ungheria, Belgio, Messico, Francia, Nigeria, Spagna, Paesi Bassi, Svezia, Filippine, Germania, Israele, Singapore, Cile, Colombia, Giappone, Italia, Svizzera, Turchia, Emirati Arabi Uniti, Canada, Stati Uniti, Regno Unito, Arabia Saudita, Brasile, Sudafrica.

Tali attacchi generano sulle aziende che li subiscono un notevole impatto negativo sia dal punto di vista economico, sia per quanto concerne la perdita di fiducia da parte degli utenti. Un'organizzazione che non appare in grado di tutelare i dati personali della propria utenza, in particolare se si tratta di informazioni sensibili, rischia di trovare molte difficoltà nel tentativo di riabilitare completamente la propria immagine.

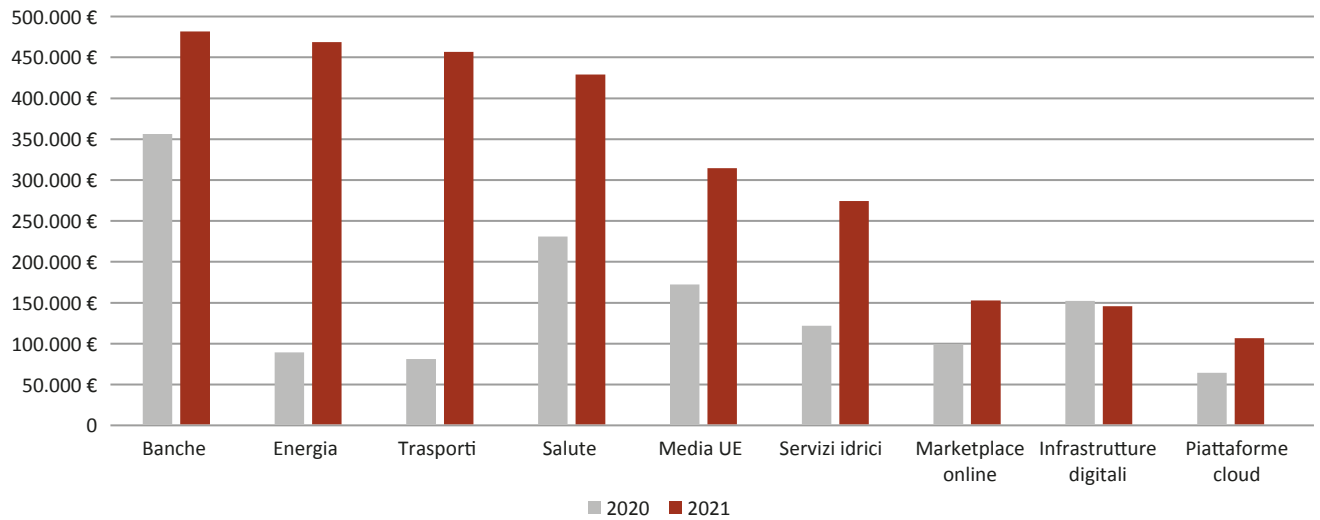
A tal proposito, nell'ultima versione del report *"NIS Investments"*[5], pubblicato dall'ENISA a novembre 2022, si evidenzia come il **danno economico medio prodotto da un grave incidente di sicurezza informatica in UE ammonti a €200 mila**. L'indagine è stata condotta intervistando esponenti di 1080 organizzazioni residenti in tutti e 27 gli Stati Membri (40 per paese), appartenenti ai settori economici sottoposti alla direttiva NIS e suddivisi in due macrocategorie, ovvero gli "Operatori di servizi essenziali" (OSE)[6] e i "*Digital Service Providers*"[7] (DSP).

Analizzando nello specifico i singoli settori coinvolti nell'indagine è possibile notare come le organizzazioni europee che subiscono i danni più rilevanti in caso di incidente di sicurezza informatica grave siano le **banche**, con una **perdita media che si attesta a quota €475 mila.** (Fig. 1.6). Al secondo posto si posizionano le organizzazioni del comparto **energia**, con un **danno medio di circa €462 mila**, che precede il **settore trasporti (€450 mila**). I soggetti mediamente meno danneggiati sono le piattaforme cloud (€104 mila per incidente), le infrastrutture digitali (€143 mila) e i marketplace online (€150 mila). È interessante notare come le aziende più esposte, ovvero quelle che si occupano di servizi digitali, sono anche quelle che ricevono l'impatto più contenuto da un incidente grave di sicurezza informatica: questo risultato può trovare giustificazione nel fatto che tali aziende sono molto più attrezzate a rispondere ad un evento malevolo.

Dai dati sopracitati risulta evidente come sia

Fig. 1.6: Costo medio di un grave incidente di sicurezza informatica in UE per settore

Fonte: ENISA, NIS Investments Report, novembre 2022



5 https://www.enisa.europa.eu/publications/nis-investments-2022
6 OSE – energia; trasporti; bancario; finanziario; salute; servizi idrici; infrastrutture digitali.
7 DSP (Fornitori di servizi digitali) – marketplace online; cloud computing provider; motori di ricerca online.

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.

Secondo quanto emerso dal sopramenzionato report di ENISA, la **spesa media per la sicurezza informatica** effettuata da parte degli OSE/DSP[8] europei nel corso del 2021 si è attestata **a quota €4 milioni.** Mediamente, le entità economiche europee pubbliche e private destinano alla cybersicurezza il **7,2% del proprio budget IT.** Analizzando nel dettaglio i singoli settori si osserva come tra gli OSE/DSP le **organizzazioni che spendono di più in sicurezza informatica siano quelle del settore bancario**, che investono in media €8,5 milioni (Fig. 1.7). Al secondo posto figurano quelle dell'energia, con €5,5 milioni medi, seguite dai Marketplace online (€3,8 milioni).

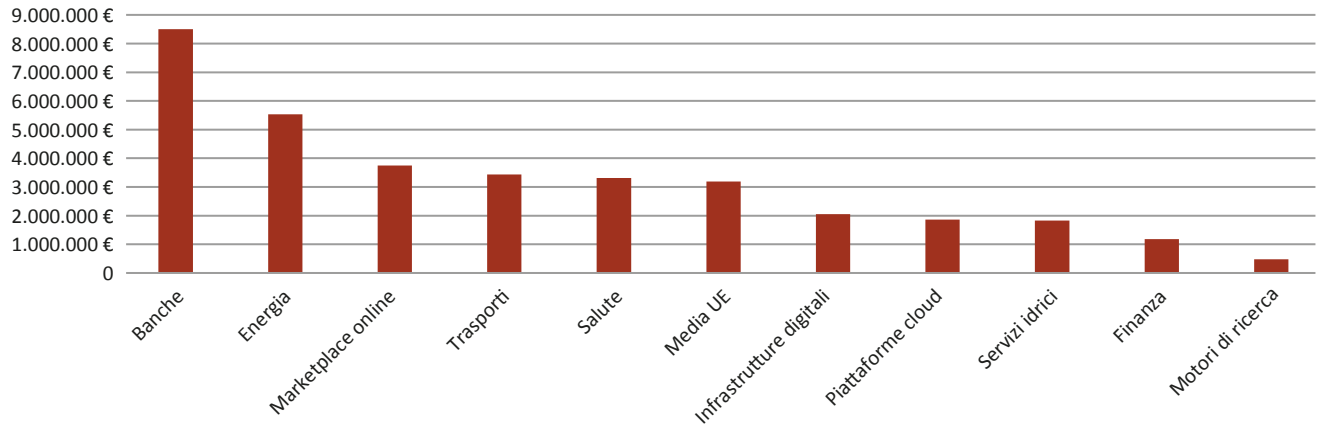
1.2 L'evoluzione del quadro normativo europeo

1.2.1. Il Cybersecurity Package: dalla strategia UE in materia di cibersicurezza all'adozione della direttiva NIS 2

La sempre più massiccia digitalizzazione ed il conseguente aumento dei rischi legati alla sicurezza informatica ha determinato un crescente intervento delle istituzioni europee a partire dal 2013, anno in cui è stata lanciata la prima strategia europea sulla cybersecurity. Gli anni a seguire sono stati costellati da numerose e rilevanti iniziative tese a creare un ecosistema digitale quanto più possibile sicuro: nel 2016, in particolare, è stata adottata la **direttiva NIS (direttiva n. 1148/2016)** con la quale sono state adottate per la prima volta misure organiche nel settore della cibersicurezza ed è stato implementato un sistema di cooperazione tra UE e Stati Membri in materia. Nel 2019, invece, il **Reg. n. 881/2019,** di cui si dirà più approfonditamente nel cap. 5, ha conferito mandato

Fig. 1.7: Spesa media in sicurezza informatica degli OSE/DSP per settore (2021)

Fonte: ENISA, NIS Investments Report, novembre 2022



Note: OSE – Operatore servizi essenziali / DSP – Fornitore di servizi digitali

8 Operatori di servizi essenziali (OSE), Fornitori di servizi digitali (DSP)

permanente all'Agenzia dell'UE per la sicurezza informatica (ENISA), chiamata, attraverso il conferimento di maggiori risorse e l'attribuzione di nuovi compiti, a ricoprire un ruolo chiave nella creazione e nel mantenimento del quadro europeo di certificazione della cibersicurezza e, tra le varie funzioni ad essa assegnate, a predisporre la cornice per l'adozione di schemi di certificazione specifici.

Il 2020 rappresenta un anno particolarmente importante per le politiche sulla cybersecurity che ha visto il lancio, da parte della Commissione europea, del "Cybersecurity package", costituito dalla "**Strategia dell'UE in materia di cibersicurezza per il decennio digitale**", una nuova **direttiva sulla resilienza delle entità critiche** ed una **proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista)**.

La strategia, in particolare, ha declinato proposte concrete di iniziative politiche, di regolamentazione e di investimento in tre aree d'azione dell'UE:

1. **Resilienza, sovranità tecnologica e leadership.** In questa linea d'azione, in particolare, la Commissione propone di: a) riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito di una **direttiva NIS riveduta**; b) creare una **rete di centri operativi per la sicurezza** all'interno dell'UE; c) prevedere un **sostegno dedicato alle piccole e medie imprese** (PMI) nel quadro dei poli dell'innovazione digitale e maggiori sforzi per migliorare le competenze della forza lavoro, attirare e trattenere i migliori talenti in materia di cybersicurezza e investire per una ricerca e un'innovazione aperta, competitiva e basata sull'eccellenza; d) realizzare un'**infrastruttura di comunicazione quantistica** sicura per l'Europa; e) garantire **reti mobili di ultima generazione sicure** attraverso il completamento dell'attuazione del pacchetto di strumenti per il 5G entro il secondo trimestre del 2021; f) approntare nuove **norme orizzontali volte a migliorare la cybersicurezza di tutti i prodotti connessi e servizi associati** presenti nel mercato interno; g) creare **una presenza rafforzata lungo la catena di approvvigionamento tecnologico** per promuovere la propria strategia industriale e la propria leadership in materia di tecnologie digitali e cybersicurezza lungo la catena di approvvigionamento digitale (comprendente dati e cloud, tecnologie dei processori di nuova generazione, connettività ultra sicura e reti 6G), in linea con i propri valori e priorità; h) **migliorare le competenze della forza lavoro**, per attrarre e trattenere i migliori talenti in materia di cybersicurezza e per investire nella ricerca e nell'innovazione di livello mondiale;
2. **Sviluppo di capacità operative di prevenzione, dissuasione e risposta.** Nell'ambito di tale linea d'azione, invece, la Commissione propone: a) la predisposizione di un'**unità congiunta per il ciberspazio** con la funzione di piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cybersicurezza all'interno dell'UE, con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera; b) **ampliare e migliorare la capacità delle forze dell'ordine** di indagare sulla criminalità informatica, rispettando pienamente i diritti fondamentali e perseguendo il necessario equilibrio tra i vari diritti e interessi, attuando pienamente una legislazione adatta allo scopo; c) **aggiornare le linee guida di attuazione del pacchetto di strumenti della diplomazia informatica** anche al fine di aumentare l'efficienza del processo decisionale e continuare ad organizzare regolarmente esercitazioni e valutazioni sul pacchetto di

strumenti della diplomazia informatica stesso; d) promuovere le **capacità di cyberdifesa** presentando una revisione del quadro strategico in materia di cyberdifesa al fine di migliorare ulteriormente il coordinamento e la cooperazione tra attori dell'UE; e) facilitare lo sviluppo di una "**visione e strategia militari dell'UE sul ciberspazio come dominio operativo**" per le missioni e le operazioni militari della PSDC, sostenere sinergie tra l'industria civile, della difesa e dello spazio e rinforzare la cybersicurezza delle infrastrutture spaziali critiche nell'ambito del programma spaziale;

3. **Promozione di un ciberspazio globale e aperto.** Nella terza linea d'azione, la Commissione mira a: a) **rafforzare la cooperazione** con i paesi terzi, le organizzazioni internazionali e la comunità multi-partecipativa; b) promuovere **comportamenti responsabili degli Stati nel ciberspazio,** promuovendo, coordinando e consolidando le posizioni degli Stati membri presso le sedi internazionali, sviluppando una posizione dell'Unione sull'applicazione del diritto internazionale nel ciberspazio**,** guidando la protezione e la promozione dei **diritti umani e delle libertà fondamentali** online e completando il **secondo protocollo aggiuntivo alla convenzione di Budapest;** c) promuovere con forza il **modello multi-partecipativo per la governance di Internet** consolidando scambi regolari e strutturati con il settore privato, il mondo accademico e la società civile.

Il 27 dicembre 2022 è stata invece pubblicata sulla Gazzetta Ufficiale dell'UE la **Direttiva n. 2557/2022 sulla resilienza dei soggetti critici** (Direttiva CER – Resilience of Critical Entities) che abroga la direttiva 2008/114/CE, il cui termine di recepimento per gli Stati membri è fissato al 17 ottobre 2024. Tale direttiva, in particolare, mira ad aumentare la resilienza di soggetti, negli Stati membri, che sono fondamentali per la fornitura di servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno, in una serie di settori che sono alla base del funzionamento di molti altri settori dell'economia dell'Unione. Sono esclusi dal campo di applicazione della direttiva gli enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati. La direttiva CER detta norme armonizzate volte a garantire la fornitura di servizi essenziali nel mercato interno, accrescere la resilienza dei soggetti critici e migliorare la cooperazione transfrontaliera tra le autorità competenti e prevede che entro il 17 luglio 2026 ogni stato individui i soggetti critici per i settori dell'energia, dei trasporti, bancario, delle acque potabili, delle acque reflue, della produzione, trasformazione e distribuzione di alimenti, della sanità, dello spazio, delle infrastrutture dei mercati finanziari e delle infrastrutture digitali, e di determinati aspetti della pubblica amministrazione. La stessa direttiva fissa per i soggetti critici obblighi volti a rafforzare la loro resilienza e la loro capacità di fornire servizi nel mercato interno, stabilisce norme riguardanti la vigilanza sui soggetti critici e l'esecuzione, definisce procedure comuni di cooperazione e comunicazione sull'applicazione della stessa e prescrive misure intese a raggiungere un livello di resilienza elevato dei soggetti critici al fine di garantire la fornitura di servizi essenziali nell'Unione e migliorare il funzionamento del mercato interno.

A carico degli **Stati membri** è posto l'obbligo di adottare, entro il 17 gennaio 2026, una strategia per rafforzare la resilienza dei soggetti critici di cui vengono dettagliatamente individuati i contenuti minimi e di compiere una valutazione del rischio sulla base di un elenco non esaustivo dei servizi essenziali nei settori e nei sottosettori indicati stilato dalla Commissione entro il 17 novembre 2023 e dei criteri individuati

dalla stessa direttiva. Gli stessi Stati sono chiamati a sostenere i soggetti critici nel rafforzamento della loro resilienza e a cooperare con gli altri Stati consultandosi per i soggetti critici che utilizzano infrastrutture critiche fisicamente collegate tra due o più Stati membri, fanno parte di strutture societarie collegate o associate a soggetti critici in altri Stati membri e sono stati individuati come soggetti critici in uno Stato membro e forniscono servizi essenziali ad altri Stati membri o in altri Stati membri.

I **soggetti critici**, invece, una volta ricevuta la relativa designazione, sono tenuti ad effettuare una valutazione dei rischi rilevanti (compresi tutti quelli naturali o di origine umana) che potrebbero perturbare la fornitura dei loro servizi essenziali e ad adottare misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la propria resilienza, in base alle informazioni pertinenti fornite dagli Stati membri in merito alla valutazione del rischio dello Stato membro e in base ai risultati della valutazione del rischio dagli stessi compiute. Agli stessi soggetti critici è richiesto, altresì, di notificare senza indebito ritardo all'autorità competente gli incidenti che perturbano o possono perturbare in modo significativo in modo significativo la fornitura di servizi essenziali. Specifiche previsioni sono dettate al Capo IV per l'individuazione dei soggetti critici di particolare rilevanza europea.

Dal punto di vista istituzionale, è istituito il **gruppo per la resilienza dei soggetti critici**, composto da rappresentanti degli Stati membri e della Commissione, con compiti di assistenza alla Commissione, chiamato a favorire la condivisione delle migliori prassi, ad agevolare lo scambio di informazioni e ad analizzare strategie e relazioni. A livello nazionale, ogni Stato membro è chiamato a designare o istituire una o più **autorità competenti** responsabili dell'applicazione della direttiva a livello nazionale ed un **punto di contatto unico** con funzioni di collegamento ed obblighi di relazione alla Commissione, entro il 17 luglio 2028, e successivamente ogni due anni, in merito alle notifiche ricevute ed alle azioni intraprese.

Nella medesima data – 27 dicembre 2022 – è stata infine pubblicata la **Direttiva n. 2555/2022 (NIS 2)** che è entrata in vigore lo scorso 17 gennaio 2023 e che dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024. Tale direttiva, in particolare, rappresenta la risposta all'esigenza di riformare la direttiva NIS che ha fissato specifici obiettivi che avrebbero dovuto tradursi nell'adozione coordinata da parte degli Stati membri di misure tecniche e organizzative adeguate ed armonizzate per il rafforzamento dei livelli di sicurezza dei sistemi informativi e delle reti, nonché nel miglioramento della gestione degli incidenti cyber, ma che invece si è mostrata incapace di garantire uniformità normativa e di fornire una risposta efficace all'incremento dei rischi per la sicurezza conseguenti alla diffusa digitalizzazione dei processi e dei servizi.

Pertanto, pur confermando gran parte degli obiettivi e degli strumenti della direttiva NIS, la NIS 2, partendo dalla constatazione del rafforzamento del ruolo di alcune categorie di soggetti e del sopraggiungere di rischi nuovi in settori ulteriori rispetto a quelli individuati, è innanzitutto intervenuta **ampliando la platea di soggetti destinatari della normativa** dalla stessa fissata. Ed infatti, se l'originaria Direttiva NIS si rivolge – e si rivolgerà fino alla sua abrogazione – a quegli operatori privati che svolgono la loro attività in sette settori ritenuti "essenziali" dall'Unione europea, ovvero quelli dell'energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari, dell'acqua potabile, della sanità e delle infrastrutture digitali, cui si affiancano anche i fornitori di servizi digitali e, dunque, coloro che operano nei settori dell'e-commerce, dei motori di ricerca e del cloud computing, la Direttiva NIS 2 ha incluso nel proprio campo di applicazione ulteriori soggetti attivi in settori definiti "ad alta criticità", ovvero

quelli delle acque reflue, della gestione dei servizi ICT (*business-to-business*), della pubblica amministrazione e dello spazio. Inoltre, ha previsto anche la tipologia dei c.d. "altri settori critici", includendovi i servizi postali e di corriere, la gestione dei rifiuti, la fabbricazione, la produzione e la distribuzione di sostanze chimiche, la produzione, la trasformazione e la distribuzione di alimenti, la fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, la fabbricazione di computer e prodotti di elettronica e ottica, la fabbricazione di apparecchiature elettriche, la fabbricazione di macchinari e apparecchiature n.c.a., la fabbricazione di autoveicoli, rimorchi e semirimorchi e di altri specifici mezzi di trasporto, i fornitori di servizi digitali e le organizzazioni di ricerca.

All'ampliamento dell'ambito di applicazione si accompagna anche il **superamento della precedente impostazione legata ai concetti di "operatore di servizi essenziali" e di "fornitore di servizi digitali",** liberamente identificati dagli Stati membri dell'Unione europea attraverso criteri spesso disomogenei, in favore di due nuove categorie di attori, quella dei "**soggetti essenziali"** e quella dei **"soggetti importanti"** e l'introduzione di un **criterio dimensionale** tale per cui la disciplina si applica a tutti quei soggetti pubblici o privati ricompresi nelle tipologie denominate "alta criticità" o "altri settori critici" che prestino i loro servizi o svolgano le loro attività all'interno dell'Unione e siano considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superino i massimali per le medie imprese di cui al paragrafo 1 del medesimo articolo. Inoltre, indipendentemente dalle dimensioni, vengono comunque assoggettate alla Direttiva NIS 2 anche ulteriori particolari tipologie di soggetti, tra cui i fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico, coloro che forniscono servizi di registrazione dei nomi di dominio, taluni enti della pubblica amministrazione, nonché i soggetti definiti c.d. "critici" dalla Direttiva 2022/2557 (Direttiva CER) appena descritta. Agli Stati membri è riconosciuta la facoltà di prevedere che la direttiva si applichi ad enti della pubblica amministrazione a livello locale e ad istituti di istruzione, in particolare ove svolgano attività di ricerca critiche. Sono espressamente esclusi dall'ambito di applicazione della direttiva gli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati. Se questi sono i riferimenti normativi, spetterà comunque agli Stati membri stilare (entro il 17 aprile 2025), anche attraverso le informazioni fornite dai soggetti interessati, un elenco dei soggetti essenziali ed importanti.

Per quanto concerne gli obblighi a carico dei soggetti rientranti nel campo di applicazione della direttiva, sono previste misure più stringenti e specifiche in termini di cyber risk management, di segnalazione e condivisione delle informazioni relative agli incidenti di sicurezza e viene introdotto un approccio basato sul concetto del c.d. "multirischio". Ciò comporta che le misure tecniche, operative e organizzative comprendano almeno i seguenti aspetti: a) le politiche di analisi dei rischi e di sicurezza dei sistemi informatici; b) la gestione degli incidenti; c) la continuità operativa, come la gestione del *backup* e il ripristino in caso di disastro, e la gestione delle crisi; d) la sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; e) la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; f) le strategie e le procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza; g) le pratiche di igiene informatica di base e di formazione in

materia di cibersicurezza; h) le politiche e le procedure relative all'uso della crittografia e, se del caso, della cifratura; i) la sicurezza delle risorse umane, le strategie di controllo dell'accesso e gestione degli attivi; l) l'uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Cruciali gli obblighi di segnalazione in caso di "**incidente significativo**", ossia un incidente che abbia causato o sia in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato e/o si sia ripercosso o sia in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. In presenza di tali condizioni, la direttiva prevede che i soggetti interessati trasmettano un preallarme entro il termine di 24 ore dalla conoscenza dell'incidente, una notifica entro il termine di 72 ore dalla conoscenza dell'incidente, che aggiorni – se necessario – le informazioni del preallarme ed una relazione finale entro un mese dalla trasmissione della notifica, il cui contenuto minimo è dettagliato dalla stessa direttiva.

Molto rilevanti le **misure di vigilanza e di esecuzione**, alle quali saranno sottoposti – in misura differente – i soggetti essenziali e importanti e che includono *audit* regolari e mirati sulla sicurezza, scansioni di sicurezza, ovvero ispezioni *in loco*, vigilanza e richieste di informazioni (solo *ex post*, in caso di soggetti importanti).

Le **sanzioni** per la violazione delle misure di gestione dei rischi di *cybersecurity* o degli obblighi di segnalazione potranno arrivare a un massimo di almeno 10 milioni di euro (ridotti a 7, in caso di soggetti importanti) o a un massimo di almeno il 2 % (ridotto all'1,4%, in caso di soggetti importanti) del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto appartiene, se superiore.

1.2.2. Creazione della resilienza, sovranità tecnologica e leadership: l'istituzione del Centro di competenza per la cibersicurezza a Bucarest e della rete di centri nazionali di coordinamento

In attuazione della strategia descritta nel paragrafo precedente, il 20 maggio 2021 è stato adottato il **Regolamento n. 887/2021** che istituisce, per il periodo compreso fra il 28 giugno 2021 e il 31 dicembre 2029 (salvo proroghe), **il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento** con sede a Bucarest definendone composizione, compiti ed obiettivi.

Tale regolamento, in particolare, mira a rafforzare le capacità europee di sicurezza informatica, promuovere l'eccellenza della ricerca ed accrescere la competitività dell'industria dell'Unione in questo campo. Il Centro di competenza, in particolare, è chiamato a svolgere compiti strategici e di esecuzione svolgendo un ruolo essenziale nel perseguimento degli obiettivi di cybersicurezza e fiducia declinati all'art.6 del Reg. 694/2021 che si sostanziano nel sostegno a sviluppo ed acquisizione di attrezzature, infrastrutture di dati e strumenti avanzati per la cybersicurezza, rafforzamento delle conoscenze, delle capacità e delle competenze europee connesse alla cybersicurezza, condivisione ed integrazione delle migliori prassi, miglioramento della resilienza agli attacchi informatici, acquisizione di maggiore consapevolezza dei rischi e di una migliore conoscenza dei processi di cybersicurezza e rafforzamento della cooperazione tra il settore civile e il settore della difesa per quanto riguarda i progetti, i servizi, le competenze e le applicazioni a duplice uso nell'ambito della cybersicurezza.

Il Centro è inoltre chiamato a contribuire all'attuazione di Orizzonte Europa, con specifico riguardo al pilastro II, sezione 3.1.3., dell'allegato I della decisione (UE) 2021/764 del Consiglio e, dunque, ad

agire per il rafforzamento della resilienza agli attacchi informatici e la creazione di un efficace effetto deterrente a livello informatico, lo sviluppo e il mantenimento di capacità strategiche essenziali in materia di cybersicurezza per la tutela del mercato unico digitale e, in particolare, per assicurare la protezione di reti essenziali e sistemi informativi e fornire servizi fondamentali di cybersicurezza.
Lo stesso regolamento prescriveva agli Stati Membri di designare, entro il 29 dicembre 2021, il **centro nazionale di coordinamento** che viene valutato dalla Commissione chiamata ad emettere un parere entro tre mesi dalla richiesta da parte dello Stato circa il possesso in capo all'ente individuato dei requisiti necessari per raggiungere gli obiettivi individuati. I centri nazionali di coordinamento, che confluiscono nella rete e figurano in un elenco pubblicato dal Centro di competenza, sono chiamati a fungere da punti di contatto a livello nazionale per la comunità al fine di assistere il Centro di competenza nell'assolvimento della sua missione e nel conseguimento dei suoi obiettivi, fornire consulenza, promuovere la partecipazione ai progetti transfrontalieri e alle azioni relative alla cybersicurezza finanziati dai pertinenti programmi dell'Unione, fornire assistenza tecnica, sostenere e promuovere la partecipazione degli enti pertinenti alle attività condotte dal Centro di competenza, dalla rete e dalla comunità, e monitorare, se del caso, il livello di impegno nello sviluppo e nella diffusione della ricerca in tema di cybersicurezza, e il relativo ammontare di sostegno finanziario pubblico. Accanto al Centro ed alla rete, opera la **comunità** che riunisce i principali portatori di interessi per quanto concerne le capacità in materia di cybersicurezza nell'ambito tecnologico, industriale, accademico e della ricerca nell'Unione, coinvolgendo i centri nazionali di coordinamento, i poli europei dell'innovazione digitale, se del caso, e le istituzioni, gli organi e gli organismi competenti dell'Unione, quali l'ENISA. I membri della comunità, una volta valutati idonei dai centri nazionali e registrati come tali dal Centro di competenza, assistono quest'ultimo nell'assolvimento della sua missione e nel conseguimento dei suoi obiettivi operando a stretto contatto con il Centro di competenza e i centri nazionali di coordinamento, partecipando ad attività formali o informali e ai gruppi di lavoro, svolgendo attività specifiche previste dal programma di lavoro annuale e, se del caso, assistendo il Centro di competenza e i centri nazionali di coordinamento nella promozione di progetti specifici.

1.2.3. Il Cyber Resilience Act (CRA). La proposta della Commissione per una maggior tutela dei consumatori dagli attacchi informatici. Lo stato della procedura e le posizioni emerse

Sempre in attuazione di quanto previsto nella Strategia lanciata nel 2020, il 15 settembre scorso la Commissione Europea ha pubblicato una **proposta di regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (Cyber Resilience Act-CRA)**. Tale proposta, in particolare, mira a salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o software con una componente digitale attraverso la fissazione di regole armonizzate per l'immissione sul mercato di prodotti o software con una componente digitale, l'individuazione di requisiti di cybersecurity che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, la fissazione di obblighi per ogni fase della catena del valore e la declinazione di un obbligo generale di diligenza per l'intero ciclo di vita di tali prodotti.
In particolare, la proposta della Commissione parte dalla constatazione che i prodotti hardware e software sono sempre più soggetti ad attacchi informatici di successo, il cui costo globale stimato è di 5,5 trilioni di euro entro il 2021 e che ciò sia conseguenza di un basso livello di sicurezza informatica e dell'incapacità degli utenti di scegliere dispositivi sicuri o di usarli in

maniera appropriata. Per risolvere tali criticità, la proposta di regolamento disciplina l'immissione sul mercato di prodotti con elementi digitali al fine di garantire la sicurezza informatica di tali prodotti, fissa i requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e gli obblighi per gli operatori economici per quanto riguarda la sicurezza informatica, individua i requisiti essenziali dei processi di gestione delle vulnerabilità per garantire la sicurezza informatica dei prodotti con elementi digitali durante l'intero ciclo di vita e gli obblighi per gli operatori economici in relazione a tali processi e detta regole di sorveglianza del mercato e di *enforcement* della disciplina dalla medesima introdotta.

Nel definire l'ambito applicativo, la proposta si riferisce ai prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione logica o fisica diretta o indiretta di dati a un dispositivo o a una rete, individuando tra i prodotti con elementi digitali, quelli critici (suddivisi in Classe I e II) e fissa una serie corposa di obblighi a carico di produttori, importatori e distributori. I prodotti definiti come critici e rientranti nella Classe II, in particolare, non possono essere oggetto di autocertificazione di base da parte del produttore, ma necessitano del rilascio di una certificazione da parte di un ente di certificazione accreditato.

I **produttori**, in particolare, sono chiamati a: a) realizzare un ***assessment* dei rischi cyber** associati al prodotto con elementi digitali – da includere nella documentazione tecnica da produrre ai fini dell'immissione sul mercato – e di tenerne conto durante la progettazione, lo sviluppo, la produzione, la distribuzione ed in tutte le fasi di vita del prodotto allo scopo di minimizzare i rischi di cybersecurity, prevenire gli incidenti di sicurezza e ridurne gli impatti; b) osservare **obblighi di diligenza** nel caso in cui decidano di integrare componenti provenienti da terze parti nella logica di garantire che non ci siano compromissioni della sicurezza del prodotto; c) **documentare** in maniera proporzionata alla natura del prodotto ed ai rischi, gli aspetti concernenti il prodotto, incluse le vulnerabilità di cui venga a conoscenza; d) a dotarsi di appropriate policy e procedure, incluse quelle di identificazione e gestione delle vulnerabilità; e) **fornire informazioni ed istruzioni sul prodotto che siano chiare e comprensibili**; f) mettere in atto **correttivi** nel caso in cui emerga o vi sia ragione di pensare che il prodotto o i processi messi in atto non siano conformi alla disciplina prevista; g) **cooperare con le autorità di vigilanza** fornendo informazioni chiare e comprensibili, mettendo in atto misure per eliminare i rischi di cibersicurezza ed anche informando le stesse autorità dell'eventuale incapacità di essere compliant con le norme dettate; h) **informare l'ENISA** (entro 24 ore) di eventuali vulnerabilità e/o incidenti (ENISA informa EUCyCLONe nel caso in cui le informazioni ricevute siano rilevanti per la gestione coordinata di incidenti di cybersecurity su larga scala ed inserisce tali informazioni nel report biennale da inviare al Gruppo di Cooperazione); i) **informare gli utenti** dell'incidente, fornendo informazioni su eventuali azioni da compiere per mitigarne l'impatto. Tali obblighi si applicano anche a importatori o distributori che immettano sul mercato il prodotto sotto il proprio nome o marchio o apportino una modifica sostanziale al prodotto. Alla medesima conclusione si giunge rispetto a qualunque persona fisica o giuridica che apporti una modifica sostanziale al prodotto.

Agli **importatori,** è invece prescritto di verificare che il produttore abbia attivato le procedure di conformità di cui all'art. 24 ed abbia prodotto la redazione tecnica, che il prodotto sia munito della marcatura CE e che sia accompagnato dalle informazioni ed istruzioni per l'uso (di cui devono verificare la chiarezza e comprensibilità) e di non mettere sul mercato il prodotto nel caso in cui ritenga che lo stesso non abbia i requisiti essenziali prescritti (informando anche il produttore e l'autorità di vigilanza nel caso di rischi di cybersecurity). Agli stessi è altresì richiesto

di comunicare, senza ritardo, al produttore, eventuali non compliance con la normativa e vulnerabilità (nel caso di significativo rischio è prescritta anche la comunicazione, senza ritardo, alle autorità di vigilanza degli Stati in cui gli importatori rendono disponibile il prodotto), conservare per 10 anni dall'immissione sul mercato del prodotto, la documentazione attestante la conformità dello stesso ai requisiti richiesti e collaborare con le autorità di sorveglianza.

Ai **distributori,** infine, è prescritto di verificare che il prodotto possieda la marcatura CE e che produttore e importatore abbiano osservato gli obblighi sugli stessi gravanti. Anche ai distributori è vietato immettere sul mercato il prodotto nel caso in cui ritengano che lo stesso non possieda i requisiti essenziali previsti, è fatto obbligo di informare il produttore e l'autorità di vigilanza nel caso sussistano significativi rischi di cibersicurezza, di cooperare con le autorità e di comunicare eventuali impossibilità di essere compliant con la disciplina prevista dal regolamento.

Ciò che emerge, dunque, è la definizione di un articolato set di obblighi tesi a creare, di fatto, una catena di verifica e controllo reciproco molto robusta.

Dal punto di vista procedurale, la proposta descrive accuratamente le **procedure di verifica della conformità dei prodotti con elementi digitali** ai requisiti prescritti ed attribuisce agli Stati membri il compito di individuare un'autorità di notifica ("*notifying authority*") – di cui vengono declinati i requisiti essenziali – deputata a definire le procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio. Rispetto a questi ultimi, in particolare, la proposta fissa stringenti requisiti di indipendenza, professionalità, competenza, vietando espressamente che la remunerazione dei manager e del personale possa essere collegata al numero o all'esito degli assessment compiuti e prescrivendo specifici obblighi di segretezza rispetto a tutte le informazioni ricevute nello svolgimento delle proprie attività.

Molto rilevante la previsione dell'**art. 18 "*Presunzione di conformità*"** con la quale viene attribuito alla Commissione il potere di specificare, mediante atti di esecuzione, i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali o a parti di essi di cui all'allegato I. Inoltre, se del caso, la Commissione specifica se un certificato di cibersicurezza rilasciato nell'ambito di tali sistemi elimina l'obbligo per un fabbricante di effettuare una valutazione di conformità da parte di terzi per i requisiti corrispondenti.

Rispetto a **sorveglianza** ed ***enforcement***, la proposta di regolamento affida agli Stati membri la designazione di un'autorità deputata alla sorveglianza del mercato e dei prodotti con elementi digitali (con la garanzia che tale autorità disponga delle necessarie risorse umane e finanziarie), alla cooperazione con le medesime autorità degli altri Stati membri e, ove opportuno, con quelle preposte alla supervisione dell'osservanza della normativa sulla protezione dei dati (queste ultime, in particolare, hanno il potere, per l'esercizio delle proprie funzioni, di accedere alla documentazione prevista dalla proposta in esame).

Molto rilevanti i **poteri attribuiti alla Commissione**. Ed infatti, per i prodotti che presentino un elevato rischio di cybersecurity, la proposta prevede che, nel caso in cui l'autorità di sorveglianza accerti una non compliance non limitata al territorio nazionale, la stessa avvisi la Commissione e gli altri Stati membri fornendo informazioni anche sui risultati delle valutazioni compiute e sulle azioni che l'operatore è stato chiamato ad attuare. In caso di disaccordo di uno Stato membro circa le misure adottate o nell'ipotesi in cui la Commissione le ritenga contrarie al diritto UE, la proposta prevede che quest'ultima attivi una consultazione (*Union safeguard procedure*, art. 44) con gli Stati membri e gli operatori interessati all'esito della quale – entro 9 mesi dalla notifica – la stessa valuti se la misura nazionale sia giustificata o no. Sempre con riguardo ai prodotti

che presentino un significativo rischio di cybersecurity, alla Commissione è anche riconosciuto il potere di richiedere ad un'autorità nazionale di sorveglianza di operare la relativa valutazione e, in eccezionali circostanze che giustifichino un immediato intervento per preservare il buon funzionamento del mercato interno, in mancanza di un intervento dell'autorità di sorveglianza nazionale, il potere di azionare l'ENISA informando prontamente l'autorità nazionale.

Aspro il **regime sanzionatorio** che prevede sanzioni amministrative pecuniarie fino a 15.000.000 di euro o, se il trasgressore è un'impresa, fino al 2,5% del suo fatturato mondiale totale annuo per l'esercizio precedente, a seconda di quale sia il valore più elevato nel caso di violazione delle disposizioni contenute negli artt. 10 e 11 e dunque degli obblighi a carico dei produttori. Tali importi scendono a 10.000.000 di euro o al 2% nel caso di inosservanza degli altri obblighi e a 5.000.000 o l'1% nel caso di invio di informazioni scorrette, incomplete o fuorvianti agli organismi di valutazione o all'autorità di vigilanza a seguito di richiesta.

In Parlamento europeo tale proposta è stata assegnata alla commissione ITRE (rapporteur Nicola Danti).

Il Consiglio, invece, nella relazione presentata il 6 dicembre scorso, ha espresso un apprezzamento generale per la proposta della Commissione, ma al contempo ha formulato una richiesta di chiarimento in merito all'applicabilità della disciplina al software as a service, ha proposto di escludere dall'ambito di applicazione della proposta i prodotti destinati esclusivamente a scopi militari ed ha rilevato l'importanza di valutare l'onere della proposta per l'industria, in particolare per le PMI e di approfondire il ruolo dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), oltre a chiarire, a livello generale, le interazioni con altri atti legislativi in materia.

Il 15 novembre 2022 lo **European Data Protection Supervisor (EDPS)**, ha pubblicato un'opinion (la 23/2022), dedicata al Cyber Resilience Act in cui sono stati analizzati i punti di contatto e le interferenze della proposta della Commissione con il GDPR, evidenziando come la definizione di un quadro giuridico uniforme in materia di requisiti essenziali di cybersicurezza per l'immissione di prodotti con elementi digitali sia molto importante per salvaguardare i diritti e le libertà fondamentali, compresi i diritti alla privacy e alla protezione dei dati personali. Lo stesso EDPS ha inoltre incoraggiato l'inclusione dei principi di *privacy by design e by default* tra i requisiti di cybersicurezza e l'inserimento di previsioni che chiariscano come la disciplina proposta non incida sull'applicazione delle vigenti disposizioni dell'Unione europea in materia il trattamento dei dati personali, compresi i compiti e i poteri delle autorità di controllo indipendenti.

1.2.4. Focus 5G: le iniziative europee per reti 5G sicure

L'esigenza di implementare efficaci standard di sicurezza assume rilevanza peculiare con riguardo alle reti 5G proprio in considerazione dell'ampia serie di servizi digitali che sono in grado di abilitare e la conseguente necessità di scongiurare le gravi ed impattanti conseguenze di malfunzionamenti sistemici e diffusi. Partendo da tali constatazioni e dal desiderio di far rivestire all'Unione europea un ruolo da leader a livello mondiale, la Commissione europea, il 26 marzo 2019 ha adottato la **Raccomandazione n. 2019/534** sulla cybersecurity delle reti 5G con la quale ha evidenziato i rischi di cybersecurity rispetto a tali reti e presentato orientamenti sulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi. In particolare, per affrontare i rischi di cybersecurity nelle reti 5G, il documento poneva in evidenza la necessità di considerare non solo i **fattori tecnici**, ma anche **fattori ulteriori e diversi** come, ad esempio, requisiti normativi o di altro tipo imposti ai fornitori di apparecchiature per le

tecnologie dell'informazione e della comunicazione, il modello di governance esistente nel Paese analizzato, il rischio generale di influenza da parte di un paese terzo, l'assenza di accordi di cooperazione sulla sicurezza o di disposizioni analoghe, quali le decisioni di adeguatezza, tra l'Unione e il paese terzo interessato per quanto riguarda la protezione dei dati, etc. La raccomandazione individuava, inoltre, un **set di azioni** tese a consentire, a livello nazionale ed europeo, un'adeguata valutazione dei rischi e ad individuare un'eventuale serie comune di misure da adottare per attenuare i rischi di cybersecurity relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare le reti 5G ed individuava una **roadmap** chiara e stringente secondo cui gli Stati membri avrebbero dovuto valutare i rischi, aggiornare i requisiti di sicurezza e i metodi di gestione dei rischi applicati alle reti 5G, aggiornare i pertinenti obblighi imposti alle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico.

Al fine di dare attuazione a quanto previsto nella raccomandazione appena descritta, il **9 ottobre 2019** è stata pubblicata dal gruppo di cooperazione NIS, composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA, una **relazione sulla valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti di quinta generazione** la quale, partendo dai risultati delle valutazioni nazionali dei rischi per la cibersicurezza, effettuate da tutti gli Stati membri dell'UE, ha individuato le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo), nonché diversi rischi strategici. In particolare, nell'individuare le più importanti sfide per la sicurezza che possono manifestarsi o acuirsi (rispetto alle reti precedenti) con l'avvento delle reti 5G, tale relazione si concentra, da un lato, sulle innovazioni abilitate da tali reti (con riguardo sia al software che alle numerose applicazioni e servizi resi possibili dal 5G) e, dall'altro, al ruolo dei fornitori nella realizzazione e nell'uso delle reti 5G nonché al grado di dipendenza da singoli fornitori.

Tale documento, dopo aver riportato un'analisi del contesto, ha evidenziato le specifiche tecniche associate alla tecnologia 5G. In seguito, sono stati identificati e descritti nel dettaglio gli asset utilizzati per il 5G, individuando per ciascuno gli impatti potenziali in termini di perdita di riservatezza, integrità e disponibilità. È stata poi proposta una tassonomia delle minacce che possono coinvolgere la tecnologia 5G associando ciascuna alle capacità di specifici attori (entità statuali, cyber criminali, hacktivisti, ecc.). Sulla base dell'analisi effettuata sono state quindi proposte alcune raccomandazioni per i Paesi membri, per gli stakeholder del mercato 5G e per le autorità nazionali competenti sul tema di sicurezza del 5G. Ad integrazione del rapporto degli Stati membri dell'UE sulle valutazioni del rischio a livello dell'UE sulla sicurezza 5G appena descritto, il **21 novembre 2019,** l'ENISA ha pubblicato un *Threat Landscape for 5G Networks*, valutando le minacce legate alle reti 5G. Si tratta di un rapporto interessante, nel quale, sulla base anche del contributo offerto da gruppi e organismi di standardizzazione 5G e stakeholder 5G come operatori, fornitori, organizzazioni nazionali e internazionali, sono state individuate le sfide e le possibili minacce nella sicurezza delle reti 5G, è stato definito un diagramma degli asset, formulata una tassonomia delle minacce, identificata l'esposizione dei diversi asset e valutate le motivazioni dell'agente di minaccia.

Anche il Consiglio, nelle proprie conclusioni del **3 dicembre 2019** ha appoggiato i rilievi formulati dal gruppo di cooperazione NIS sottolineando l'importanza di adottare un approccio coordinato e di assicurare un'efficace attuazione della raccomandazione – mediante adozione di tutte le misure necessarie nell'ambito delle rispettive competenze per garantire la sicurezza e l'integrità delle reti di comunicazione elettronica, in particolare le reti 5G – al fine di evitare la frammentazione del mercato unico.

Il **29 gennaio 2020** è stata invece pubblicata dalla Commissione la Comunicazione ***"Dispiegamento del 5G sicuro – Attuazione del pacchetto di strumenti dell'UE"*** nella quale, preso atto dell'assoluta rilevanza del 5G per molti servizi essenziali e, dunque, della strategica necessità per l'Unione di garantire la cybersecurity delle reti 5G in un momento in cui gli attacchi informatici sono in aumento, più sofisticati che mai e ad opera di un'ampia gamma di soggetti, viene dato conto di come nell'ambito della cooperazione NIS ed a seguito del completamento da parte degli stati membri delle procedure di valutazione dei rischi delle proprie infrastrutture di rete 5G, il gruppo di cooperazione NIS abbia pubblicato una relazione sulla valutazione dei rischi coordinata a livello dell'UE sulla cybersecurity di tali reti in cui sono state individuate le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo) che interessano le reti 5G.

Nella medesima data lo stesso gruppo di cooperazione NIS ha pubblicato il **pacchetto di strumenti dell'UE** (**Toolbox sul 5G**) comprendente misure di attenuazione dei rischi, che tratta tutti i rischi individuati nella relazione coordinata sulla valutazione dei rischi individuando e descrivendo una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia, che possono essere attuate per attenuare i rischi individuati. Il documento, in particolare, nell'evidenziare come l'Europa sia una delle regioni più avanzate nel mondo in relazione al lancio commerciale dei servizi 5G (entro la fine del 2020, infatti, i primi servizi 5G dovrebbero essere disponibili in 138 città europee), fa il punto su alcuni dei settori rispetto ai quali il 5G opererà quale fattore abilitante una serie di importanti applicazioni e, nello specifico, ***e-health*** (con riguardo da un lato, alla possibilità di monitorare a distanza dello stato di salute dei pazienti e delle loro cartelle e di formulare una diagnosi intelligente e, dall'altro, all'impiego di robot in ausilio dei medici nell'ottica di migliorare le performance mediche), **reti energetiche intelligenti** (ad alta efficienza, con minori interruzioni di servizio su piccola scala e con installazioni più semplici e dal minor impatto ambientale), **fabbriche del futuro** (con monitoraggio a distanza di processi e macchinari), **media ed intrattenimento** (con riferimento, in particolare, allo sviluppo di applicazioni come la realtà virtuale e lo streaming video) e **mobilità** (con lo sviluppo della mobilità connessa e automatizzata con obiettivo zero incidenti e l'implementazione della connettività in tutte le modalità di trasporto).

L'obiettivo dichiarato dal documento è identificare un possibile insieme comune di misure in grado di mitigare i principali rischi per la sicurezza informatica delle reti 5G (così come sono stati identificati nella relazione di valutazione del rischio coordinata dall'UE) e fornire una guida per la selezione delle misure da adottare al fine di creare un solido quadro di misure che garantisca un adeguato livello di sicurezza informatica delle reti 5G in tutta l'UE ed un approccio coordinato tra gli Stati membri. Le misure presentate nel pacchetto contribuiscono al raggiungimento di una serie di importanti obiettivi di sicurezza che si autoalimentano e che rivestono grande rilevanza per affrontare i rischi identificati nel rapporto di valutazione dei rischi e proteggere la riservatezza, l'integrità e la disponibilità delle reti 5G. Tali obiettivi, nello specifico, si sostanziano: a) nel rafforzare la sicurezza nella progettazione, implementazione e funzionamento delle reti; b) innalzare gli standard di sicurezza di base per la sicurezza di prodotti e servizi; c) minimizzare l'esposizione ai rischi derivanti dal profilo di rischio dei singoli fornitori; d) evitare o limitare le principali dipendenze da un singolo fornitore nelle reti 5G; e) promuovere un mercato diversificato, competitivo e sostenibile per le apparecchiature 5G. Tale documento, in particolare, ha evidenziato la crucialità degli operatori di rete mobile e dei loro fornitori, responsabili, questi ultimi, della fornitura del software e dell'hardware necessari per il funzionamento delle

reti ed ha identificato: 1) **8 misure strategiche**, comprendenti il rafforzamento dei poteri normativi delle autorità per l'esame dell'approvvigionamento e dello spiegamento della rete, misure specifiche per affrontare i rischi legati a vulnerabilità non tecniche (ad esempio, rischio di interferenza da parte di un paese terzo o rischi di dipendenza), nonché possibili iniziative per promuovere una catena di approvvigionamento e di valore 5G sostenibile e diversificata, al fine di evitare rischi sistemici di dipendenza a lungo termine; 2) **11 misure tecniche,** comprendenti misure per rafforzare la sicurezza delle reti e delle attrezzature 5G ed in particolare la sicurezza delle tecnologie, del software, dei processi, delle persone e dei fattori fisici.

Nel tracciare le conclusioni, il pacchetto invita gli Stati membri ad attuare misure e disporre di poteri per attenuare i rischi, rafforzando i requisiti di sicurezza per gli operatori delle reti mobili, valutando il profilo di rischio dei fornitori, applicando restrizioni adeguate ai fornitori considerati ad alto rischio, comprese le necessarie esclusioni per gli asset critici, garantendo che ogni operatore disponga di un'adeguata strategia multifornitore per evitare o limitare l'eventuale forte dipendenza da un unico fornitore ed evitare la dipendenza da fornitori considerati ad alto rischio.

La Commissione, nel manifestare la propria volontà di continuare a fornire pieno sostegno ed intraprendere tutte le azioni pertinenti nell'ambito delle proprie competenze al fine di sostenere l'attuazione del pacchetto di strumenti da parte degli Stati membri e di rafforzarne l'impatto, ha invitato questi ultimi a delineare, entro il 30 aprile 2020, azioni concrete e misurabili per attuare la serie di misure chiave raccomandate nelle conclusioni del pacchetto di strumenti dell'UE e a preparare, entro il 30 giugno 2020, una relazione del gruppo di cooperazione NIS sullo stato di attuazione in ciascuno Stato membro di tali misure chiave, in base alle relazioni presentate e al monitoraggio effettuato periodicamente, in particolare nell'ambito del gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA. Ebbene, il 24 luglio il gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, ha pubblicato una relazione sui progressi degli Stati membri nell'attuazione del toolbox sulla sicurezza 5G in cui si è fatto il punto sul livello di maturità raggiunto dai vari paesi nell'implementazione delle misure contenute nel Toolbox. Dall'adozione del pacchetto, sono stati compiuti progressi per rafforzare la sicurezza delle reti 5G con la maggioranza degli Stati membri che applica o è sul punto di applicare restrizioni nei confronti dei fornitori ad alto rischio.

L'11 maggio 2022 gli Stati membri dell'UE, con il sostegno della Commissione europea e dell'ENISA, hanno pubblicato una **relazione sulla cibersicurezza di Open RAN,** un nuovo tipo di architettura di rete 5G che, nei prossimi anni, fornirà modalità alternative di realizzazione della parte di accesso radio delle reti 5G basata su interfacce aperte e che evidentemente pone questioni specifiche in termini di sicurezza.

Su tale contesto si vanno ora ad innestare le novità introdotte dalla direttiva NIS 2 già analizzate e la procedura legislativa di adozione del Cyber Resilience Act.

CAPITOLO 2

LA CIBERSICUREZZA IN ITALIA

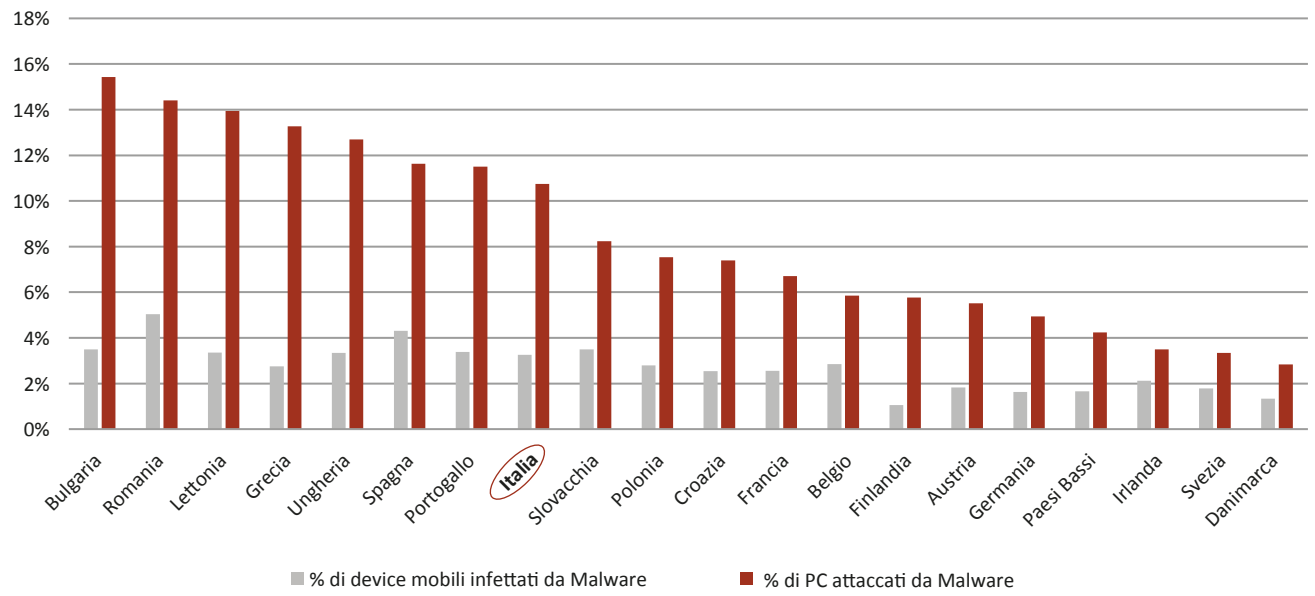
2.1 Lo stato della cibersicurezza in Italia

Per comprendere quanto il problema della criminalità informatica sia diffuso a livello capillare sia in Italia che nel resto d'Europa basta osservare gli ultimi dati pubblicati da Comparitech (aggiornati a settembre 2022), i quali stimano che l'8,47% dei computer e il 2,7% dei dispositivi mobili utilizzati all'interno dell'Unione Europea siano stati infettati da malware. Focalizzando l'attenzione sul contesto italiano è possibile notare come il nostro Paese risulti uno dei più bersagliati dai criminali informatici, infatti, **il 3,26% dei dispositivi mobili e il 10,74% dei pc utilizzati nel nostro Paese risultava essere stato infettato con un malware**. Questo dato è notevolmente superiore a quello fatto registrare da altre grandi economie europee come Germania, che presenta un 1,63% di infezioni sul mobile e 4,94% da PC, e Francia, 2,56% mobile e 6,71% PC (Fig. 2.1).

Il primato del nostro Paese per le azioni informatiche ostili trova conferma anche in un'analisi che il Politecnico di Milano ha condotto in collaborazione con il Clusit e che vede l'Italia in testa per numero di attacchi gravi (143) segnalati tra gennaio 2018 e giugno 2021, davanti a Francia (95), Germania (75) e Spagna (29) (Fig. 2.2).
D'altro canto, nonostante l'Italia presenti il triste primato tra le altre grandi economie UE per penetrazione di malware nel device e per attacchi informatici gravi, la survey condotta da Sophos (già citata nel paragrafo precedente) ha rilevato come la percentuale di **imprese colpite da ransomware** nel nostro Paese[9] sia sensibilmente più bassa rispetto ai principali competitor dell'Unione (Fig. 2.3). In particolare, l'incidenza dei ransomware sul totale degli intervistati si è attestata a quota 61%: un dato che, seppur estremamente elevato e preoccupante, risulta inferiore rispetto a quanto rilevato in Germania (67%), in Spagna (71%) e in Francia (73%).

Fig. 2.1: Percentuale di devices che hanno subito attacchi informatici per area geografica (2022)

Fonte: Which countries have the worst (and best) cybersecurity? - Comparitech, settembre 2022



9 Il campione di imprese intervistate in Italia ammonta a 200 unità.

Fig. 2.2: Attacchi gravi tra gennaio 2018 a giugno 2021, per Paese

Fonte: Clusit – PoliMi (giugno 2021)

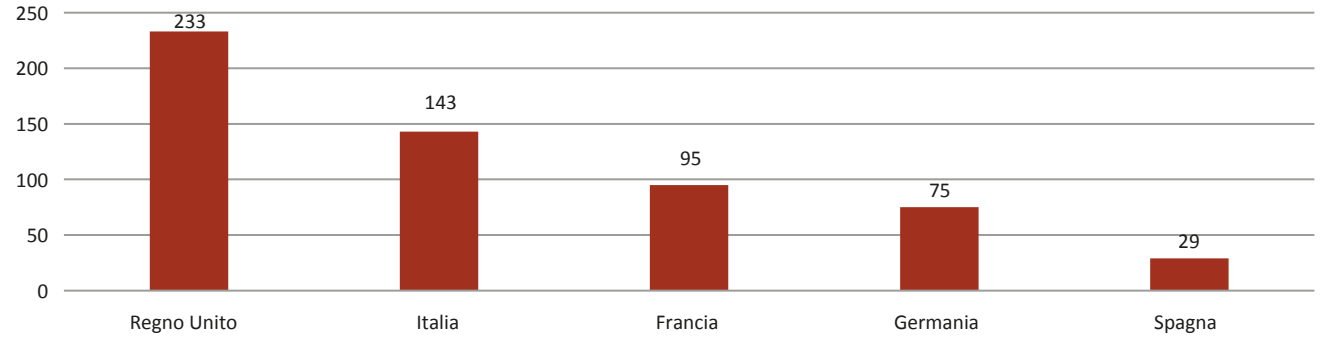
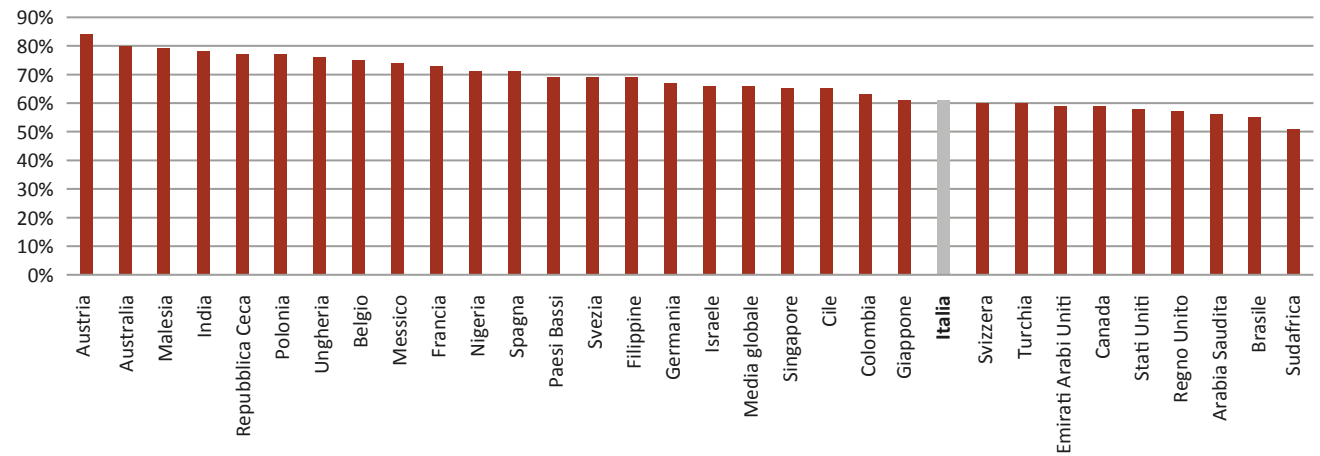


Fig. 2.3: Percentuale di imprese attaccate con un ransomware per Paese (2022)

Fonte: Sophos, The State of Ransomware 2022

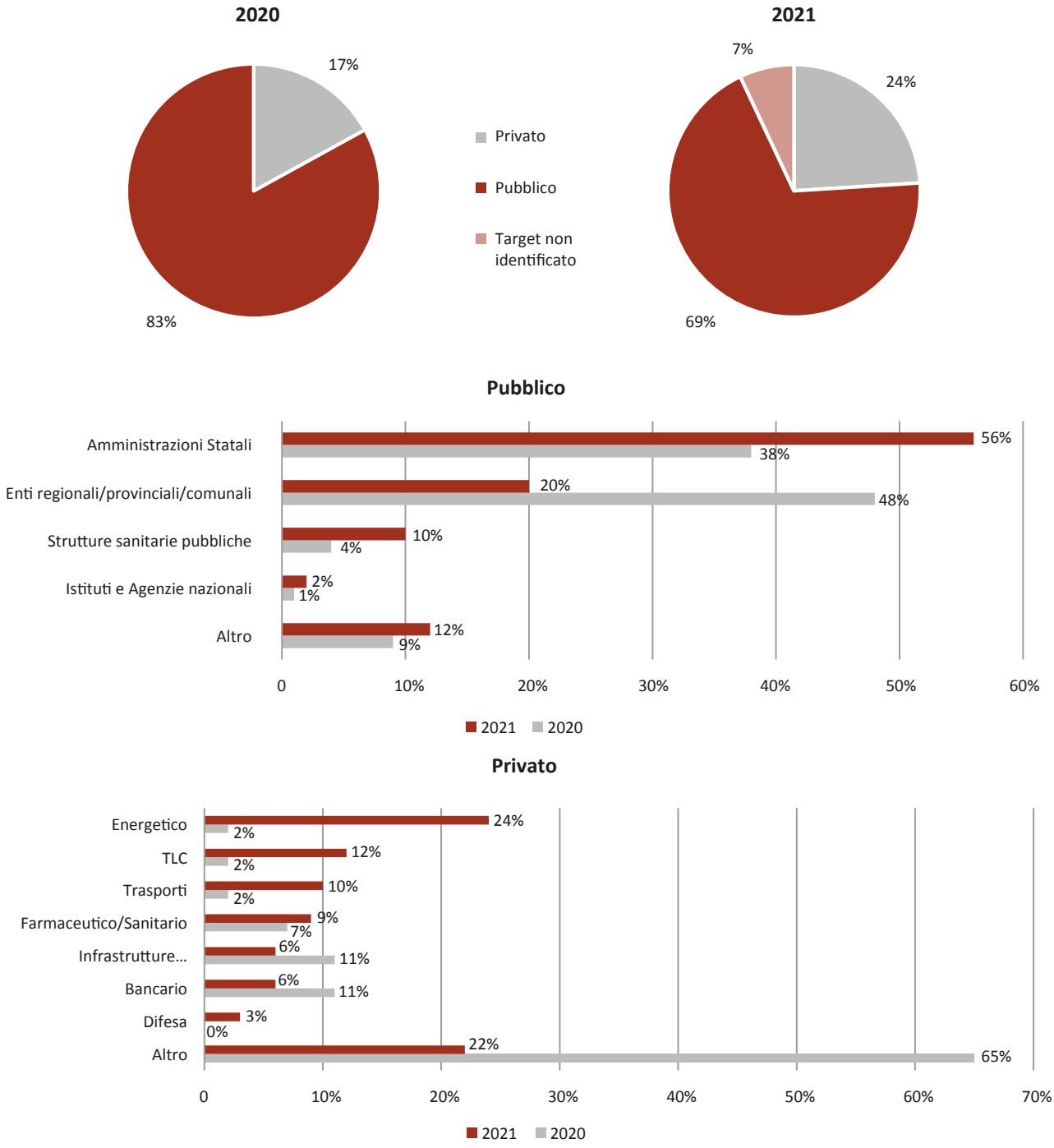


Concentrando l'attenzione sul panorama italiano, l'ultima "Relazione sulla politica dell'informazione per la sicurezza"[10] restituisce una fotografia di quali siano le Pubbliche Amministrazioni e i settori industriali più colpiti. Per quanto concerne le prime, si osserva come queste nel 2021 siano risultate l'obiettivo privilegiato dei cybercriminali, attirando il 69% delle azioni ostili accertate in Italia (Fig. 2.4): un dato che, seppure in calo, rende l'idea dell'importanza di innalzare le difese cibernetiche delle amministrazioni pubbliche. Gli enti più bersagliati risultano le **amministrazioni statali, divenute il target di più della metà degli attacchi individuati (56%),** precedendo gli enti locali (20%). Inoltre, è proseguito anche nel 2021 il preoccupante trend riguardante le azioni malevole dirette a **strutture sanitarie pubbliche**, **passate dal 4% al 10%,** cresciute

10 Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza 2021", pubblicata a febbraio 2022.

Fig. 2.4: Attacchi informatici critici avvenuti in Italia per tipologia di target ed esito

Fonte: Relazione sulla politica dell'informazione per la sicurezza 2021, Presidenza del Consiglio dei Ministri



quindi di 6 p.p. dopo una crescita del 3% già registrata nel periodo di osservazione precedente, coincidente con lo scoppio della pandemia di Covid-19.

Riguardo al **settore privato**, i soggetti che hanno subìto il maggior numero di azioni ostili sono quelli del **comparto energetico**, la cui quota è passata dal 2% del 2020 al **24% del 2021**, seguiti dalle **TLC** che si sono attestate sul **12%** (+10 p.p.). A crescere sono anche gli attacchi sferrati verso le organizzazioni appartenenti al settore dei trasporti (+8 p.p.) e al farmaceutico/sanitario (+2 p.p.). Tendenza opposta è invece quella fatta registrare dalle infrastrutture digitali/servizi IT e dal bancario, che passano entrambi dall'11% al 6%.

La situazione appena descritta appare ancor più allarmante se si considera che, secondo gli ultimi dati diffusi da ENISA, le organizzazioni italiane – e in particolare OSE/DSP – siano solo al 19° posto nella UE per quota del budget IT investita in sicurezza dell'informazione (Fig. 2.5). Osservando i dati si apprende infatti che, se da un lato le **aziende italiane risultano terze per volume di spesa in valore assoluto (€4 milioni)**, in termini percentuali queste investono **solo il 6,6% del proprio budget IT in sicurezza, contro una media UE del 7,2%**.

A tal proposito, è interessante osservare come, secondo le ultime previsioni di mercato diffuse da Statista, i ricavi del comparto della sicurezza informatica in Italia sembrerebbero destinati a crescere notevolmente nei prossimi anni (Fig. 2.6). Nel dettaglio, i ricavi del settore cybersecurity dovrebbero aumentare del 25% entro i prossimi tre anni, passando dagli €1,75 miliardi del 2022 ai €2,18 miliardi previsti per il 2026.

Infine, è interessante notare come tutte le componenti dei ricavi (servizi IT, software e hardware) dovrebbero presentare un andamento positivo nei prossimi anni: i servizi IT appaiono quelli con il maggiore potenziali di crescita entro il 2026 (+33%), il che sembra evidenziare il graduale spostamento anche della sicurezza informatica verso un modello "*as a service*", in cui il servizio viene erogato da un provider in modalità cloud.

Fig. 2.5: Budget medio investito in sicurezza dell'informazione da parte degli OSE/DSP per Stato membro (2021)

Fonte: ENISA, NIS Investments Report, novembre 2022

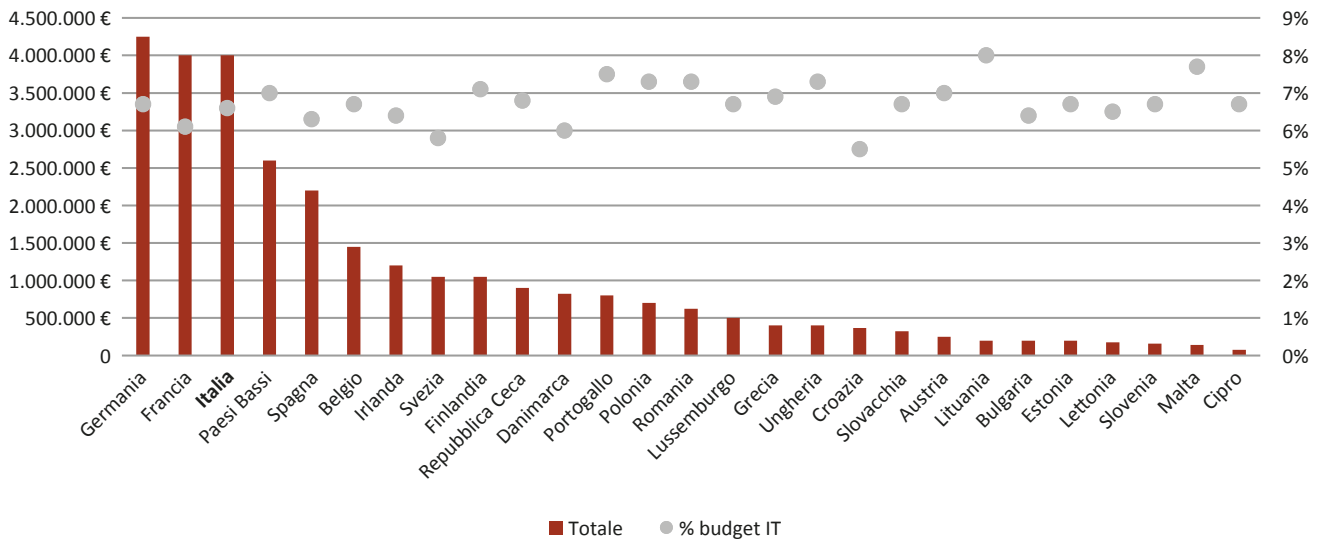
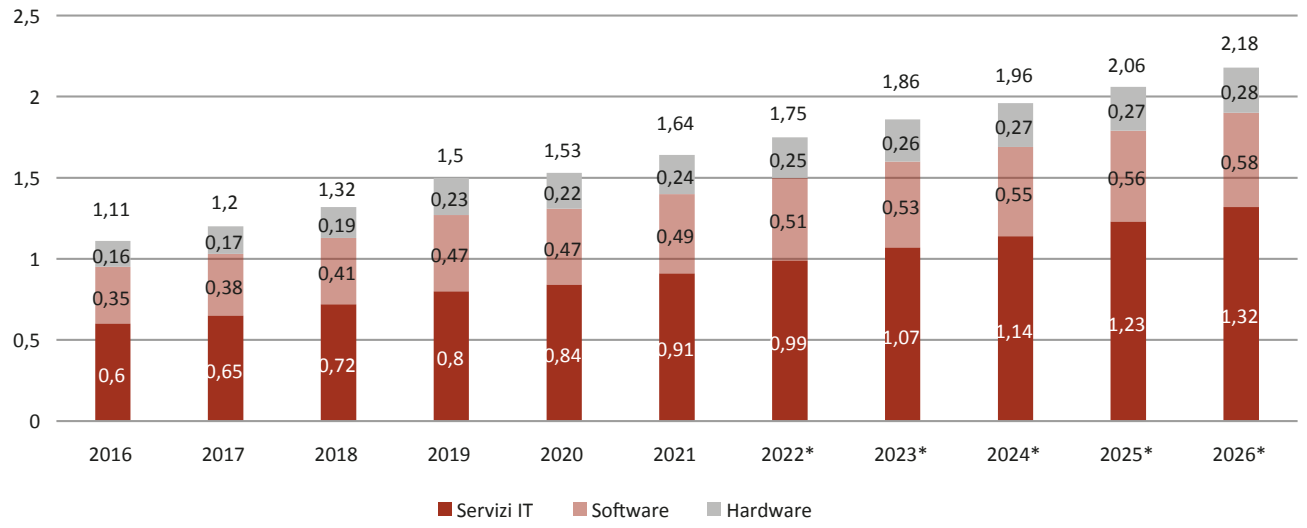


Fig. 2.6: Ricavi della cybersecurity in Italia (€ miliardi)

Fonte: Statista Technology Market Outlook (giugno 2022)



Note: dati previsionali

2.2 Il quadro normativo nazionale ed il sistema di governance della cibersicurezza

2.2.1. Dall'istituzione dell'ACN all'adozione della strategia nazionale di cibersicurezza

La centralità assunta dal dominio cibernetico porta con sé, come evidenziato nel paragrafo precedente, un incremento dei rischi legati alla sicurezza, cui si accompagna la necessità, ormai davvero ineludibile, di rafforzare le misure ed accrescere gli investimenti per prevenire e contrastare gli illeciti, sempre più aggressivi e sofisticati, che imprese, cittadini e pubbliche amministrazioni si trovano a dover affrontare.

Partendo da tale constatazione, il **Piano nazionale di ripresa e resilienza** (PNRR) individua la sicurezza cibernetica come uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo". Tale investimento, in particolare, mira alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica di cui si dirà nel paragrafo 2.2.3., e può contare su uno stanziamento pari a ca. 620 milioni di euro, di cui 241 per la creazione di una infrastruttura per la cybersicurezza, 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC e 15 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato. Guardando alle aree di intervento, il PNRR indica il rafforzamento dei presidi di front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse nazionale, il consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'hardware e del software, il potenziamento del personale delle forze di polizia dedicate alla prevenzione e investigazione del

crimine informatico e l'implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.
Il Piano ha previsto, inoltre, l'individuazione di un nuovo organismo per la sicurezza informatica nazionale per guidare l'architettura nazionale generale della cybersicurezza.
Tale previsione ha ricevuto attuazione con la pubblicazione, il 14 giugno 2021, del **D.L. n. 82/2021 recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*"** (convertito con la legge 4 agosto 2021, n. 109) che ha sancito l'inizio di una nuova era per la cybersicurezza a livello nazionale. Ed infatti, partendo dalla constatazione della crescente centralità assunta dalla cybersecurity e della complessità del quadro normativo e regolamentare di riferimento, frutto di una serie spesso confusa e disordinata di interventi che si sono succeduti nel tempo e che hanno frazionato tra diverse autorità – 23 – le competenze in materia di cybersicurezza, è stata istituita l'Agenzia, alla quale sono state attribuite la grandissima parte delle competenze in materia.
Il D.L. in questione, in particolare, pur attribuendo in via esclusiva al **Presidente del Consiglio** l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, l'adozione della strategia nazionale di cybersicurezza (sentito il Comitato interministeriale per la cybersicurezza – CIC), la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale, ha definito un nuovo assetto in materia di cibersicurezza che trova nell'**Agenzia** il fulcro. Quest'ultima, invero, è 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, è chiamata a predisporre la strategia nazionale di cibersicurezza, ad assicurare, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, il coordinamento tra i soggetti pubblici coinvolti in materia di cibersicurezza a livello nazionale, promuovere 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, operare 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 cibersicurezza, accreditare le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, assumere 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 di cui si dirà nei paragrafi successivi, 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), acquisire 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 svolgere 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 cibersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti.
Se ACN è dunque la principale autorità preposta a livello nazionale ed internazionale alla salvaguardia della cybersicurezza, il decreto, 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 cibersicurezza, 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 cibersicurezza nazionale, esercitare l'alta sorveglianza sull'attuazione della strategia nazionale di cibersicurezza, 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 cibersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cibersicurezza 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 cibersicurezza nazionale.

Presso l'Agenzia è poi costituito il **Nucleo per la cybersicurezza**, a supporto del Presidente del Consiglio dei ministri nella materia della cibersicurezza, 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 cibersicurezza 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 cibersicurezza, 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, nel dicembre 2021 sono stati pubblicati i regolamenti di organizzazione e funzionamento, del personale e di contabilità, mentre nel febbraio 2022 è stata avviata la fase di primo reclutamento che si concluderà a dicembre e che porterà a 300, entro la fine del 2023, le unità a supporto delle attività dell'ACN.

Il **regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale**, in particolare, è 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 (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.

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 di organizzazione e funzionamento ha previsto l'istituzione del **Comitato tecnico-scientifico** (CTS) i cui componenti – 9, nominati lo scorso giugno – 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 cybersicurezza, 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).

La struttura organizzativa dettata dal decreto in esame include il **Computer Security Incident Response Team nazionale** (il "CSIRT Italia"), con funzione di prevenzione, monitoraggio, rilevamento, analisi e risposta ad incidenti cibernetici, il **Centro di Valutazione e Certificazione Nazionale** (CVCN), che si occuperà – con piena operatività assicurata dal 30 giugno 2022 – di verificare la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT in uso nelle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese ed il **Centro Nazionale di Coordinamento in materia di cybersicurezza nell'ambito industriale, tecnologico e della ricerca**.

L'attività dell'ACN è stata immediatamente densa di iniziative non solo per quanto attiene il trasferimento delle funzioni e competenze ad essa attribuite dalla legge istitutiva – relative al CSIRT Italia, all'istituzione del Nucleo per la cybersicurezza, all'attuazione della legge sul Perimetro di sicurezza nazionale cibernetica e al Punto unico di contatto per la Direttiva NIS dell'UE (settembre 2021) nonché di MISE e AgID (rispettivamente a giugno ed ottobre 2022) – ma anche e soprattutto per l'adozione di documenti di rilevanza strategica straordinaria per l'ecosistema nazionale. Si tratta, in particolare, della **Strategia Cloud Italia**, documento sintetico di indirizzo strategico per l'implementazione e il controllo del cloud nella Pubblica amministrazione, pubblicato nel settembre 2021 cui ha fatto seguito, a gennaio 2022, la definizione del modello per la classificazione dei dati e dei servizi della PA e i requisiti per le infrastrutture digitali e per i servizi cloud destinati a trattare dati e servizi strategici, critici e ordinari e della **strategia nazionale di cybersicurezza 2022-2026 ed il relativo piano di implementazione** presentati il 27 maggio scorso.

Tale strategia, in particolare, partendo dalla constatazione della crescente interconnessione dei servizi nello spazio cibernetico, della sempre maggiore fluidità del confine tra la dimensione digitale e quella reale e di una ancora troppo limitata consapevolezza dei rischi di sicurezza (cui si accompagna, peraltro, una crescente complessità degli attacchi), pone in luce l'esigenza di porre la cybersicurezza al centro della trasformazione digitale anche nella logica di conseguire l'autonomia nazionale strategica e definire, dunque,

adeguate strategie di cibersicurezza volte a pianificare, coordinare e attuare misure tese a rendere il Paese sicuro e resiliente anche nel dominio digitale ed assicurare la fiducia dei cittadini nella possibilità di sfruttarne i relativi vantaggi competitivi, nella piena tutela dei diritti e delle libertà fondamentali.

Per realizzare tale macro-obiettivo, la strategia fa ricorso a due leve: da un lato, mettere in sicurezza infrastrutture, sistemi e informazioni dal punto di vista tecnico, attraverso un ripensamento della cibersicurezza da intendersi non come un costo bensì come un investimento, un vero e proprio fattore abilitante per lo sviluppo e la competitività del sistema paese; dall'altro, accompagnare il progresso culturale ad ogni livello della società, verso un approccio "security-oriented", indispensabile per tutelare il sistema valoriale e democratico nazionale.

Centrale, al di là degli attori istituzionali a diverso titolo chiamati ad esercitare competenze in materia cyber, l'approccio "whole-of-society" secondo cui a svolgere un ruolo attivo sono chiamati tutti gli attori e, dunque, gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza, quest'ultima concepita dunque non più solo come un indiretto beneficiario delle misure contemplate nel Piano di implementazione della strategia, ma anche protagonista nell'implementazione della strategia stessa, nell'idea che l'obiettivo ultimo della sicurezza cibernetica nazionale possa essere raggiunto solo attraverso un gioco di squadra che veda fattivamente coinvolte tutte le componenti socio-economiche.

Per quanto concerne le sfide da affrontare, la strategia ne mette a fuoco cinque:

1. assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione e del tessuto produttivo, al fine di assicurare servizi sicuri ed incentivarne l'utilizzo da parte dei cittadini;
2. anticipare l'evoluzione della minaccia cyber, prevedendo, prevenendo ed arginando il più possibile gli impatti di eventuali attività cyber offensive;
3. contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida;
4. gestire le crisi cibernetiche, favorendo il coordinamento tra tutti i soggetti pubblici e privati interessati e garantire una risposta pronta in caso di eventi cyber sistemici;
5. perseguire l'autonomia strategica nazionale ed europea nel settore del digitale con riguardo, in particolare, alla produzione di software ed alle cc.dd. Emerging and Disruptive Technologies (es. IA e quantum computing) attraverso cui detenere un controllo diretto sui dati conservati, elaborati e trasmessi mediante tali tecnologie.

Se queste sono le sfide, con riferimento, invece, agli **obiettivi**, la strategia ne individua tre, protezione, risposta e sviluppo, per ciascuno dei quali declina una serie di misure – complessivamente 82 – con relativi attori responsabili, prevedendo inoltre la definizione di metriche e di Key Performance Indicator (KPI), quali strumenti che consentano di misurarne l'effettiva attuazione ed efficacia.

In particolare, in relazione all'obiettivo "**protezione**", il piano di implementazione individua i seguenti macro-temi con correlate misure: a) scrutinio tecnologico, rispetto al quale le 4 misure individuate sono tese a rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro, all'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati, allo sviluppo dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa e all'attivazione, presso ACN, di un nucleo ispettivo centrale e delle omologhe unità ispettive presso i predetti ministeri; b) definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente. In tale ambito, la strategia

evidenzia la necessità di supportare lo sviluppo degli schemi di certificazione in materia di cibersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo, introdurre norme giuridiche che valorizzino l'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione e nelle gare pubbliche, adottare linee guida sulla cybersecurity per le PP.AA. e promuovere iniziative di sensibilizzazione, tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale e definire una politica nazionale sulla divulgazione coordinata di vulnerabilità; c) conoscenza approfondita del quadro della minaccia cibernetica, attraverso la realizzazione di un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale; d) potenziamento capacità cyber della Pubblica Amministrazione, coordinando interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini, qualificando i servizi cloud per la P.A. e facilitando la migrazione dei dati e dei servizi sul cloud; e) sviluppo di capacità di protezione per le infrastrutture nazionali, promuovendo lo sviluppo di procedure, processi e sistemi di monitoraggio e controllo delle configurazioni BGP nazionali, l'implementazione di una infrastruttura di risoluzione DNS nazionale al servizio degli operatori pubblici e privati, lo sviluppo e l'implementazione di un servizio nazionale di gestione delle copie dei backup "a freddo" e l'utilizzo delle migliori pratiche di gestione dei domini di posta elettronica della P.A.; f) promozione dell'uso della crittografia, sviluppando tecnologie/sistemi di cifratura nazionale in ambito non classificato e promuovendo l'uso della crittografia in ambito non classificato, quale impostazione predefinita e comunque fin dalla fase di progettazione di reti, applicazioni e servizi; g) definizione e implementazione di un piano di contrasto alla disinformazione online, mediante un'azione di coordinamento nazionale per prevenire e contrastare – anche attraverso campagne informative – la disinformazione online.

Per quanto concerne, invece, l'obiettivo "**risposta**", il piano individua una serie di iniziative riconducibili ai seguenti ambiti tematici: a) sistema di gestione crisi nazionale e transnazionale, rispetto a quale la strategia evidenzia l'importanza di sviluppare un sistema di coordinamento continuativo di tutte le Amministrazioni che compongono il NCS, contribuire alla fattiva ed efficace attivazione dei meccanismi europei di risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala, agevolare modalità di notifica unitaria degli incidenti di sicurezza cibernetica allo CSIRT ed assicurare il periodico aggiornamento delle procedure operative relative alle misure di risposta connesse ai vari scenari della minaccia cyber per le determinazioni del Presidente del Consiglio; b) servizi cyber nazionali per i quali realizzare un sistema di raccolta e analisi HyperSOC per aggregare, correlare ed analizzare eventi di sicurezza di interesse stipulando apposite convenzioni con gli Internet Service Provider (ISP), creare un'infrastruttura di High Performance Computing dedicata alla cybersecurity nazionale per il potenziamento dei servizi cyber nazionali dell'Agenzia e sviluppare strumenti di simulazione, basati sull'Intelligenza Artificiale e il machine learning, per supportare le fasi di prevenzione, scoperta, risposta e predizione degli impatti di attacchi cyber di natura sistemica, creare una rete di CERT settoriali integrata con lo CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati, creare un ISAC presso l'ACN, con il compito di coordinare la collazione e l'analisi di informazioni operazionali e strategiche a maggior valor aggiunto prodotte dai vari servizi cyber nazionali e promuovere la creazione di ISAC settoriali integrati con l'ISAC dell'ACN; c) esercitazioni di cybersicurezza da

promuovere sia a livello nazionale che internazionale al fine di accrescere la resilienza del Paese; d) definizione del posizionamento e della procedura nazionale in materia di attribuzione mediante la definizione di un documento sul posizionamento e sulla procedura nazionale in materia di attribuzione; e) contrasto al cybercrime, attraverso il potenziamento delle capacità di prevenzione e contrasto al crimine informatico da parte della Polizia Postale e delle comunicazioni e delle Forze di polizia anche mediante specifiche attività di addestramento, assicurando una puntuale rilevazione statistica dei dati relativi ai reati informatici e quelli favoriti dall'informatica, acquisiti dalle Forze di polizia e dall'Autorità giudiziaria, per agevolarne l'analisi, anche al fine di eventuali integrazioni normative e rafforzando ulteriormente la cooperazione internazionale e lo scambio informativo in materia di contrasto al crimine informatico; f) rafforzamento della capacità di deterrenza in ambito cibernetico.

Con riguardo, infine, all'obiettivo "sviluppo", la strategia si sofferma sulle questioni di seguito indicate: a) Centro nazionale di coordinamento. Rispetto a tale topic, la strategia individua una serie di misure che si sostanziano nel realizzare e promuovere la partecipazione a progetti volti a supportare lo sviluppo di capacità, tecnologie e infrastrutture di cibersicurezza, mediante l'accesso ai pertinenti programmi di finanziamento dell'UE e supportare l'operatività dei Digital Innovation Hub e favorirne le sinergie con il Centro nazionale di coordinamento, con i Centri di competenza ad alta specializzazione e con i Cluster tecnologici, per agevolare il trasferimento tecnologico verso le PMI; b) sviluppo di tecnologia nazionale ed europea, specie nei segmenti più innovativi e sensibili (ad es. cloud ed edge computing, tecnologie basate su blockchain, spazio, ecc.), attraverso l'avvio di dedicate progettualità; c) realizzazione di un "parco nazionale della cybersicurezza", che ospiti le infrastrutture necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali, dotato di una struttura "diffusa", con ramificazioni distribuite sull'intero territorio nazionale; d) sviluppo industriale, tecnologico e della ricerca, promuovendo l'internazionalizzazione delle imprese italiane che offrono prodotti e servizi di cybersecurity, implementando un Piano per l'industria cyber nazionale volto a sostenere imprese e startup per la progettazione e la realizzazione di prodotti e servizi ad alta affidabilità, incoraggiando la creazione di Product Security Incident Response Team (PSIRT) da parte degli operatori privati, per accrescere le loro capacità di gestire le vulnerabilità di prodotti ICT e per contribuire all'adozione di policy di divulgazione coordinata di vulnerabilità; e) impulso all'innovazione tecnologica e alla digitalizzazione, favorendo la ricerca e lo sviluppo, specialmente nelle nuove tecnologie e promuovendo l'inclusione dei principi di cybersicurezza, promuovendo la digitalizzazione e l'innovazione della P.A. e del sistema produttivo nazionale.

Se questi sono gli obiettivi, ampio spazio e numerose misure sono state declinate nella strategia rispetto ai **fattori abilitanti** e, nello specifico a formazione e cooperazione**.** Rispetto al primo, la formazione, la strategia individua numerose misure tese, in particolare, a potenziare lo sviluppo di percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity praticamente in ogni ordine e grado, anche mediante investimenti orientati alla formazione del personale docente, al fine di allineare l'offerta educativa alla domanda del mercato del lavoro, attivare Istituti Tecnici Superiori (ITS) con percorsi di cybersecurity che prevedano almeno un 30% del tempo dedicato ad attività di tirocinio, rafforzare programmi di alternanza scuola-lavoro, favorire programmi di scambio a livello europeo ed internazionale, elaborare uno strumento di formazione e sensibilizzazione online, rivolto alla cittadinanza in generale, che consente, al termine del percorso, di auto-testare le competenze e le sensibilità acquisite e di ottenere un attestato,

prevedere incentivi per lo sviluppo di startup operanti nel settore della cybersecurity e partnership pubblico-privato con aziende di cybersecurity a conduzione femminile, potenziare la formazione del personale diplomatico così da rafforzare le capacità di cyber diplomacy e prevedere per tutti i lavoratori pubblici e privati, inclusi quelli di livello apicale, il costante aggiornamento professionale, anche attraverso percorsi di formazione in materia di sicurezza cibernetica. Con riguardo, invece, alla **cooperazione,** la strategia persegue il fine di rafforzare il ruolo dell'Italia nei consessi multilaterali impegnati in ambito sicurezza cibernetica e nella definizione di policy/regolamentazioni in materia di cibersicurezza, realizzare un ecosistema nazionale volto a sviluppare capacità di capacity building a favore di Paesi terzi ed istituire tavoli operativi permanenti con i soggetti Perimetro, suddivisi per settore, che svolgano a livello operativo specifici compiti in materia di prevenzione, allertamento, risposta agli incidenti e ripristino.

Centrale anche il tema delle **risorse**, rispetto alle quali la strategia annuncia, oltre agli strumenti finanziari già assegnati alle Amministrazioni con competenza in materia cyber, appositi fondi previsti di anno in anno dalle leggi di bilancio, per supportare specifici progetti di interesse. A ciò si aggiungeranno i finanziamenti che l'Agenzia sarà chiamata a gestire in quanto Centro Nazionale di Coordinamento (NCC), che confluendo nella rete dei centri nazionali di coordinamento, consentirà al paese di accedere ai finanziamenti provenienti dai programmi Orizzonte Europa ed Europa Digitale. Rispetto al PNRR, la stessa strategia richiama la Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo" ed in particolare l'investimento 1.5 "Cybersecurity", sopra richiamato, per complessivi 623 milioni di euro, rimesso all'ACN quale Soggetto Attuatore e che prevede la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio cyber, con strette connessioni, a livello nazionale e internazionale, con tutti i principali partner della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia.

2.2.2. L'evoluzione della disciplina sul Golden Power. Gli ambiti di intervento e le semplificazioni introdotte

La disciplina Golden Power trova origine e fondamento nel **decreto-legge 15 marzo 2012, n. 21** (convertito, con modificazioni, in legge 11 maggio 2012, n. 56) che, negli anni, è stato oggetto di numerosissime modifiche ed integrazioni, anche su spinta europea, tutte orientate ad estendere e/o rafforzare l'esercizio dei poteri speciali. Ed infatti, il **D.L. 25 marzo 2019, n. 22** (convertito, con modificazioni, dalla legge n. 41 del 20 maggio 2019), ha introdotto, nel D.L. n. 21 del 2012, l'articolo 1-bis, che disciplina l'esercizio dei poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G, mentre il **D.L. 21 settembre 2019, n. 105** (convertito, con modificazioni, dalla legge n. 133 del 18 novembre 2019) ha esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori strategici, coordinandolo con l'attuazione del Regolamento 2019/452 in materia di controllo degli investimenti esteri diretti nell'Unione europea. Da ultimo, il **D.L. n. 21/2022** (convertito con legge 20 maggio 2022, n. 51), recante "Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina", nel Titolo IV ha dedicato il Capo I al Golden Power, introducendo una serie di importantissime novità che di fatto hanno ridisegnato la disciplina sui poteri speciali.

Tralasciando la puntuale analisi delle varie modifiche che si sono succedute nel tempo e soffermando dunque l'attenzione sull'impianto normativo vigente, gli ambiti di intervento del Golden Power sono tre: 1) difesa e sicurezza nazionale; 2) tecnologia 5G; 3) energia, trasporti, comunicazioni e nuovi settori di cui al Reg. 2019/452.

Con riguardo alle **imprese che svolgono attività di rilevanza strategica per il sistema di difesa e sicurezza**

nazionale (così come individuate dal DPCM 6 giugno 2014 n. 108), il Governo ha il potere di imporre specifiche condizioni relative alla sicurezza degli approvvigionamenti, alla sicurezza delle informazioni, ai trasferimenti tecnologici, al controllo delle esportazioni nel caso di acquisto, a qualsiasi titolo, di partecipazioni (lett. a), esercitare il veto all'adozione di specifiche delibere dell'assemblea o degli organi di amministrazione (lett. b), opporsi all'acquisto di partecipazioni da parte di un soggetto diverso dallo Stato italiano, enti pubblici italiani o soggetti da questi controllati, qualora l'acquirente venga a detenere un livello della partecipazione al capitale con diritto di voto in grado di compromettere nel caso specifico gli interessi della difesa e della sicurezza nazionale (lett. c).

Al fine di consentire l'eventuale esercizio dei poteri da parte del Governo, nelle ipotesi sub a), b) e c) è prevista una notifica alla Presidenza del Consiglio, chiamata ad esercitare i propri poteri entro 45 gg. dalla ricezione della stessa notifica, ferma restando la possibilità di richiedere informazioni all'impresa notificante (con conseguente sospensione di tale termine, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni, termine che sale a 20 gg nel caso di informazioni richieste a soggetti terzi). In caso di incompletezza della notifica, il termine di quarantacinque giorni decorre invece dal ricevimento delle informazioni o degli elementi che la integrano. Decorsi i predetti termini si configura il silenzio-assenso e pertanto l'operazione può essere effettuata. Il Dipartimento per il coordinamento amministrativo (DICA) della Presidenza del Consiglio dei Ministri è l'ufficio competente per la gestione dei procedimenti amministrativi per le notifiche presentate e svolge attività di coordinamento, attività propedeutiche all'esercizio dei poteri speciali e attività istruttorie. Lo stesso art. 1 prescrive, infine, un aggiornamento triennale dei decreti di individuazione delle attività di rilevanza strategica per il sistema di difesa e di sicurezza nazionale[11].

Per quanto concerne, invece, l'esercizio dei golden powers rispetto alla **tecnologia 5G**, il riferimento normativo, introdotto per la prima volta ad opera del D.L. 25 marzo 2019, n. 22 (c.d. Decreto Brexit), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41 e successivamente modificato dal D.L. 21/2022, è contenuto nell'art. 1 *bis,* rubricato "*Poteri speciali inerenti ai servizi di comunicazione elettronica a banda larga con tecnologia 5G, basati sulla tecnologia cloud e altri attivi*". Tale disposizione, in particolare, fermi restando gli obblighi previsti dalla normativa sul perimetro di sicurezza nazionale cibernetica, prescrive alle imprese che, anche attraverso contratti o accordi, intendano acquisire, a qualsiasi titolo, beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività descritte al comma 1, ovvero componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, la notifica alla Presidenza del Consiglio dei ministri, prima di procedere alla predetta acquisizione, di un piano annuale, modificabile con cadenza quadrimestrale. Si supera, pertanto il riferimento al singolo contratto in favore di una **pianificazione annuale** che deve indicare il programma di acquisti, fornire dati dettagliati identificativi dei relativi, anche potenziali, fornitori, la descrizione dei beni, dei servizi e delle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione ed alla manutenzione, un'informativa completa sui contratti in corso e sulle prospettive di sviluppo della rete 5G, ogni ulteriore informazione funzionale a fornire un dettagliato quadro delle modalità di sviluppo dei sistemi di digitalizzazione del notificante, nonché

11 Con DPCM 6 giugno 2014, n. 108 è stato adottato il Regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale.

dell'esatto adempimento alle condizioni e alle prescrizioni imposte a seguito di precedenti notifiche, un'informativa completa relativa alle eventuali comunicazioni effettuate al CVCN, inclusiva dell'esito della valutazione, ove disponibile, e delle relative prescrizioni, qualora imposte. Tale pianificazione deve altresì contenere i contratti o gli accordi relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G già autorizzati, in relazione ai quali resta ferma l'efficacia dei provvedimenti autorizzativi già adottati. Si tratta di un intervento assolutamente rilevante che certamente semplifica e riduce gli adempimenti a carico delle imprese ma che rivela, inevitabilmente, i limiti connessi alla difficoltà di realizzare una pianificazione *ex ante* così dettagliata (che trovano comunque con correttivo nella possibilità di modifica del piano con cadenza quadrimestrale).

Tale criticità assume particolare rilevanza per lo sviluppo di **reti 5G private**, ossia quelle non offerte al pubblico, ma realizzate per beneficiare delle potenzialità della tecnologia 5G singoli enti o aziende. L'importanza di tali reti è crescente in considerazione dei benefici che le stesse offrono e che si sostanziano non solo nella nota capacità di banda e ridotta latenza tipiche del 5G, ma anche, dato il carattere privato di tali reti, nella possibilità di limitare l'accesso solo ai dispositivi autorizzati garantendo standard di privacy e sicurezza più elevati, di disporre di reti totalmente virtualizzate, automatizzate e funzionanti in maniera ottimale grazie programmi di intelligenza artificiale o di machine learning e di avere reti suddivisibili in sotto-bande da utilizzare per attività con esigenze di banda e di latenza differenti. In considerazione delle caratteristiche di tali reti e della spiccata dinamicità che caratterizza le richieste di mercato, è emersa, nel corso delle audizioni svoltesi alle Camere nell'ambito della procedura di conversione del D.L. 21/2022, che tuttavia non ha trovato accoglimento nel testo di legge, una richiesta di deroga dall'inserimento di progetti relativi a reti 5G private nel Piano annuale da notificare (eventualmente fissando una soglia economica come riferimento per poter fruire di tale opzione) e la previsione di una relazione in via consuntiva.

Tornando alla procedura per l'esercizio dei poteri speciali in relazione alla tecnologia 5G, il termine per l'esercizio del potere di veto o l'imposizione di eventuali condizioni o prescrizioni è fissato in 30 giorni dalla notifica, prorogabile di 20 gg, ulteriormente prorogabili per una sola volta di ulteriori 20 gg nei casi di particolare complessità (tale termine si sospende per una sola volta nel caso di richieste istruttorie rivolte al notificante o a soggetti terzi chiamati a dare riscontro rispettivamente entro 10 e 20 gg dalla richiesta). All'inutile decorso del termine assegnato per l'esercizio dei poteri speciali, il piano si intende approvato.

I commi da 5 a 9 stabiliscono, invece, il regime sanzionatorio applicabile alla violazione di obblighi imposti ai sensi dei precedenti commi (3% del fatturato per mancata notifica) e le ulteriori misure per garantire la piena attuazione della relativa disciplina.

La stessa disposizione rimette, infine, ad uno o più DPCM la possibilità di identificare ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud così come l'individuazione di misure di semplificazione delle modalità di notifica, dei termini e delle procedure relativi all'istruttoria ai fini dell'eventuale esercizio dei poteri in tale ambito.

Per quanto riguarda, infine, l'esercizio dei poteri speciali sugli **asset strategici nei settori dell'energia, dei trasporti e delle comunicazioni,** il riferimento normativo è contenuto nell'art. 2 del D.L. n. 21/2012 come successivamente modificato, che attribuisce ad uno o più DPCM – da adottare entro centoventi giorni dalla data di entrata in vigore della presente disposizione e da aggiornare almeno ogni tre anni – l'individuazione di reti e impianti, ivi compresi quelli necessari ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali, i beni e i rapporti di rilevanza strategica per l'interesse nazionale, anche

se oggetto di concessioni, comunque affidate, incluse le concessioni di grande derivazione idroelettrica e di coltivazione di risorse geotermiche, nei settori dell'energia, dei trasporti e delle comunicazioni. La medesima disposizione affida ad altri DPCM, da adottare secondo le medesime procedure e tempistiche – l'individuazione di settori ulteriori rispetto a quelli fissati dal Reg. 2019/452[12].

L'esercizio dei poteri speciali in tale ambito si fonda, in particolare, sulla sussistenza di una minaccia di grave pregiudizio per gli interessi pubblici relativi alla **sicurezza ed al funzionamento delle reti e degli impianti ed alla continuità degli approvvigionamenti** e concerne le delibere, gli atti e le operazioni poste in essere da società che detengono asset strategici nei settori sopraindicati.

Nei settori delle comunicazioni, dell'energia, dei trasporti, della salute, agroalimentare e finanziario, ivi incluso quello creditizio e assicurativo, sono soggetti all'obbligo di notifica anche gli acquisti, a qualsiasi titolo, di partecipazioni da parte di soggetti appartenenti all'Unione europea, ivi compresi quelli residenti in Italia, di rilevanza tale da determinare l'insediamento stabile dell'acquirente in ragione dell'assunzione del controllo della società la cui partecipazione è oggetto dell'acquisto.

Rispetto agli investimenti esteri in grado di incidere sulla sicurezza o sull'ordine pubblico, il comma 6 dell'art. 2 individua una serie di elementi da tenere in considerazione ed in particolare la circostanza che l'acquirente sia direttamente o indirettamente controllato dall'amministrazione pubblica, compresi organismi statali o forze armate, di un Paese non appartenente all'Unione europea, anche attraverso l'assetto proprietario o finanziamenti consistenti, che l'acquirente sia già stato coinvolto in attività che incidono sulla sicurezza o sull'ordine pubblico in uno Stato membro dell'UE e che vi sia un grave rischio che l'acquirente intraprenda attività illegali o criminali. A ciò si aggiunge la precisazione che i poteri speciali in tal caso siano esercitati esclusivamente sulla base di criteri oggettivi e non discriminatori in applicazione di una serie di criteri volti a verificare la sussistenza di legami fra l'acquirente e paesi terzi che non riconoscono i principi di democrazia o dello Stato di diritto, che non rispettano le norme del diritto internazionale o che hanno assunto comportamenti a rischio nei confronti della comunità internazionale e l'idoneità dell'assetto risultante dall'atto giuridico o dall'operazione a garantire la sicurezza e la continuità degli approvvigionamenti, il mantenimento, la sicurezza e l'operatività delle reti e degli impianti.

Quanto all'ambito applicativo dei poteri speciali, il D.L. 8 aprile 2020, n. 23, convertito, con modificazioni, dalla L. 5 giugno 2020, n. 40 (cd. Decreto "Liquidità") ha esteso la disciplina golden power a tutti i **settori strategici** individuati nell'art. 4.1 del Reg. n. 452/2019 e, dunque: a) **infrastrutture critiche**, siano esse fisiche o virtuali, tra cui l'energia, i trasporti, l'acqua, la salute, le comunicazioni, i media, il trattamento o l'archiviazione di dati, le infrastrutture aerospaziali, di difesa, elettorali o finanziarie (intendendo incluso, in tale espressione, il settore creditizio, bancario e assicurativo) e le strutture sensibili, nonché gli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture; b) **tecnologie critiche e prodotti c.d. dual use**, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cibersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie

12 Il Reg. n. 452/2019 ha istituito un quadro comune per il controllo (screening) degli investimenti esteri diretti nell'Unione, fornendo, all'art. 4, paragrafo 1, un elenco non tassativo dei fattori che possono essere presi in considerazione dagli Stati membri e dalla Commissione per determinare se un investimento estero incida sulla sicurezza o sull'ordine pubblico, comprendente infrastrutture critiche come l'energia, i trasporti, l'acqua, la salute, le comunicazioni, il trattamento o l'archiviazione di dati, le infrastrutture aerospaziali, di difesa, elettorali o finanziarie, nonché altri interessi strategici come la sicurezza alimentare e la libertà e il pluralismo dei media.

e le biotecnologie; c) **sicurezza dell'approvvigionamento di fattori produttivi critici**, tra cui l'energia e le materie prime, nonché la sicurezza alimentare; d) **accesso a informazioni sensibili**, compresi i dati personali, o la capacità di controllare tali informazioni; e) **libertà e pluralismo dei media**.

Successivamente, con i **DPCM n. 179 del 18 dicembre 2020** recante regolamento per l'individuazione dei beni e dei rapporti di interesse nazionale nei settori di cui all'articolo 4, paragrafo 1, del regolamento (UE) 2019/452 e **n. 180 del 23 dicembre 2020**, recante regolamento per l'individuazione degli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, entrati in vigore il 14 gennaio 2021, il Governo ha completato il quadro normativo per l'applicazione della normativa golden power, individuando gli attivi di rilevanza strategica nei settori energia, trasporti, comunicazioni e negli altri settori rilevanti ex art. 4 del Reg. n. 452/2019.

Il **decreto n. 179/2020**, in particolare, ha distinto cinque macrocategorie di beni e rapporti rilevanti ai fini dell'esercizio del controllo sugli investimenti esteri diretti: a) le **infrastrutture critiche**, definite come *"le infrastrutture essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione"*; b) le **tecnologie critiche**, ossia "*le tecnologie essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale della popolazione, nonché per il progresso tecnologico*"; c) i **fattori produttivi critici**, corrispondenti ai "*beni e i rapporti essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione*"; d) le **informazioni critiche**, vale a dire "*le informazioni essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione*"; e infine, e) le **attività economiche di rilevanza strategica**, che sono "*le attività economiche essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale della popolazione, nonché per il progresso tecnologico*". Per quanto concerne l'ambito di applicazione dei poteri speciali, a fronte dell'ampiezza dei settori sopra elencati, si precisa che, fermo l'obbligo di notifica dell'operazione, i poteri speciali di cui si applicano nella misura in cui la tutela della sicurezza e dell'ordine pubblico non sia adeguatamente garantita dalla sussistenza di una specifica regolamentazione di settore, anche di natura convenzionale, connessa a uno specifico rapporto concessorio.

Il **decreto n. 180/2020**, invece, ha sostituito il precedente DPR n. 85/2014 andando ad aggiungere, nel settore dell'energia, gli immobili fondamentali connessi all'utilizzo delle reti e delle infrastrutture legate al trasporto del gas naturale, all'approvvigionamento di energie e gas da altri Stati, alla rete nazionale di trasmissione dell'elettricità e, nel settore dei trasporti, gli spazioporti nazionali, gli interporti di rilievo nazionale e le reti stradali e autostradali di interesse nazionale. Per quanto concerne, invece, le comunicazioni (art. 3), gli asset di rilevanza strategica sono individuati nelle **reti dedicate e nella rete di accesso pubblica agli utenti finali** in connessione con le reti metropolitane, i **router di servizio e le reti a lunga distanza**, nonché negli **impianti utilizzati per la fornitura dell'accesso agli utenti finali dei servizi rientranti negli obblighi del servizio universale e dei servizi a banda larga e ultra-larga**, e nei relativi rapporti convenzionali (inclusi gli elementi dedicati, anche laddove l'uso non sia esclusivo, per la connettività, la sicurezza, il controllo e la gestione relativi a reti di accesso di telecomunicazioni in postazione fissa).

I termini per l'esercizio dei poteri speciali sono i medesimi fissati dall'art. 1 rispetto ai settori della difesa e della sicurezza nazionale.

In attuazione dell'art. 2-quater "*Misure di semplificazione dei procedimenti e prenotifica*", con **DPCM 1°**

agosto 2022, n. 133, pubblicato sulla G.U. del 9 settembre ed entrato in vigore il successivo 24 settembre scorso, è stato adottato il **Regolamento recante disciplina delle attività di coordinamento della Presidenza del Consiglio dei ministri propedeutiche all'esercizio dei poteri speciali.** Tale regolamento, in particolare, persegue il fine di semplificare la procedura di notifica e ridurre il numero di notifiche che, come si approfondirà meglio *infra,* sono passate da 83 a 496 in soli due anni. Entrando nel merito delle innovazioni introdotte, certamente la più rilevante, per l'impatto deflattivo che ad essa si accompagna, è l'introduzione dell'istituto della **prenotifica** previsto dall'art. 7 del regolamento**.** All'impresa interessata alla definizione di acquisizioni, delibere, costituzioni, o altri atti o operazioni in progetto, in particolare, è consentito trasmettere un'informativa alla Presidenza del Consiglio dei Ministri in merito a tale progetto, al fine di ricevere entro 30 giorni una pronuncia che dichiari, rispettivamente, l'applicabilità/inapplicabilità della normativa Golden Power con conseguente sussistenza/insussistenza dell'obbligo di notifica, oppure l'applicabilità della normativa Golden Power ma l'insussistenza dell'obbligo di notifica, in quanto manifestamente assenti gli estremi per l'esercizio dei poteri speciali (nel caso di applicabilità della disciplina è prevista la possibilità di adottare raccomandazioni). Dalla mancata adozione di alcuna decisione da parte del Gruppo di Coordinamento entro i 30 giorni previsti, discende per i soggetti prenotificanti l'obbligo di presentare una formale notifica.

Molto importante anche l'**intervento di semplificazione contenuto nell'art. 6** che consente al Gruppo di Coordinamento, su proposta dal Ministero responsabile dell'istruttoria e della proposta per l'esercizio dei poteri speciali, di adottare decisioni di non esercizio dei poteri speciali autonomamente, in caso di unanimità tra le amministrazioni rappresentate nello stesso Gruppo di Coordinamento e, dunque, senza la necessaria convocazione e delibera del Consiglio dei Ministri.

L'art. 8 si occupa invece della **cooperazione con la Commissione e con gli Stati membri per le notifiche relative ad investimenti esteri diretti ai sensi del Reg. 2019/452**, prevedendo la notifica alla Commissione e agli altri Stati membri, da parte del Dipartimento per il coordinamento amministrativo, anche su indicazione del Ministero responsabile per l'istruttoria, degli investimenti esteri diretti nel territorio italiano. Lo stesso Dipartimento è incaricato di raccogliere eventuali informazioni supplementari (anche attraverso audizione) e di fungere da punto di raccordo tra Commissione e Stati membri da un lato, e Presidente e componenti del Gruppo di coordinamento, dall'altro. Lo stesso regolamento declina la procedura per l'irrogazione delle sanzioni amministrative.

Da ultimo, nella logica di valutare l'impatto dell'esercizio dei poteri speciali ed apprestare interventi compensativi a sostegno delle imprese destinatarie delle relative misure, con **D.L. 5 dicembre 2022, n. 187**, **recante misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici, convertito con legge 1° febbraio 2023, n. 10**, si è tornati ad occuparsi del Golden Power prevedendo, all'art. 2, "*Misure economiche connesse all'esercizio del golden power*", la possibilità, per un'impresa che sia stata destinataria dell'esercizio dei poteri speciali, di presentare istanza al Ministero delle imprese e del made in Italy, al quale è rimessa la relativa valutazione, per l'accesso a misure di sostegno della capitalizzazione dell'impresa, idonee a consentire un rafforzamento patrimoniale, ai fini dell'accesso con priorità al Fondo per la salvaguardia dei livelli occupazionali e la prosecuzione dell'attività di impresa[13] anche tenendo conto delle segnalazioni degli enti territoriali ai fini del

13 Si tratta delle misure previste dall'art. 43 del decreto-legge 19 maggio 2020, n. 34, convertito, con modificazioni, dalla legge 17 luglio 2020, n. 77.

mantenimento della continuità operativa e dei livelli occupazionali nel loro territorio. Allo stesso Ministero è inoltre consentito, di concerto con il Ministero dell'economia e delle finanze, sempre su istanza dell'impresa notificante, chiedere di valutare con priorità la sussistenza dei presupposti per l'accesso agli interventi erogati dal patrimonio destinato (Patrimonio Rilancio), costituito ai sensi dell'art. 27, comma 1, del decreto-legge 19 maggio 2020, n. 34 convertito, con modificazioni, dalla legge 17 luglio 2020, n. 77. Nei due anni successivi all'esercizio dei poteri speciali l'impresa è infine ammessa a formulare istanza per l'accesso prioritario agli strumenti dei contratti di sviluppo e degli accordi per l'innovazione.

2.2.3. Dal completamento all'implementazione della disciplina sul perimetro di sicurezza cibernetica

Con l'adozione, il 21 settembre 2019, del **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, 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.

Per raggiungere tale obiettivo, la disciplina istitutiva del perimetro 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 e che, seppur in ritardo, è finalmente giunto a completamento. Il complesso puzzle normativo, in particolare, è frutto dei seguenti decreti:

1. **DPCM 30 luglio 2020, n. 131:** ha definito 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, sono tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge ed ha declinato 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;
2. in attuazione di quanto previsto dal DPCM appena descritto, il 25 novembre 2021 è stato adottato il **DPCM provvedimentale** con il quale è stata definita la **lista segreta degli oltre 100 soggetti pubblici e privati inclusi nel perimetro** tenuti, pertanto, a predisporre annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi essenziali e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT (Computer Security Incident Response Team) attivo presso la Presidenza del Consiglio;
3. **DPR 5 febbraio 2021 n. 54** (pubblicato sulla G.U. del 23 aprile 2021): ha definito le **procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa** (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per

l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi;

4. **DPCM 14 aprile 2021, n. 81** (pubblicato sulla G.U. dell'11 giugno 2021): contiene il regolamento in materia di **notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici,** che classifica gli incidenti e i relativi obblighi di notifica al CSIRT (con tempistiche diversificate), disciplina la notifica volontaria degli incidenti, 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 e fissa le modalità e i termini di adozione delle misure di sicurezza;
5. **DPCM 15 giugno 2021** (pubblicato sulla G.U. del 19 agosto 2021): ha individuato le **categorie di beni, sistemi e servizi ICT destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica** ed in particolare: 1) componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione); 2) componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati; 3) componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali; 4) applicativi software per l'implementazione di meccanismi di sicurezza. Lo stesso decreto prevede l'aggiornamento almeno annuale delle categorie individuate;
6. **DPCM 18 maggio 2022, n. 92** (pubblicato sulla G.U. del 15 luglio 2022): ha adottato il regolamento in materia di **accreditamento dei laboratori di prova** e di raccordi tra il CVCN, i laboratori di prova accreditati ed i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa. Tale ultimo DPCM, in particolare, nel riconoscere la possibilità di richiedere l'accreditamento al CVCN alle amministrazioni pubbliche e agli enti pubblici, nonché ai soggetti privati aventi sede legale nel territorio nazionale titolari di un laboratorio di prova, ha fissato i **requisiti generali per l'accreditamento**, richiedendo, tra l'altro, il possesso delle necessarie conoscenze, competenze ed esperienze e la disponibilità sul territorio nazionale di locali e mezzi adeguati a svolgere le attività di test. Tra i **motivi ostativi all'accreditamento**, spiccano per rilevanza le previsioni tese a scongiurare qualsiasi rischio di commistione degli interessi del laboratorio con quelli delle imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura di beni, sistemi o servizi ICT rientranti nelle categorie da sottoporre a test e la previsione contenuta al comma 5 dell'art. 9. Quest'ultima, infatti, vieta l'accreditamento *"ove sussistano motivi ostativi inerenti alla sicurezza della Repubblica"* e individua, tra gli elementi oggetto di valutazione, la circostanza che il soggetto privato richiedente sia controllato, direttamente o indirettamente, da persone fisiche o giuridiche, incluse amministrazioni pubbliche, che abbiano la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale fuori dal territorio nazionale ovvero sia direttamente o indirettamente sottoposto all'influenza di dette persone fisiche o giuridiche, anche attraverso l'erogazione di finanziamenti consistenti.

Il decreto in esame ha poi puntualmente indicato i contenuti della **domanda di accreditamento** distinguendo a seconda della natura pubblica o provata del richiedente ed ha individuato le fasi della procedura che vede **protagonista il CVCN**. È quest'ultimo, infatti, che svolge le verifiche preliminari, opera la verifica tecnico documentale richiedendo eventuali integrazioni, delega la visita ispettiva e la verifica della capacità tecnica del laboratorio di prova di eseguire i test per i quali ha richiesto l'accreditamento, acquisisce il verbale redatto all'esito dell'ispezione, trasmette tutta la documentazione alla commissione di accreditamento per il rilascio del relativo parere e, in caso di esito positivo dello stesso, rilascia al richiedente il certificato di accreditamento, che ha durata triennale ed è rinnovabile. Il tutto, entro 180 gg. dalla ricezione da parte del CVCN della domanda di accreditamento. Allo stesso CVCN è affidata, tra le altre funzioni, quella di stabilire le metodologie di test, la vigilanza sull'attività dei LAP nel corso delle attività di test, la redazione e l'aggiornamento periodico della lista dei beni, sistemi e servizi ICT oggetto di valutazione, per i quali sia stato emesso un rapporto di prova, la cura dei raccordi con i LAP e i CV, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio, la vigilanza sull'attività dei LAP e la verifica del mantenimento dei requisiti da parte degli stessi, l'eventuale sospensione o revoca ed il rinnovo dell'accreditamento (ove richiesto). Il CVCN, i CV e i LAP, al verificarsi di un incidente sulle reti, sui sistemi informativi e sui servizi informatici di pertinenza deputati allo svolgimento delle funzioni oggetto dell'accreditamento, sono chiamati a notificare al CSIRT secondo le modalità dallo stesso indicate entro il termine di sei ore dal momento in cui sono venuti a conoscenza dell'incidente.

L'adozione dell'ultimo DPCM, consentendo la creazione di una rete strutturata di LAP, rappresenta un passo avanti importante per il potenziamento della resilienza delle infrastrutture digitali e per la realizzazione delle misure previste dal piano di implementazione della strategia nazionale di cybersicurezza[14].

Con provvedimento dell'11 agosto 2022 l'ACN ha approvato le **determinazioni tecniche** previste dal Regolamento in materia di accreditamento dei laboratori di prova, fissando per le varie aree di accreditamento, i requisiti tecnici e logistici, le misure di sicurezza informatica per i LAP, i requisiti di competenza ed esperienza, le modalità di notifica delle limitazioni di operatività superiori a 24 ore e di comunicazione e raccordo tra il CVCN e i LAP.

È dunque giunto a completamento il complesso puzzle normativo sul perimetro di sicurezza ed il quadro che emerge è il seguente: i soggetti pubblici e privati che offrono tali servizi o svolgono funzioni essenziali e che sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici (interno, difesa, spazio e aerospazio, energia, telecomunicazioni,

14 Ci si riferisce, in particolare alle seguenti misure: a) Misura #1: Rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro e per l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati; b) Misura #2: Sviluppare le capacità dei centri di valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza; c) Misura #5: Supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato; d) Misura #8: Introdurre norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale; e) Misura #53: Promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.

economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro) dalle Amministrazioni competenti nei rispettivi settori, sono tenuti a predisporre annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT attivo presso la Presidenza del Consiglio. Tali soggetti, inoltre, sono tenuti a comunicare al CVCN l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici" e rientranti nelle categorie sopra descritte ed il CVCN, entro un tempo massimo di 60 giorni dalla comunicazione, può indicare al soggetto incluso nel perimetro eventuali condizioni a cui i fornitori dovranno attenersi e test di hardware e software che dovranno essere eseguiti. Tali condizioni e test sono inseriti nei bandi di gara e nei contratti con specifiche clausole che condizionano il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. I test richiesti possono essere effettuati presso i laboratori di prova accreditati dallo stesso CVCN o presso i CV del Ministero della Difesa e dell'Interno e devono essere conclusi nel termine di sessanta giorni.

Nella logica di favorire la compliance a tale complessa disciplina, l'ACN ha elaborato un documento che raccoglie i riscontri ai quesiti emersi con maggiore frequenza nelle interlocuzioni con i soggetti e fornisce informazioni di carattere generale attinenti alle finalità e all'ambito di operatività del Perimetro, agli adempimenti e ai termini da rispettare, nonché alle modalità di comunicazione con l'Agenzia. A ciò si aggiungono indicazioni specifiche sulle modalità ed i criteri di individuazione, descrizione e comunicazione all'Agenzia dei beni ICT da inserire nel Perimetro, nonché sulle misure di sicurezza, rispetto a cui sono stati descritti sia gli elementi di carattere generale, sia le modalità di implementazione in relazione a specifiche misure. Sono state infine definite le modalità di descrizione e trasmissione per l'assolvimento dell'obbligo di comunicare all'ACN l'avvenuta implementazione delle misure stesse e considerate le modalità e le tempistiche di notifica degli incidenti.

2.3 Esercizio dei poteri speciali e il perimetro di sicurezza cibernetica

2.3.1 L'andamento delle notifiche e i settori di intervento

I dati pubblicati nella relazione sull'attività del Governo svolta sulla base dei poteri speciali[15] confermano la tendenza incrementale delle notifiche ai sensi del decreto-legge 21/2012. Nel 2021, in particolare, il numero totale di informative presentate è pari a **496**, **in aumento di circa il 45% rispetto all'anno precedente**. Il trend è crescente per tutti i settori previsti dal decreto-legge n. 21 del 2012: difesa e sicurezza nazionale (articolo 1), tecnologia 5G (articolo 1-bis) ed energia, trasporti, comunicazioni e nuovi settori del Regolamento (UE) 2019/452 (articolo 2).

Per quanto riguarda il comparto **difesa e sicurezza nazionale**, nel 2021 **le notifiche pervenute sono 51**, in crescita di circa il 38% rispetto all'anno precedente, e rappresentano il 10,3% del totale delle notifiche avvenute nell'anno solare (Fig. 2.7).

Sul versante **tecnologia 5G**, le notifiche ai sensi dell'articolo 1-bis hanno iniziato ad essere presentate a partire dal 2019. Nel 2021, il loro numero è pari a **20**, in aumento di una sola unità rispetto all'anno precedente, e rappresentano circa il **4% del totale** (Fig. 2.8).

15 Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, anno 2021, Camera dei Deputati, presentata dal Sottosegretario di Stato alla Presidenza del Consiglio dei ministri Garofoli e trasmessa alla Presidenza il 30 giugno 2022.

Fig. 2.7: Difesa e sicurezza nazionale: il trend delle notifiche

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)

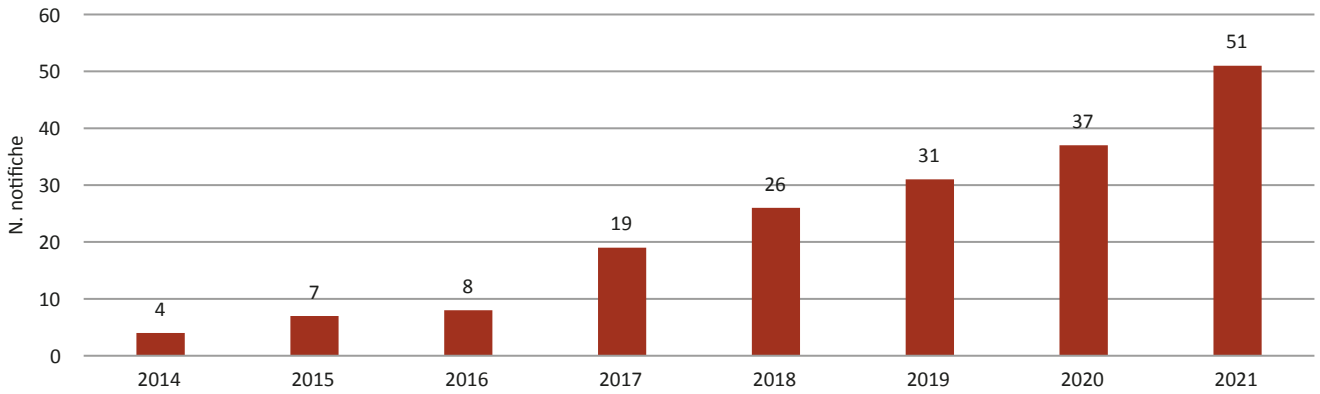
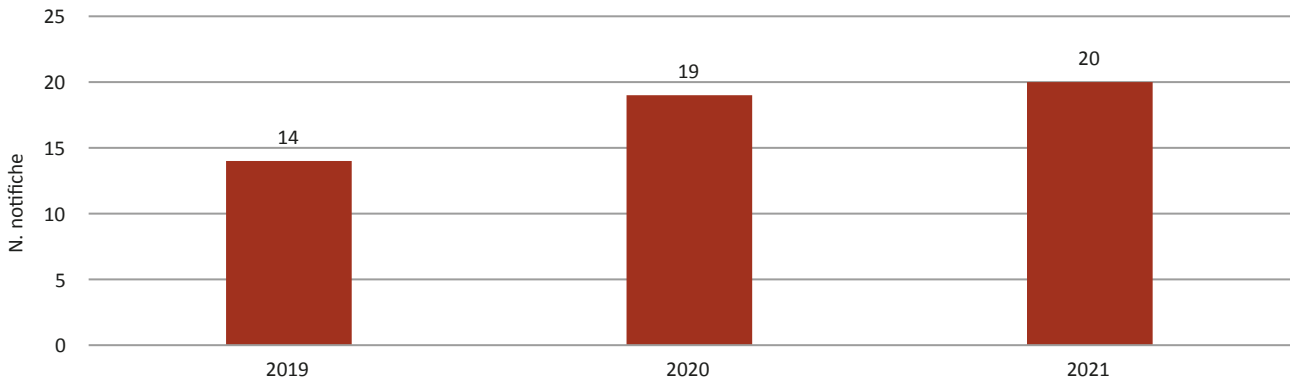


Fig. 2.8: Tecnologia 5G: il trend delle notifiche

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)



Infine, rispetto alle altre macrocategorie, si evidenzia un **incremento significativamente maggiore delle notifiche pervenute ai sensi dell'articolo 2 (energia, trasporti e comunicazioni)**, dovuto principalmente all'ampliamento di tale categoria, la quale comprende, ora, anche i settori indicati nel Reg. (UE) 2019/452. Nel 2021, le notifiche in tale comparto rappresentano **l'85,7% del totale, in crescita di circa il 49% rispetto al 2020 e di oltre il 1000% rispetto al 2019** (Fig. 2.9).

Considerando la collocazione temporale delle notifiche nel periodo gennaio 2021 – dicembre 2021, è possibile osservare che le informative sono state presentate per la maggior parte nella seconda metà dell'esercizio, **da giugno a dicembre** (Fig. 2.10).

Per ogni notifica pervenuta, sulla base del settore merceologico coinvolto, viene individuata un'amministrazione responsabile dell'istruttoria**. Nel 2021, la maggior parte delle notifiche (188 su 496) è stata**

Fig. 2.9: Energia, trasporti, comunicazioni e nuovi settori del Regolamento (UE) 2019/452: il trend delle notifiche

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)

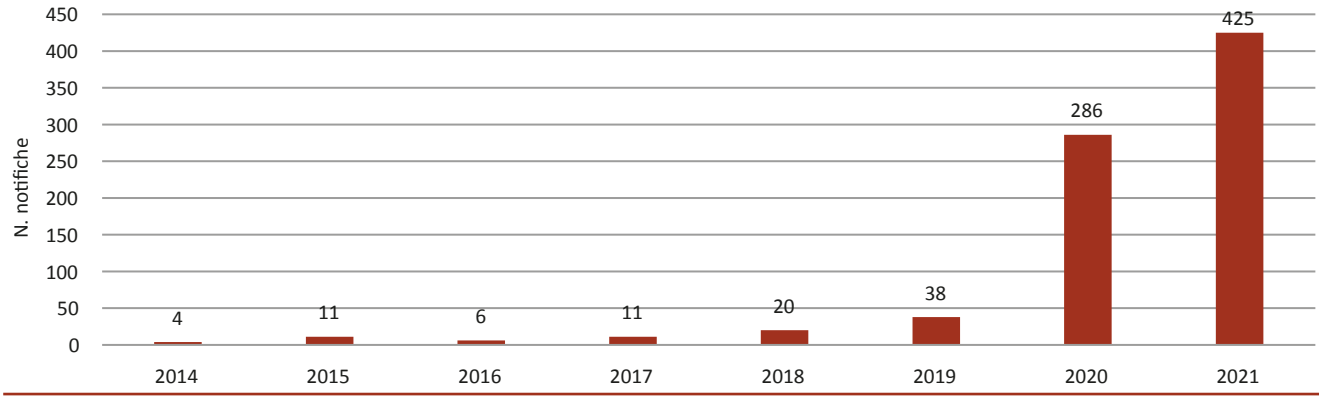


Fig. 2.10: Suddivisione mensile delle notifiche (anno 2021)

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)

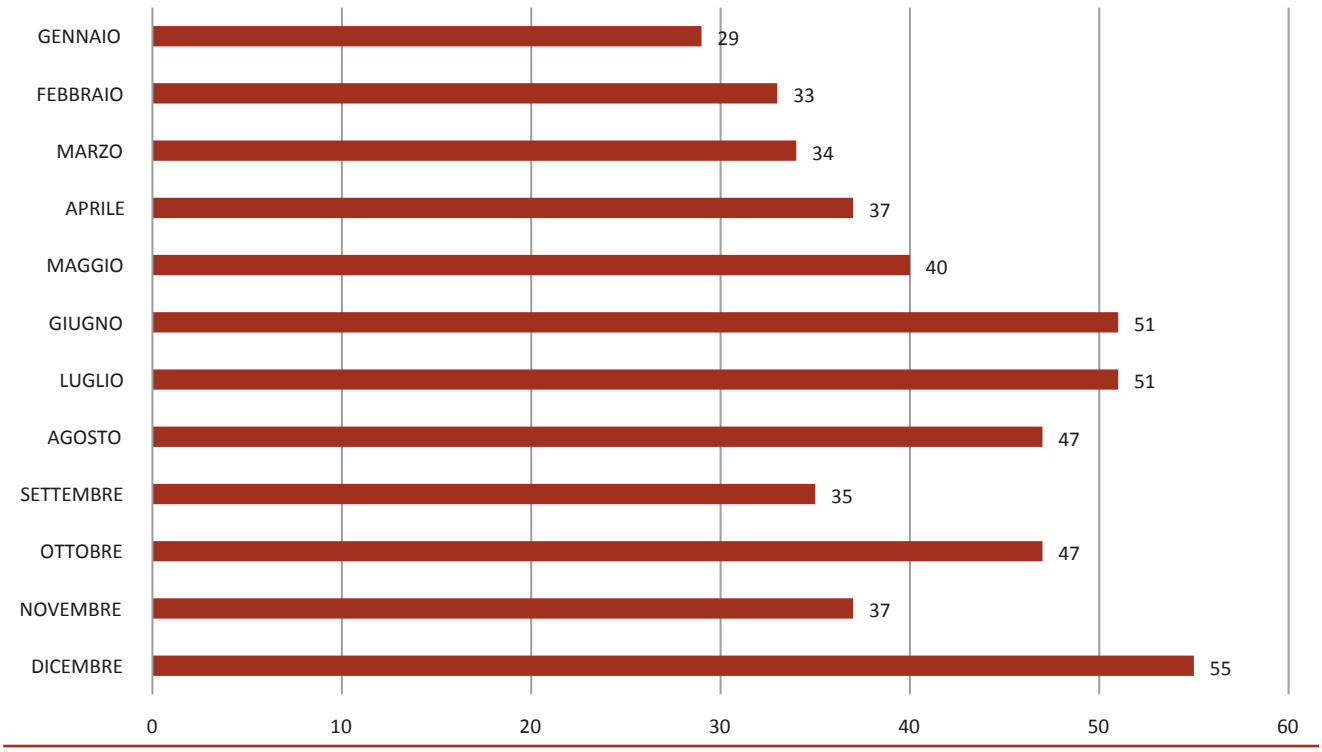


Fig. 2.11: La responsabilità istruttoria delle notifiche

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)

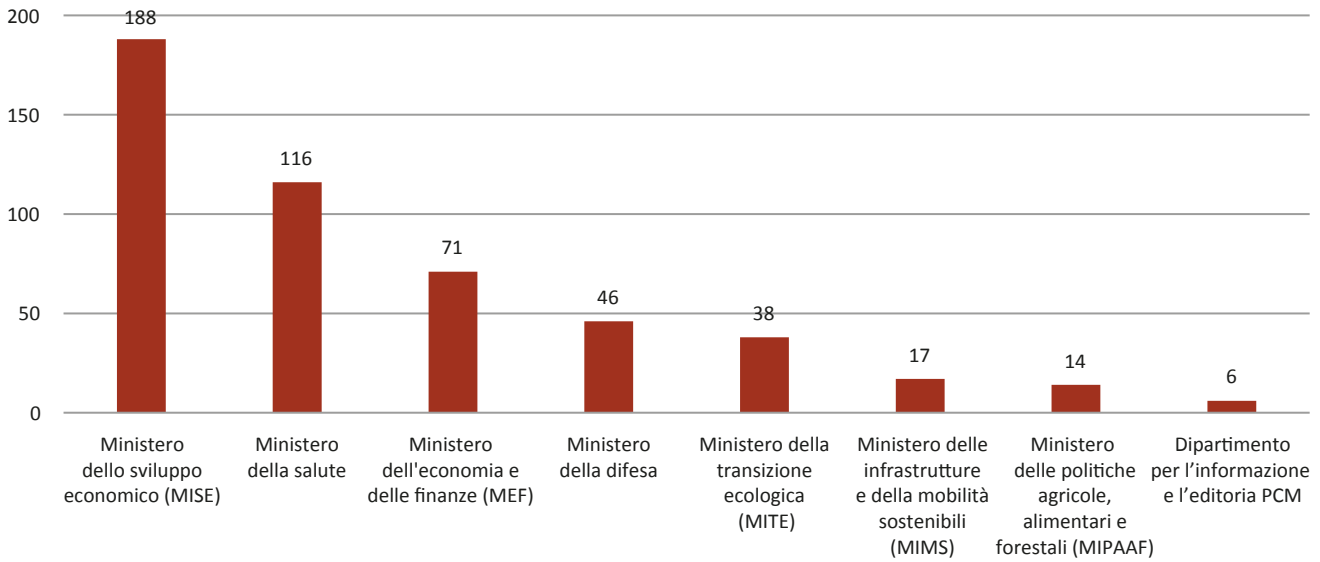


Fig. 2.12: Esercizio e non esercizio dei poteri speciali (anno 2021)

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)

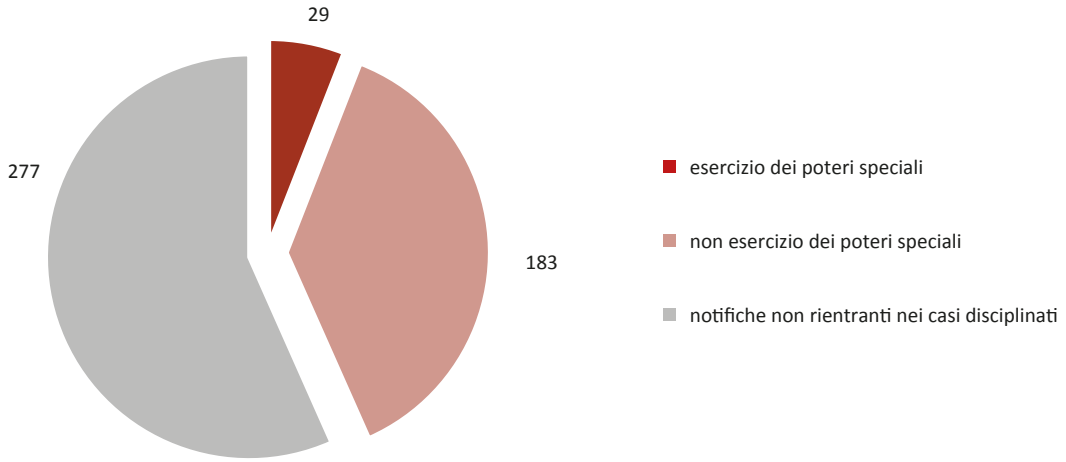
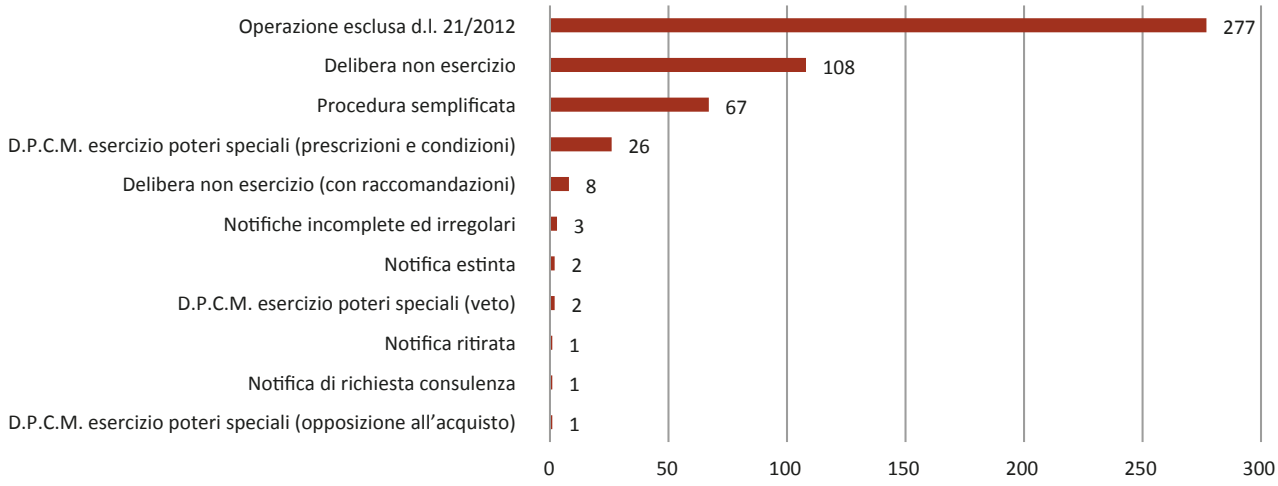


Fig. 2.13: Esito dettagliato della trattazione delle notifiche (anno 2021)

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)



assegnata al Ministero dello Sviluppo economico. Si osserva anche un notevole coinvolgimento del Ministero della Salute (116 notifiche), che ai sensi del d.P.C.M. 179/2020 è tra le nuove amministrazioni competenti per l'istruttoria della disciplina *Golden Power*. Seguono il MEF e il Ministero della Difesa, rispettivamente con 71 e 46 notifiche (Fig. 2.11).

All'esito dell'istruttoria, delle **496 notifiche** pervenute nel corso del 2021, **per 29 di esse sono stati esercitati i poteri speciali** (Fig. 2.12). Nello specifico:

- **26** notifiche sono state oggetto di esercizio dei poteri speciali mediante imposizione di specifiche condizioni e prescrizioni;
- per **2** notifiche è stato esercitato il potere di opposizione all'acquisto;
- per **1** notifica è stato esercitato il potere di veto.

Al contrario, per **183 notifiche non sono stati esercitati i poteri speciali**:

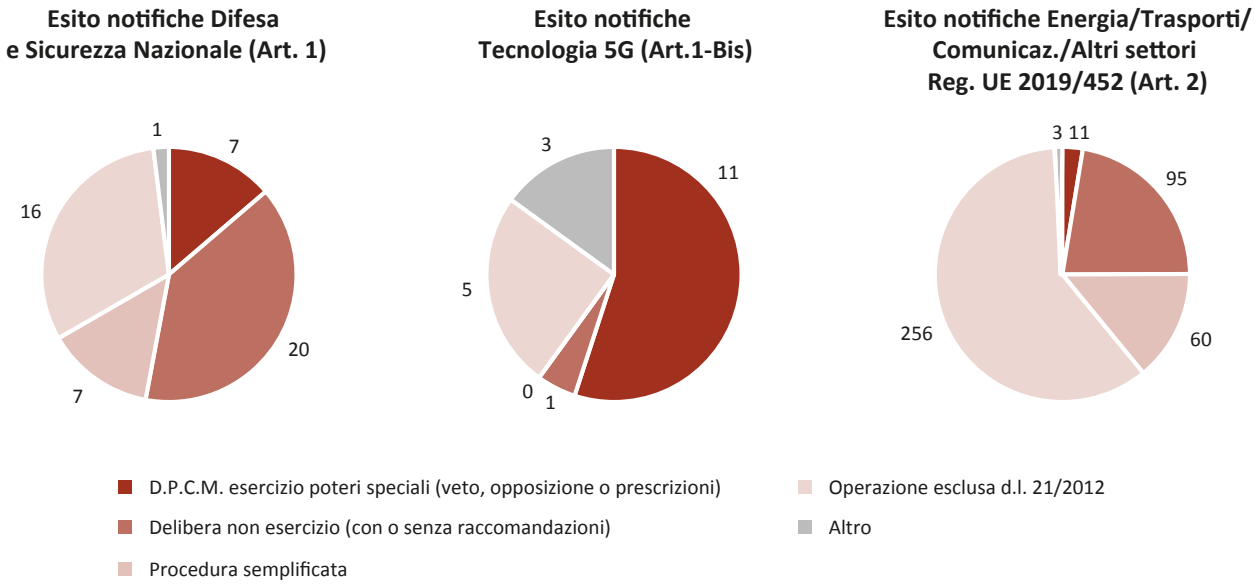
- per **108** è stata adottata una delibera di non esercizio dei poteri speciali;
- per **67** è stato disposto il non esercizio dei poteri speciali con procedura semplificata prevista dall'articolo 1, comma 1-bis, e dall'articolo 2, comma 1 e 1-ter, del decreto-legge n. 21 del 2012, in quanto riguardanti operazioni infragruppo per le quali non è stata rilevata minaccia di grave pregiudizio per gli interessi nazionali;
- per **8** notifiche, nella delibera di non esercizio dei poteri speciali, sono state previste delle raccomandazioni rivolte al soggetto notificante;

Infine, **277** sono state ritenute non rientranti nella disciplina Golden power (Fig. 2.13); **3** notifiche sono state ritenute incomplete o irregolari; **2** sono state estinte a seguito dell'entrata in vigore del decreto-legge 21 marzo 2022; **1** notifica è stata ritirata; con **1** notifica si richiedeva soltanto una consulenza sull'applicabilità della normativa Golden power (Fig. 2.14).

Per quanto concerne la suddivisione settoriale, la situazione complessiva riportata in figura 2.8 mostra come, a fronte di un ***esercizio effettivo dei poteri speciali* piuttosto simile** – rispettivamente 7 casi per la Difesa e la Sicurezza nazionale, 11 per la Tecnologia 5G e 11 per Energia, Trasporti, Comunicazioni e

Fig. 2.14: Esito della trattazione delle notifiche per settore (anno 2021)

Fonte: Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Camera dei Deputati (2021)



nuovi settori, i differenti ambiti delle tre aree presentino "confini" piuttosto differenti. Infatti, **oltre a presentare dimensioni diverse in termini complessivi, rispettivamente 51 notifiche per Difesa e Sicurezza, 20 per Tecnologia 5G e ben 425 Energia, Trasporti, Comunicazioni e altri settori, si osserva come le operazioni notificate ma "escluse" dall'ambito dei poteri speciali siano rispettivamente 16 per il primo comparto, 5 per il secondo e ben 256 per il terzo**. Allo stesso modo, infine, si rilevano diversi ordini di grandezza anche per quanto concerne le ***procedure semplificate***, utilizzate rispettivamente in 7 casi nell'ambito Difesa e Sicurezza e mai nei casi che ricadono nella tecnologia 5G, a fronte di ben 60 casi per quanto concerne Energia, Trasporti, Comunicazioni e altri settori.

CAPITOLO 3

LA CONSAPEVOLEZZA DELL'IMPORTANZA DELLA CIBERSICUREZZA: A CHE PUNTO SIAMO E ATTIVITÀ IN CORSO

3.1 La cibersicurezza per cittadini e imprese: lo stato dell'arte

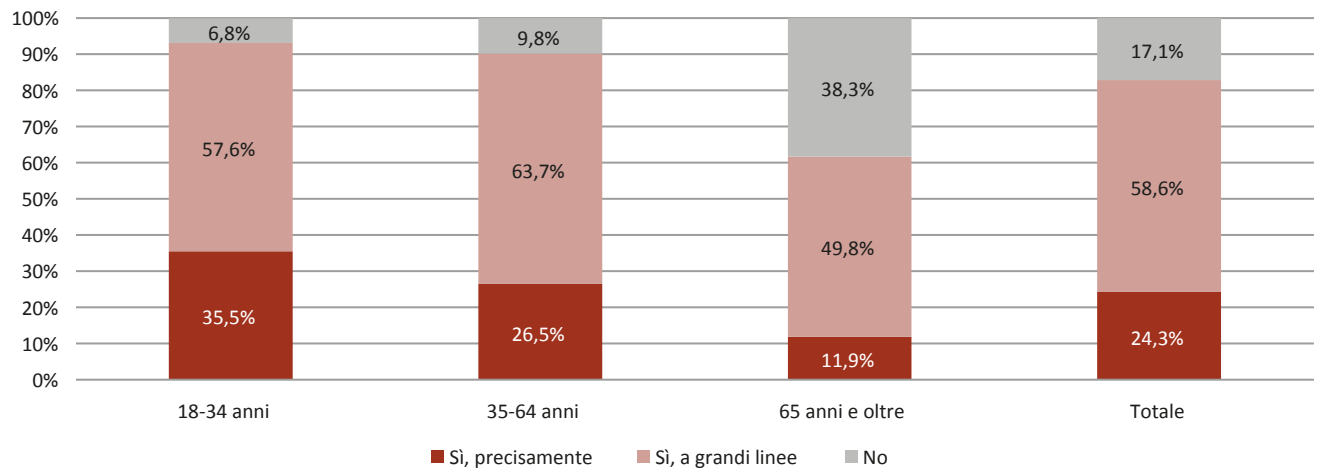
L'accelerazione portata dalla trasformazione digitale nell'ultimo decennio ha spostato il fulcro della maggior parte delle attività umane sul web, imponendo a tutte le categorie di individui di interfacciarsi con dispositivi elettronici. Oggi l'utilizzo di internet è fondamentale per comunicare, lavorare, informarsi ed accedere a servizi offerti sia dai privati che dalle pubbliche amministrazioni. Se da un lato questo repentino cambiamento ha aperto un nuovo mondo di opportunità per individui e imprese, dall'altro ha fatto sì che anche persone senza alcun rudimento riguardo il funzionamento delle nuove tecnologie si affacciassero ai canali digitali, esponendosi a nuove minacce come il cyber-crime.

A tal proposito, il rapporto del Censis denominato "Il valore della cybersecurity"[16], pubblicato il 22 aprile 2022, mette in evidenza quanto **gran parte della popolazione italiana risulti ancora ampiamente impreparata** ad affrontare problematiche di sicurezza informatica. Analizzando i dati diffusi dall'istituto si osserva **come solo il 24,3% degli italiani dichiari di avere una buona conoscenza di cosa si intende per cibersicurezza**, il 58,6% degli stessi ne ha un'idea approssimata, mentre il 17,1% è completamente a digiuno riguardo la sicurezza informatica (Fig. 3.1).

Osservando la distinzione per età anagrafica appare evidente come gli individui meno istruiti sul tema, e di conseguenza meno attrezzati a rispondere alle minacce dei cybercriminali, siano gli ultrasessantacinquenni, ovvero quella generazione di persone non native digitali che solo negli ultimi anni si è avvicinata al mondo digitale**. Quasi il 40% degli individui oltre i 65 anni di età non ha nessuna conoscenza riguardo la cybersecurity**, mentre il 49,8% degli stessi la conosce solo approssimativamente. **Ad avere una buona conoscenza di cosa si intenda per sicurezza informatica è solo un ultrasessantacinquenne su dieci**, contro circa un individuo **su quattro nella fascia 35-64 anni** e **uno su tre nella fascia 18-34**. È dunque evidente l'amplissima porzione della popolazione che necessita di policy e attività di formazioni ad hoc.

Fig. 3.1: Italiani che dichiarano di sapere cosa si intende per cybersecurity, per età anagrafica (2022)

Fonte: Indagine Censis, 2022



16 https://www.censis.it/sicurezza-e-cittadinanza/1%C2%B0-rapporto-censis-deepcyber-il-valore-della-cybersecurity

Fig. 3.2: Italiani che hanno dichiarato di aver subito alcune minacce informatiche per tipologia (2022)

Fonte: Indagine Censis, 2022

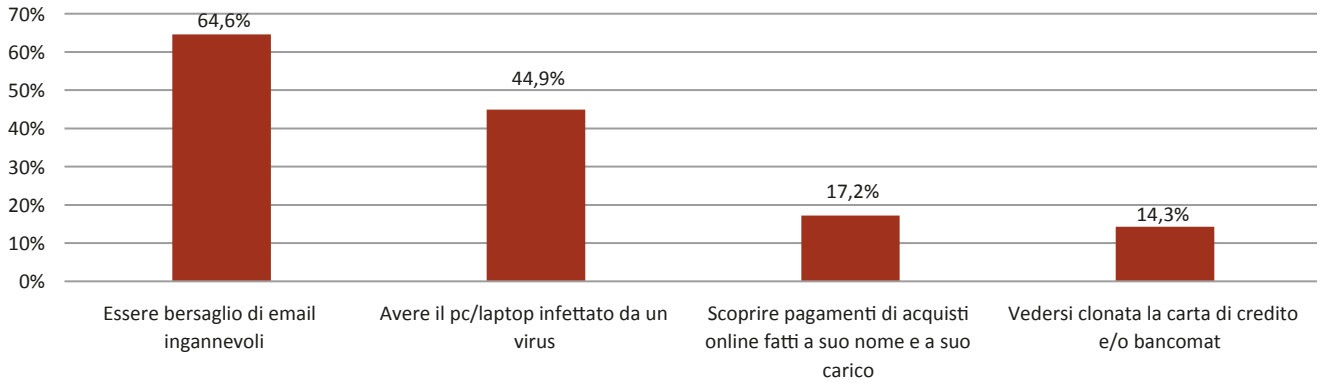
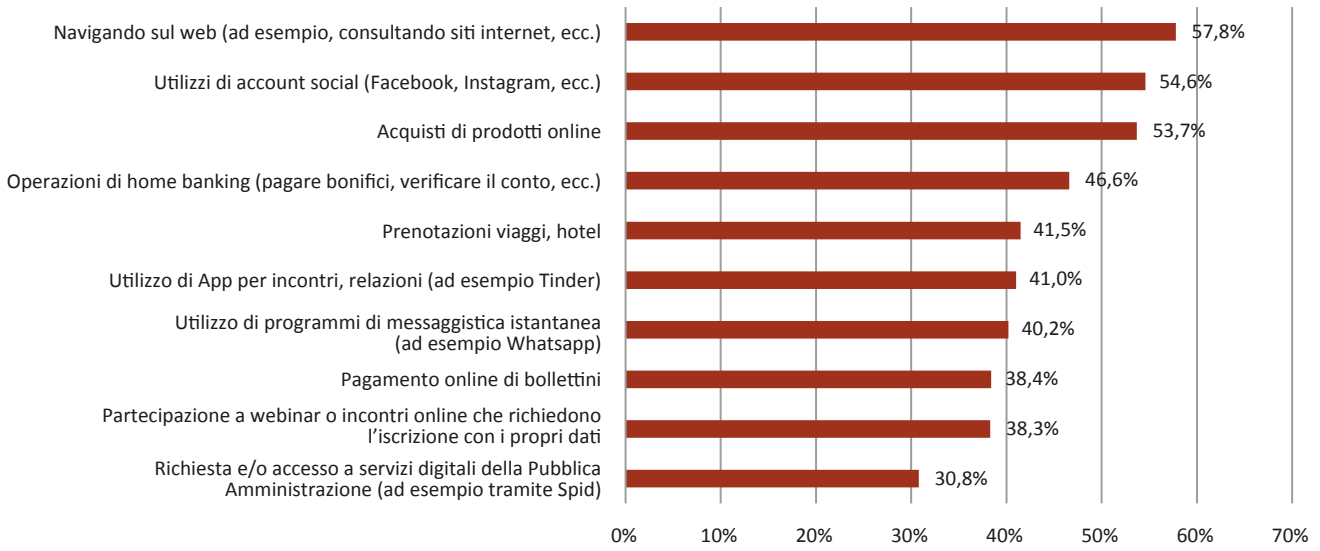


Fig. 3.3: Attività digitali in cui gli italiani ritengono più alto il rischio per la sicurezza dei propri dati personali (2022)

Fonte: Indagine Censis, 2022



D'altra parte, **nonostante pochi italiani siano a conoscenza di cosa sia la sicurezza informatica, più della metà degli stessi si è imbattuto in una o più minacce informatiche nel corso della propria vita** (Fig. 3.2).
In particolare, il **64,6% dei cittadini italiani è stato bersaglio del cosiddetto fenomeno del *phishing***, ovvero la ricezione di mail ingannevoli volte a truffare i malcapitati inducendoli a rivelare informazioni personali delicate, ad esempio il numero di carta di credito o le proprie credenziali bancarie. Un ulteriore 44,9% della popolazione del nostro Paese ha avuto un PC o un laptop infettato da un virus informatico.
Le problematiche appena descritte generano spesso gravi conseguenze, che possono essere riscontrare nelle dichiarazioni fornite al Censis. Infatti, dai dati dell'istituto emerge come **il 17,2% dei nostri concittadini,**

evidentemente a seguito dell'azione di cybercriminali, **ha scoperto pagamenti di acquisti fatti a proprio nome e a proprio carico** e **il 14,3% degli stessi si è visto clonare la carta di credito o il bancomat**.

Secondo l'analisi condotta dal Censis, **l'attività digitale che gli italiani ritengono più pericolosa per i propri dati personali è** probabilmente anche quella più comune, ovvero **la navigazione sui siti web**, segnalata come rischiosa dal **57,8%** dei nostri concittadini (Fig. 3.3).

Il primato della navigazione è da considerarsi singolare se si osserva che, a dispetto di tutte le altre operazioni presenti in classifica, è l'unica attività elencata che non richiede la compilazione di *form* contenenti informazioni personali. Al secondo posto si trova **l'utilizzo di account social** (54,6%), probabilmente le piattaforme digitali su cui gli individui passano più tempo e anche quelle su cui viene inserito il maggior numero di dati personali. È interessante notare, inoltre, come le attività che implicano lo scambio di denaro online siano presenti solo dal terzo posto in classifica in poi. **L'acquisto di prodotti online è ritenuto a rischio da poco più della metà degli italiani (53,7%)**, le operazioni di home banking dal 46,6% e le prenotazioni di viaggi e hotel dal 41,5%. Questo è probabilmente dovuto al forte incremento delle misure di sicurezza online che grandi piattaforme e istituti finanziari hanno operato negli ultimi anni. Infine, **è interessante notare come l'attività ritenuta meno pericolosa sia l'accesso ai servizi digitali offerti dalle Pubbliche Amministrazioni, operazione ritenuta a rischio "solo" dal 30,8% degli italiani**.

La mancanza di consapevolezza riguardo la sicurezza informatica non è una problematica riscontrabile solo tra i cittadini. Nonostante il web stia diventando la vetrina privilegiata per quasi tutte le attività economiche, il **livello di competenze relative alla cybersecurity all'interno delle imprese italiane**, soprattutto per chi occupa funzioni esecutive, **è estremamente basso**. Osservando i dati raccolti dal Censis emerge come **solo il 39,7% dei lavoratori intervistati ha ricevuto una formazione specifica sulla sicurezza informatica**, percentuale che scende al 23,5% per quanto riguarda operai ed esecutivi. Il problema, anche se meno accentuato, è comunque riscontrabile anche tra chi svolge funzioni amministrative: **circa un impiegato su due (47,8%) e il 43,2% dei dirigenti non ha ricevuto una formazione sulla sicurezza cibernetica** (Fig. 3.4).

Fig. 3.4: Lavoratori che hanno ricevuto una formazione specifica sulla cybersecurity, per ruolo svolto in azienda (2022)

Fonte: Indagine Censis, 2022

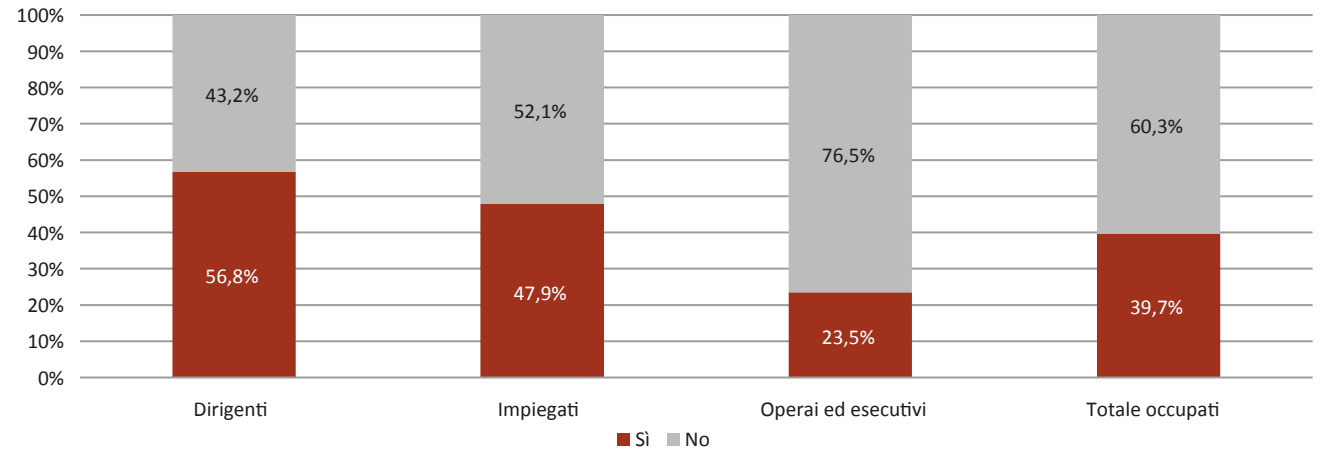
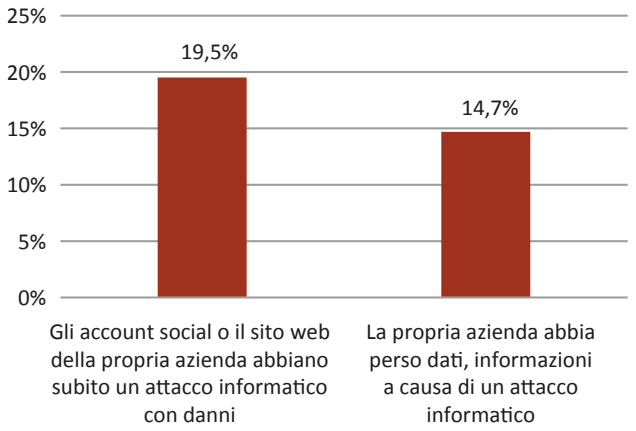


Fig. 3.5: Lavoratori a cui è capitato che (2022)

Fonte: Indagine Censis, 2022



Se si considera che gran parte delle azioni malevole subìte dalle imprese sono frutto di errori umani compiuti da soggetti che, inconsapevolmente, offrono un punto d'accesso ai cybercriminali nelle reti aziendali, si comprende quanto sia **importante che tutti i dipendenti che si interfacciano con i sistemi informatici aziendali ricevano un adeguata formazione in cibersicurezza**.

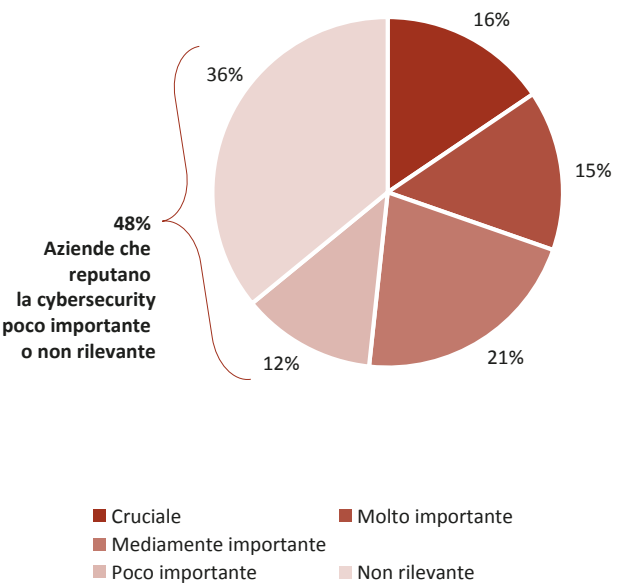
Focalizzando l'attenzione sullo scenario italiano, dai dati pubblicati dal Censis emerge che **il 19,5% dei lavoratori ha dichiarato che la propria azienda è stata vittima di un attacco informatico** sul proprio portale web e/o sul proprio account social, in cui peraltro si sono verificati **danni**. Inoltre, **il 14,7%** dei dipendenti ha affermato che a seguito di un attacco informatico subito si è verificata una **perdita di dati** (Fig. 3.5).

Dai dati sopracitati emerge quanto la mancanza di alfabetizzazione digitale resti ad oggi un problema estremamente diffuso anche nei contesti business. Questa tesi è certificata dagli ultimi dati contenuti nel "Rapporto sulla situazione e prospettive delle imprese dopo l'emergenza sanitaria covid-19" pubblicato dall'ISTAT[17] a febbraio 2022, che evidenziano come **la formazione digitale risulti un aspetto cruciale per l'impresa solo per il 16% delle aziende residenti nel nostro Paese** (Fig. 3.6).

In particolare, a preoccupare è il dato che evidenzia come **per quasi un'azienda su due (48%) la formazione digitale risulti secondaria, nel dettaglio "poco importante" per il 12% delle imprese rispondenti e addirittura assolutamente "non rilevante" per il 36%.** Date queste premesse appare evidente come ancora oggi avvengano così tanti incidenti di sicurezza informatica. Infatti, alle tecniche sempre più sofisticate messe in atto dai cybercriminali, si somma una non adeguata comprensione dei rischi da parte non solo dei lavoratori, ma anche degli stessi dirigenti delle imprese (soprattutto nelle realtà più piccole e meno strutturate).

Fig. 3.6: Rilevanza della formazione digitale per le imprese (2022)

Fonte: ISTAT



Note: Valutazioni espresse dalle imprese di 3 addetti e oltre

17 https://www.istat.it/it/files/2022/02/REPORT-COVID-IMPRESE_2022.pdf

3.2 Le best practices nell'ambito della formazione digitale e sulla sicurezza informatica

Per ridurre i rischi derivanti dalle minacce informatiche è necessario operare un profondo lavoro sull'aumento del livello di consapevolezza degli utenti, poiché il "fattore umano" gioca spesso un ruolo fondamentale negli incidenti di sicurezza informatica. Ingannare un individuo non adeguatamente consapevole delle conseguenze delle proprie azioni appare infatti molto più semplice che forzare sistemi di difesa complessi ed in continuo aggiornamento. Come anticipato nel paragrafo precedente, quasi due italiani su tre sono bersaglio di mail fraudolente, tramite cui malintenzionati provano a farsi consegnare le credenziali o a infettare i device delle vittime con allegati che nascondono malware.

Rendere gli individui consapevoli dei rischi a cui vanno incontro è quindi l'arma principale per incrementare la sicurezza dell'ecosistema informatico, in un contesto in cui sempre più individui utilizzano frequentemente gli strumenti informatici. Secondo gli ultimi dati diffusi da Eurostat (Fig. 2.7), nell'ultimo decennio la quota di italiani che utilizzano internet ha raggiunto nel 2022 l'86,14% della popolazione. Nonostante ciò, osservando gli ultimi dati diffusi dalla stessa Eurostat sulle competenze informatiche, è possibile notare come **solo il 59,8% dei cittadini della penisola ha competenze almeno basilari relative alla sicurezza informatica**. In generale, osservando la scomposizione demografica per età, si osserva come – ad esclusione dei minori di 16 anni – **la quota di persone a digiuno di cibersicurezza cresce in maniera proporzionale all'età anagrafica**. In particolare, analizzando i dati emerge come un italiano **su quattro tra i 16 e i 54 anni non ha conoscenze di sicurezza informatica di base**, quota che sale ad **uno su tre se si considera la fascia di età 55-74** e addirittura a **due su tre per gli over 75** (Fig. 3.7).

Dai dati appena descritti traspare in modo evidente l'importanza di individuare iniziative che riescano a raggiungere l'intera popolazione del nostro Paese, comunicando messaggi chiari che possano essere pienamente appresi da tutti a prescindere dal livello di alfabetizzazione digitale posseduta.

Fig. 3.7: Quota di italiani che utilizzano internet e di individui che hanno almeno competenze basilari di sicurezza informatica (2022)

Fonte: Eurostat

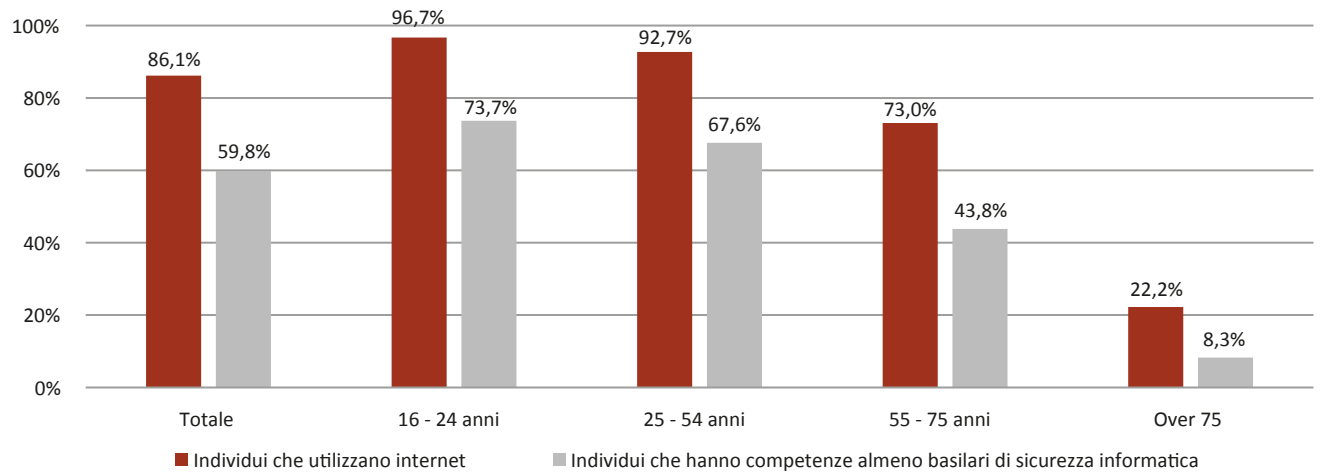


Fig. 3.8: Truck della Polizia Postale

Fonte: Profilo Twitter "Una Vita da Social"

Una delle autorità pubbliche più dinamiche da questo punto di vista è la **Polizia Postale**, attiva in decine di iniziative finalizzate a sensibilizzare la popolazione sui pericoli che si celano sulla rete, sia a livello nazionale, sia in collaborazione con i piccoli comuni. Tra le campagne informative più interessanti lanciate dalla Polizia Postale negli ultimi anni, una delle più note è denominata "**Una vita da Social"** e si svolge grazie all'utilizzo di un Truck (Fig. 3.8) che gira nelle province del Paese offrendo momenti formativi sulle minacce del web destinati principalmente ai più giovani. In base alle ultime informazioni diffusi dall'Ente, **l'iniziativa ha permesso alla Polizia di raggiungere oltre 2 milioni di studenti, 220 mila genitori e 125 mila insegnanti in circa 300 città**.

Oltre alle attività svolte su input delle autorità pubbliche, esistono anche importati campagne nate su spunto della cittadinanza. Uno dei principali esempi di questo tipo è **l'associazione "Parole O_Stili"** nata a Trieste su iniziativa di 300 tra professionisti della comunicazione d'impresa, della comunicazione politica, influencer e blogger. Questa associazione cerca di trasmettere agli individui la consapevolezza che le nostre azioni nel mondo virtuale sono reali e come tali hanno una conseguenza diretta nella vita delle persone.

L'iniziativa "Parole O_Stili" è principalmente volta a sensibilizzare le persone circa gli effetti deleteri dell'utilizzo di un linguaggio violento e discriminatorio sulla rete collaborando con scuole, università, Comuni, altre associazioni e istituzioni e società private. Per portare avanti il proprio messaggio, l'associazione ha creato un **manifesto contenente 10 principi da rispettare quanto si comunica sulle piattaforme digitali per non arrecare danno a sé stessi e agli altri utenti della rete**. Più di 75 aziende, 300 Comuni italiani e 21.000 insegnanti hanno già firmato il Manifesto e questi numeri stanno salendo rapidamente. Sulla stessa lunghezza d'onda di "Parole O Stili" è l'iniziativa denominata "**Giovani ambasciatori per la cittadinanza digitale**" sviluppata dal "Moige", ovvero un'associazione composta da genitori, insegnanti, educatori nonché membri della cittadinanza che si impegnano per tutelare la salute dei minori.

"Giovani ambasciatori per la cittadinanza digitale" ha l'obiettivo di sensibilizzare gli studenti riguardo il cattivo uso di device informatici e piattaforme social, occupandosi anche di formare docenti e genitori su come prevenire le situazioni che portano i ragazzi a cadere nelle insidie del web. Il Moige, attraverso quest'iniziativa, è riuscito a raggiungere oltre 62 mila studenti e, per rendere le attività più pervasive, si è recentemente dotato di un Centro mobile on the road, che permette all'associazione di divulgare più efficacemente contenuti realizzati da esperti del settore. Tra le Istituzioni che hanno dato il proprio appoggio al progetto figurano il DIS, la Polizia Postale, il Ministero dell'Istruzione, l'ANCI e l'Ambasciata degli Stati Uniti d'America nonché un cospicuo numero di realtà provenienti dal mondo dell'impresa.

A livello internazionale, una delle principali iniziative sulla sicurezza informatica è certamente la **"*Mobile Malware Awarness Campaign*" sviluppata dallo *European Cybercrime Centre* dell'Europol per aiutare gli individui a proteggere i propri dispositivi mobili dai criminali informatici.** La

campagna è stata portata avanti sviluppando materiale di sensibilizzazione che fornisce una panoramica delle principali minacce e vulnerabilità dei device mobili in 20 lingue, tra cui l'Italiano[18]. Vengono inoltre forniti una serie di suggerimenti sui comportamenti da adottare per svolgere in modo sicuro le attività quotidiane ed evitare di cadere nei tentativi di raggiri dei criminali informatici.

3.3 Le funzioni di impulso di ACN e gli obiettivi della strategia nazionale per accrescere l'*awareness*

Con la pubblicazione, il 14 giugno 2021, del **D.L. n. 82/2021 recante "*Disposizioni urgenti in materia di cibersicurezza, definizione dell'architettura nazionale di cibersicurezza e istituzione dell'Agenzia per la cibersicurezza nazionale*"** (convertito con la legge 4 agosto 2021, n. 109) è iniziata, come già rilevato nei paragrafi precedenti, una nuova era per la cibersicurezza a livello nazionale che trova nel trasferimento di quasi tutte le competenze e funzioni in materia di cybersecurity all'ACN il punto di svolta in termini di semplificazione, chiarezza e certezza del diritto. L'ACN, infatti, è 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, è chiamata a predisporre la strategia nazionale di cibersicurezza e ad una lunga serie di funzioni tra cui assicurare il coordinamento tra i soggetti pubblici coinvolti in materia di cibersicurezza a livello nazionale, promuovere la realizzazione di azioni comuni dirette ad assicurare la sicurezza cibernetica di imprese e PA, e operare come Autorità nazionale di certificazione della cibersicurezza, assumendo inoltre tutte le funzioni in materia già attribuite al MiSE, al DIS e alla Presidenza del Consiglio dei ministri. La medesima ACN è inoltre chiamata ad assumere le iniziative idonee a valorizzare la crittografia come strumento di cibersicurezza, provvedere alla qualificazione dei servizi cloud per la P.A., a sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, curare e promuovere la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente.

Alla stessa ACN sono attribuite importantissime funzioni anche rispetto ad ***awareness*, formazione e ricerca**. Ed infatti, all'agenzia è attribuito il compito di svolgere attività di comunicazione e promozione della consapevolezza in materia di cibersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia, di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cibersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati (con la possibilità di avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno) e predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile.

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 tecnico-scientifico** (CTS) per i cui componenti – riunitisi per la prima volta nel luglio scorso – è prescritto il possesso di una indiscussa competenza, a livello nazionale e internazionale, negli ambiti di attività dell'Agenzia, in particolare nel contesto della

18 https://www.commissariatodips.it/gioco.pdf

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[19].
Rispetto alle funzioni di impulso, la **strategia nazionale di cibersicurezza 2022-2026 ed il relativo piano di implementazione** già analizzati nei paragrafi precedenti, partendo dalla constatazione della crescente interconnessione dei servizi nello spazio cibernetico, della sempre maggiore fluidità del confine tra la dimensione digitale e quella reale e di una ancora troppo limitata consapevolezza dei rischi di sicurezza (cui si accompagna, peraltro, una crescente complessità degli attacchi), **hanno posto in luce l'esigenza di porre la cibersicurezza al centro della trasformazione digitale** anche nella logica di conseguire l'autonomia nazionale strategica e definire, dunque, adeguate strategie di cibersicurezza volte a pianificare, coordinare e attuare misure tese a rendere il Paese sicuro e resiliente anche nel dominio digitale ed assicurare la fiducia dei cittadini nella possibilità di sfruttarne i relativi vantaggi competitivi, nella piena tutela dei diritti e delle libertà fondamentali.
Per realizzare tale macro-obiettivo, la strategia fa ricorso a due leve: da un lato, **mettere in sicurezza infrastrutture, sistemi e informazioni dal punto di vista tecnico**; dall'altro, **accompagnare il progresso culturale ad ogni livello della società, verso un modello "*security-oriented*"**, indispensabile per tutelare il sistema valoriale e democratico nazionale, che trova nell**'approccio "whole-of-society"** il proprio fondamento. A svolgere un ruolo attivo sono infatti chiamati tutti gli attori e, dunque, gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza, quest'ultima concepita dunque non più solo come un indiretto beneficiario delle misure contemplate nel Piano di implementazione della strategia, ma anche protagonista nell'implementazione della strategia stessa, nell'idea che l'obiettivo ultimo della sicurezza cibernetica nazionale possa essere raggiunto solo attraverso un gioco di squadra che veda fattivamente coinvolte tutte le componenti socio-economiche.
Per quanto concerne le **sfide** da affrontare, la strategia ne mette a fuoco cinque:

1. **assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione e del tessuto produttivo**, al fine di garantire servizi sicuri ed incentivarne l'utilizzo da parte dei cittadini;
2. **anticipare l'evoluzione della minaccia cyber**, prevedendo, prevenendo ed arginando il più possibile gli impatti di eventuali attività cyber offensive;
3. **contrastare la disinformazione online** nel più ampio contesto della cd. minaccia ibrida;
4. **gestire le crisi cibernetiche**, favorendo il coordinamento tra tutti i soggetti pubblici e privati interessati e garantire una risposta pronta in caso di eventi cyber sistemici;
5. **perseguire l'autonomia strategica nazionale ed europea nel settore del digitale** con riguardo, in particolare, alla produzione di software ed alle cc.dd. "Emerging and Disruptive Technologies" (es. IA e quantum computing) attraverso cui detenere un controllo diretto sui dati conservati, elaborati e trasmessi mediante tali tecnologie.

Se queste sono le sfide, con riferimento, invece, agli **obiettivi**, la strategia ne individua tre, **protezione, risposta e sviluppo**, per ciascuno dei quali declina una serie di misure – complessivamente 82 – con relativi attori responsabili, prevedendo inoltre la definizione di metriche e di Key Performance Indicator (KPI), quali strumenti che consentano di misurarne l'effettiva attuazione ed efficacia.

19 È esclusa la percezione di qualsiasi compenso durante il periodo di carica di 2 anni (con possibilità di rinnovo per un ulteriore anno).

Soffermando l'attenzione sui **fattori abilitanti** e, dunque, **formazione**, **promozione della cultura della sicurezza cibernetica** e **cooperazione**, ampio spazio e numerose misure sono state declinate nella strategia e nel relativo piano di implementazione.

Rispetto alla **formazione**, la strategia parte dall'esigenza di **stimolare la creazione di una solida forza lavoro nazionale**, composta da esperti e giovani talenti in possesso delle capacità e delle **competenze necessarie da impiegare a vantaggio di imprese e pubbliche amministrazioni**, sia rispetto alle tecnologie informatiche in generale, che rispetto a quelle relative alla sicurezza cibernetica. Per raggiungere tale obiettivo, la stessa strategia enfatizza l'importanza di rendere più familiari agli **studenti** le tecnologie informatiche (introducendo l'informatica come disciplina a partire dalla scuola primaria ed in tutti i tipi di percorso di studio), favorire l'inserimento in **carriere tecnico-scientifiche** (contrastando anche il divario di genere attualmente esistente) focalizzate su tematiche legate alla cibersicurezza rivendendo programmi e percorsi e la stessa **organizzazione degli ITS**, prevedere il continuo aggiornamento della didattica e della **preparazione del corpo docente**, destinare risorse alla formazione specialistica e all'aggiornamento professionale nei settori pubblico e privato, realizzare un sistema nazionale di certificazione di tali professionalità (sia in ambito scolastico/accademico che lavorativo), mediante **l'attivazione di percorsi di formazione ad hoc approvati dall'ACN**, prevedere percorsi di formazione specifici per i non specialisti della materia, rivolti ai **dipendenti di Pubbliche Amministrazioni** e soggetti privati e potenziare le capacità di **cyber diplomacy**, attraverso percorsi mirati per il personale diplomatico. Si prevede inoltre che tali azioni siano sviluppate grazie alla collaborazione con Università, scuole secondarie di secondo grado, Regioni – in base ad appositi accordi – oltre che con Amministrazioni pubbliche e soggetti privati, il cui ruolo, nelle varie possibili declinazioni, è particolarmente valorizzato sia nella strategia che nel relativo piano di implementazione.

In linea con l'approccio generale che mira, come evidenziato, a rendere partecipi tutti della sfida della sicurezza, la strategia ritiene essenziale la **promozione della cultura della sicurezza cibernetica** con l'obiettivo di accrescere la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber. A tal fine, esortando tutti gli attori a tenere comportamenti sicuri e virtuosi nello spazio cibernetico, la strategia evidenzia la necessità di **predisporre un programma capillare di educazione digitale** (da sviluppare anche online) a beneficio della collettività, sensibilizzare tutte le risorse impiegate nelle organizzazioni pubbliche e private a partire dei manager e promuovere la gestione consapevole del cd. "rischio residuo", anche attraverso l'adozione di strumenti di autovalutazione basati su specifici "cyber index", che permettano alle organizzazioni di gestire autonomamente il livello di esposizione.

Rispetto, infine, alla **cooperazione,** la strategia esorta ad incrementare questo aspetto, da un lato, a livello nazionale, a livello governativo, nel rapporto pubblico-privato, pubblico-pubblico, nonché con accademia e ricerca; dall'altro, a livello internazionale, partecipando in modo proattivo alle iniziative europee e internazionali e promuovendo collaborazioni bilaterali.

Trasversale agli obiettivi sopra descritti, nonché ai richiamati fattori abilitanti, è la Partnership Pubblico-Privato (PPP) che vede il settore pubblico agire sinergicamente con quello privato, il mondo accademico e della ricerca, i media, le famiglie e gli individui per rafforzare la resilienza cibernetica della nazione e della società complessivamente considerata.

Nel declinare le misure da mettere in campo per raggiungere gli obiettivi indicati nella strategia, il piano di implementazione ne individua diverse che vanno ad incidere su **consapevolezza, formazione e ricerca in materia di cibersicurezza**. In particolare, nell'ambito dell'obiettivo protezione, si prevedono **iniziative di sensibilizzazione** per favorire l'applicazione del

"Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity", opportunamente aggiornati in linea con il quadro della minaccia, da parte della PA, delle imprese e delle PMI (misura 11) ed il monitoraggio continuo e l'analisi di minacce, vulnerabilità e attacchi per rafforzare la situational awareness ed accrescere le capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence (misure 12 e 17). Tra le misure declinate nell'obiettivo sviluppo, invece, sono previste azioni per realizzare e **promuovere la partecipazione del mondo industriale, accademico, della ricerca e della società civile** a progetti volti a supportare lo sviluppo di capacità, tecnologie e infrastrutture di cibersicurezza (misura 46), supportare l'operatività dei Digital Innovation Hub e favorirne le sinergie con il Centro nazionale di coordinamento, con i Centri di competenza ad alta specializzazione e con i Cluster tecnologici. A ciò si aggiungono **iniziative per agevolare il trasferimento tecnologico verso le PMI** (misura 47), realizzare un "parco nazionale della cibersicurezza" per lo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali (misura 49), **favorire la ricerca e lo sviluppo**, specialmente nelle nuove tecnologie, anche mediante finanziamenti, rivolti in particolare alle startup e alle PMI innovative ed incentivare l'attività dei Centri di competenza e di ricerca attivi sul territorio nazionale (misura 54).

Molte le iniziative destinate ad impattare sui fattori abilitanti sopra citati. Rispetto alla **formazione**, con le misure 59, 60 e 61 si mira a **sviluppare percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity**, ad **attivare Istituti Tecnici Superiori (ITS)** con percorsi di cybersecurity con una significativa docenza aziendale (50%) ed un tirocinio (almeno 30% del tempo) e **sviluppare un sistema nazionale di certificazione dell'apprendimento e dell'acquisizione di specifiche professionalità**, non solo tecniche, sia a livello di istruzione secondaria di secondo grado, sia a livello universitario e professionale. A ciò si aggiunge l'elaborazione di uno **strumento di formazione e sensibilizzazione online, rivolto alla cittadinanza in generale** (con possibilità di auto-testare le competenze e le sensibilità acquisite e di ottenere un attestato, misura 62), la **previsione di fondi da dedicare alla formazione professionale nei settori pubblico e privato**, al fine di agevolare il passaggio dal mondo scolastico a quello del lavoro e conseguire, così, una sovranità nazionale digitale delle competenze (misura 63), l'organizzazione di iniziative e competizioni nazionali in materia di cibersicurezza e innovazione tecnologica (misura 65) e la previsione di meccanismi per agevolare la transizione di studenti e neolaureati, con competenze in cybersecurity, verso il mondo del lavoro, mediante programmi di alternanza scuola-lavoro e di inserimento quali stage e apprendistato, nonché incentivi all'assunzione di personale "junior" (misura 66).

Rispetto invece all'obiettivo di **promozione della cultura della sicurezza cibernetica**, la misura 71 prevede l'avvio di iniziative e campagne di sensibilizzazione volte a **promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico**, che tengano conto anche le esigenze di particolari fasce della popolazione come le persone anziane e diversamente abili, oltre che di alcune categorie di pubblici dipendenti (come, ad esempio, i magistrati) mentre la misura 72 mira a **promuovere l'educazione digitale, comprensiva di aspetti di sicurezza cibernetica, per tutti i livelli di istruzione scolastica**, affinché si diffondano conoscenze tecniche e operative sulla gestione sicura delle informazioni e delle tecnologie di comunicazione. La misura 73, infine, mira a **proteggere i minori dai crimini informatici** prevedendo l'implementazione di un'autonoma strategia nazionale, con relativo piano d'azione che contempli iniziative come la realizzazione di campagne di sensibilizzazione indirizzate non solo ai minori, ma anche a genitori, tutori ed educatori.

CAPITOLO 4

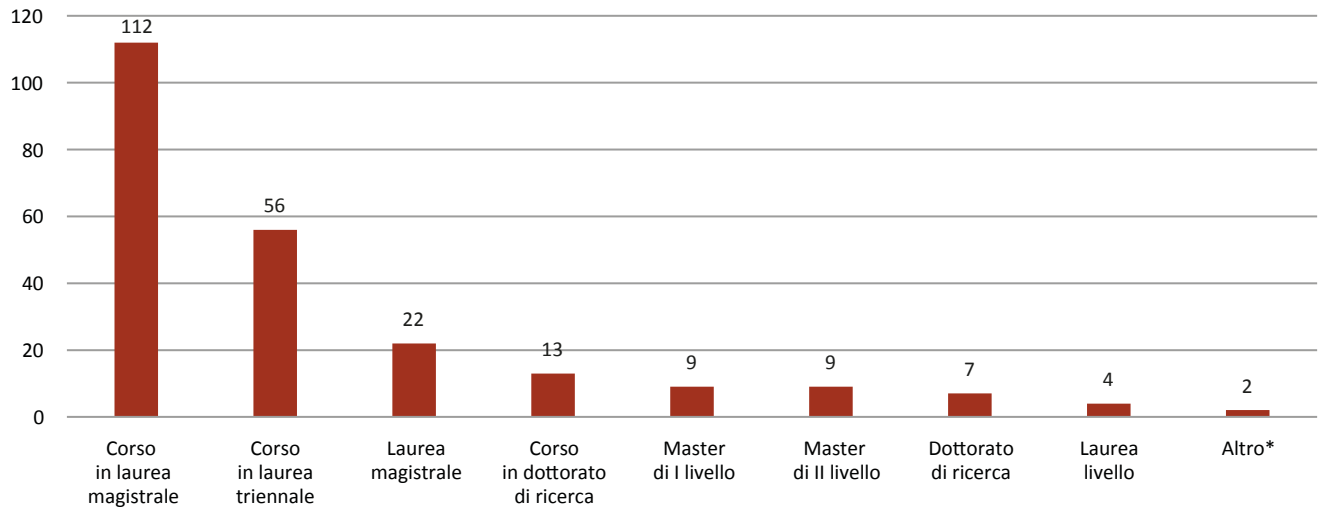
L'OFFERTA FORMATIVA IN MATERIA DI CIBERSICUREZZA

4.1 Corsi e Master

A partire dallo scorso gennaio 2022, l'Istituto per la Competitività (I-Com) ha avviato un monitoraggio delle attività di formazione sulla cibersicurezza in ambito universitario sul territorio italiano. A gennaio 2023[20], si registra la presenza di **234 corsi di formazione** universitaria, in notevole crescita rispetto ai 79 individuati a inizio 2022. I corsi analizzati includono sia insegnamenti singoli all'interno di corsi di laurea più generici[21] ("***offerta formativa non specializzata***"), sia corsi di laurea specifici sul tema, insieme a Master e Dottorati ("***offerta formativa specializzata***"). Nel dettaglio, su un totale di 97 Università statali e non statali (private, straniere e telematiche) riconosciute dal Miur, il monitoraggio ha rilevato per l'anno accademico 2022/2023 un totale di 234 unità tra insegnamenti e corsi di studio sulla cybersecurity. Tra questi, sono stati osservati 112 insegnamenti singoli all'interno di corsi di laurea magistrale, 56 insegnamenti singoli all'interno delle lauree triennali e 13 corsi singoli all'interno di dottorati di ricerca, a fronte di **4 lauree triennali, 22 lauree magistrali, 7 dottorati e 18 master interamente dedicati alla cybersecurity**. A tal proposito, si osserva come il numero dei corsi singoli, e conseguentemente il totale dei corsi rilevati, non costituisca un **indicatore del livello di approfondimento** o di specializzazione sui temi della cibersicurezza, proprio perché **la maggior parte dell'offerta si compone di insegnamenti singoli all'interno di corsi di laurea più generici**, in particolar modo in corsi di laurea magistrali, che sono con tutta evidenza difficilmente confrontabili con lauree e percorsi specificamente incentrati sulla sicurezza cibernetica.

Fig. 4.1: Offerta formativa specializzata e non specializzata in materia di cybersecurity per tipo (a.a. 2022-23)

Fonte: I-Com, gennaio 2023



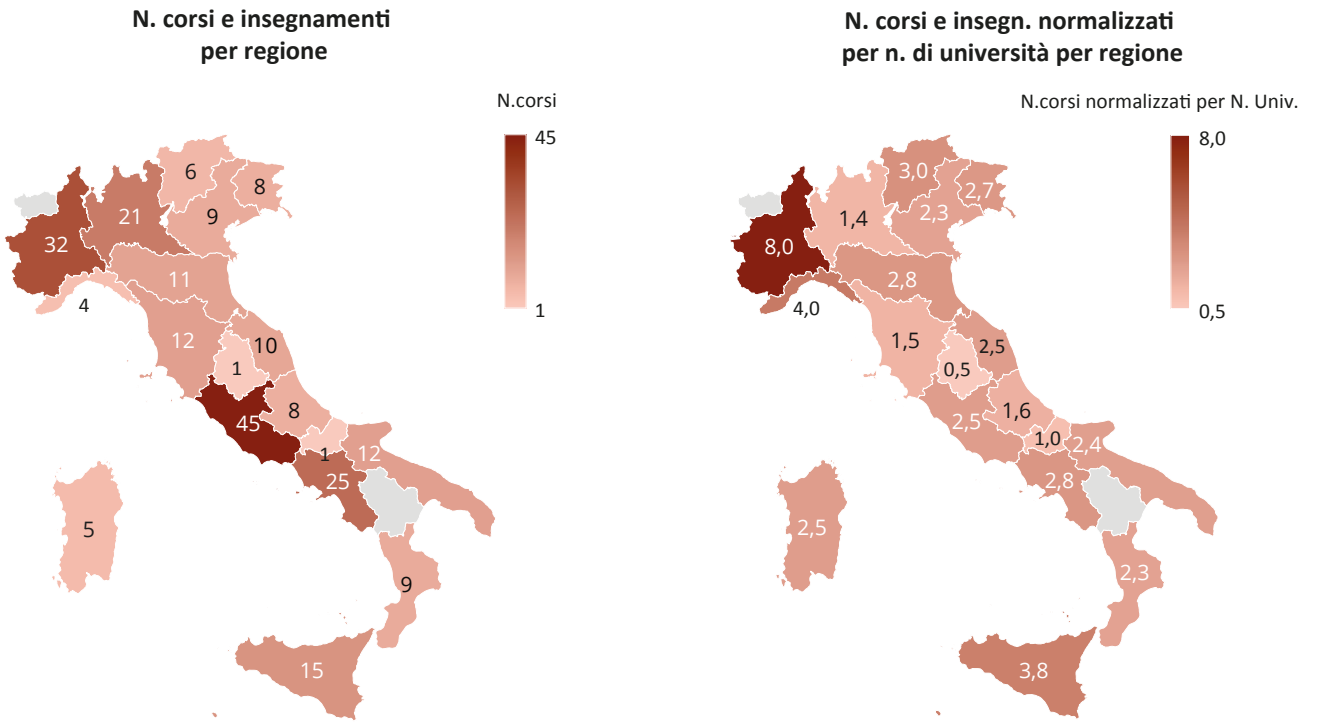
** include corsi generici sulla cybersecurity che possono essere seguiti per ottenere crediti formativi, nonché singoli corsi all'interno di Master*

20 Il monitoraggio condotto nel 2022 è stato aggiornato e rimodulato all'inizio dell'anno in corso, includendo l'offerta formativa 2022-2023 disponibile sui siti web delle università statali e non statali, incluse quelle online.

21 Esempio: un insegnamento in Cibersicurezza all'interno della LM in Informatica.

Fig. 4.2: Offerta formativa sulla cybersecurity per regione (a.a. 2022-2023)

Fonte : I-Com, gennaio 2023



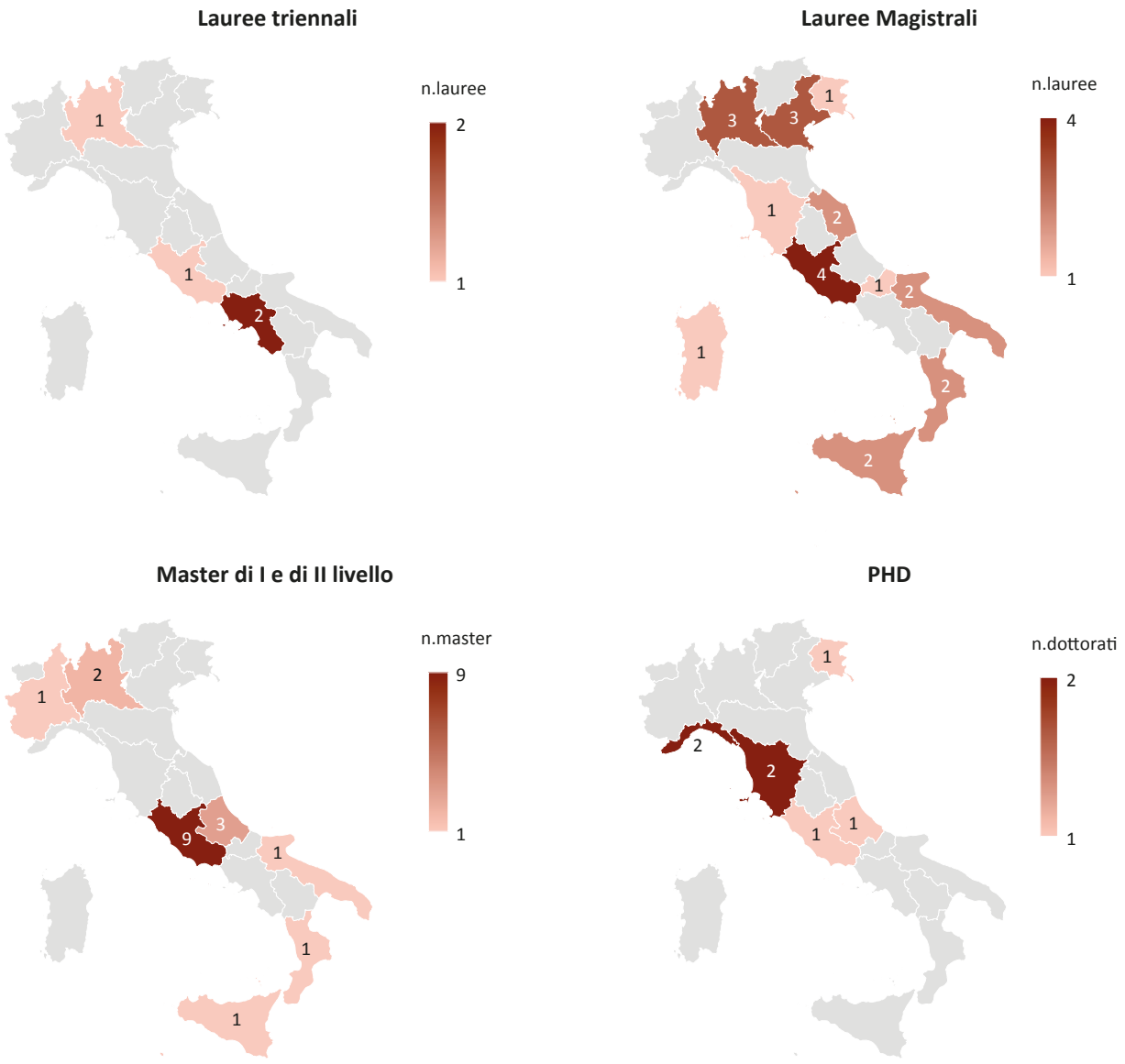
Allo stesso tempo, è interessante notare come le **lauree specifiche sul tema della cibersicurezza siano in aumento, giunte a quota 26** (gennaio 2023) rispetto alle 13 rilevate a gennaio 2022. Tuttavia queste appaiono ancora **relativamente poche** e quasi **tutte collocate,** salvo rare eccezioni, **nel ciclo magistrale**. A tal proposito si osserva che, qualora ciò dovesse dipendere dalla maggiore rigidità dei corsi di laurea triennale, **potrebbe essere opportuno da un lato introdurre criteri di maggiore flessibilità, e dall'altro puntare su un maggiore coinvolgimento degli ITS** (cfr. paragrafo successivo), sia in termini di preparazione per il prosieguo della formazione, sia in quanto preparazione a sé stante per formare tecnici già pronti per essere introdotti, quantomeno rispetto a specifici aspetti, nel mondo del lavoro.

Parallelamente, si osserva come la **formazione specializzata post-laurea** si affianchi a quella universitaria con numeri molto simili, ovvero **ben 25 corsi "specializzati" tra master e dottorati** a fronte delle 26 tra lauree triennali e quinquennali dedicate. Pertanto, è importante notare come **la formazione specializzata in materia di cibersicurezza in Italia abbia raggiunto quota 51 corsi di studio interamente dedicati.**

Per quanto concerne la **distribuzione dell'offerta formativa (specializzata e non specializzata) a livello regionale, si osserva come questa appaia piuttosto disomogenea** (Fig. 4.2), con una forte concentrazione nel **Lazio** (45 corsi) e in **Piemonte** (32 corsi), seguite da **Campania** (25) e **Lombardia** (21 corsi). Il Piemonte, in particolare, risulta nettamente primo in termini di corsi in cybersecurity normalizzati per il numero di università presenti sul territorio regionale (con un rapporto di 8:1), seguito da Liguria (4:1)

Fig. 4.3: Offerta formativa specializzata sulla cybersecurity per regione (a.a. 2022-2023)

Fonte: I-Com

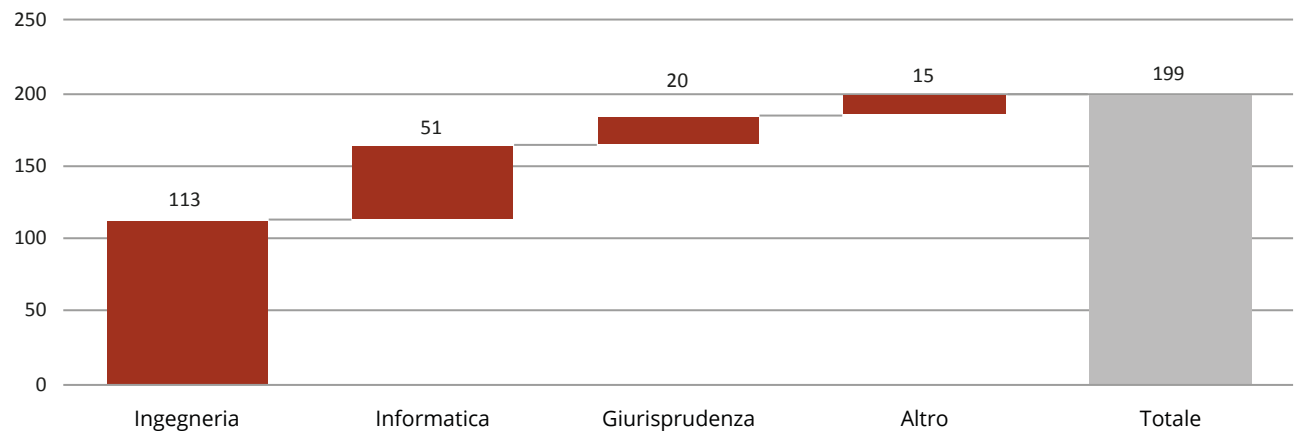


Note: l'offerta formativa specializzata comprende una Laurea Triennale, una Laurea Magistrale, , un Master I Livello, un Master II Livello o un Phd incentrati sul tema della cybersecurity

e Sicilia (3,8:1). D'altro canto, sono 29 le Università che non presentano nella propria offerta formativa alcun insegnamento o un corso di studio relativo alla cybersecurity. A livello regionale, a gennaio 2023 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere.

Fig. 4.4: Insegnamenti e corsi di studio per dipartimento (a.a. 2022-2023)

Fonte: I-Com



Nota: rispetto ai dottorati di ricerca, ai master di I° e II° livello e ad eventuali insegamenti connessi non è stato attribuito il dipartimento di appartenenza

Analizzando la **distribuzione geografica e universitaria dell'offerta formativa specializzata, ovvero comprendente corsi di studi interamente dedicati alla cybersecurity, il Lazio si conferma la regione più interessata con 15 percorsi complessivi**, catalizzando gran parte dell'offerta sia in termini di lauree dedicate (5 tra magistrali e triennali), sia per quanto concerne la specializzazione post-laurea, composta da 9 master e 1 dottorato attivi. Tra le altre regioni, la Lombardia presenta 1 laurea triennale, 3 magistrali e 2 master.

Nel contesto della formazione specializzata, è interessante notare anche l'**elevato numero di master specifici sui temi della cibersicurezza**: su tutto il territorio nazionale ne sono stati rilevati 18, **9 di I Livello e ulteriori 9 di II Livello**, di cui **oltre la metà con sede nel Lazio**.

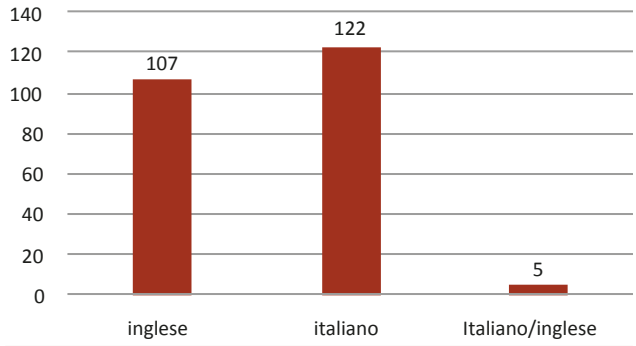
Complessivamente l'alto numero di Master sembrerebbe suggerire un'**elevata domanda di approfondimento post-laurea su questi temi**, probabilmente dovuta a un mismatch – sebbene in progressiva riduzione – tra domanda e offerta di tali competenze sul mercato del lavoro e alla diffusione della **consapevolezza** che tali conoscenze possano costituire un **valore aggiunto** nel mondo del lavoro.

Analizzando il numero di insegnamenti o corsi di studio sulla cibersicurezza divisi **per dipartimento**, si osserva come **oltre la metà di essi faccia capo a dipartimenti di ingegneria** (113), ovvero più del doppio di quelli di offerti dai dipartimenti di informatica (51). Circa il 10% del totale, ovvero 20 tra corsi o insegnamenti, fanno capo a dipartimenti di giurisprudenza, mentre 15 sono relativi ad altri dipartimenti (economia, scienze, chimica e architettura).

Un ulteriore dato interessante riguarda la lingua: in particolare, dall'analisi emerge che ben **107** dei **234** corsi rilevati sono in **lingua inglese**, evidenziando le caratteristiche internazionali e internazionalizzanti di tali materie. L'**inglese** è lievemente **predominante per le lauree magistrali specificamente incentrate sui temi della cybersecurity** (12 in inglese, 9 in italiano e 1 ibrida) **mentre i master sono quasi interamente in italiano (17 su 18), probabilmente a riprova del maggiore legame col mondo aziendale**. Infine, si rileva un profilo più internazionale nei **dottorati: 5 su 7 sono attualmente in inglese.**

Fig. 4.5: Lingua utilizzata per gli insegnamenti e corsi di studio in cybersecurity (a.a. 2022-2023)

Fonte: I-Com



4.2 Stato dell'arte e riforma degli ITS

Gli Istituti Tecnici Superiori, o ITS, vengono definiti dal Ministero dell'Istruzione italiano come "**scuole di eccellenza ad alta specializzazione tecnologica post diploma che permettono di conseguire il titolo di tecnico superiore**". Questa tipologia di Istituti è stata introdotta nel 2010 con l'obiettivo di formare personale tecnico in aree strategiche per lo sviluppo del tessuto economico del nostro Paese. I percorsi formativi sviluppati dagli ITS sono afferenti a **sei aree tecnologiche**: Efficienza energetica, Mobilità sostenibile, Nuove tecnologie della vita, Nuove tecnologie per il Made in Italy, Tecnologie innovative per i beni e le attività culturali, Tecnologie della informazione e della comunicazione. Il ruolo di tali Istituti è quindi di fungere da anello di congiunzione tra la realtà scolastica e quella lavorativa, offrendo agli studenti gli strumenti utili a rispondere alle competenze richieste dal mercato del lavoro.

Secondo l'ultimo rapporto di monitoraggio pubblicato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE), **nel 2022 risultano presenti sul territorio nazionale 120 ITS** (Fig. 4.6). La regione che ospita il numero maggiore di istituti è la **Lombardia (20),** seguita dalla **Sicilia (11),** mentre al terzo posto si trovano a pari merito Calabria, Campania e Toscana (9). Parametrando il dato sulla diffusione regionale alla popolazione si osserva come ad emergere siano in particolare la Calabria (4,9 ogni milione di abitanti), la Liguria (4 ogni milione di abitanti) e l'Abruzzo (3,9 per milione di abitanti).

Relativamente alle aree strategiche, prevalgono nettamente le "Nuove tecnologie per il made in Italy" con 49 unità, che al loro interno si articolano a loro volta in 5 sottosezioni afferenti ad altrettanti settori economici (Servizi alle imprese, Sistema agro-alimentare, Sistema casa, Sistema meccanica, Sistema moda), seguite dalla "Mobilità Sostenibile" (20), l' "Efficienza energetica" (15), le "Tecnologie innovative per i beni e le attività culturali" (14), le Tecnologie dell'informazione e della comunicazione (14) e le nuove tecnologie della vita (8).

Nonostante i profili lavorativi formati attraverso gli Istituti Tecnici Superiori siano individuati selezionando le principali competenze richieste sul mercato – quindi potenzialmente tra le figure con la maggiore possibilità di trovare un'occupazione – **il numero di ragazzi che sceglie questa tipologia di formazione è notevolmente inferiore rispetto a quello delle altre maggiori economie europee** (Fig. 4.7). Osservando i dati contenuti nel rapporto "Next Generation digITALY", pubblicato a settembre 2022 da The European House-Ambrosetti, si osserva come nel 2019 il numero di studenti italiani iscritti a scuole di istruzione post secondaria non terziaria ammonti a **circa 19 mila, contro gli oltre 740 mila fatti registrare dalla Germania, i 26 mila della Francia e i 25 mila della Spagna**.

I dati sopracitati mostrano piuttosto chiaramente il gap di competenze che esiste tra l'Italia e gli altri principali paesi europei, sottolineando ancora una volta la criticità – più volte espressa dal mondo dell'impresa – di non riuscire a **reperire sul mercato competenze adeguate per sopperire alle necessità lavorative**, in particolare quelle che dovrebbero sfruttare le nuove tecnologie digitali. Inoltre, un'indagine conoscitiva effettuata da Ambrosetti, in cui sono state intervistate

Fig. 4.6: Distribuzione degli ITS per regione e per area strategica (2022)

Fonte: Istituti Tecnici Superiori – Monitoraggio nazionale 2022 (INDIRE)

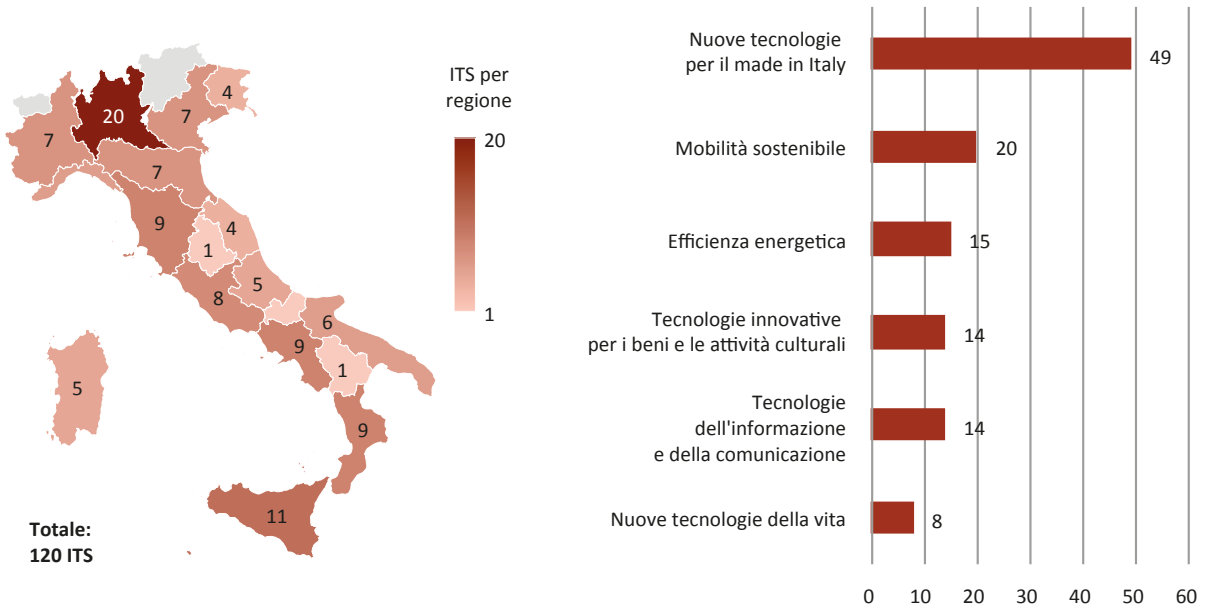
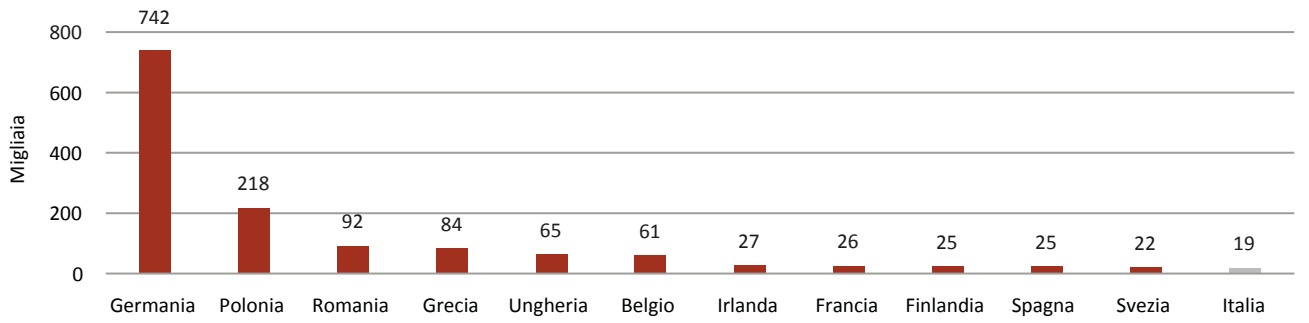


Fig. 4.7: Studenti iscritti a istruzione post secondaria non terziaria per Paese (2019)

Fonte: elaborazione The European House - Ambrosetti su dati Eurostat, 2022



oltre 150 imprese, ha fatto emergere la **non adeguatezza delle competenze degli studenti che terminano l'attuale percorso formativo negli ITS** (Fig. 4.8.). In particolare, solo per il 26% dei rispondenti la scuola fornisce le competenze di base che sono necessarie alle imprese, mentre il restante 74% ha affermato come sia necessario un maggiore allineamento con le esigenze del settore (Fig. 4.8).

Per quanto concerne i percorsi degli ITS dedicati esplicitamente al **comparto ICT,** i dati mostrano come gli **studenti iscritti** agli indirizzi in quest'area strategica siano **appena 889** (Fig. 4.9). D'altro canto, un elemento positivo è rappresentato dall'imponente crescita registrata nell'ultimo quinquennio, che ha portato ad un aumento del 346% del numero di ragazzi che scelgono quest'area formativa.

Fig. 4.8: Ritenete adeguato il livello di formazione dei diplomati degli Istituti di formazione professionale e ITS?

Fonte: The European House – Ambrosetti, 2022

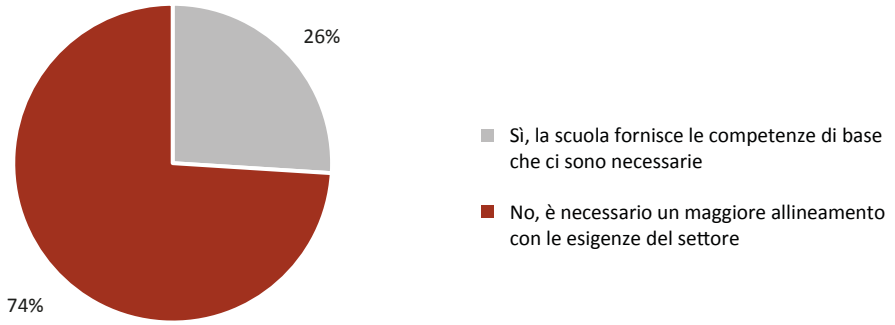
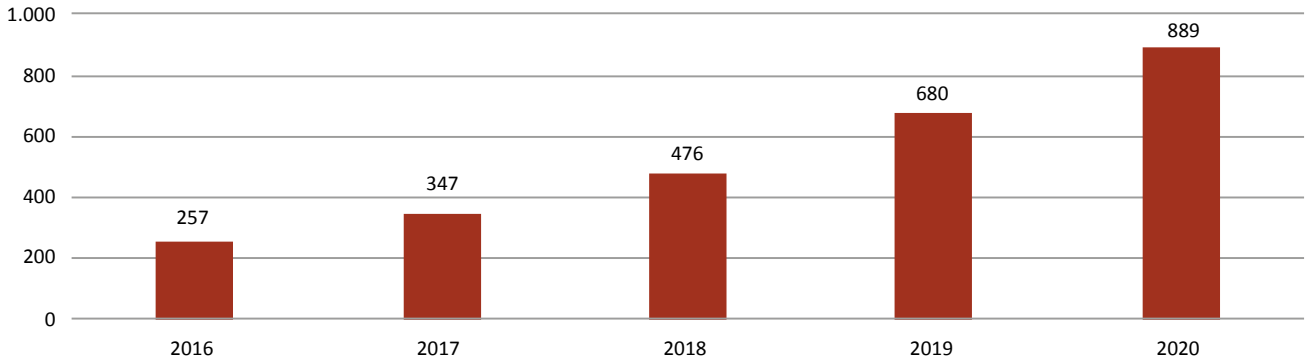


Fig. 4.9: Studenti iscritti in percorsi ICT di Istituti Tecnici Superiori, 2016-2020

Fonte: The European House – Ambrosetti, 2022



4.3 La riforma degli ITS

Se questo è lo stato dell'arte, uno degli interventi senza dubbio più rilevanti annunciato nella Missione 4 del PNRR è senza dubbio la **riforma del sistema ITS,** attraverso il potenziamento del modello organizzativo e didattico, il consolidamento degli stessi ITS nel sistema ordinamentale dell'Istruzione terziaria professionalizzante e il rafforzamento della presenza attiva nel tessuto imprenditoriale dei singoli territori, garantendo un'integrazione dei percorsi ITS con il sistema universitario delle lauree professionalizzanti. Lo stesso **PNRR** mira al potenziamento dell'offerta degli enti di formazione professionale terziaria attraverso la creazione di network con aziende, università e centri di ricerca tecnologica/scientifica, autorità locali e sistemi educativi/formativi con l'obiettivo di incrementare il numero degli ITS (raddoppiandolo), potenziare i laboratori con tecnologie 4.0, formare docenti in grado di adattare i programmi formativi ai fabbisogni delle aziende locali e sviluppare una piattaforma digitale nazionale per le offerte di lavoro rivolte agli studenti in possesso di qualifiche professionali.

Quanto annunciato dal PNRR ha preso vita con la pubblicazione sulla G.U. del 26 luglio scorso, della **L. n. 99 del 15 luglio 2022.** La riforma degli ITS che diventano Istituti Tecnologici Superiori – ITS Academy aperti a giovani e adulti in possesso di un diploma di

scuola secondaria di secondo grado o di un diploma quadriennale di istruzione e formazione professionale, unitamente a un certificato di specializzazione dei corsi di istruzione e formazione tecnica superiore di almeno 800 ore, mira a rendere la formazione terziaria professionalizzante più attrattiva e ad arricchire l'offerta anche in risposta alle esigenze del tessuto produttivo dei territori ed all'evoluzione del mercato del lavoro e dell'economia. Rispetto all'offerta formativa e, dunque, all'individuazione delle specifiche aree tecnologiche, la riforma focalizza l'attenzione, in particolare, su transizione ecologica, compresi i trasporti, la mobilità e la logistica, la transizione digitale, le nuove tecnologie per il made in Italy, compreso l'alto artigianato artistico, le nuove tecnologie della vita, i servizi alle imprese e agli enti senza fine di lucro, le tecnologie per i beni e le attività artistiche e culturali e per il turismo, le tecnologie dell'informazione, della comunicazione e dei dati e l'edilizia, rimettendone l'individuazione ad un successivo decreto e distingue i percorsi formativi in due livelli[22].

Il vero punto di forza della riforma risiede nel **più forte legame col mondo delle imprese**. Ed infatti, è previsto che l'attività formativa sia svolta per almeno il 60% del monte orario complessivo da docenti provenienti dal mondo del lavoro e che gli stage aziendali e i tirocini formativi, obbligatori almeno per il 35% del monte orario complessivo, possano essere svolti anche all'estero con l'adeguato sostegno di borse di studio. Il mondo delle imprese diventa centrale anche rispetto alle nuove regole per l'avvio di un ITS; infatti, la nuova disciplina subordina la possibilità di avviare un nuovo ITS in una Provincia alla presenza, tra l'altro, di almeno una o più imprese legate all'uso delle tecnologie di cui si occuperà l'ITS Academy e consente di diventare soggetti fondatori di un ITS. Rispetto al tema dei finanziamenti, la nuova legge riconosce per le erogazioni liberali in denaro effettuate in favore delle fondazioni ITS Academy a partire dal periodo d'imposta 2022 (attraverso gli strumenti di pagamento indicati) un credito d'imposta nella misura del 30% che sale al 60% nel caso in cui l'erogazione sia effettuata in favore di fondazioni ITS Academy operanti nelle Province in cui il tasso di disoccupazione è superiore a quello medio nazionale. Molto rilevante l'istituzione di "reti di coordinamento di settore e territoriali", per condividere buone pratiche e laboratori, incentivare gemellaggi tra fondazioni di Regioni diverse e favorire la conoscenza degli ITS Academy attraverso campagne informative ed attività di orientamento. Guardando alle risorse, la legge, in una logica di rafforzamento degli ITS, ha istituito anche un apposito Fondo presso il Ministero dell'Istruzione con una dotazione di euro 48.355.436 euro annui a decorrere dal 2022 da distribuire alle regioni (per il 2022 il riparto è stato disposto con decreto del 26 agosto scorso) al netto di un 5% destinato alla realizzazione delle misure nazionali di sistema, tra le quali il monitoraggio e la valutazione. Rispetto al modello di governance, la medesima legge ha istituito presso il Ministero dell'istruzione il Comitato nazionale ITS Academy per l'istruzione tecnologica superiore chiamato a proporre le linee generali di indirizzo dei piani triennali di programmazione delle attività formative adottati dalle Regioni, le direttrici per il consolidamento, il potenziamento e lo sviluppo dell'offerta formativa, l'aggiornamento, con cadenza almeno triennale, delle aree tecnologiche e delle figure professionali per ciascuna area, criteri e modalità per la costituzione delle Reti di coordinamento di settore e territoriali e programmi per la costituzione e lo sviluppo, d'intesa con le regioni interessate, di campus multiregionali, in relazione a ciascuna area tecnologica, e di campus multisettoriali tra ITS Academy di aree tecnologiche e ambiti diversi.

22 5° livello EQF, di durata biennale, ovvero suddiviso in quattro semestri, con almeno 1.800 ore di formazione comprendenti ore di attività teorica, pratica e di laboratorio e 6° livello EQF, di durata triennale, ovvero suddiviso in sei semestri, con almeno 3.000 ore di formazione comprendenti ore di attività teorica, pratica e di laboratorio.

Si tratta di una riforma assolutamente importante che ad oggi, complice il cambio di Governo e la priorità data ad alcuni provvedimenti essenziali, a partire dalle legge di bilancio, è ancora in attesa dell'adozione dei decreti attuativi, 19, di cui 17 richiedono il previo accordo della Conferenza Stato-Regioni, indispensabili ad assicurare la piena operatività della riforma. Poiché, in particolare, il termine fissato per l'adozione dei decreti riguardanti le aree di riferimento, le linee guida dello schema di Statuto e le tabelle nazionali di corrispondenza, è inutilmente decorso lo scorso ottobre, il 29 novembre è stata tra l'altro presentata un'interrogazione al Senato da parte della senatrice Mariastella Gelmini, tesa, appunto, a conoscere le "tempistiche previste per dare piena attuazione" alla riforma sugli Istituti Tecnologici Superiori.

CAPITOLO 5

LE METODOLOGIE DI TEST E L'IMPORTANZA DELLA STANDARDIZZAZIONE INTERNAZIONALE

5.1 L'evoluzione delle certificazioni a livello internazionale

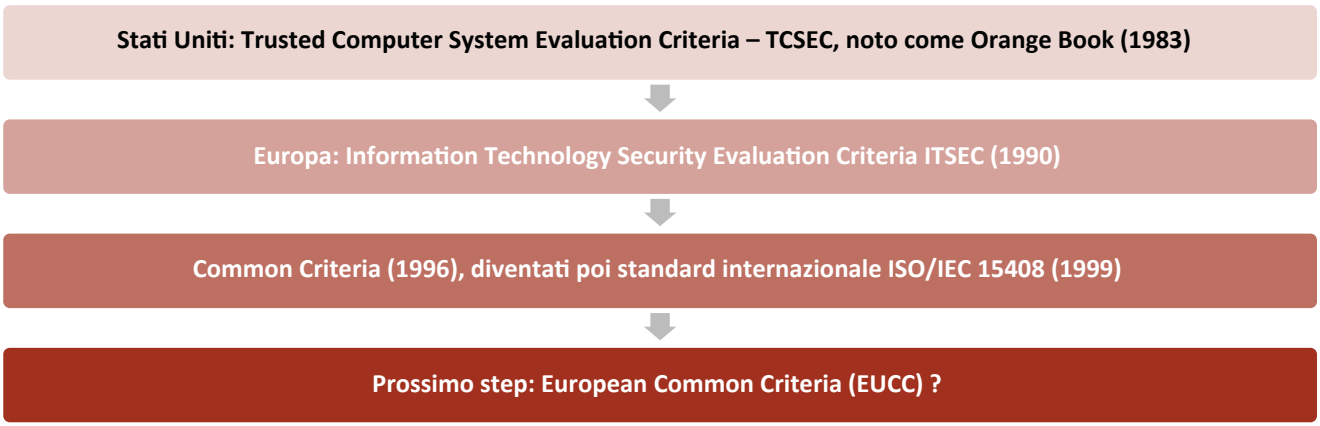
Poiché il cyberspazio è un mondo sempre più caratterizzato da confini evanescenti e dinamici, uno sforzo volto al regolamentarne e uniformarne gli usi e le caratteristiche richiede inevitabilmente sinergie tra tutti gli Stati oggi chiamati a dettarne le regole mediante, da un lato, l'esercizio della propria sovranità e, dall'altro, la messa in campo di azioni congiunte a livello internazionale. È infatti ormai opinione diffusa, in particolare nel contesto europeo, che la spinta verso una sempre maggiore interoperabilità e standardizzazione rappresenti una delle principali chiavi anche per garantire ulteriore affidabilità e sicurezza all'ecosistema digitale e ai prodotti e servizi che in esso vengono forniti.

Anche l'Italia è ben consapevole dell'importanza delle collaborazioni internazionali e della necessità che ciascuno Stato agisca per impedire che il proprio territorio o le proprie infrastrutture ICT siano usati per condurre attività cybercriminali. In linea con il lavoro avviato nel contesto Comunitario, il Governo italiano nel 2021 ha infatti rilasciato un position paper[23] specificatamente incentrato sull'applicabilità del diritto internazionale alla cybersicurezza. Il documento, realizzato dal Ministero degli Affari esteri e della cooperazione internazionale, parte dalla constatazione delle difficoltà di individuare gli autori di illeciti nel cyberspazio e di apprestare contromisure adeguate all'attacco cibernetico, sottolineando il valore della legge internazionale e la necessità di garantire la tutela dei diritti umani includendola nell'ambito degli obblighi di due diligence in capo agli Stati e nelle aree di responsabilità del settore privato.

La sensibilità su tali argomentazioni a livello internazionale trova la sua origine negli Stati Uniti, con la nascita del *Trusted Computer System Evaluation Criteria* – **TCSEC**, noto come *Orange Book* (nel 1983). Questa pubblicazione, che identificava i requisiti fondamentali per la definizione dell'efficacia dei controlli di sicurezza di un sistema informatico, poneva particolare enfasi sul trattamento di informazioni sensibili, strategiche e classificate (Fig. 5.1).

Fig. 5.1: L'evoluzione degli standard di certificazione

Fonte: elaborazioni I-Com



23 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

Nel 1990, la risposta europea si è concretizzata nella redazione dell'*Information Technology Security Evaluation Criteria* – **ITSEC** – uno standard che tuttavia non ha mai raggiunto la diffusione inizialmente auspicata. Sviluppato e adottato da Francia, Germania, Regno Unito e Olanda, questo sistema ha introdotto per la prima volta il concetto di "*Target*" e l'utilizzo di un documento di analisi detto "*Security Target*", che accompagna il processo di valutazione e il cui contenuto doveva essere esaminato e approvato prima che l'obiettivo stesso fosse valutato[24]. Successivamente, sulla base dell'ITSEC sono stati creati nel 1996 i **Common Criteria**, che forniscono livelli di valutazione definiti in modo simile e che riprendono sia il concetto di *Target* che la centralità del documento *Security Target*. In seguito, grazie alla certificazione dell'ISO, l'Organizzazione internazionale per la normazione *(International Organization for Standardization),* questi sono divenuti nel 1999 **standard internazionale ISO/IEC 15408**, imponendosi come punto di riferimento globale per la valutazione della sicurezza informatica.

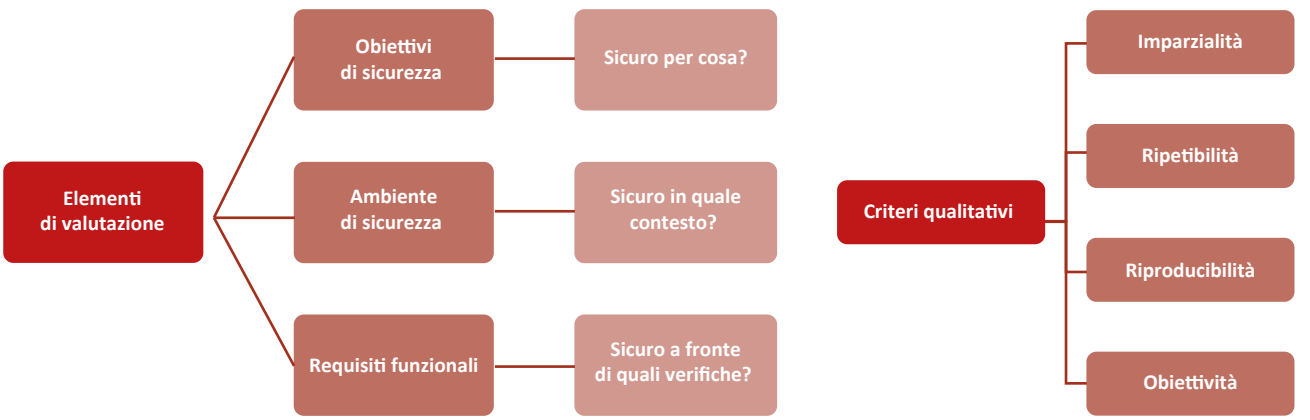
5.1.1 Il funzionamento dei Common Criteria

L'ottenimento di certificazioni per i propri apparati ICT è un processo che in genere gli operatori effettuano volontariamente, per mostrare a clienti business e utenti finali il proprio livello di affidabilità. Allo stesso tempo, in alcuni casi le Autorità Nazionali possono definire alcune eventuali obbligatorietà. Per quanto concerne l'Italia, la ricerca di profili specializzati nell'utilizzo di Common Criteria da parte della nascente Agenzia per la Cybersicurezza e le molteplici innovazioni normative, che rafforzano i poteri di Governo e Agenzia in materia, sembrano indicare l'interesse per questo tipo di certificazioni, al fine di autorizzare l'utilizzo di prodotti e sistemi ICT nelle reti di telecomunicazioni italiane.

A livello tecnico, i Common Criteria hanno la funzione di definire dei criteri per rendere misurabili, e quindi comparabili in maniera oggettiva e incondizionata, le proprietà legate alla sicurezza di un prodotto o di un sistema informatico (Fig. 5.2). Questi sono strutturati in modo da rispettare criteri qualitativi tali da garantire alla documentazione prodotta un elevato livello

Fig. 5.2: I Common Criteria: elementi di valutazione e criteri qualitativi

Fonte: elaborazioni I-Com su varie



24 Commissione europea, Direzione generale della Società dell'informazione e dei media, *Information Technology Security Evaluation Criteria (ITSEC) : Provisional evaluation criteria: Document COM(90) 314*, Publications Office, 1992.

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 non deve comprendere stime di carattere soggettivo (**obiettività**).

La documentazione prodotta in ottemperanza di questi criteri evidenzia gli elementi fondamentali dell'oggetto della valutazione, ovvero del ***Target of Evaluation*** (TOE). Per ottenere la certificazione è necessario identificare tre elementi fondamentali in relazione al TOE sotto esame. Il primo consiste negli **obiettivi di sicurezza**, che definiscono l'intenzione per cui si intende operare la valutazione (ad esempio contrastare una minaccia, assicurare il rispetto delle leggi, ovvero si intende specificare "sicuro per cosa"). Il secondo elemento riguarda **l'ambiente di sicurezza**, che delinea il contesto in cui il TOE 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"). Il terzo elemento è relativo ai **requisiti funzionali**, che identificano le verifiche di sicurezza e il corrispondente livello di *assurance* garantito da queste ("sicuro a fronte di quali verifiche").

Sulla base della struttura indicata dai Common Criteria, in Italia attualmente vige uno **Schema Nazionale** per la certificazione della sicurezza di prodotti e sistemi ICT nell'ambito dei *dati classificati* risalente al 1995. Nel 2003 si è aggiunto un **Secondo Schema Nazionale**[25] indicato per la fornitura di servizi di certificazioni nel contesto della Pubblica Amministrazione e negli ambiti non ricompresi nella Sicurezza Nazionale. Organismi essenziali di questi sistemi sono **i laboratori preposti alla valutazione**, che conducono le analisi ed elaborano la documentazione necessaria ai fini della valutazione, e gli **enti di certificazione**, che emettono la certificazione di sicurezza e accreditano i laboratori.

Nel contesto italiano, tali strutture assumono una declinazione particolare e suddivisa, risultando in una architettura sviluppata su tre livelli che coinvolge nel processo enti differenti in base alla tipologia di dati trattati (dati certificati, funzioni strategiche o commerciali)[26]. Ciò nonostante, è importante evidenziare come le strutture di entrambi questi schemi siano modellate sulla base degli standard internazionali di riferimento (ITSEC e Common Criteria), così da permettere, **in attesa di uno standard comunitario**, l'adozione del principio del mutuo riconoscimento a livello europeo, per cui gli Stati europei riconoscono le certificazioni erogate da altri Stati europei (Fig. 5.3).

A livello operativo, il processo di certificazione dei Common Criteria viene eseguito per mezzo del ***Vulnerability Assessment*** e poggia su due documenti critici per la definizione del TOE: il *Protection Profile* e il già citato *Security Target*. Quest'ultimo è il documento che **descrive** il **prodotto oggetto della valutazione** (il TOE) e costituisce di fatto il prodotto finale del processo di valutazione. Il contenuto del Security Target è composto da svariati elementi[27], tra cui i requisiti di sicurezza (SFR) e di garanzia (SAR), che risultano determinanti per misurare quantitativamente il

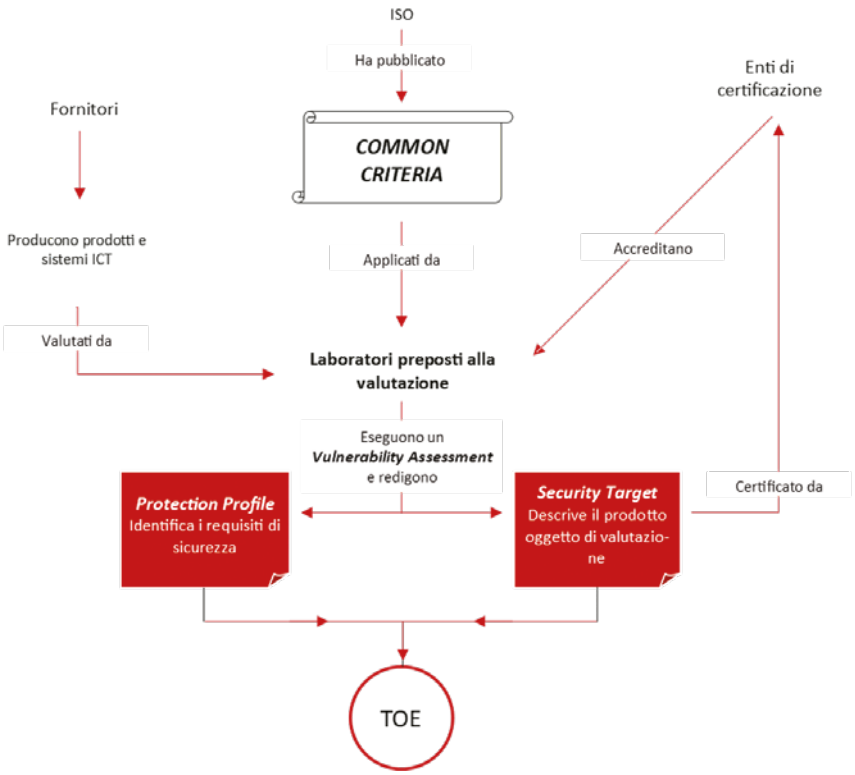
25 DPCM 30 ottobre 2003

26 Per i dati classificati 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. Nel caso di funzioni critiche o strategiche si fa invece riferimento al Centro Valutazione e Certificazione Nazionale (CVCN). Infine, per quanto riguarda invece i prodotti e sistemi ICT commerciali, l'autorità di certificazione è l'Organismo di Certificazione della Sicurezza Informatica (OCSI) che si occupa di accreditare gli apposti Laboratori per la Valutazione della Sicurezza (LVS).

27 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.

Fig. 5.3: Il funzionamento degli schemi nazionali

Fonte: elaborazioni I-Com



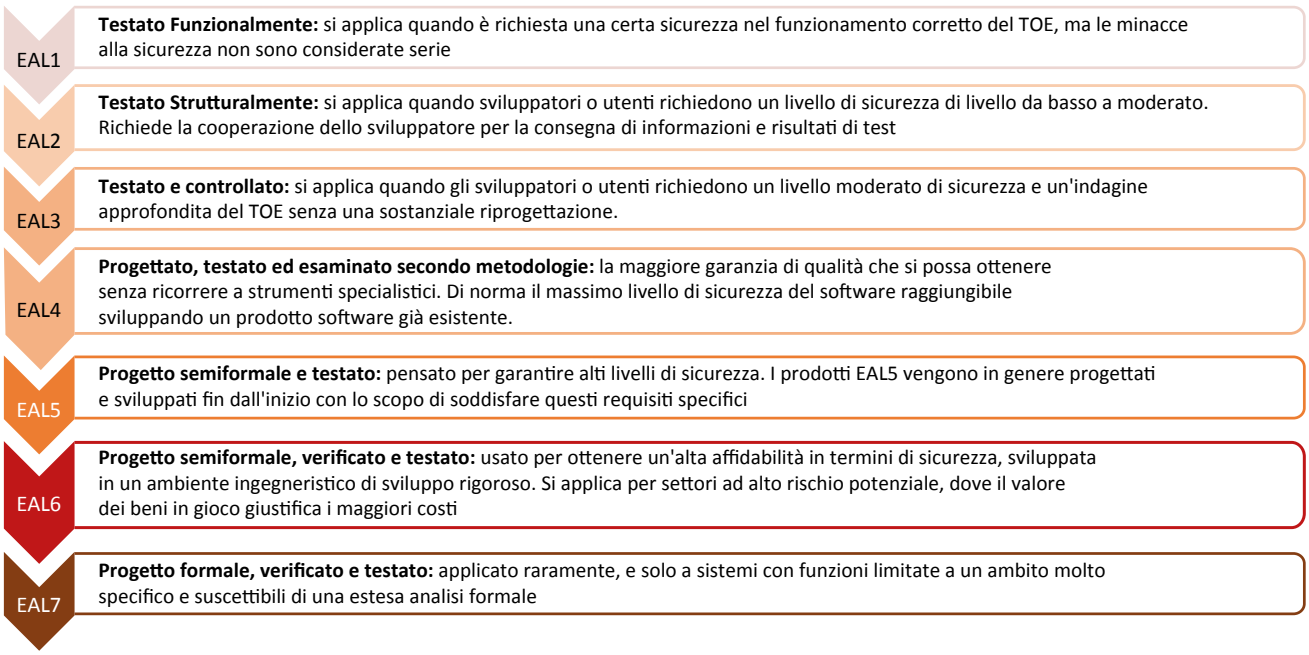
grado di sicurezza del TOE stesso[28]. Il **Protection Profile**, invece, è un documento che descrive gli obiettivi di sicurezza, le minacce, l'ambiente e i requisiti funzionali e di garanzia per una certa categoria di prodotto/sistema ICT. Non vengono pertanto descritti in modo particolare i prodotti specifici 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 da template di riferimento per la stesura del Security Target, 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 specifici che qualificano la 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 e si è in presenza di minacce poco rilevanti; seguono l'EAL2

28 I requisiti di sicurezza, ovvero i Security Functional Requirements (SFR), specificano funzionalità di sicurezza individuali che un prodotto o un sistema possono fornire. Nel caso dei Common Criteria queste sono racchiuse in un catalogo in cui le funzioni vengono suddivise in 12 famiglie. I requisiti di garanzia, ovvero Security Assurance Requirements (SAR), invece descrivono le misure prese durante lo sviluppo e la valutazione del prodotto in modo da garantire l'aderenza con i SFR. Il catalogo dei SAR comprende 8 famiglie, ma la specifica dei SAR cambia di valutazione in valutazione.

Fig. 5.4: I 7 livelli di sicurezza EAL

Fonte: elaborazioni I-Com su varie



(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 Common Criteria. E' indicato nei casi di minaccia medio-alta ed è il livello più richiesto dai committenti** (Fig. 5.4).

5.1.2 I pro e contro dei sistemi di certificazione

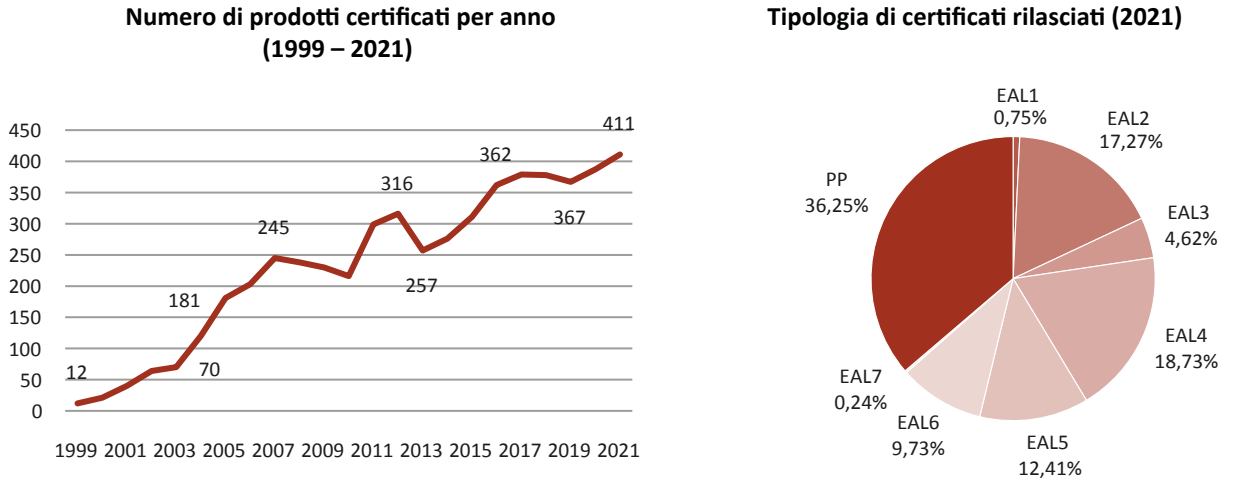
Con il diffondersi di una sempre maggiore consapevolezza dei potenziali rischi cibernetici derivanti dall'espansione costante del mercato digitale nel suo insieme, **l'apprezzamento per i sistemi condivisi di valutazione è cresciuto costantemente negli anni**. Questo è **evidenziato dall'aumento di richieste di certificazione ricevute e di certificazioni rilasciate** che, secondo lo studio Jtsec, **nel 2021 ha raggiunto il valore più alto della storia**[29], rafforzando una tendenza in forte crescita, particolarmente marcata soprattutto dal 2013 ad oggi, e segnando un aumento del +6% rispetto al 2020 (Fig. 5.5).

Per il fornitore del prodotto ICT, il vantaggio maggiore derivante dall'ottenimento della certificazione riguarda la **competitività** sul mercato: difatti, tale prodotto certificato gode di maggiore fiducia da parte dei consumatori e pertanto di maggiore domanda rispetto ai prodotti non certificati. Inoltre, in presenza di uno standard comune di valutazione, i consumatori

29 Secondo Jtsec, che ha monitorato l'evoluzione del numero di certificazioni attraverso tecniche di *web crawling*, il 2021 è stato l'anno con il più alto numero di certificazioni Common Criteria nella storia, con 411 attestazioni registrate. Dati Jtsec – *"Common Criteria Statistics Report for 2021"* (febbraio 2022).

Fig. 5.5: Tendenze dei certificati Common Criteria

Fonte: Jtsec – *"Common Criteria Statistics Report for 2021"*



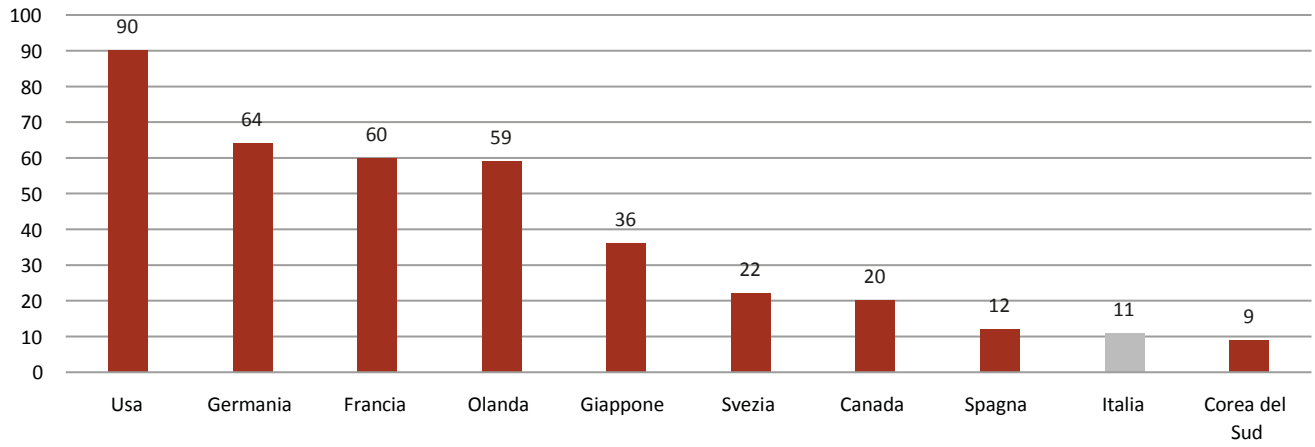
operano facilmente **confronti tra i prodotti**, riponendo maggiore fiducia nei fornitori che hanno ottenuto certificazioni e che hanno dunque ricevuto un riconoscimento ufficiale per le loro competenze. Il rilascio della certificazione può inoltre garantire l'accesso a **mercati chiusi o specializzati** che necessita di requisiti minimi di sicurezza per prodotti, come ad esempio il mercato bancario. In più, **in attesa di standard comunitari, i Common Criteria offrono ai governi nazionali uno strumento per garantire che i sistemi IT utilizzati nel Paese siano sicuri, consentendo di contrastare rischi sistemici**: gli standard di sicurezza dovrebbero infatti essere utilizzati per la verifica anche di infrastrutture e servizi in ambiti particolarmente strategici e dal considerevole valore di mercato, tra cui ad esempio quello delle apparecchiature di rete 5G, come evidenziato nel contesto del **Cybersecurity Act**[30], tra i cui obiettivi figurano appunto **l'armonizzazione dei criteri di sicurezza a livello di Unione attraverso una politica comune**. **Una maggiore armonizzazione è particolarmente auspicata anche dai produttori, in quanto lo scenario estremamente complesso e frammentato produce ancora considerevoli ostacoli non solo al raggiungimento degli standard prefissati, ma anche in termini più generali alla ricerca innovativa di soluzioni e allo sviluppo di livelli minimi di fiducia condivisi tra produttori e consumatori.**

Tra le numerose difficoltà riscontrate nel raggiungere gli standard auspicati si evidenzia come la **documentazione richiesta dai sistemi nazionali aumenti considerevolmente i costi della valutazione**, oggi a carico del fornitore, costituendo una barriera ad un uso efficiente di tali controlli. In generale, i **costi** del

30 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=EN. "L'ENISA dovrebbe incoraggiare gli Stati membri, i fabbricanti o i fornitori prodotti TIC, servizi TIC o processi TIC a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di Internet possano adottare le misure necessarie a garantire la propria cibersicurezza e incentivarli a farlo. In particolare, i fabbricanti e i fornitori di servizi di prodotti TIC, servizi TIC o processi TIC dovrebbero fornire tutti i necessari aggiornamenti e richiamare, ritirare o riciclare i prodotti TIC, i servizi TIC o i processi TIC non conformi alle norme in materia di cibersicurezza, mentre gli importatori e i distributori dovrebbero garantire che i prodotti TIC, servizi TIC e processi TIC che immettono sul mercato dell'Unione siano conformi ai requisiti applicabili e non presentino rischi per i consumatori dell'Unione."

Fig. 5.6: Top 10 Paesi per certificazione prodotti con Common Criteria (2021)

Fonte: Jtsec – *"Common Criteria Statistics Report for 2021"*



processo sono inoltre già di per sé **elevati** poiché – oltre al tempo impiegato – la valutazione richiede **l'utilizzo di risorse specializzate**, costituendo pertanto una **potenziale barriera all'ingresso (o alla permanenza) nel mercato, per quegli operatori di medie dimensioni** (piccoli Carriers, piccoli vendors) che attualmente non prevedono i Common Criteria nei loro processi interni.

Parallelamente, elementi di criticità del sistema dei Common Criteria sono rappresentati dai **lunghi tempi di esecuzione della valutazione e del rilascio delle certificazioni**, ritenuti non conformi al dinamismo e alla velocità di evoluzione del settore digitale. Difatti, ad eccezione dei livelli EAL1 e EAL2, che possono richiedere anche "solo" poche settimane, **i livelli dal terzo in poi possono impiegare un orizzonte temporale di vari mesi**, il che espone il prodotto/sistema al **rischio di essere divenuto obsoleto nel momento del rilascio della certificazione**. L'esiguo numero complessivo di prodotti assicurati nel corso dello scorso anno, che secondo Jtsec ha raggiunto quota 411 a livello mondiale, è prova del fatto che sono solo pochi i prodotti che riescono a completare tutto l'iter in tempi ragionevoli, mentre molti altri sono costretti ad affrontare percorsi molto più lunghi. Su questo pesa inevitabilmente la struttura stratificata su livelli dei Common Criteria, la quale prevede che al crescere del livello di *assurance* crescano anche le verifiche a cui i prodotti devono essere sottoposti.

Altro importante elemento riguarda il **tempo addizionale** che verrà impiegato dal CVCN e dai laboratori indipendenti **per rendere effettive le procedure di valutazione**. Sembra infatti delinearsi una discrepanza, evidenziata dagli operatori del settore, tra l'effettiva capacità di assorbimento dei test da parte dei laboratori, che potrebbe aggirarsi tra i 10-15 test l'anno condotti con i Common Criteria, e il numero di prodotti da certificare, che è proporzionale al numero di aziende coinvolte all'interno del perimetro di sicurezza cibernetica (oltre 300). A tal proposito, i dati rilevati da Jtsec indicano per il 2021 l'avvenuta certificazione di 11 prodotti in Italia (Fig. 5.6).

Inoltre, le rigidità alla base dei Criteria non permettono di mantenere la certificazione per prodotti/sistemi su cui vengono installate nuove patch per aggiornamenti. Infatti, **in caso di aggiornamenti o modifiche, il prodotto in questione deve essere sottoposto nuovamente all'intero processo di valutazione**,

comportando non solo un ulteriore incremento nei costi della valutazione per i produttori, ma anche un sostanziale **disincentivo ad investire nello sviluppo di migliorie e innovazioni** per i beni e i servizi in questione. 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. Tali criticità, in un contesto in cui le certificazioni potrebbe diventare obbligatoria per talune tipologie di prodotti di rete, sono assolutamente da tener presenti anche considerando la questione dei prodotti già operativi, per i quali la richiesta di certificazioni retroattive rischia di comportare oneri molto elevati per i fornitori coinvolti e di impattare direttamente anche sugli equilibri del mercato.

5.2 Gli altri approcci internazionali per il mobile: il NESAS

Un altro modello di certificazione, il NESAS (*Network Equipment Security Assurance Scheme*), è stato sviluppato direttamente dall'associazione degli operatori di rete mobile e delle industrie adiacenti, GSMA,[31] con l'obiettivo di definire un quadro di garanzia della sicurezza condiviso nell'ambito delle **reti mobili**. Questo si basa su specifiche tecniche che, sebbene non siano formalmente ratificate dagli organismi di standardizzazione riconosciuti, risultano di fatto vincolanti per gli operatori di rete in quanto soggetti a contratti legali e accordi internazionali di roaming. Di conseguenza, anche se il meccanismo con cui le specifiche emanate da GSMA vengono adottate è differente, queste sono in sostanza paragonabili agli standard pubblicati dal 3GPP.

Il NESAS nasce per fornire un insieme comune di requisiti a garanzia della sicurezza finalizzati ad introdurre una base comune a tutti i prodotti, indipendentemente dai requisiti individuali del singolo Stato. **Tali requisiti e l'intero processo di certificazione sono pensati per essere utilizzati a livello globale**, lasciando che i fornitori di apparecchiature si concentrino sulla creazione e sul miglioramento del prodotto, dovendo garantire la conformità ad un **unico insieme di requisiti significativi** che al contempo sia in grado di assicurare un efficace livello di sicurezza. Come per i Common Criteria, lo schema si pone l'obiettivo di fornire agli operatori di rete mobile strumenti per valutare, in modo misurabile, confrontabile e standardizzato, il livello di sicurezza raggiunto dai prodotti di rete.

A tal fine, il NESAS fornisce il framework per l'implementazione del SECAM (Security Assurance Methodology). Questa metodologia di valutazione, introdotta dal 3GPP per rendere la sicurezza misurabile e seguire una base standardizzata comune, comprende **l'analisi dei processi con cui i fornitori delle apparecchiature di rete sviluppano i propri prodotti e la valutazione della gestione del loro ciclo di vita.** A ciò si aggiunge la creazione di requisiti di sicurezza e specifiche per i test, denominate **Security Assurance Specifications (SCAS).**

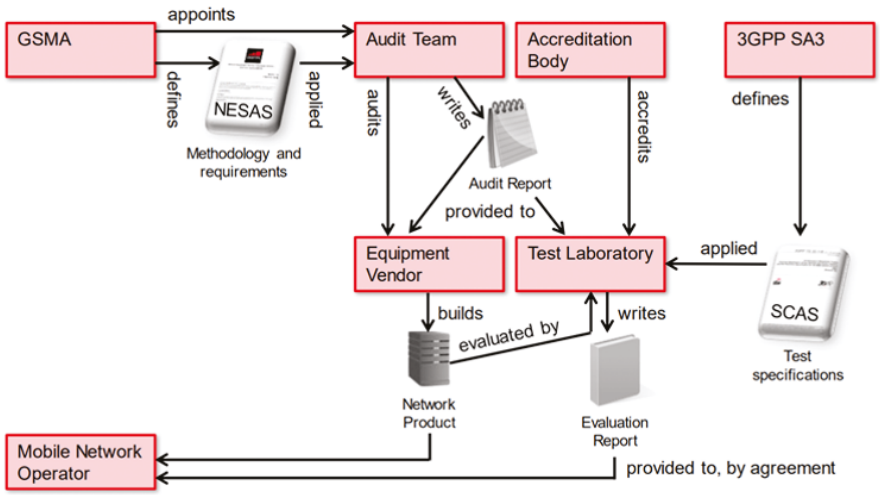
L'obiettivo consiste quindi nel mettere insieme un singolo set di requisiti in grado di formare la c.d. *security baseline*, un insieme di requisiti che definiscono la capacità di un prodotto di resistere agli attacchi. A livello procedurale, la valutazione della sicurezza dello schema NESAS coinvolge diverse fasi e attori (Fig. 5.7).

Da un lato, si osserva come i test riguardino sia le apparecchiature dei *vendor*, sia i loro processi interni. La valutazione del prodotto, invece, viene condotta da laboratori certificati da GSMA, che applicano test

31 La GSMA è l'associazione di categoria che conta attualmente circa 800 membri che operano in oltre 200 Paesi e che è stata progressivamente coinvolta nello sviluppo degli standard tecnici.

Fig. 5.7: Il funzionamento del NESAS

Fonte: GSMA, 2022



di sicurezza standardizzati e predefiniti. Nel dettaglio, le specifiche per i test vengono definite dal 3GPP, mentre GSMA, oltre alla valutazione delle procedure per l'accreditamento del laboratorio di prova, fornisce i requisiti e la metodologia per l'Auditor. Quest'ultimo si occupa di effettuare l'assessment sul fornitore di apparecchiature e sulle sue procedure.

In generale, essendo in gran parte realizzato dagli stessi operatori che compongono la filiera, il NESAS appare avere caratteristiche che tengono fortemente conto delle esigenze del settore. Per le stesse ragioni, grazie alla velocità con cui viene realizzata la procedura sia per i nuovi prodotti, sia per le versioni aggiornate dei prodotti esistenti, appare maggiormente applicabile. Ad esempio, un elemento di accelerazione per i *vendor*, e che consiste in un **considerevole vantaggio in termini di tempi e costi**, è costituito dal fatto di **dover effettuare la valutazione delle procedure una sola volta** nel caso in cui le procedure interne utilizzate siano le stesse per la realizzazione di molteplici prodotti finali. Questo consente di **evitare la moltiplicazione dei requisiti di sicurezza** cui conformare le proprie apparecchiature e incrementare le capacità interne di migliorare e mantenere livelli di sicurezza adeguati. Inoltre, per gli operatori di rete, si evidenzia **il venir meno della necessità di sviluppare specifici requisiti di sicurezza,** che vengono realizzati su base associativa (all'interno di GSMA) e quindi dividendosi i costi. Positivi anche i risvolti per i governi e le autorità nazionali, soprattutto in termini di **universale applicabilità** del sistema di sicurezza e per la **possibilità di farlo interfacciare con le certificazioni nazionali**, innalzando ulteriormente il livello di sicurezza se necessario.

Tali qualità rendono il NESAS uno schema di certificazione che può vantare una **considerevole diffusione**, in particolare tra le grandi aziende del settore digitale, dove risulta essere particolarmente apprezzato. Tra i Participating Vendors di NESAS risultano infatti esserci tanto alcune grandi compagnie europee, quali Nokia ed Ericsson, che alcuni fornitori extra-europei come Samsung, Huawei, ZTE e Mavenir. Parallelamente, anche alcuni governi nazionali hanno riconosciuto ufficialmente lo standard NESAS. Anche in questo caso figurano sia Paesi UE, come Germania e Paesi Bassi, sia Paesi asiatici, come Singapore e Thailandia.

5.3 Lo sviluppo degli European Common Criteria per garantire un approccio standardizzato e favorire l'accesso al mercato

Sebbene i Common Criteria si siano rivelati uno strumento particolarmente valido negli ultimi vent'anni, contribuendo ad innalzare sostanzialmente il livello di sicurezza di servizi e prodotti digitali, i recenti sviluppo tecnologici ed economici hanno posto nuovamente l'attenzione sulla necessità di sviluppare e promuovere sistemi in grado di far combaciare più agilmente la rinnovata attenzione circa i **fenomeni di cybersecurity con i ritmi sempre più dinamici e flessibili dei mercati digitali**.

L'Unione Europea, già dal 2019 con la pubblicazione del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio (noto come **Cyber Security Act – CSA**), aveva iniziato a porre l'attenzione politica e normativa su tali considerazioni, **sostenendo esplicitamente la creazione di un nuovo sistema di certificazioni** sulla sicurezza cibernetica che fosse **uniforme** in tutta l'UE. Con tale regolamento, infatti, si iniziavano già a esplicitare alcuni aspetti cruciali e caratterizzanti di tale passaggio, stabilendo, ad esempio, i **principali requisiti orizzontali** per gli schemi europei di certificazione auspicati dall'Unione – ritenuti fondamentali per permettere a tali futuri certificati europei per prodotti ICT, servizi ICT o processi ICT di essere riconosciuti e utilizzati in tutti gli Stati membri.

In conformità con l'Articolo 48 (2) del Cybersecurity Act, l'ENISA ha istituito un gruppo di lavoro specifico[32] con l'obiettivo di sostenere e promuovere la stesura di tali Common Criteria Europei, detti **EUCC** (*Common Criteria based European candidate cybersecurity certification scheme*), sulla base dei Common Criteria esistenti. La prima bozza dell'EUCC (la cosiddetta Versione 1.0), ha impostato il nuovo schema comunitario su un modello che riprende gli schemi ISO/IEC 15408 e ISO/IEC 18045, esplicitando come sia intenzione di questo "***gradualmente sostituire gli attuali schemi di certificazione nazionali***", basati anch'essi sui Common Criteria, che attualmente operano sotto l'accordo di mutuo riconoscimento SOG-IS MRA[33]. Inoltre, pone come obiettivo la certificazione di sicurezza dei prodotti e servizi ITC che attualmente non appartengono a nessun altro schema specifico ma che si preveda possano, in un futuro prossimo, entrare a far parte di nuovi schemi specifici sviluppati per particolari tecnologie o mercati[34].

In conformità con l'Articolo 49(3)[35], nel maggio 2020 l'ENISA ha avviato un processo di **consultazione di tutti gli stakeholder interessati**, i cui risultati sono stati pubblicati nel maggio 2021 e posti alla base della **Versione 1.1** degli EUCC[36].

L'ipotesi di EUCC pone l'obiettivo principale di **stabilire una certificazione uniforme** in grado di raggiungere i **due livelli di garanzia di sicurezza** più alti previsti dall'Articolo 52 del CSA, ovvero quello "sostanziale" ("*substantial*") e quello "alto" ("*high*"), mediante valutazioni effettuate da terze parti indipendenti e il coinvolgimento di autorità nazionali. L'EUCC rinuncia invece ad includere il livello "*basic*" previsto nel CSA, ritenuto fuori dallo scopo dell'EUCC e più consono ad integrazioni in altri futuri schemi di certificazione con requisiti di sicurezza inferiori e minori esigenze

32 Nominato "EUCC Ad Hoc Working Group" (EUCC-AHWG), è presieduto dall'ENISA ed è composto da 20 membri nominati che rappresentano il settore industriale e circa 12 rappresentanti degli enti di accreditamento e degli Stati membri.
33 Senior Officials Group – Information Systems Securit. Mutual Recognition Agreement
34 ENISA riporta gli esempi dell'IoT, dei servizi cloud e delle comunicazioni mobili.
35 Art 49(3): *"Nella preparazione di una proposta di sistema, l'ENISA consulta tutti i pertinenti portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo."*
36 ENISA – Cybersecurity Certification: Candidate EUCC Scheme V1.1.1. 25th May 2021.

dal punto di vista tecnico e procedurale. Come per i Common Criteria, il livello di garanzia viene assegnato in base al livello identificato nel *Vulnerability Assessment* e riportato con la classificazione AVA, per il quale i primi due livelli (AVA_VAN.1 e AVA_VAN.2) sono considerati di livello "sostanziale", mentre dal terzo al quinto (da AVA_VAN.3 a AVA_VAN.5) sono considerati di livello "alto". L'EUCC dovrebbe inoltre includere la possibilità di certificare i *Protection Profiles*, che permetterebbero una definizione armonizzata di requisiti di sicurezza associati a categoria specifiche di prodotti.

Da un **punto di vista metodologico**, l'EUCC stabilisce che le certificazioni verranno rilasciate da enti accreditati e riconosciuti (ISO/IEC 17065), i quali potrebbero differenziarsi da quelli ad oggi riconosciuti a livello nazionale. Una procedura più rigorosa riguarda tuttavia il rilascio delle **certificazioni di livello "alto", per le quali sarà necessaria autorizzazione da parte delle corrispondenti autorità nazionali di certificazione per la sicurezza informatica, o da organismi di certificazione da esse autorizzati.** In linea con i procedimenti già adoperati negli attuali Common Criteria sono invece i processi di valutazione della sicurezza dei prodotti, che saranno condotti da **laboratori accreditati**[37] i quali potranno essere interni o esterni all'organismo di certificazione corrispondente.

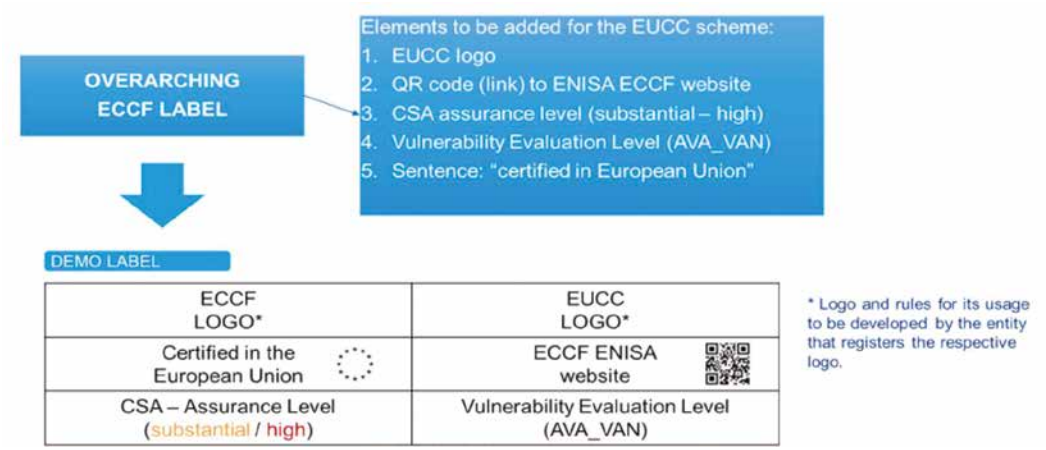
Nella prima versione degli EUCC vengono inoltre specificati gli **attori** che possono far uso del nuovo schema continentale, identificati in **quattro categorie** distinte: la prima riguarda i **produttori o fornitori** che desiderano valutare la qualità della sicurezza dei loro prodotti ICT attraverso una certificazione rilasciata da terzi; la seconda i **fornitori** di servizi/processi/prodotti ICT che desiderano beneficiare dell'evidenza di sicurezza dei propri prodotti per i loro clienti; la terza riguarda le **autorità** attive nel settore della regolamentazione del mercato; e la quarta riguarda gli **utenti finali** che possono beneficiare di tale sistema in termini di affidabilità e sicurezza del sistema digitale. Sebbene si favorisca una sostanziale continuità con i precedenti sistemi di certificazione nazionali, sia in termini di qualità e standard coperti dai certificati, che in termini di compatibilità metodologica, l'EUCC predispone diversi elementi di discontinuità volti ad **affrontare** le principali **criticità** che tali sistemi presentano nel **rapporto** con le **dinamiche** di **mercato**, in particolare **allungamento dei tempi** e **incremento dei costi**.

Gli elementi di discontinuità rispetto ai Common Criteria applicati nei sistemi nazionali non sono infatti tanto nella struttura del meccanismo, quanto nella **volontà da parte delle istituzioni europee di affrontare alcune delle principali criticità che tali sistemi presentavano nel rapporto con le dinamiche di mercato**. Particolare attenzione è data al superamento di quelle pratiche che prevedono un eccessivo allungamento dei tempi e un incremento dei costi. Tra gli obiettivi preposti figurano infatti anche **l'adozione di nuove procedure armonizzate per la gestione della criticità non previste al momento del rilascio** e una **procedura di valutazione rapida** per le correzioni e le modifiche successive dei prodotti. In questa direzione si muove il cosiddetto ***Patch Management*** ovvero la possibilità di **aggiornare, correggere, migliorare un programma** al fine di superare vulnerabilità di sicurezza e altri errori (*bug*) generici. Come spiegato nei paragrafi precedenti, l'attuale sistema di Common Criteria prevede infatti di dover procedere a nuove verifiche per l'intero prodotto/servizio ad ogni modifica, portando non solo a tempistiche anacronistiche rispetto alla dinamicità del mercato digitale, ma anche a perdite di efficienza sia da un punto di vista finanziario, con un accrescimento esponenziale dei costi al progredire delle tecnologie, che dal punto di vista procedurale, con percorsi di certificazione ripetuti più volte anche per componenti invariate del prodotto/servizio

37 IT Security Evaluation Facilities, ITSEF.

Fig. 5.8: L'etichetta EUCC

Fonte: ENISA



in questione. Al fine di superare questa criticità, la bozza dell'EUCC prevede il cosiddetto "***testing once principle***", ovvero la possibilità che il produttore includa preventivamente un meccanismo di gestione delle patch già ad origine, anch'esso da analizzare durante le procedure di certificazione del prodotto. In questo modo, l'UE garantisce **l'applicabilità di tale meccanismo nel caso di futuri interventi sul prodotto**, così da avere un prodotto costantemente aggiornato e "*patchato*" pur **mantenendo lo stato di certificazione** originale del prodotto in questione.

Parallelamente si intende introdurre **nuovi criteri armonizzati volti a rafforzare il mantenimento dei certificati nel tempo**, così da limitare i tempi e i costi per i produttori. Durante la durata di validità del certificato, si prevede infatti che i prodotti vengano sottoposti a processi di **aggiornamento in risposta alle possibili modifiche** che potrebbero incidere sullo status di certificazione. Tali attività di mantenimento dovrebbero includere le revisioni da parte dell'ente di certificazione e, quando necessario, valutazioni specifiche da parte dei laboratori indipendenti.

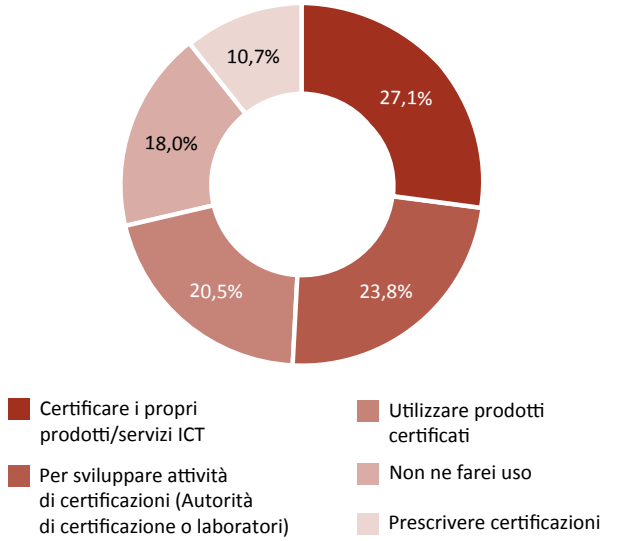
Si intende inoltre garantire maggiore trasparenza e **rafforzare la fiducia dei consumatori finali**, nonché sensibilizzarli circa l'impegno che l'Unione – in collaborazione con tutti gli stakeholder – ha profuso sui temi della cybersicurezza. Si prevede infatti la **nascita di un sito specificatamente dedicato alle certificazioni di cybersicurezza** contenente le linee guida del sistema adottato e gli status delle certificazioni emesse, oltre ad **un'etichetta specifica per i prodotti** certificati che mostri (oltre al logo degli EUCC e ad un QR Code di richiamo al sito), il livello di sicurezza assicurato e il livello AVA corrispondente.

Nel complesso, dunque, l'introduzione degli EUCC non solo costituirebbe un traguardo importante in termini di miglioramento della sicurezza dei prodotti connessi e delle infrastrutture critiche, ma renderebbe tali sistemi di certificazione anche maggiormente *market-friendly*, semplificando e internazionalizzando (mediante mutuo-riconoscimento) le procedure e quindi riducendone le tempistiche di realizzazione. Allo stesso modo, la creazione di un approccio standardizzato dovrebbe ridurre al minimo la richiesta di misure aggiuntive di certificazione a livello nazionale, evitando di ripetere le procedure già svolte in altri Paesi europei.

Dalle consultazioni condotte da ENISA con **gli**

Fig. 5.9: Intenzione di usare gli EUCC (% dei rispondenti)

Fonte: ENISA, *"Public Consultation on EUCC"*, maggio 2021



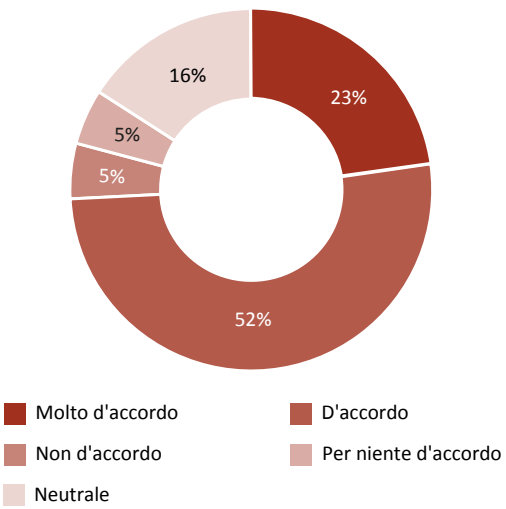
stakeholder del mercato digitale[38], è emerso che l'introduzione degli European Common Criteria raccoglierebbe il consenso della maggioranza degli attori interessati. **L'82% dei rispondenti ha dichiarato infatti che farebbe uso di tale sistema di certificazioni comunitario**: in particolare, il 33% ha indicato di voler certificare i propri prodotti/servizi ICT con il sistema EUCC (principalmente produttori/sviluppatori e organizzazioni commerciali), il 29% intende farne uso per sviluppare attività terze legate alla certificazione [ad esempio, le *Certification Body* (CB) o le *Evaluation Facility/Testing Laboratory* (ITSEF)] e il 25% prevede di fare uso degli EUCC come utilizzatore finale o cliente, ovvero utilizzando e acquistare prodotti certificati EUCC.

Inoltre, **secondo circa ¾ dei rispondenti**, **gli EUCC rafforzerebbero le condizioni del mercato digitale europeo.** In particolare, risultano favorevoli il **52%** dei rispondenti e molto favorevoli un **ulteriore 23% degli intervistati**. Per garantire il raggiungimento degli esiti sperati, particolare importanza è data alla trasversalità e flessibilità degli EUCC e alla loro capacità di essere applicabili a ogni settore dell'economia, oltre che all'importanza di un loro riconoscimento reciproco su base mondiale. Indispensabili sono anche i passi avanti auspicati in termini di tempistiche più brevi e costi minori, ad esempio derivanti dal superamento dei test ripetuti e l'applicazione del cosiddetto *testing once principle*.

I prossimi passi verso l'attuazione dello Schema prevedono la convocazione di consultazioni interservizio da parte della Commissione, alla quale dovrà poi seguire l'approvazione dei rappresentanti degli Stati membri (*Comitology)*, nonché la stesura da parte della Commissione dell'***Implementing Act***, atto esecutivo con cui lo schema dovrebbe diventare ufficialmente parte

Fig. 5.10: Impatto positivo degli EUCC sulle condizioni del mercato UE (% di rispondenti)

Fonte: ENISA, *"Public Consultation on EUCC"*, maggio 2021



38 Queste hanno coinvolto 114 rispondenti, il 77% dei quali provenienti da paesi EU/EEA e il 20% da paesi extra EU/EEA. Inoltre, il 32% delle risposte proviene da paesi che partecipano negli attuali sistemi di certificazione SOG-IS MRA, e il 33% da paesi aderenti al Common Criteria Recognition Arrangement (CCRA). Infine, il 28% proviene da paesi in cui sono stati adottati sistemi nazionali di certificazione, mentre solo il 2% viene da paesi dove non esistono certificazioni per la sicurezza informatica.

della legislazione europea. Tuttavia, si prevede che questo processo impiegherà ancora diverso tempo per essere concluso, con una piena attuazione del sistema che probabilmente richiederà nuove discussioni in sede comunitaria e la stesura di linee guida per facilitare il periodo di transizione. Sono ad esempio in programma incontri tra le autorità nazionali sulla regolamentazione del "*patch management*" e lo sviluppo di una strategia per il mantenimento dello schema possibilmente in sinergia con gli altri schemi, ad esempio quello sul cloud e sul 5G. Nella migliore delle ipotesi, pertanto, i certificati potranno essere emessi a partire dal 2024. È previsto in ogni caso un periodo di transizione di due anni, al termine del quale le certificazioni nazionali assorbite dagli EUCC dovrebbero cessare di operare.

5.4 Certificazioni volontarie e laboratori

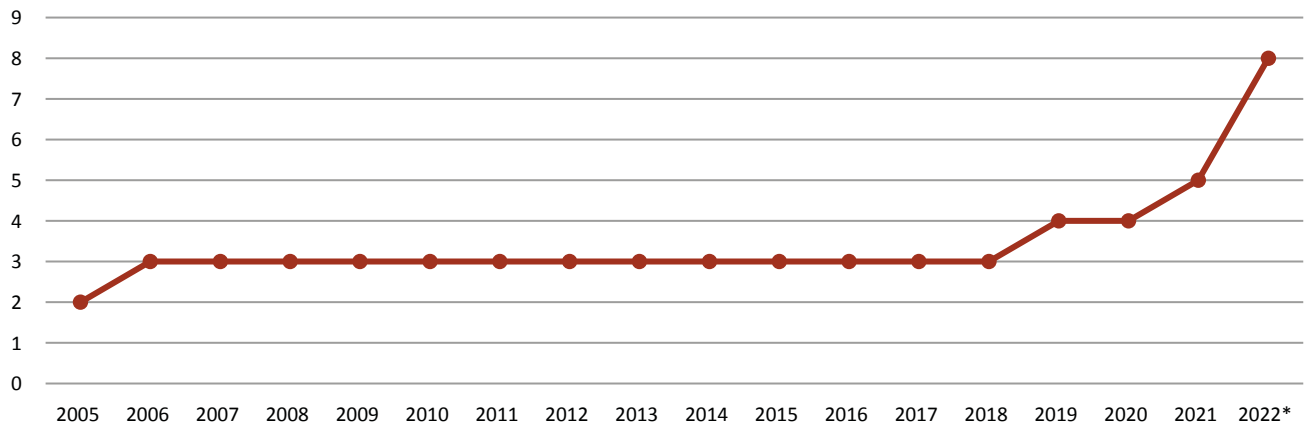
L'Organismo di Certificazione (OCSI) è l'ente deputato alla gestione dello "Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione". Tale schema, introdotto dal DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004), raccoglie l'insieme delle procedure e delle regole necessarie per la valutazione e la certificazione di sistemi o prodotti ICT o di Profili di Protezione e agisce in conformità con gli standard internazionali ISO/IEC IS-15408 (*Common Criteria*), nonché con i criteri europei ITSEC e ITSEM. Oltre all'OCSI nell'ambito dello Schema Nazionale operano:

- il Committente, ovvero qualsiasi soggetto che commissiona la valutazione di sistemi, prodotti o Profili di Protezione;
- il Fornitore, che può incarnare anche il ruolo di Committente, è il soggetto che fornisce l'Oggetto della Valutazione (ODV) o sue componenti;
- l'Assistente, un soggetto formato e abilitato dall'OCSI per fornire supporto tecnico al Committente o al Fornitore;
- i Laboratori per la Valutazione della Sicurezza (LVS), ovvero strutture accreditate dall'OCSI deputate ad effettuare le valutazioni, che possono anche assistere il Committente nel processo. Per svolgere la propria attività, gli LVS si avvalgono inoltre di Valutatori, ovvero figure professionali formate ed abilitate dall'OCSI.

Per essere abilitati ad effettuare le valutazioni, gli LVS devono rispettare una serie di requisiti fondamentali, tra i quali, oltre a quelli sostanziali come l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, figurano anche la disponibilità di locali e mezzi adeguati ad effettuare valutazioni, la presenza di personale competente e iscritto nell'elenco dell'OCSI e la conformità alle norme UNI CEI EN ISO/IEC 17025 e UNI CEI EN 45011 (per quanto applicabili) nonché la capacità di conservare tali requisiti nel tempo.
Osservando i dati disponibili sul portale dell'OCSI è possibile notare come, allo stato attuale, risultino abilitati sul territorio italiano appena 8 Laboratori per la Valutazione della Sicurezza, cui se ne aggiungono altri tre presenti al di fuori del nostro Paese. Nonostante il numero totale dei laboratori possa sembrare piuttosto esiguo, analizzando le date di accreditamento degli stessi si osserva come tali organizzazioni siano più che raddoppiate nell'ultimo quadriennio (Fig. 5.11). Nei primi dieci mesi dell'anno in corso si sono aggiunti alla lista degli LVS tre strutture che rappresentano un aumento del 60% rispetto al 2021.
Per quanto concerne il percorso effettivo compiuto per arrivare alla certificazione di un prodotto, si osserva come questo si articoli in due momenti principali, ovvero "il processo di certificazione" e la "fase di certificazione". Il **processo di certificazione** è il momento in cui vengono valutate le caratteristiche di sicurezza del sistema, prodotto o Profilo di Protezione e si articola a sua volta in tre fasi distinte denominate

Fig. 5.11: LVS accreditati presenti sul territorio italiano per anno

Fonte: Portale "Organismo di Certificazione della Sicurezza Informatica" – ACN



*Note: *Aggiornato al 2 novembre 2022*

preparazione, conduzione e conclusione.

Nella prima fase, come si desume dal nome della stessa, vengono predisposte dal LVS e dal Committente le attività prodromiche alla valutazione per definire il "Traguardo di Sicurezza", un documento che specifica le funzioni di sicurezza che l'ODV dovrebbe svolgere, l'ambiente operativo in cui questo è destinato a operare e il livello di garanzia rispetto al quale viene valutato. In questa fase, dopo aver verificato l'assenza di elementi che possano pregiudicare il buon esito della valutazione, il laboratorio predispone il Piano di Valutazione (PDV), un documento che descrive le attività che saranno svolte dal LDV, i tempi e le risorse necessarie. Si osserva come, prima di passare alla fase operativa, l'adeguatezza dal PDV debba essere approvata dall'OCSI.

La Conduzione della valutazione comprende tutte le attività svolte dal LVS, con il supporto del Committente, volte alla verifica delle qualità dell'ODV. In questo caso il laboratorio può predisporre Rapporti di Osservazione, finalizzati a richiedere altro materiale utile alla valutazione, chiarimenti o modifiche all'ODV e/o al Traguardo di Sicurezza.

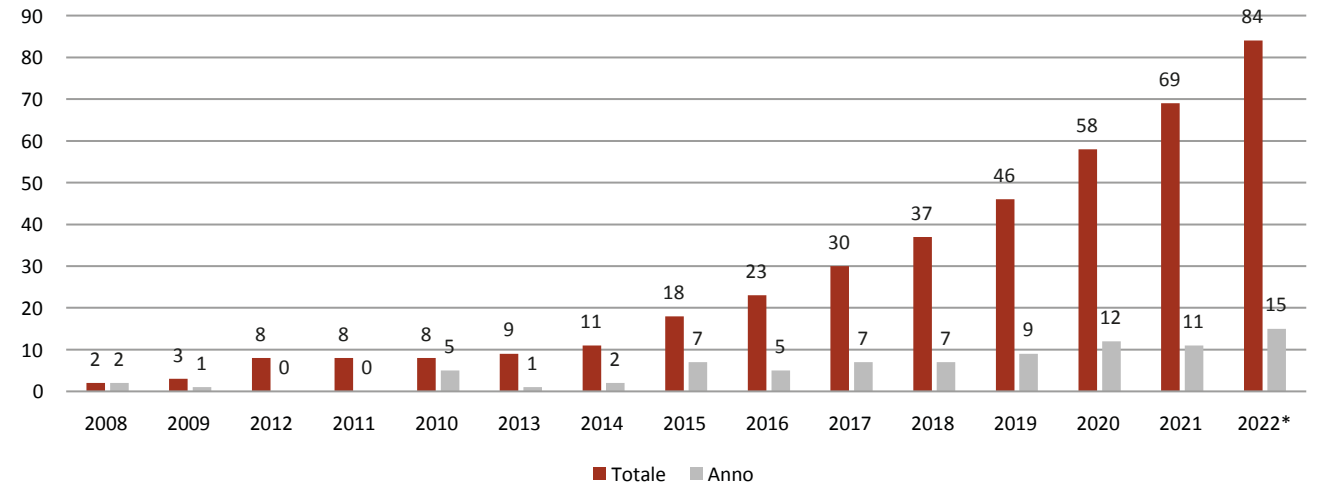
La conclusione della valutazione consiste invece nel momento in cui, verificati i risultati di tutte le analisi effettuate, il LVS redige il Rapporto Finale di Valutazione (RFV), che racchiude i verdetti intermedi e finali emessi e le relative motivazioni.

La **fase di certificazione**, come anticipato precedentemente, consiste in una fase separata dal processo di certificazione e riguarda il momento in cui l'OCSI, dopo aver esaminato il Rapporto Finale di Valutazione (RFV) stilato dal LVS e dopo averlo valutato positivamente, produce una doppia documentazione: il Rapporto di Certificazione, che attesta lo svolgimento dell'attività di valutazione secondo i criteri prescritti e in conformità con quanto definito nel Piano di Valutazione, e il Certificato, concludendo definitivamente l'iter.

Secondo i dati presenti sul portale dell'OCSI, **dal 2008 al 2022 sono stati emessi 84 certificati nell'ambito dello Schema Nazionale di Valutazione della Sicurezza ICT** (Fig. 5.12). In particolare, osservando l'andamento temporale, emerge come il numero di certificazioni abbia cominciato ad assumere consistenza dal 2015 in poi, mentre prima di questa data si limitava a poche unità. Nei soli primi dieci mesi del 2022

Fig. 5.12: Andamento certificati emessi nell'ambito dello Schema Nazionale di Valutazione della Sicurezza ICT

Fonte: Portale "Organismo di Certificazione della Sicurezza Informatica" – ACN



sono state rilasciate 15 certificazioni, più di quante ne siano state prodotte nell'intero 2021, e altri 13 sistemi, prodotti o Profili di Protezione risultano attualmente in corso di valutazione.

5.5 Dal Cybersecurity Act al D.Lgs. 3 agosto 2022, n. 123: le certificazioni della cibersicurezza nel contesto europeo e nazionale

Se la direttiva NIS, oggi superata dalla NIS 2, è intervenuta a disciplinare in maniera organica il tema della sicurezza delineando la cornice normativa ed organizzativa nell'UE e rinsaldando la cooperazione tra stati membri ed istituzioni, il **Regolamento n. 881/2019** del 17 aprile 2019 (noto come "Cybersecurity Act"), al fine di garantire il buon funzionamento del mercato interno e perseguendo nel contempo un elevato livello di cybersicurezza, cyberresilienza e fiducia all'interno dell'Unione, ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'**ENISA** ed ha delineato un quadro per l'introduzione di **sistemi europei di certificazione della cybersecurity** in grado di garantire un livello adeguato di cybersecurity dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cybersecurity nell'Unione.

In particolare, mentre i primi 45 articoli disciplinano poteri, competenze ed organizzazione dell'ENISA, a partire dall'art. 46, il regolamento fissa il **quadro europeo di certificazione della cybersecurity**, introducendo un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti, i servizi e i processi TIC.

Il successivo art. 47 assegna, invece, alla Commissione il compito di pubblicare un **programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza** – il primo entro il 28 giugno 2020 – in cui sono individuate le priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza ed è stilato, sulla base di specifiche motivazioni, un elenco di prodotti TIC, servizi TIC e processi TIC o delle relative categorie che possono beneficiare

dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cybersecurity. Sulla base di tale programma – o in casi ulteriori e diversi debitamente motivati – la Commissione può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente. In attuazione di tali previsioni, la Commissione ha già conferito mandato ad ENISA per l'elaborazione dei primi tre sistemi europei di certificazione della cibersicurezza: 1) Certificazione della cibersicurezza basata su Common Criteria e Metodologie Comuni di Valutazione (ISO/ IEC 15408 e ISO/IEC 18045); 2) Certificazione della cibersicurezza per i servizi cloud; 3) Reti 5G.

La **certificazione della cibersicurezza è volontaria** (art. 56), ferma restando la valutazione periodica dell'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati da parte della Commissione e la possibilità, per la stessa, di **valutare l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza** per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e migliorare il funzionamento del mercato interno, concentrandosi, innanzitutto, sui settori indicati nella NIS (ora NIS 2).

Agli Stati membri è **preclusa l'introduzione di nuovi sistemi nazionali di certificazione della cibersicurezza** per prodotti TIC, servizi TIC e processi TIC **già coperti da un sistema europeo** di certificazione della cibersicurezza in vigore mentre è prescritto, al fine di evitare la frammentazione del mercato interno, di informare la Commissione e il Gruppo europeo per la certificazione della cybersecurity (ECCG) di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cibersicurezza. In tale logica, **ogni Stato membro è chiamato a designare una o più autorità nazionali di certificazione della cibersicurezza** nel proprio territorio oppure, con l'accordo di un altro Stato membro, a designare una o più autorità nazionali di certificazione della cibersicurezza stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.

Il Regolamento individua, poi, con particolare rigore, un'ampia gamma di obiettivi di sicurezza connessi all'istituzione dei sistemi europei di certificazione e suddivide in tre, sulla base del **livello di rischio associato al previsto uso del prodotto, servizio o processo TIC**, in termini di probabilità e impatto di un incidente, i livelli di affidabilità dei prodotti, servizi e processi TIC: **di base, sostanziale ed elevato**, declinando, in riferimento a ciascuno dei tre livelli, le specifiche attività di valutazione previste nonché il ricorso ad attività sostitutive di effetto equivalente qualora le attività di valutazione previste non siano appropriate.

Nello specifico, un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità "sostanziale" assicura che i prodotti TIC, servizi TIC e processi TIC per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità "elevato", invece, assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative.

Il medesimo regolamento istituisce il **Gruppo europeo per la certificazione della cybersecurity**, composto da rappresentanti delle autorità nazionali di certificazione della cybersecurity o da rappresentanti

di altre autorità nazionali competenti, con compiti di assistenza, proposta, collaborazione e consulenza nei rapporti con la Commissione ed ENISA.
Quanto alla valutazione dell'impianto normativo introdotto, il regolamento prevede che entro il 28 giugno 2024, e successivamente ogni cinque anni, la Commissione valuti l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue prassi di lavoro, l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie.
In attuazione del descritto regolamento, il 4 settembre 2022 è entrato in vigore il **D.Lgs. n. 123/2022,** recante, per l'appunto, norme di adeguamento della normativa nazionale alle disposizioni del Titolo III "Quadro di certificazione della cibersicurezza" del Reg. 2019/881. Si tratta di un intervento normativo molto importante che **ha individuato nell'ACN l'autorità nazionale di certificazione della cibersicurezza in Italia**, le modalità di cooperazione con le altre autorità pubbliche nazionali ed europee e con l'Organismo di accreditamento e la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione.
Ad ACN, in particolare, è affidato il compito di definire l'organizzazione e le procedure per lo svolgimento dei compiti in materia di certificazione della cibersicurezza alla stessa attribuiti, autorizzare gli organismi di valutazione della conformità e vigilare sulle attività degli organismi di valutazione della conformità pubblici, controllare il mercato in ambito nazionale ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersicurezza, irrogare le sanzioni previste per i casi di violazioni, assistere l'Organismo di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità, rilasciare (ed eventualmente revocare o chiedere di revocare) i certificati di cibersicurezza, di cui il regolamento dichiara espressamente la natura volontaria.
Lo stesso decreto consente ai fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC di rilasciare sotto la propria responsabilità **dichiarazioni UE di conformità** di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema, con obbligo in capo agli stessi di rendere disponibile all'ACN, per il periodo stabilito nel corrispondente sistema europeo di certificazione, la dichiarazione, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC o servizi TIC al sistema.
Per quanto concerne **accreditamento ed autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova ed esperti dell'Agenzia** (chiamati a supportare le prove tecniche l'ACN conduce nella propria attività di vigilanza), a quest'ultima è affidato il compito di redigere, aggiornare e rendere pubblici due elenchi di esperti e di laboratori di prova da essa abilitati ad operare a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia (con impossibilità, per gli stessi, di effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità sostanziale o di base in ambito nazionale e di essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati).
Importante il ruolo dell'ACN anche rispetto all**'attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cibersicurezza**. Ed infatti, al fine di elevare il livello nazionale di cibersicurezza, l'ACN può realizzare progetti di ricerca, ivi inclusi quelli per lo sviluppo di software, e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale ed è chiamata a monitorare gli sviluppi nel campo della certificazione della cibersicurezza, anche consultando i portatori di interesse nazionale del settore e scambiando informazioni, esperienze e buone

pratiche con la Commissione europea e le altre autorità nazionali.
Il decreto legislativo in esame disciplina, infine, il diritto di presentare reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità e di adire l'autorità giudiziaria avverso le decisioni assunte dall'Agenzia o dagli organismi di valutazione della conformità.

In attuazione di tale decreto, nell'agosto del 2022, come già rilevato, l'ACN ha adottato determinazioni tecniche in materia di accreditamento dei laboratori di prova che supporteranno il CVCN, Centro di Valutazione e Certificazione Nazionale, nella valutazione e nella certificazione di prodotti ICT rispetto a vincoli di cyber security.

CONCLUSIONI E SPUNTI DI POLICY

La centralità assunta dall'ecosistema digitale nel corso degli ultimi anni ha aperto un mondo di nuove opportunità per i cittadini, per le imprese e per le pubbliche amministrazioni, portandosi dietro anche nuove tipologie di minacce come il cybercrime, sempre più pervasivo anche rispetto ad eventi di carattere geopolitico o persino bellico.

Le analisi presentate nel rapporto hanno mostrato la crescente rilevanza degli attacchi condotti sia a livello internazionale che a livello italiano, aprendo la riflessione su una serie di questioni che includono **l'aumento della resilienza** sia in relazione alle pubbliche amministrazioni centrali e locali, sia a livello di grandi aziende, sia rispetto alle Pmi, senza dimenticare le capacità di comprendere i rischi e di difendersi da parte dei privati cittadini.

In un contesto sempre più digitalizzato che vede crescere per frequenza, complessità e gravità gli attacchi informatici rivolti a imprese, cittadini e pubbliche amministrazioni, l'UE, seppur con tempistiche spesso dilatate, legate alla complessità delle procedure di adozione degli atti legislativi, ha inteso reagire dando vita ad un articolato e sempre più dettagliato complesso di norme che persegue il fine ultimo di creare un ecosistema digitale sicuro di cui tutti gli attori a vario titolo coinvolti possano avere fiducia. A partire dall'**adozione della direttiva NIS nel 2016**, che non è purtroppo riuscita nell'intento di armonizzare le discipline nazionali e si è dimostrata non in grado di far fronte all'evoluzione tecnologica che sempre più ha permeato nuovi settori esclusi dal proprio ambito di applicazione, per andare avanti con **l'adozione del Cybersecurity Act (Reg. n. 881/2019)** fino a giungere al lancio del **Cybersecurity Package nel 2020** – comprensivo di strategia sulla cybersecurity, proposta di revisione della direttiva NIS e proposta di direttiva sulla resilienza delle entità critiche (direttiva Cer) – è stato crescente e sempre più pervasivo l'intervento europeo in materia di cibersicurezza soprattutto con riferimento ai settori che presentano maggiori criticità.

La **direttiva NIS 2**, in particolare, che è entrata in vigore lo scorso 17 gennaio e dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024, amplierà i settori e le tipologie di entità critiche che rientrano nel campo di applicazione (anche attraverso la fissazione di chiari limiti dimensionali), rafforzerà gli standard di sicurezza nelle imprese e nelle catene di approvvigionamento, semplificherà gli obblighi di comunicazione fornendo indicazioni chiare in merito al concetto di incidente significativo ed alle tempistiche e contenuti della segnalazione ed introdurrà più rigorose misure di vigilanza e requisiti di applicazione più severi, comprese sanzioni armonizzate in tutta l'UE.

La **direttiva CER**, il cui termine di recepimento per gli Stati membri è fissato al 17 ottobre 2024, va a sostituire la direttiva europea sulle infrastrutture critiche del 2008 al fine espresso di tenere conto delle evoluzioni in atto ampliando dunque il novero delle entità considerate critiche o vitali per la società e l'economia e di rafforzare la resilienza delle infrastrutture critiche a una serie di minacce, tra cui i rischi naturali, gli attacchi terroristici, le minacce interne o il sabotaggio. A tal fine ogni Paese Ue è chiamato ad adottare una propria strategia nazionale entro il 2026, indicare una o più autorità competenti responsabili della corretta applicazione e del rispetto della direttiva a livello nazionale e designare, all'interno dell'autorità competente, un unico punto di contatto per assicurare la cooperazione transfrontaliera con le autorità competenti degli altri Stati membri. Gli Stati membri devono inoltre assicurarsi che i soggetti critici adottino

misure tecniche e organizzative per garantire la loro resilienza, ivi comprese quelle di prevenzione degli incidenti, protezione fisica delle aree sensibili, mitigazione delle conseguenze degli incidenti, recupero dagli incidenti, gestione della sicurezza dei dipendenti, aumento della consapevolezza tra il personale.

Da ultimo, con la presentazione della proposta di regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (**Cyber Resilience Act-CRA**), l'UE punta a fissare regole armonizzate per l'immissione sul mercato di prodotti o software con una componente digitale, requisiti di cybersecurity che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, obblighi per ogni fase della catena del valore e un obbligo generale di diligenza per l'intero ciclo di vita di tali prodotti. L'intenzione è dunque quella di assicurare che i prodotti tech (sia software che hardware) sbarchino sul mercato europeo con il minor numero di vulnerabilità possibili e di offrire ai consumatori le informazioni necessarie per valutare le caratteristiche di sicurezza cyber dei prodotti e scegliere quelli più sicuri. Tale proposta rappresenta un tassello senza dubbio importante che parte dalla constatazione della centralità assunta dal digitale nel vivere quotidiano di cittadini, imprese e pubbliche amministrazioni e dunque appresta tutele analoghe a quelle previste per i prodotti difettosi che possono arrecare danni materiali. Per raggiungere tale obiettivo pone obblighi molto stringenti in capo a tutta la supply chain e specifiche tutele in favore dei consumatori che saranno destinatari di un'ampia serie di informazioni tra cui il risk assessment che dovrebbe sì consentire di valutare i rischi cui espone l'utilizzo del prodotto (oltre alle istruzioni per l'utilizzo ed alle informazioni sulle procedure da seguire per l'installazione degli aggiornamenti di sicurezza) ma che presenta una complessità tale da suscitare qualche dubbio circa l'effettivo potenziale di efficacia di tale misura.

Lo scenario normativo attuale impone alle aziende di attivarsi immediatamente innanzitutto per valutare se l'azienda operi in uno degli ambiti di applicazione definiti, monitorare e verificare l'attuazione nazionale, rivedere e/o aggiornare la governance e le procedure di sicurezza aziendali, valutare la conformità dei fornitori dal punto di vista della sicurezza e, se necessario, rafforzare le misure contrattuali per ottenere il livello di efficacia concordato, assicurare che il personale dirigente e i dipendenti siano adeguatamente formati sulle politiche interne di sicurezza informatica nonché mettere in campo esercitazioni procedurali ed operare verifiche tecniche per valutare concretamente il livello delle misure di sicurezza implementate. Si tratta di una serie di adempimenti che ben si comprendono nella logica di estendere e rafforzare la cultura e gli obblighi in materia di sicurezza informatica a tutti gli attori coinvolti e creare un clima di responsabilità condivisa nei confronti della gestione del rischio e dell'adozione delle necessarie misure di prevenzione e rimedio agli attacchi informatici, ma che pongono complessità importanti soprattutto per le PMI.

In questo contesto, in seno alle istituzioni europee sono state previste una serie di misure per rafforzare la **sicurezza delle reti 5G**, sin dall'adozione della Raccomandazione n. 2019/534 sulla cybersecurity delle reti 5G per arrivare alla Comunicazione "Dispiegamento del 5G sicuro – Attuazione del pacchetto di strumenti dell'UE" ed al Toolbox del 2020 con il fine di identificare un insieme comune di misure in grado di mitigare i principali rischi per la sicurezza informatica delle reti 5G (così come sono stati identificati nella relazione di valutazione del rischio coordinata dall'UE) e fornire una guida per la selezione delle misure da adottare al fine di creare un solido quadro di misure che garantisca un adeguato livello di sicurezza informatica delle reti 5G in tutta l'UE ed un approccio coordinato tra gli Stati membri.

Si tratta di un articolato e molto complesso sistema di norme che al pur condivisibile fine di assicurare standard di sicurezza elevati porta con sé le inevitabili difficoltà interpretative ed applicative tipiche di norme molto tecniche che si succedono nel tempo e che necessitano di essere metabolizzate e messe a regime dal sistema, innanzitutto dai soggetti che ne sono destinatari e che si trovano a dover assolvere obblighi sempre crescenti per numero e complessità.

A **livello europeo**, di particolare interesse risultano i lavori in seno all'ENISA per la creazione degli **European Common Criteria**, standard che dovrebbero garantire livelli di sicurezza elevati ed adeguata snellezza dei processi di certificazione in termini di tempi di conseguimento dei certificati e di mantenimento degli stessi anche in seguito agli aggiornamenti software.

Allo stesso tempo, le tempistiche di rilascio – previste non prima del 2024 – richiedono verosimilmente l'analisi di soluzioni ponte per far sì che gli operatori di rete possano garantire sufficienti livelli di sicurezza e una rapida transizione verso lo standard 5G. In questo senso, l'utilizzo di standard più snelli e condivisi a livello internazionale – il **NESAS** ad esempio **per la parte 5G** già costituisce un'ottima soluzione immediatamente disponibile, così come nel **mondo ICT** potrebbe esserlo l'adozione di un **subset ridotto di test** derivante dallo standard originario dei **Common Criteria** – permetterebbe da subito di garantire un adeguato livello di sicurezza riducendo i costi e i tempi che i player industriali devono sostenere e spingere al contempo verso un rapido incremento delle certificazioni volontarie.

A **livello italiano**, l'**istituzione della nuova Agenzia** ha garantito il superamento di un sistema che vedeva le funzioni e le competenze in materia di cybersecurity polverizzate tra una miriade di autorità che agivano secondo logiche, obiettivi e priorità diversi e che ponevano non poche difficoltà soprattutto alle imprese obbligate ad interagire con vari interlocutori, in favore di un nuovo ecosistema che ruota sostanzialmente intorno ad un solo soggetto in grado di assicurare uniformità e prevedibilità di azione e, dunque, certezza del diritto. La predisposizione della strategia per la cibersicurezza ha poi dotato il paese di una visione chiara, di obiettivi ambiziosi e di un insieme di azioni ed iniziative concrete che vanno ad impattare sugli strumenti, le procedure e le misure attraverso cui assicurare elevati standard di sicurezza.

Per rafforzare la sicurezza delle imprese dal quale 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, il D.L. n. 105/2019, convertito con la legge n. 133/2019, ha istituito il **perimetro di sicurezza nazionale cibernetica**. Da ciò discende che i soggetti pubblici e privati che offrono tali servizi o svolgono funzioni essenziali e che sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici dalle Amministrazioni competenti nei rispettivi settori, sono tenuti a predisporre annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al **CSIRT** attivo presso la Presidenza del Consiglio. Tali soggetti, inoltre, sono tenuti a comunicare al **CVCN** l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici" e rientranti nelle categorie sopra descritte ed il CVCN, entro un tempo massimo di 60 giorni dalla comunicazione, può indicare al soggetto incluso nel perimetro eventuali condizioni a cui i fornitori dovranno attenersi e test di hardware e software che dovranno essere eseguiti. Tali condizioni e test sono inseriti nei bandi di gara e nei contratti con specifiche clausole

che condizionano il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.

Accanto alla disciplina sul perimetro opera, nel sistema nazionale, la **normativa Golden Power** che attribuisce poteri speciali al Governo in settori strategici ed in particolare difesa e sicurezza nazionale, tecnologia 5G, energia, trasporti, comunicazioni e nuovi settori di cui al Reg. 2019/452.

Ebbene, il sistema di governance incentrato sull'ACN e l'ecosistema normativo che ruota intorno a Golden Power e perimetro di sicurezza nazionale cibernetica rende il nostro paese all'avanguardia nella tutela della cybersecurity e di fatto già sostanzialmente compliant con gli obblighi e le previsioni previste a livello UE con l'adozione della direttiva NIS 2. Nel contesto italiano non sembra attualmente configurarsi la necessità di ulteriori integrazioni normative in merito.

In questo contesto, un'attenzione particolare è richiesta in direzione della **protezione dalle minacce cibernetiche per le PMI e per i privati cittadini**. Per quanto concerne le prime, i dati sono particolarmente rilevanti poiché mostrano, oltre ad una preparazione deficitaria – meno del 40% dei lavoratori ha ricevuto una formazione specifica sulla cybersecurity – anche una scarsa consapevolezza del problema, giacché quasi la metà delle imprese oltre i 3 dipendenti intervistate da Istat ritiene che la cibersicurezza sia poco importante o non rilevante.

Un discorso a parte va fatto per la cittadinanza. Se circa un quarto degli italiani dichiara di avere una buona conoscenza di cosa si intende per cibersicurezza, più della metà degli stessi si è imbattuto in una o più minacce informatiche nel corso della propria vita, non di rado con esiti alquanto spiacevoli come l'aver ricevuto email di phishing (64,6% dei cittadini), l'aver scoperto pagamenti di acquisti fatti a proprio carico (17,2%) e l'aver subìto la clonazione della propria carta di credito o del bancomat (14,3%).

In questo senso, le iniziative volte a sensibilizzare la cittadinanza sul tema sembrano, seppur lodevoli, ancora relativamente poche e spesso messe in campo solo da aziende private che faticano ad estendere la partecipazione ad un piu' ampio ecosistema. Queste attivita' andrebbero intensificate, con una più intensa collaborazione pubblico-privato ed un coordinamento centrale capace di poter mettere a fattore comune gli sforzi e poter aspirare in questo modo a raggiungere risultati effettivi per il paese con il coinvolgimento di una parte sempre piu' ampia della popolazione nazionale

Dati piuttosto incoraggianti provengono invece dal versante della **formazione specialistica**. Il monitoraggio condotto da I-Com sulle attività di formazione sulla cibersicurezza in ambito universitario ha evidenziato un interesse decisamente crescente per queste tematiche da parte del mondo accademico, con 234 tra corsi e insegnamenti offerti a gennaio 2023 rispetto ai 79 individuati a gennaio 2022. In particolare, a livello nazionale risultano attivi 4 lauree triennali, 22 lauree magistrali, 7 dottorati e 18 master (di primo e di secondo livello) interamente incentrati sulla cybersecurity. Nel complesso, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 51 corsi di studio interamente dedicati. Per quanto riguarda la distribuzione regionale dell'offerta formativa complessiva, questa appare piuttosto disomogenea con una forte concentrazione nel Lazio (45 tra corsi e singoli insegnamenti), Piemonte (32), Campania (25) e Lombardia (21). Di conseguenza, ulteriori azioni potrebbero essere intraprese per incentivare **una maggiore capillarità a livello territoriale** di tale formazione specialistica, fattore di cui potrebbe beneficiare l'intero ecosistema sia in termini di formazione delle nuove leve, sia per quanto concerne la formazione di forza

lavoro specializzata al servizio della protezione cibernetica delle imprese e delle stesse PA.

In questo senso, anche nell'ottica di estendere il più possibile la formazione specialistica nell'ambito della cibersicurezza, particolarmente rilevante potrebbe rivelarsi la **riforma degli Istituti Tecnici Superiori**, i quali potrebbero fungere da anello di congiunzione tra la realtà scolastica e quella lavorativa. Attualmente, la formazione garantita dai 120 ITS attivi sul territorio viene ritenuta non sufficiente da parte delle imprese. Pertanto, una maggiore specializzazione di questo tipo di Istituti sulle tematiche connesse alla cibersicurezza potrebbe costituire un ulteriore tassello in direzione della costruzione e del rafforzamento di un ecosistema della cibersicurezza maggiormente resiliente di fronte alle crescenti minacce provenienti dal web. Cruciale sarà innanzitutto l'adozione dei decreti attuativi la cui mancanza rende al momento di fatto ancora non operativa la riforma varata.

Crediti fotografici:
Copertina - Mehaniq/shutterstock.com
Capitolo 1 - PLMT/shutterstock.com
Capitolo 2 - Harvepino/shutterstock.com
Capitolo 3 - Chor muang/shutterstock.com
Capitolo 4 - Gorodenkoff/shutterstock.com
Capitolo 5 - Thapana_Studio/shutterstock.com

Impaginazione:
kreas.it

icom cibersicurezza

icom istituto per la competitività

Roma
Piazza dei Santi Apostoli 66 - 00187
www.i-com.it

Bruxelles
Avenue des Arts 50 - 1000
www.i-comEU.eu

info@i-com.it