icom
istituto per la competitività

RAPPORTO OSSERVATORIO
SULLA CIBERSICUREZZA

LA SFIDA DELLA CIBERSICUREZZA PER UN'ITALIA SEMPRE PIÙ DIGITALE.

Politiche, competenze, regole

FEBBRAIO 2024

icom
istituto per la competitività

RAPPORTO OSSERVATORIO
SULLA CIBERSICUREZZA

LA SFIDA DELLA CIBERSICUREZZA PER UN'ITALIA SEMPRE PIÙ DIGITALE.

Politiche, competenze, regole

FEBBRAIO 2024

CURATORI
Stefano da Empoli
Silvia Compagnucci
Domenico Salerno

AUTORI
Silvia Compagnucci
Alessandro D'Amato
Enrica Lipilini
Domenico Salerno
Valerio Vinco

Il presente report è aggiornato alla data del 2 febbraio 2024

I-Com Edizioni
© 2024 I-Com servizi srl
ISBN 9791280680143
Febbraio 2024

INDICE

EXECUTIVE SUMMARY 7

CAPITOLO 1
IL QUADRO EUROPEO E ITALIANO DELLA CYBERSECURITY 19

1.1. Lo scenario europeo e nazionale degli attacchi cibernetici 21
1.2. Lo stato degli investimenti in cybersicurezza in UE e in Italia 25

CAPITOLO 2
L'ECOSISTEMA NORMATIVO SULLA CYBERSECURITY 35

2.1. L'approccio alla cybersecurity. EU vs Cina e Stati Uniti 37
2.2. L'evoluzione del framework europeo sulla cybersecurity 39
2.2.1. Il Cybersecurity Package ed il nuovo scenario tracciato dalla NIS 2 39
2.2.1.1. I primi chiarimenti applicativi sulla direttiva NIS2 *45*
2.2.2. Il Cybersecurity Act e le modifiche proposte 46
2.2.3. Il Cyber Resilience Act (CRA). Dalla proposta della Commissione allo stato della procedura 48
2.2.4. Assicurare la resilienza operativa digitale del settore finanziario: il Digital Operational Resilience Act (DORA) 51
2.3. L'ecosistema normativo nazionale sulla cybersecurity 53
2.3.1. L'ACN ed il nuovo modello di governance cyber. Gli obiettivI della strategia e del piano di implementazione 53
2.3.2. Il recepimento della direttiva NIS2 in Italia 60
2.3.3. Il recepimento della direttiva CER in Italia 63
2.3.4. Il Perimetro di Sicurezza Nazionale Cibernetica 64
2.3.5. L'evoluzione della disciplina sul Golden Power 70
2.3.5.1. Esercizio dei poteri speciali e andamento delle notifiche *75*
2.3.6. Gli scenari in discussione. Il disegno di legge sulla cybersicurezza 80

CAPITOLO 3
L'EVOLUZIONE DELLE CERTIFICAZIONI A LIVELLO EUROPEO 83

3.1. Il funzionamento e le tendenze di utilizzo dei *Common Criteria* 85
3.2. Verso gli European *Common Criteria* 89

CAPITOLO 4
IL QUADRO REGOLATORIO EUROPEO E NAZIONALE IN CYBERSICUREZZA E LA PERCEZIONE DELLE IMPRESE 95

4.1. Nota metodologica e analisi del campione 97
4.2. Analisi dei risultati 98
4.3. Conclusioni dell'indagine 113

CAPITOLO 5
LA CYBERSICUREZZA ALLA BASE DELLA COOPERAZIONE TRA PUBBLICO E PRIVATO **117**

5.1. Il partenariato pubblico-privato (PPP) applicato alla sicurezza informatica: vantaggi e criticità 119
5.1.1. Le principali iniziative di PPP in ambito nazionale 123
5.1.2. I Competence Center per l'orientamento e la formazione in cybersecurity 126
5.2. Le start-up di cibersicurezza e il *Cyber Innovation Network* dell'ACN 129
5.3. Altre forme di collaborazione tra pubblico e privato 133

CAPITOLO 6
LE COMPETENZE IN CIBERSICUREZZA: A CHE PUNTO SIAMO E ATTIVITÀ IN CORSO **139**

6.1. La cybersicurezza per i cittadini: lo stato dell'arte 141
6.2. L'impegno delle imprese per la sicurezza informatica 144
6.3. Le *best practices* per la formazione ICT & cyber 147
6.4. L'offerta formativa nazionale in materia di cibersicurezza 150
6.4.1. Corsi, Master e Dottorati di ricerca 150
6.4.2. Lo stato dell'arte e la riforma degli ITS 154
6.4.3. La sicurezza informatica nei corsi ITS 157

CONCLUSIONI **163**

EXECUTIVE SUMMARY

CAPITOLO 1
Lo stato della cibersicurezza in Europa e in Italia

La costante e ingente evoluzione dell'ecosistema digitale ha generato una vasta gamma di nuove opportunità per individui e imprese. Allo stesso tempo, al crescente impiego delle nuove tecnologie si è accompagnata l'intensificazione di rilevanti rischi, in particolare, quelli riconducibili alla minaccia cibernetica. Dai dati Clusit si evince come negli ultimi anni **il numero di cyberattacchi annuali a livello globale sia cresciuto di oltre il 60%**, passando dalle 1.554 del 2018 alle 2.489 del 2022. Inoltre, anche **i valori inerenti il primo semestre del 2023 appaiono preoccupanti**, in quanto si è raggiunta una quota di 1382 attacchi, ben **637 in più rispetto al primo semestre del 2018**.

Negli ultimi tre anni si è instaurata una tendenza che ha visto prevalere **gli attacchi con severity "Critica"**, ovvero che hanno prodotto effetti dannosi importanti per le vittime, tra cui ingenti perdite economiche e di dati. Si è passati dal **32% nel 2021, al 36% nel 2022 e al 40% nel primo semestre del 2023**. In merito alla **distribuzione geografica delle vittime**, nel primo semestre del 2023 i numeri più elevati sono quelli riconducibili al continente americano, **mentre l'Europa si posiziona seconda attraendo il 22% delle azioni dei cybercriminali**.

A livello italiano, nel primo semestre 2023 sono stati registrati **132 attacchi di particolare gravità**, che si traducono in una **media mensile di 22**, circa **dieci volte più elevata rispetto a quella rilevata nel 2018** (2,5). Il settore industriale che ha attratto il maggior numero di attacchi in Italia è la Pubblica Amministrazione (23%), seguita a breve distanza da target multipli e dalla manifatturiera (17%). In termini di severity, il dato italiano nel primo semestre del 2023 assume un andamento particolare, in quanto a **differenza di quello mondiale (40%) gli incidenti con impatto "Critico" costituiscono il 21%.** La quota più elevata di attacchi è ricondotta a una severity "Alta" (48% in Italia/38% globale) e "Media" (30% in Italia/21% mondiale), mentre una severity "Bassa" attiene solo al 2% degli episodi.

In un contesto come quello appena delineato, gli **investimenti in cybersicurezza** assumono un ruolo di significativa importanza, in quanto rappresentano la prima risposta, in termini preventivi, alle esigenze che incombono sulle imprese e che derivano dalle nuove dinamiche del cyberspazio. Secondo quanto emerso dall'ultima versione del rapporto NIS Investments", **in UE le organizzazioni francesi sono quelle che spendono di più in sicurezza informatica in valore mediano** (€6,30 milioni), **seguite dalle italiane e spagnole** che riportano una spesa rispettivamente pari a **€4,80 e €3,80 milioni**. Questi investimenti rappresentano nel caso della Francia e della Spagna il 6,7% del budget IT, mentre **per l'Italia corrispondono al 7,6%**.

CAPITOLO 2
L'ecosistema normativo sulla cybersecurity

In un contesto socioeconomico sempre più incentrato sull'offerta di servizi digitali è irrinunciabile per gli Stati apprestare misure normative e organizzative che siano in grado di far fronte ai rischi della digitalizzazione, predisponendo tutele efficaci per le risorse (umane, finanziarie e tecnologiche) a disposizione di enti pubblici e imprese da un lato, e per i diritti e le libertà fondamentali degli individui, dall'altro. Se si rivolge lo sguardo sul contesto globale, **nel mese di dicembre del 2016, la Cina ha pubblicato una propria strategia nazionale**, nella quale è rinvenibile un riferimento interessante circa l'importanza del dominio cibernetico, secondo cui esso costituirebbe un mezzo attraverso il quale promuovere la salvaguardia della pace mondiale e, al contempo, la sicurezza e gli

interessi di sviluppo nazionale. Per quanto riguarda il lato più prettamente normativo, **la cibersicurezza in Cina è regolamentata da tre atti principali: la *Cybersecurity Law* (2017), la *Data Security Law* (2021) e la *Personal Information Protection Law* (2021)**. Anche gli **USA** si sono attivati già da diverso tempo nella definizione di una propria strategia di cibersicurezza, **puntando particolarmente su una politica estera in ambito cyber**, la quale – naturalmente – si è evoluta col tempo. Tra gli ultimi interventi, **a marzo 2023 l'amministrazione Biden ha chiarito la strategia di cybersecurity** che guiderà gli Stati Uniti per i prossimi anni, **mentre lo scorso 30 ottobre è stato reso noto l'*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* nell'ambito del quale è possibile rintracciare un focus dedicato alla cybersicurezza**.

In questo contesto generale, l'UE sta delineando un ecosistema normativo della cibersicurezza particolarmente articolato. Nel 2020, in particolare, la Commissione europea ha lanciato il "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). Se la strategia ha declinato proposte concrete di iniziative politiche, di regolamentazione e di investimento per rafforzare resilienza, sovranità tecnologica e leadership, sviluppare capacità operative di prevenzione, dissuasione e risposta e promuovere un ciberspazio globale e aperto, il 27 dicembre 2022 è stata pubblicata sulla G.U. dell'UE la Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (Direttiva CER – Resilience of Critical Entities), 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 e a migliorare la cooperazione internazionale tra le autorità competenti.

Partendo dalla constatazione della frammentazione normativa conseguente al recepimento della direttiva NIS, all'esito di un ampio e complesso dibattito, il 17 gennaio 2023 è entrata in vigore la **Direttiva NIS 2 (Dir. n. 2555/2022)**, che ha ampliato l'ambito di applicazione soggettivo, abbandonando la precedente distinzione tra OSE e DSP, in favore di una suddivisione tra soggetti essenziali e soggetti importanti (introducendo una soglia per l'applicabilità della disciplina alle imprese), ha prescritto l'adozione di misure tecniche, organizzative e operative adeguate e proporzionate, ha declinato obblighi di segnalazione in caso di incidenti significativi, ha previsto misure di vigilanza e individuato misure per garantire la sicurezza della supply chain. Il 14 settembre 2023 la Commissione europea ha pubblicato i primi orientamenti sull'applicazione di alcune norme fondamentali della Direttiva NIS2 nei quali sono fornite importanti indicazioni circa l'implementazione degli obblighi e la compliance al nuovo assetto normativo.

Se la direttiva NIS, oggi superata dalla NIS2, 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 (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 e ha delineato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity. Sull'impianto del regolamento sta intervenendo la Commissione che ha lanciato una proposta di regolamento per quanto riguarda i servizi di sicurezza gestiti.

Sempre in attuazione di quanto previsto nella Strategia del 2020, il **15 settembre 2022** la Commissione ha pubblicato una **proposta di regolamento** sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali **(*Cyber Resilience Act* – CRA)**. 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. Sulla proposta della Commissione, Parlamento e Consiglio hanno raggiunto un **accordo provvisorio sul testo il 30 novembre scorso** che, pur mantenendo l'impianto generale proposto dalla Commissione che tuttavia aveva già subito diverse modifiche nel corso dell'*iter*, introduce una metodologia più semplice per la classificazione dei prodotti digitali, fissa in almeno 5 anni il periodo di sostegno per un prodotto digitale (esclusi i prodotti di cui sia previsto un periodo di utilizzo più breve), fissa obblighi di segnalazione relativi alle vulnerabilità attivamente sfruttate e agli incidenti innanzitutto nei confronti delle autorità nazionali competenti anche se è rafforzato il ruolo dell'ENISA, introduce ulteriori misure di sostegno per le piccole imprese e microimprese, comprese specifiche attività di sensibilizzazione e formazione, nonché il sostegno alle procedure di prova e di valutazione della conformità. Quanto al periodo di applicazione delle norme, nella logica di prevedere per i fabbricanti tempistiche di adeguamento idonee, esso è fissato in tre anni dall'entrata in vigore del regolamento. In ultimo, il 17 gennaio 2023 è entrato in vigore – ma si applicherà dal prossimo 17 gennaio – il **Reg. n. 2554/2022 (DORA)**, che si prefigge l'obiettivo di rafforzare e armonizzare i requisiti di cybersecurity di un'**ampia varietà di entità finanziarie**, sia di stampo tradizionale, sia nuovi attori come i fornitori di servizi per le cripto-attività e fornitori di servizi ICT (es: fornitori di servizi cloud), attraverso la prescrizione di una serie di adempimenti suddivisibili in sei pilastri.

Così come l'UE è impegnata nella definizione di un set di regole in grado di assicurare un'efficace tutela della cybersecurity, anche l'Italia è stata fortemente impegnata negli ultimi anni nella creazione di **un nuovo ecosistema normativo ruotante intorno all'istituzione**, in attuazione delle previsioni del PNRR, **dell'Agenzia per la cybersicurezza nazionale (ACN)** individuata come la principale autorità preposta a livello nazionale ed internazionale alla salvaguardia della cybersicurezza. L'ACN, in particolare, oltre a 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, è titolare di un'ampia gamma di competenze anche rispetto all'*awareness,* formazione e ricerca.

Un'altra importante sfida in ambito nazionale concerne l'**implementazione della NIS2**. Lo scorso 27 luglio, in particolare, è stato presentato alla Camera il disegno di legge recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023" (Atto Camera 1342), che all'art. 3 si occupa specificamente dei principi e dei criteri per l'esercizio della delega per il recepimento della direttiva NIS2. Il ddl dopo essere stato approvato dalla Camera il 20 dicembre, è attualmente al vaglio del Senato. Nella medesima legge di delegazione europea all'esame del Senato, l'art. 5 definisce princìpi e criteri direttivi specifici per l'esercizio della delega per il recepimento della direttiva CER (2022/2557).

Sempre nella logica di rafforzare l'ecosistema nazionale della cybersecurity, il **21 settembre 2019**, il **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, ha istituito **il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)** 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 e un regolamento governativo di esecuzione e che, seppur in ritardo, è finalmente giunto a completamento**. In virtù della disciplina disegnata, 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, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro) dalle Amministrazioni competenti nei rispettivi settori, sono tenuti a predisporre e aggiornare 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 Italia attivo presso la Presidenza del Consiglio. Tali soggetti, inoltre, sono tenuti – dal 30 giugno 2022 – a comunicare al CVCN l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici" (contenuti nell'elenco di beni ICT). A seguito di questa comunicazione, prende inizio il procedimento di verifica e valutazione dinanzi al CVCN, che si suddivide in tre macro fasi: verifiche preliminari, preparazione all'esecuzione dei test ed esecuzione dei test di hardware e software.

Sempre nella logica di accrescere la sicurezza, la **disciplina Golden Power**, che trova origine e fondamento nel decreto-legge 15 marzo 2012, n. 21 (convertito, con modificazioni, in legge 11 maggio 2012, n. 56), negli anni, ha subito 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. Inoltre, **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. Una novità rilevante per quanto concerne **l'ambito di applicazione della disciplina GP**, è stata introdotta con il **d. l. n. 104/2023 (c.d. Decreto Asset)** autorizza l'applicazione del golden power a tecnologie particolarmente critiche, inclusi l'IA, la cybersecurity e i macchinari per la produzione di chip.

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, 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 sono passate da 342 a 608 in soli due anni (2020-2022).
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.
In un contesto ad elevata complessità in cui la procedura di recepimento della NIS2 è in corso e la disciplina sul perimetro di sicurezza nazionale cibernetica vive le prime stagioni applicative, secondo le notizie apprese e gli annunci pubblicati, il 25 gennaio scorso il Consiglio dei Ministri avrebbe approvato un nuovo disegno di legge sulla cybersicurezza al fine espresso di rafforzare la normativa attuale per riuscire a contrastare l'avanzata offensiva del cybercrimine in Italia. Si tratta di un'iniziativa importante che da un lato inasprisce pene e sanzioni per gli hacker e, dall'altro, allarga il perimetro di soggetti tenuti a dotarsi di sistemi di cybersicurezza includendovi espressamente le regioni e le province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali. Tali soggetti, in particolare, dal punto di vista organizzativo, sarebbero chiamati ad individuare, laddove non presente, un referente per la cybersicurezza, a segnalare senza ritardo ad ACN, e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze ottenute e ad inviare entro settantadue ore a decorrere dal medesimo momento, una notifica completa di tutti gli elementi informativi disponibili, un incidente riconducibile a una delle tipologie individuate. A corredo di tale obbligo, sarebbe previsto, nel caso di reiterata inosservanza dell'obbligo di notifica, una sanzione amministrativa pecuniaria da €25.000 a €125.000.

CAPITOLO 3
Le certificazioni

È 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**.
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, seguito dall'ITSEC europeo e successivamente dai Common Criteria (CC). 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, sino alla piena operatività dello schema eurounitario EUCC, l'adozione del principio del mutuo riconoscimento**

a livello europeo. 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 sicurezza (SFR) e di garanzia (SAR). L'apprezzamento per i sistemi condivisi di valutazione è cresciuto costantemente negli anni, difatti secondo lo studio Jtsec, **nel 2021 si è raggiunto il valore più alto della storia, rafforzando un trend in forte crescita, particolarmente marcato soprattutto dal 2013**, **anche se va evidenziato che nel 2022 si è registrato un lieve rallentamento in tal senso**, in quanto sono stati certificati 370 prodotti, a fronte dei 399 dell'anno precedente e dei 383 del 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. Inoltre, **le rigidità alla base dei CC non permettono di mantenere la certificazione per prodotti/sistemi su cui vengono installate nuove patch per aggiornamenti**. In questo contesto, **i dati rilevati da Jtsec indicano per il 2022 l'avvenuta certificazione di 15 prodotti in Italia** (nel 2021 erano stati solo 11). 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 di cybersecurity uniforme in tutta l'UE già dal 2019, con la pubblicazione del Cybersecurity Act. 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 versione attualmente disponibile di tali meccanismi di certificazione (Versione 1.1.1) si fonda su un modello ispirato agli schemi ISO/IEC 15408 e ISO/IEC 18045 e ha lo scopo di creare un progetto comunitario volto a sostituire i singoli schemi nazionali, anch'essi basati sui Common Criteria, che operano sotto l'accordo di mutuo riconoscimento SOG-IS MRA. Le novità affrontano direttamente le criticità riscontrate, tra cui tempi e costi, ad esempio favorendo il *Patch Management*, ossia la possibilità di aggiornare, correggere, migliorare un programma, e il "*testing once principle*". **Lo scorso 31 gennaio, la Commissione europea ha adottato l'*Implementing Act*, ossia il regolamento di esecuzione con cui gli EUCC possono finalmente diventare ufficialmente parte della legislazione europea, fissando un periodo di transizione di 12 mesi (che aumentano a 24 se il processo di certificazione prende inizio entro i 12 mesi dall'entrata in vigore del regolamento), al termine del quale le certificazioni nazionali dovrebbero cessare di operare per lasciare spazio agli EUCC**.

CAPITOLO 4
La percezione delle imprese

Al fine di verificare **la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity**, con particolare riferimento al Perimetro di Sicurezza Nazionale Cibernetica (PSNC), **l'Istituto per la Competitività (I-Com) ha condotto un'indagine** (svolta tra agosto e ottobre 2023), avvalendosi anche del sostegno di alcune delle principali associazioni di categoria, che ha coinvolto 145 imprese appartenenti a vari settori.

Innanzitutto, ai soggetti partecipanti è stato chiesto di fornire **una valutazione circa l'impatto degli**

adempimenti prescritti dalle normative in cybersicurezza sulla competitività aziendale. Per il 39% delle grandi imprese la principale criticità è legata agli investimenti tecnico-organizzativi necessari alla compliance, mentre il 54% delle aziende di medie dimensioni si concentra prettamente sulla numerosità degli oneri burocratici e amministrativi richieste e, infine, il 29% delle piccole imprese si preoccupa prioritariamente dell'impatto sui rapporti con la supply chain.

Successivamente, è stato chiesto alle imprese intervistate di indicare nello specifico i fattori che rendono più difficoltosa la **compliance rispetto alle norme in materia di cybersecurity** ed è emerso che ciò sarebbe dovuto alla **mancanza di competenze idonee sia internamente, sia sul mercato del lavoro** (60 risposte in totale), seguito dall'incertezza interpretativa della normativa (52 risposte) e alla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (48 risposte).

Considerando l'aggravarsi dello scenario, sia in termini numerici che di impatto, circa le attività malevole a danno delle infrastrutture critiche anche in Italia, nonché dei maggiori adempimenti previsti dalle direttive NIS2 e CER, le quali si applicheranno a partire dal 18 ottobre 2024, è stato chiesto alle aziende partecipanti di fornire indicazioni su un **eventuale incremento delle risorse destinate alla cybersecurity**. Sul punto, si può osservare come **il 51,2% dei rispondenti stia ancora valutando tale eventualità. Diversamente, il 36,1% delle imprese ha già deciso di aumentare gli investimenti in cybersicurezza, mentre il restante 12,6% non stanzierà ulteriori risorse**.

Analizzando le risposte pervenute con riguardo alle **modalità con cui poter migliorare i livelli di sicurezza informatica**, **l'81% delle imprese ritiene che si debba puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze**. Tale opzione è risultata la più selezionata da tutte e tre le classi dimensionali considerate, a conferma del fatto che si tratta di un aspetto particolarmente sentito a livello aziendale. **La seconda scelta (65,5%) è ricaduta sul riservare più aiuti finanziari alle imprese, in quanto ciò è ritenuto necessario per stimolare gli investimenti in cybersecurity, mentre il 43% dei rispondenti sostiene che si debba rafforzare la collaborazione pubblico-privata sin dalle prime fasi del processo normativo.** Quest'ultima opzione non è stata particolarmente selezionata dalle PMI, che piuttosto hanno insistito sullo snellimento degli obblighi imposti dalle normative di cybersicurezza.

In merito all'adozione di una o più **certificazioni volontarie di cybersicurezza**, si può osservare che **la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione**. Tuttavia, **considerando solo le grandi imprese rispondenti, il 36% delle stesse ha già adottato una o più certificazioni di cybersecurity, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno**. Di converso, tra le medie imprese i risultati sono ben diversi, in quanto un mero 11% ha acquisito almeno una certificazione, mentre il 14% intende ottenere la prima certificazione entro un anno. Quanto alle piccole imprese, solo 1 ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno. Tali risultati possono trovare una motivazione negli **ostacoli che sono percepiti dalle imprese con riguardo all'ottenimento di una certificazione volontaria di cybersecurity**. In primo luogo, il principale intralcio (38% dei rispondenti) risiede nei **costi elevati del processo di certificazione**, che **non sono percepiti come proporzionati ai benefici** che ne possono conseguire. In secondo luogo, quasi il 27% sostiene che **i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi**. Il 70% dei rispondenti è parzialmente o totalmente d'accordo in merito al fatto che **standard comunitari** – come gli *European Common Criteria-based cybersecurity certification scheme* (EUCC) **possano incentivare il ricorso a tali strumenti.**

Tra coloro che hanno dichiarato di **aver adottato almeno una certificazione, i principali effetti direttamente riconducibili ad essa sono stati**: un **miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders** (45% dei rispondenti), una **maggiore consapevolezza dei dipendenti e dei collaboratori esterni** (39,7%) e **più possibilità di partecipare a bandi di gara pubblici o** privati (29,5%).

L'ultima sezione dell'indagine riguarda più nello specifico alcuni aspetti connessi al Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e alle attività del Centro di Valutazione e Certificazione Nazionale (CVCN). Più nel dettaglio, la prima domanda chiede alle imprese la loro **percezione rispetto ai test prescritti dal CVCN sui beni, sistemi e servizi Ict** di rispettiva pertinenza ed è emerso che **per il 30% dei rispondenti non si rilevano particolari criticità in tal senso, mentre il 22,7% non ha espresso un'opinione in merito**. La restante quota di feedback pervenuti evidenzia, invece, alcune problematiche: **32 soggetti ritengono che l'esecuzione di frequenti test, che allungano i tempi e incrementano i costi, possa disincentivare l'acquisto di "beni Ict" di ultima generazione; 23 aziende convengono che la necessità di esaminare tali beni Ict nel relativo ambiente operativo determini la ripetizione di test sugli stessi beni; 16 imprese si preoccupano che la parziale incertezza sulle attività di valutazione possa rappresentare un disincentivo dato il rischio reputazionale conseguente a un eventuale ko**.

Relativamente alle diverse posizioni dei rispondenti con riferimento a una **valutazione complessiva della disciplina sul PSNC**, è possibile osservare come **il 20,7%, soprattutto grandi imprese, si ritenga assolutamente soddisfatto dalle regole e dagli adempimenti previsti nell'ambito del Perimetro**. Parallelamente, poco **più del 10% considera tale normativa come eccessivamente gravosa**, recando solo un minimo beneficio per la sicurezza nazionale. Invece, **il restante 68,8% si colloca nel mezzo**. Il maggior numero, 52 imprese, ha una percezione parzialmente positiva, poiché ritiene che gli adempimenti richiesti – seppur meno aderenti alle esigenze aziendali – siano funzionali a garantire la sicurezza nazionale. Di converso, 21 rispondenti hanno denunciato che l'approccio adottato impone adempimenti sproporzionati ai soggetti inclusi nel Perimetro.

L'ultima domanda del questionario richiede agli intervistati di proporre alcuni **aspetti su cui insistere per migliorare l'ecosistema della cibersicurezza in Italia**. Sul punto**, 60 rispondenti ritengono sia opportuno superare la logica del test sul singolo oggetto in favore di una logica di accreditamento dei fornitori affidabili, prevedendo rimedi contrattuali per legge e adeguate forme di responsabilizzazione nei confronti dei fornitori stessi**. Anche la semplificazione dei test obbligatori sui beni ICT, introducendo – ad esempio – un approccio a tempi fissi con tempistiche controllate secondo una valutazione dei rischi basata su criteri standard, ha incontrato un importante consenso tra i rispondenti, precisamente 48, di cui ben 7 piccole imprese.

Con riguardo agli altri approcci proposti dalle imprese intervistate, pare opportuno fare riferimento **all'armonizzazione dei requisiti delle normative in materia di cybersicurezza, a una maggiore considerazione delle certificazioni a norma del Cybersecurity Act per la procedura di valutazione dinanzi al CVCN, oltre che a un effettivo riconoscimento sul mercato del costo necessario per garantire un elevato livello di cibersicurezza dei prodotti e servizi ICT**.

CAPITOLO 5
La cooperazione tra pubblico e privato

Il **Partenariato Pubblico-Privato (PPP)** è inteso dalla Strategia Nazionale di Cybersicurezza 2022-2026 e dal relativo Piano di Implementazione come elemento traversale agli obiettivi di protezione, risposta e sviluppo, nonché ai fattori abilitanti della formazione,

della promozione della cultura della cybersicurezza e della cooperazione. Tale istituto trova una disciplina organica all'interno del **Codice dei Contratti Pubblici**, riformato di recente attraverso il **d. lgs. n. 36/2023**, che era del tutto assente nel d. lgs. n. 163/2006 e meno strutturata nella precedente normativa in materia (d. lgs. n. 50/2016). I-Com ha mappato le principali iniziative nazionali di PPP in cybersecurity avviate negli ultimi anni, tra cui va annoverato il **Polo Strategico Nazionale (PSN)**, ossia l'infrastruttura che ha l'obiettivo di dotare la PA di tecnologie e sistemi cloud che possano beneficiare di elevate garanzie di affidabilità, resilienza e indipendenza. Inoltre, sono stati promossi vari eventi su scala nazionale per rafforzare la consapevolezza e lo scambio di idee, come richiamato dal Piano di Implementazione dell'ACN. Tra questi vi sono "**Itasec**", organizzata dal Cybersecurity National Lab del CINI e "**CyberSec**", evento promosso da Cybersecurity Italia. Il MUR ha selezionato quattordici grandi Partenariati estesi alle università, ai centri di ricerca e alle aziende sul territorio, nell'ambito dei quali è stata avanzata una proposta progettuale dal titolo **"Security and Rights in the CyberSpace" (SERICS)** che definisce un'ampia agenda di ricerca che abbraccia questioni tecniche, legali e sociali relative alla sicurezza e alla privacy. Tra i progetti volti a formare, consapevolizzare e a creare forza lavoro nazionale specializzata in cybersicurezza abbiamo, a titolo di esempio, **"CyberChallenge"**, **"OliCyber"**, **"CyberTrails"**, **"Cyber Harbour"** e il **Primo dottorato nazionale in cybersicurezza** realizzato dalla Scuola IMT Alti Studi di Lucca in collaborazione con il Laboratorio nazionale di Cybersecurity del CINI. Anche gli otto **Competence Center** istituiti dal MISE con funzione di orientamento e formazione alle imprese rientrano tra i partenariati pubbico-privati. Questi presentano focus tematici specifici, tra cui è inclusa la cibersicurezza, offrendo – anche nel caso di centri di competenza con focus differenti – singoli progetti di ricerca e innovazione sul tema.

In tema di collaborazione tra pubblico e privato, vanno considerate anche **le start-up innovative**.

I-Com ha svolto un monitoraggio su quelle che si occupano di cybersicurezza, osservandone **121 sull'intero territorio nazionale**. Per quanto concerne l'anno di costituzione, è possibile **notare un andamento in costante crescita fino al 2019**, a cui è seguito un rallentamento importante nel 2020 – causa pandemia da covid-19 – che è stato successivamente recuperato l'anno seguente, in cui si sono costituite il maggior numero di start-up in cybersicurezza su base annua (35). Tuttavia, **nel 2022 si è assistito a una contrazione significativa, con sole 11 start-up in tale ambito, tendenza calante continuata nel 2023 in cui se ne rilevano appena 4**.

In aggiunta, tra le altre **forme di collaborazione tra pubblico privato sulla cybersecurity** rientrano gli accordi con l'ACN nell'ambito delle proprie funzioni di impulso e, in particolare, le iniziative per il rafforzamento delle sinergie tra l'Agenzia e i **Cluster tecnologici** per agevolare il trasferimento tecnologico verso le PMI.

CAPITOLO 6
Le competenze in cibersicurezza

La formazione degli individui riveste un ruolo fondamentale nell'ambito della cibersicurezza. Nel merito, l'Italia è più indietro rispetto agli altri Paesi europei e presenta una diffusione di competenze digitali altamente variegata a seconda della fascia d'età. Ad esempio, le competenze digitali almeno di base sono diffuse in una quota pari al 45,8% della popolazione. Un dato interessante emerge a proposito della consapevolezza sui pericoli digitali, infatti, **rispetto agli individui che non utilizzano l'Internet of Things per timori legati alla sicurezza, l'Italia presenta quote sensibilmente più basse rispetto alla media UE**. Ciò detto, **nel corso del 2023 si è riscontrato un significativo incremento degli illeciti legati al fenomeno del falso trading online**. Più in generale, l'anno scorso

sono peggiorati numerosi dati emergenti dal report della Polizia Postale: rispetto al 2022 sono maggiori sia i casi trattati che le somme di denaro sottratte. Nell'ambito della formazione ICT delle imprese, il nostro Paese è nuovamente al di sotto della media europea. Addirittura, **la quota di imprese ICT con più di 10 addetti che erogano formazione al proprio personale è diminuita negli ultimi anni**, dal 62,1% del 2019 al 54,7% del 2022. Allo stesso tempo, sempre in Italia, il costo medio delle violazioni di dati è aumentato da 3,6 milioni di dollari nel 2021 a 3,86 nel 2023; nel medesimo periodo lo stesso dato diminuiva sia in Francia che in Germania. Tutti questi elementi segnalano una situazione allarmante per la formazione e consapevolezza dei rischi digitali in Italia, per cui **risulta necessario investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità, indipendentemente dal livello di alfabetizzazione digitale già in loro possesso**. Molte delle iniziative già attive in questo campo nascono e si sviluppano anche grazie al settore privato, spesso in collaborazione e/o col patrocinio di enti pubblici. Appare dunque utile che queste forme di collaborazione pubblico-privato possano essere rafforzate e messe maggiormente a sistema.

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 2024** presentava **520 tra corsi e insegnamenti relativi alla cibersicurezza rispetto ai 234 individuati a inizio 2023**. Nel dettaglio, l'analisi ha individuato 259 insegnamenti singoli all'interno di corsi di laurea magistrale, 105 insegnamenti singoli in lauree triennali, 44 progetti di ricerca in dottorati, 34 lauree magistrali, a fronte di 22 corsi all'interno di dottorati di ricerca, 26 master, 23 corsi singoli all'interno di master di I e II livello e 7 lauree triennali interamente dedicate alla cybersecurity. Pertanto, il totale delle lauree specifiche (triennali e magistrali) sul tema della cibersicurezza ammonta a 41, ben 15 in più rispetto a quelle rilevate a gennaio 2023. La formazione post-laurea si affianca a quella universitaria con differenze in termini quantitativi piuttosto importanti: tra progetti di ricerca in dottorati e master di primo e secondo livello sono stati conteggiati ben 70 corsi "specializzati". Nel complesso, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 111 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 (101 tra corsi e singoli insegnamenti), in Campania (53) e in Lombardia (47). Tuttavia, se si considerano i **dati normalizzati per il numero di Università presenti sul territorio regionale**, la classifica varia mostrando in prima posizione la Liguria con un rapporto 13:1, seguita da Veneto (10,8:1) e Piemonte (9,5:1). A livello regionale, a gennaio 2024 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere. In relazione alla distribuzione regionale della offerta formativa "specializzata" (lauree triennali, magistrali, master e progetti di ricerca in dottorati), il Lazio si conferma la regione più interessata con 26 percorsi complessivi, catalizzando buona parte dell'offerta sia in termini di lauree dedicate (8 tra magistrali e triennali), sia per quanto concerne la specializzazione post-laurea (10 master e 8 progetti di ricerca in dottorato). **L'elevato numero di master specifici sui temi della cibersicurezza (26) sembra suggerire un'elevata domanda di approfondimento post-laurea su questi temi.** Nell'ambito della formazione superiore, un ruolo di rilievo è rivestito dagli ITS che hanno lo scopo di formare personale tecnico in aree strategiche per lo sviluppo del tessuto economico del Paese. La **Missione 4 del PNRR sottolinea l'importanza della riforma del sistema ITS**, che si è concretizzata attraverso la **l. n. 99 del 15 luglio 2022**, alla quale si sta dando attuazione mediante diversi decreti.

Il rapporto di monitoraggio, pubblicato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE), nell'anno 2023 ha registrato sul territorio nazionale ben 142 ITS. **Il 5 ottobre 2022 è stato firmato l'Accordo per la Rete di coordinamento nazionale per lo sviluppo di percorsi formativi specifici in Cybersecurity nell'ambito degli ITS Academy, tra le cui parti rientra l'ACN**. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-Com, **gli ITS che si occupano di cybersicurezza sono il 17,6% rispetto al numero complessivo di quelli attivi**, l'offerta formativa erogata ha visto l'avvio di un numero considerevole di corsi in sicurezza informatica specifici e di singoli insegnamenti sul tema all'interno di corsi attinenti a materie differenti.

icom
istituto per la competitività

CAPITOLO 1

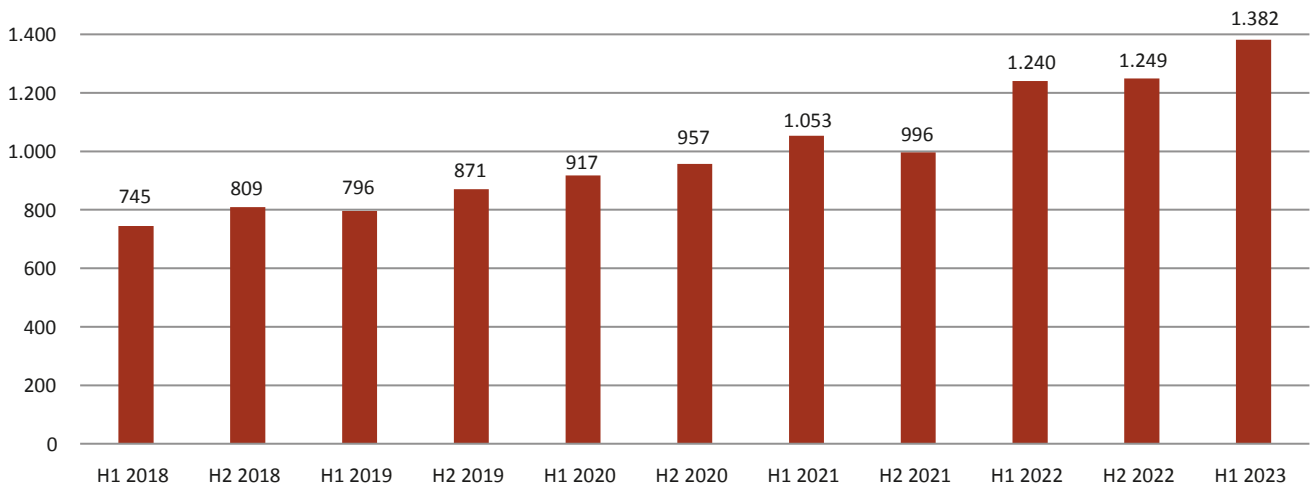
IL QUADRO EUROPEO E ITALIANO DELLA CYBERSECURITY

1.1. LO SCENARIO EUROPEO E NAZIONALE DEGLI ATTACCHI CIBERNETICI

La costante e ingente evoluzione dell'ecosistema digitale ha generato una vasta gamma di opportunità per gli individui operanti a livello pubblico e privato, consentendo la gestione a distanza dei processi interni alle organizzazioni e la possibilità di interagire con soggetti situati in tutto il mondo in maniera più efficiente e veloce. Allo stesso tempo, all'impiego delle nuove tecnologie si è accompagnata **l'intensificazione di rilevanti rischi, in particolare, quelli riconducibili alla minaccia cibernetica.** Quest'ultima ha assunto un ruolo sempre più centrale tra le sfide nazionali, eurounitarie e globali affrontate dalle Istituzioni, soprattutto in virtù dell'instabilità geopolitica degli ultimi anni che influenza il panorama della sicurezza informatica, traducendosi in **cyberattacchi sempre più gravi e numerosi**, che – potendo superare i confini politici – spingono i Paesi e le organizzazioni internazionali allo sviluppo di policy, strategie e normative che ruotino attorno (o comunque includano in maniera rilevante) alla tutela del cyberspazio.
Difatti, per comprendere l'accelerata di questo fenomeno, non va sottovalutato che **nel 2022 accanto alle tipiche dinamiche cybercriminali si è aggiunto il conflitto tra Russia e Ucraina**, che ha rivelato una serie di capacità cibernetiche offensive che sono state messe in campo a supporto di attività di **cyber-intelligence, cyber-warfare e di operazioni ibride**. Si tratta di un andamento che rallenterà difficilmente nei prossimi anni, poiché le competenze degli individui che utilizzano la rete non si sviluppano di pari passo a quelle dei c.d. "soggetti malevoli", i quali sono divenuti sempre più difficili da riconoscere e contrastare.
L'ultimo rapporto dell'Associazione Italiana per la Sicurezza Informatica (Clusit), pubblicato a ottobre 2023, fornisce una chiara panoramica di come **le minacce informatiche siano cresciute costantemente nel corso degli ultimi anni**. Lo studio ha ad oggetto l'analisi di oltre 17.000 cyber attacchi noti, andati a buon fine e di particolare gravità, a partire dal 2011, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali, o che comunque prefigurano scenari preoccupanti.

Fig. 1.1: Andamento degli attacchi informatici per semestre 2018-2023

Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023



Osservando i dati dal 2018 (Fig. 1.1), è possibile notare **come il numero di azioni malevole annuali sia cresciuto di oltre il 60%, passando dalle 1.554 del 2018 alle 2.489 del 2022**. Inoltre, anche **i valori inerenti il primo semestre del 2023 appaiono preoccupanti**, in quanto si è raggiunta una quota di **1382 attacchi, ben 637 in più rispetto al primo semestre del 2018**. Tale scomposizione mostra andamenti tipicamente peggiori nel periodo che va da luglio a dicembre degli anni di riferimento, ad eccezione del 2021, dove si è assistito a un decremento delle azioni malevole esperite, passando da 1.053 a 996.

Per quanto concerne l'analisi delle vittime di attacchi informatici classificate per categoria d'appartenenza (Fig. 1.2), secondo i dati raccolti dal Clusit nei primi sei mesi del 2023, **la maggioranza degli eventi non aveva un destinatario specifico, bensì target multipli**, che sono stati il bersaglio di quasi un quarto (20%) degli attacchi analizzati. Scendendo nel dettaglio settoriale vediamo come il comparto che è stato maggiormente vittima di azioni gravi è quello della salute (15%), seguito dalle Pubbliche Amministrazioni (12%). Diversamente, i settori dei media e del commercio hanno visto numeri decisamente inferiori (3%).

In merito alla distribuzione geografica delle vittime (Fig. 1.3), **nel primo semestre del 2023 i numeri più elevati sono quelli riconducibili al continente americano**, il quale presenta una quota crescente rispetto all'anno precedente (si è passati dal 38% al 46%). In questo panorama, **l'Europa assume la seconda posizione, attraendo il 22% delle azioni dei cybercriminali**, in calo del 2% rispetto all'anno precedente. Gli attacchi inerenti le vittime europee sopravanzano anche quelli diretti ad obiettivi multipli, ossia inerenti organizzazioni situate in continenti diversi, che sono passati dal 27% del 2022 al 22% del primo semestre dell'anno in corso. L'ultimo posto è occupato dall'Africa che nel 2022 è stata vittima dell'1% degli attacchi informatici gravi, mentre nel range di riferimento del 2023 non ne registra nessuno.

Altro aspetto rilevante è quello dell'analisi della **gravità degli attacchi** (*severity*), che mira ad offrire una corretta valutazione degli impatti degli incidenti, sia in merito alle ripercussioni tecnologiche che a quelle reputazionali, legali ed economiche. Negli ultimi tre anni (Fig. 1.4) si è instaurata una tendenza che ha vi-

Fig. 1.2: Distribuzione della tipologia delle vittime H1 2023 (%)

Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023

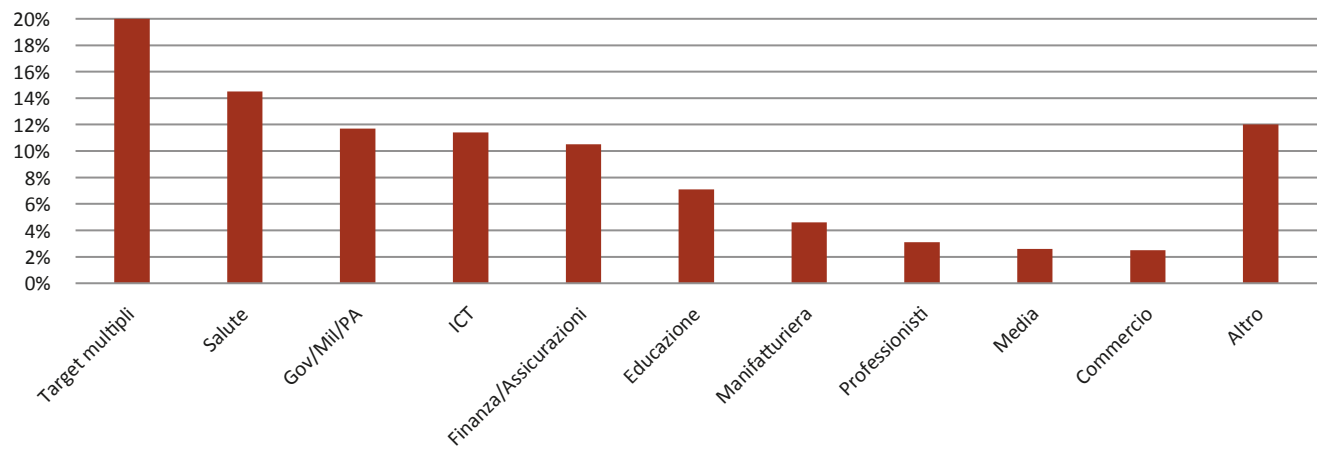


Fig. 1.3: Distribuzione geografica della tipologia delle vittime (%)

Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023

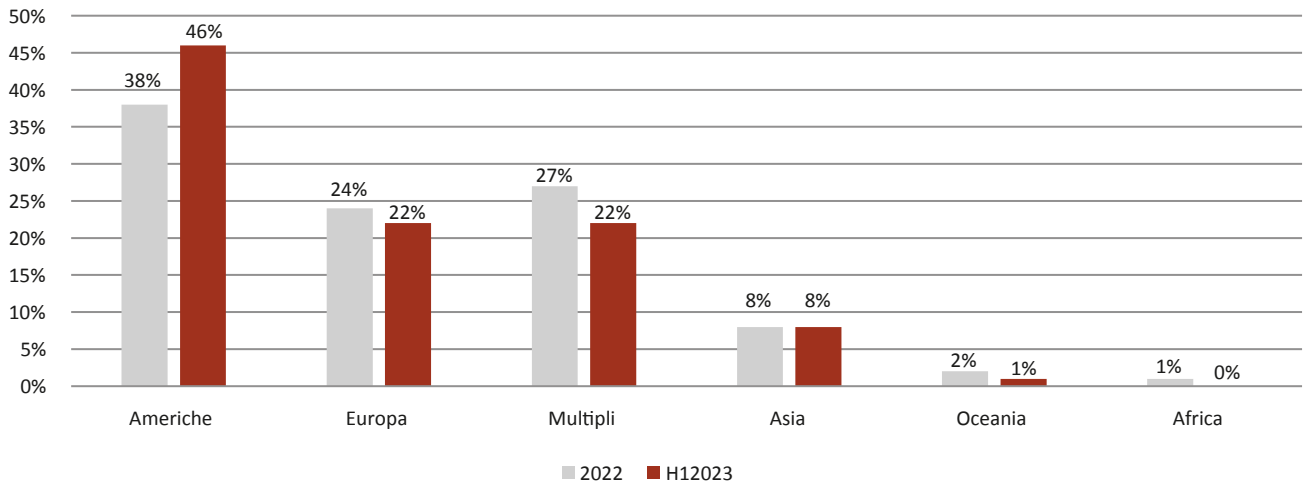
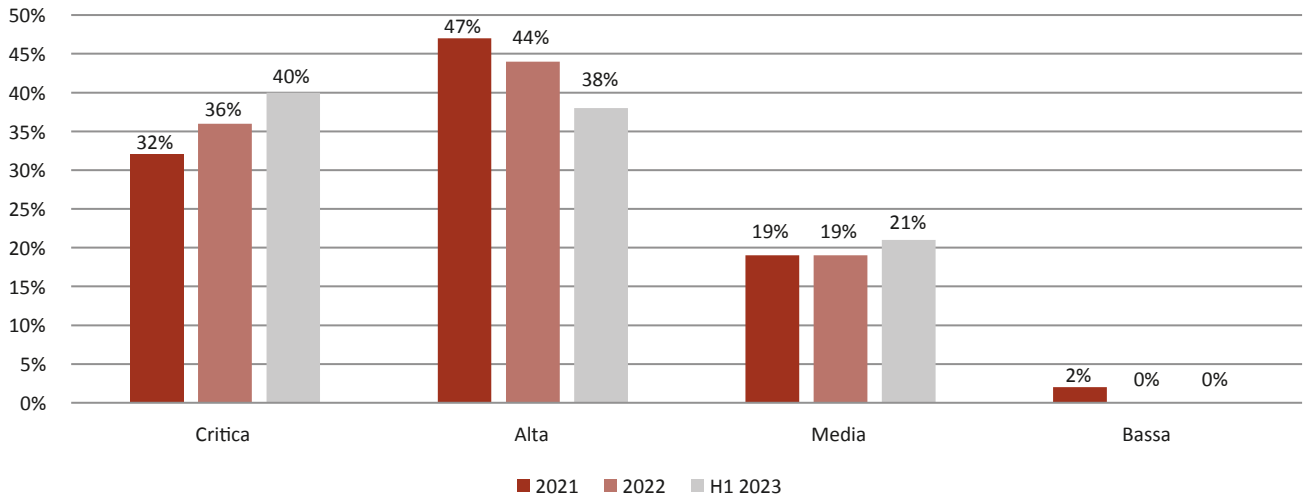


Fig. 1.4: Andamento della *severity* degli attacchi (%)

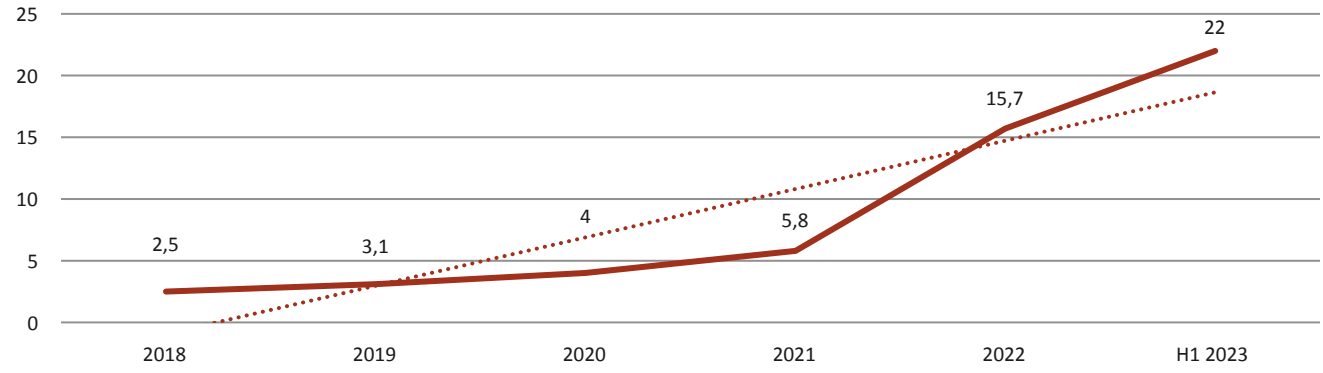
Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023



sto **prevalere gli attacchi con *severity* "Critica"**, che hanno prodotto effetti dannosi importanti per le vittime, tra cui ingenti perdite economiche e di dati. Si è passati **dal 32% nel 2021, al 36% nel 2022 e al 40% nel primo semestre del 2023**. Un grado "Alto" della *severity* è prevalso nel 2021 (47%) e nel 2022 (44%), mentre gli impatti "Medi" e "Bassi" sono risultati in lieve crescita per la prima categoria (dal 19% del 2021 al 21% del primo semestre 2023), tendendo, invece, a scomparire per la seconda.

Fig. 1.5: Distribuzione dei cyberattacchi e media mensile in Italia

Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023



Procedendo con un'analisi specifica del **contesto italiano** (Fig. 1.5), dal report fin ora menzionato emerge che lo scenario negativo già presente nel 2022 sia stato confermato anche nel primo semestre 2023, evincendo a partire dal 2018 una quota pari a **505 attacchi noti di particolare gravità che hanno coinvolto realtà italiane, di cui ben 132 verificatisi nei primi sei mesi dell'anno scorso**. Con specifico riferimento alla media mensile, dopo aver registrato nei primi anni di analisi un valore abbastanza contenuto (2,5 nel 2018; 3,1 nel 2019; 4 nel 2020; 5,8 nel 2021), essa è transitata **da 15,7 attacchi al mese rilevati nel 2022 a 22 attacchi al mese nel primo semestre 2023**.

Valutando la distribuzione delle vittime (Fig. 1.6), **la categoria merceologica per cui si rileva un maggior numero di attacchi è la Pubblica Amministrazione (23%)**, seguita a breve distanza da target multipli e dalla manifatturiera (17%). Si tratta di una ripartizio-

Fig. 1.6: Distribuzione della tipologia delle vittime in Italia nei primi sei mesi del 2023 (%)

Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023

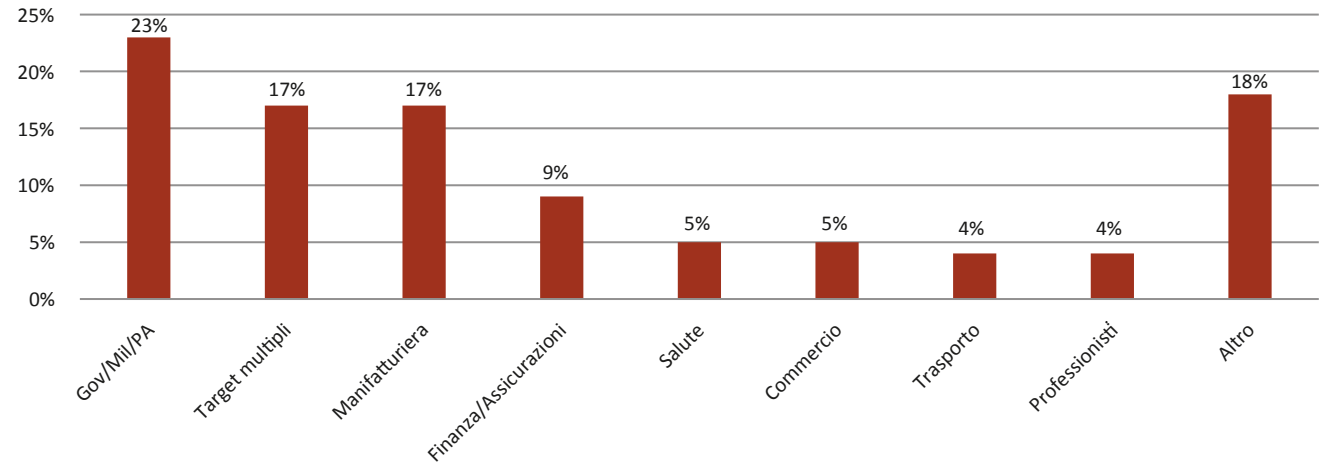
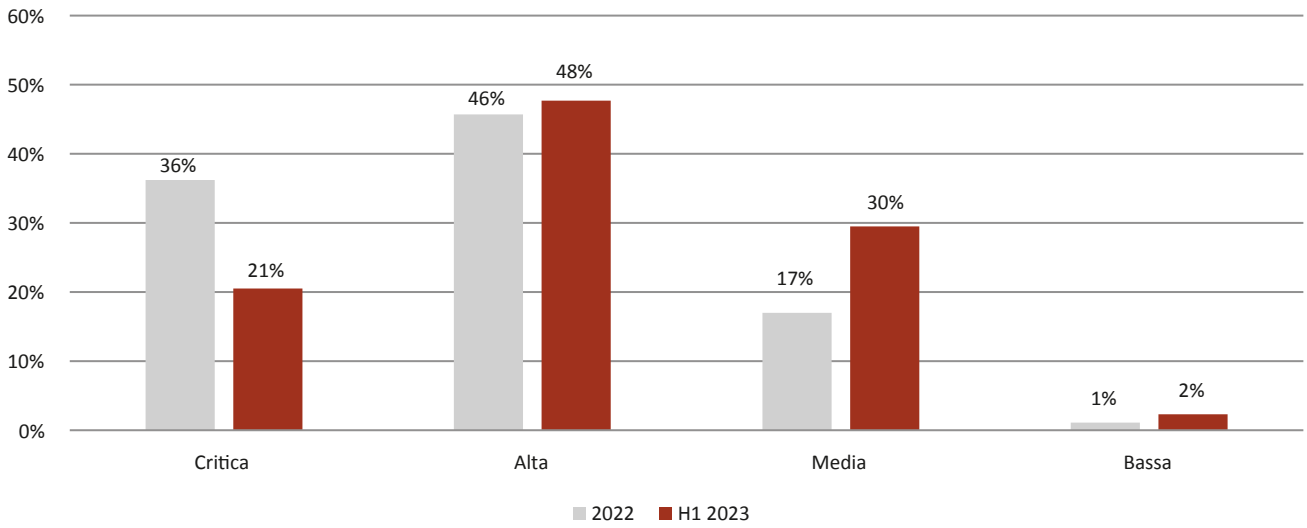


Fig. 1.7: Andamento della *severity* degli attacchi in Italia (%)

Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, ottobre 2023



ne diversa rispetto a quella del campione a livello mondiale, in cui le categorie raccolgono rispettivamente il 12%, 20% e il 5% degli attacchi (ricoprendo la terza, la prima e la settima posizione). Di converso, in coda alla classifica vi sono il commercio (5%); il trasporto[1] e i singoli professionisti (4%).

In termini di *severity*, il dato italiano nel primo semestre del 2023 assume un andamento particolare, in quanto a differenza di quello mondiale (40%) **gli incidenti con impatto "Critico" costituiscono il 21%**. La quota più elevata di attacchi è ricondotta a una *severity* **"Alta" (48% in Italia/38% globale) e "Media" (30% in Italia/21% mondiale), mentre una *severity* "Bassa" attiene solo al 2% degli episodi**. Rispetto all'anno precedente (Fig. 1.7), la *severity* "Alta" sembra assestarsi (46% nel 2022) e gli attacchi di massima criticità appaiono in riduzione, passando dal 36% del 2022 al 21% dell'ultimo semestre. Peraltro, viene rimarcata una crescita degli incidenti con severità "Media" (17% nel 2022/30% nel primo semestre 2023).

In base a quanto sin ora esposto, si riscontra che le risultanze in tema di cyber attacchi afferenti ai primi sei mesi del 2023, sia a livello globale, europeo, che nazionale, potrebbero confermare la linea di tendenza degli ultimi anni e giungere, conformemente a quanto avvenuto nel 2022, ad un suo superamento, destando ingenti preoccupazioni che sollecitano interventi adeguati a favore di una maggiore proattività dei singoli Stati.

1.2. LO STATO DEGLI INVESTIMENTI IN CYBERSICUREZZA IN UE E IN ITALIA

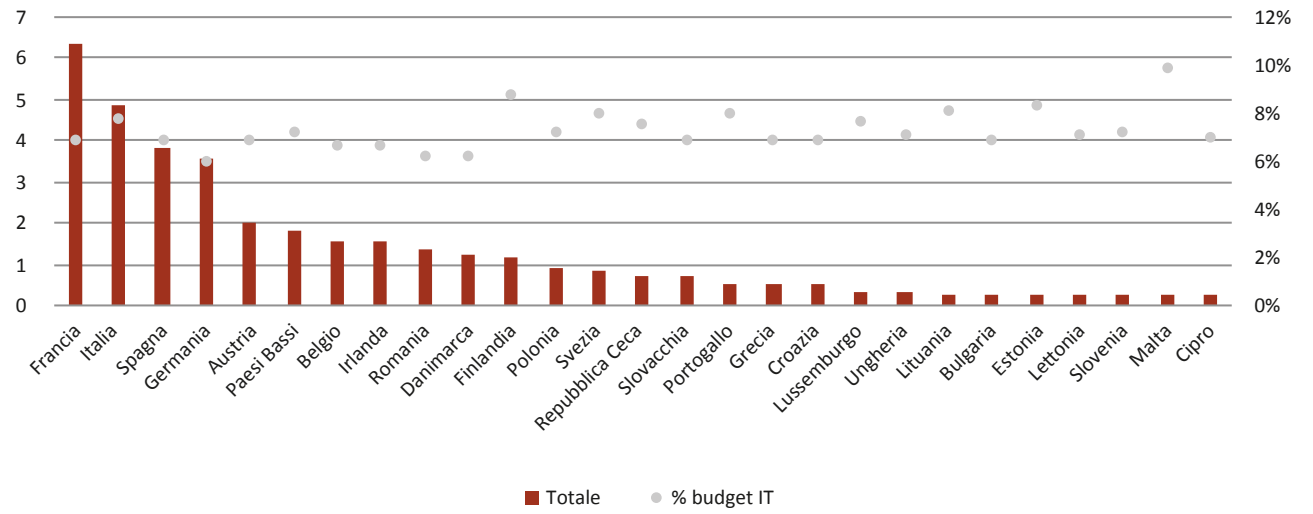
In un contesto come quello delineato nel paragrafo precedente, gli **investimenti in cybersicurezza** assumono un ruolo di significativa importanza, in quanto rappresentano la prima risposta, in termini preventivi, alle esigenze che incombono sulle imprese e che

1 Tale categoria a livello globale è inclusa nella voce "altro".

derivano dalle nuove dinamiche del cyberspazio.
Nell'ultima versione del report *"NIS Investments"*, pubblicato dall'ENISA a novembre 2023, vengono analizzate le attività di impiego economico per la sicurezza informatica a livello europeo, intervistando esponenti di **1080 organizzazioni residenti in tutti e 27 gli Stati Membri** (40 per paese), appartenenti ai settori sottoposti alla direttiva NIS e suddivisi in due macrocategorie, ovverosia gli "Operatori di servizi essenziali" (OSE)[2] e i "*Digital Service Providers*"[3] (DSP).
Secondo quanto emerso dal rapporto (Fig. 1.8), tra i singoli Paesi UE si osserva come **le organizzazioni francesi siano quelle che spendono di più in sicurezza informatica in valore mediano[4] (€6,30 milioni), seguite dalle italiane e spagnole che riportano una spesa rispettivamente pari a 4,80 e 3,80 milioni di euro**. Questi investimenti rappresentano nel caso della Francia e della Spagna il 6,7% del budget IT, mentre **per l'Italia corrispondono al 7,6%**. Malta è il Paese in cui le organizzazioni vedono la percentuale più alta del proprio budget IT allocata a favore della sicurezza informatica, precisamente si fa riferimento al 9,7%.
Passando all'analisi settoriale (Fig. 1.9) è possibile osservare che **le aziende afferenti al settore bancario siano le più propense a investire in sicurezza informatica**, presentando una **media europea di €10,6 milioni di euro nel 2022 (8% del budget IT)**. Ad esse seguono quelle del settore dell'energia, con una media di €8,8 milioni (5% del budget IT) e i Marketplace online, con una media di €4,9 milioni (9% del budget IT). Agli ultimi posti vi sono le imprese che forniscono e distribuiscono acqua potabile (€2,2 milioni, 6% del budget IT); le infrastrutture del mercato finanziario (€9 mila, 10% del budget IT) e le infrastrutture digitali (€6 mila, 11% del budget IT).

Fig. 1.8: Spesa per la sicurezza informatica degli OSE/DSP in ogni stato membro (in € milioni)

Fonte: ENISA, NIS Investments Report, novembre 2023



2 Questi comprendono i seguenti settori: energia; trasporti; bancario; finanziario; salute; servizi idrici; infrastrutture digitali.
3 Questi includono marketplace online; cloud computing provider; motori di ricerca online.
4 Il valore mediano è il valore/modalità (o l'insieme di valori/modalità) assunto dalle unità statistiche che si trovano nel mezzo della distribuzione.

Fig. 1.9: Spesa per la sicurezza informatica per settore (in € milioni)

Fonte: ENISA, NIS Investments Report, novembre 2023

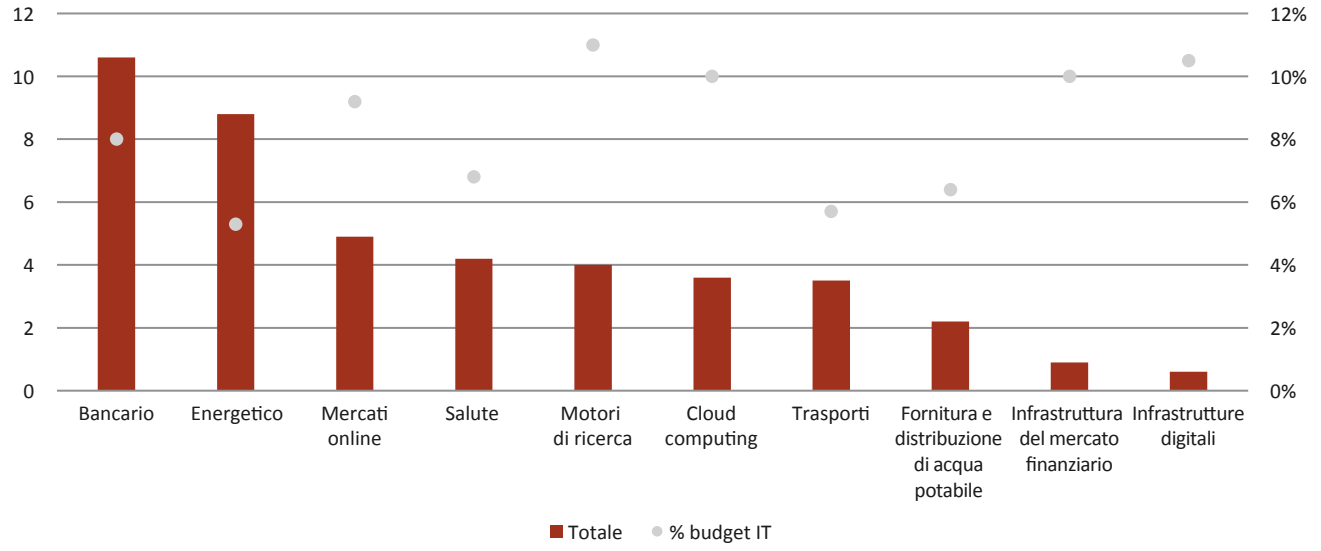
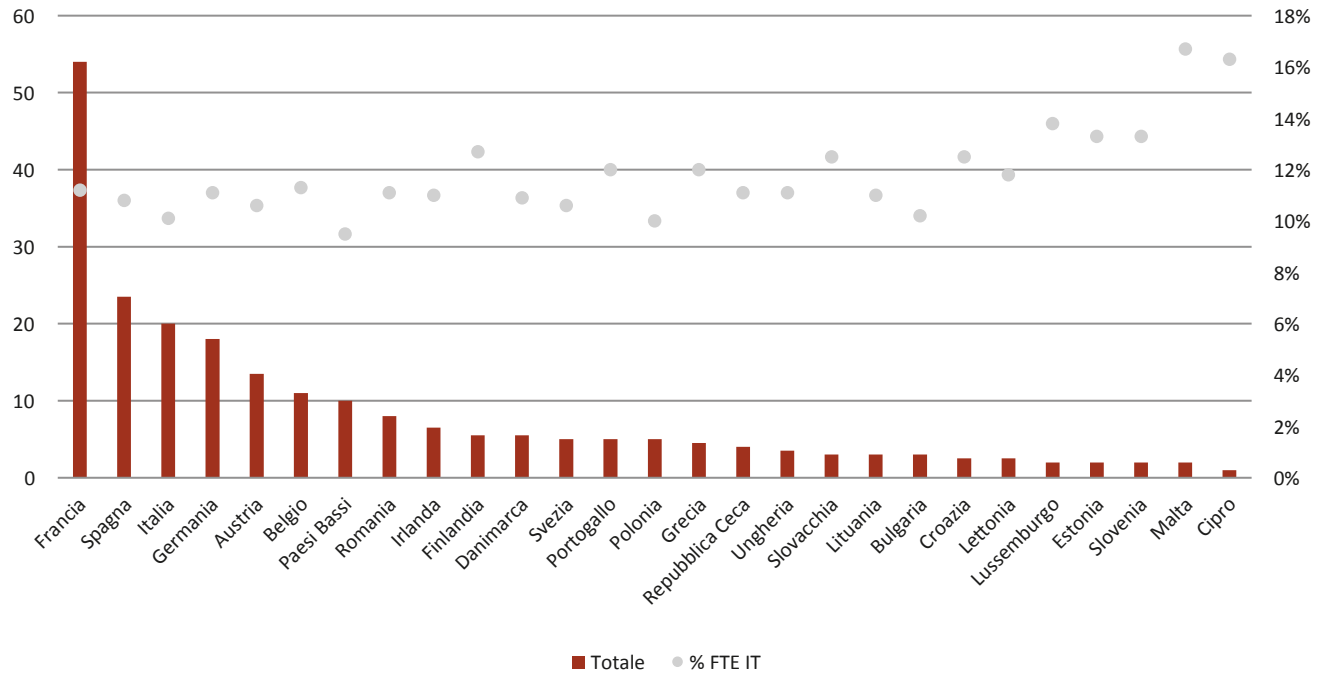


Fig. 1.10: FTE in sicurezza informatica negli OSE/DSP intervistati in ogni Stato membro

Fonte: ENISA, NIS Investments Report, novembre 2023



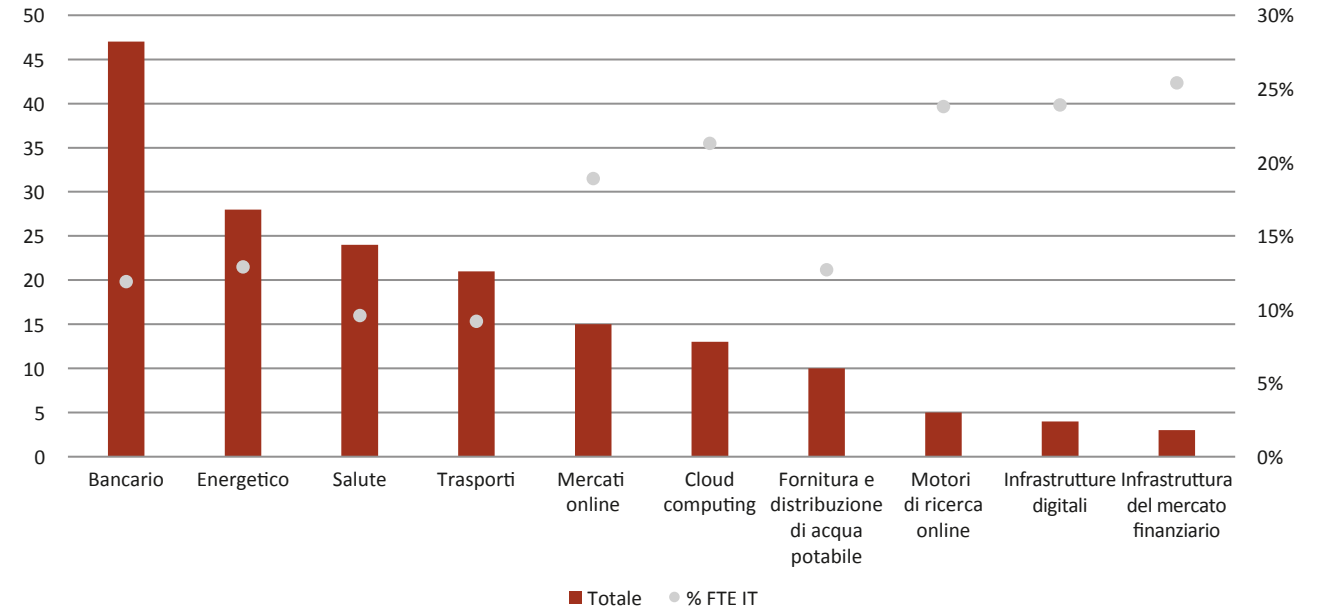
Altro dato interessante è quello attinente alla quota di ***Full-Time Equivalent*** (FTE – Equivalente a Tempo Pieno) che si occupano di sicurezza informatica negli OSE/DSP (Fig. 1.10). **La Francia primeggia sul punto, mostrando un valore mediano di 54 FTE, seguita dalla Spagna (23,5 FTE) e dall'Italia (20 FTE)**. Parametrando **la quota di personale a tempo pieno in cybersecurity al totale di FTE IT**, si evince che sono Malta e Cipro ad avere la percentuale più elevata, ossia rispettivamente il 16,7% e il 16,3%, succedute dal Lussemburgo (13,8%) e dalla Finlandia (12,7%). **L'Italia, la Polonia e i Paesi Basi si collocano in coda, con una quota di FTE in sicurezza informatica ordinatamente del 10,1%, del 10% e del 9,5% rispetto agli FTE IT**[5].

Tenendo conto dei settori NIS (Fig. 1.11), **il numero medio più elevato di FTE in cybersecurity è ricondotto alle imprese bancarie (47 FTE; 11,9% di FTE IT)**, energetiche (28 FTE; 12,9% di FTE IT) e sanitarie (24 FTE; 9,6% di FTE IT). Diversamente, i motori di ricerca online (5), le infrastrutture digitali (4) e le infrastrutture del mercato finanziario (3) detengono le quote più basse, che si innalzano se si parametra il personale a tempo pieno in sicurezza informatica con quello IT, essendo nella prima categoria economica il 23,8%, nella seconda il 23,9% e nella terza il 25,4%.

Nel report NIS Investments si indaga anche in merito al rilievo che gli OSE e i DSP comunitari, a livello territoriale e settoriale, affidano alla **formazione in cybersecurity**. Di preciso (Fig. 1.12)[6], si riscontra come **i tre paesi in cui si è registrata la maggior somma di investimenti in materia nel 2022 siano stati la Francia (€400 mila), l'Italia (€300 mila) e la Germania (€250 mila)**. Invece, la Slovenia occupa l'ultima posizione con un bilancio di €30 mila, preceduta da Malta e dalla Lettonia (€40 mila).

Fig. 1.11: FTE in sicurezza informatica come quota di FTE IT per settore

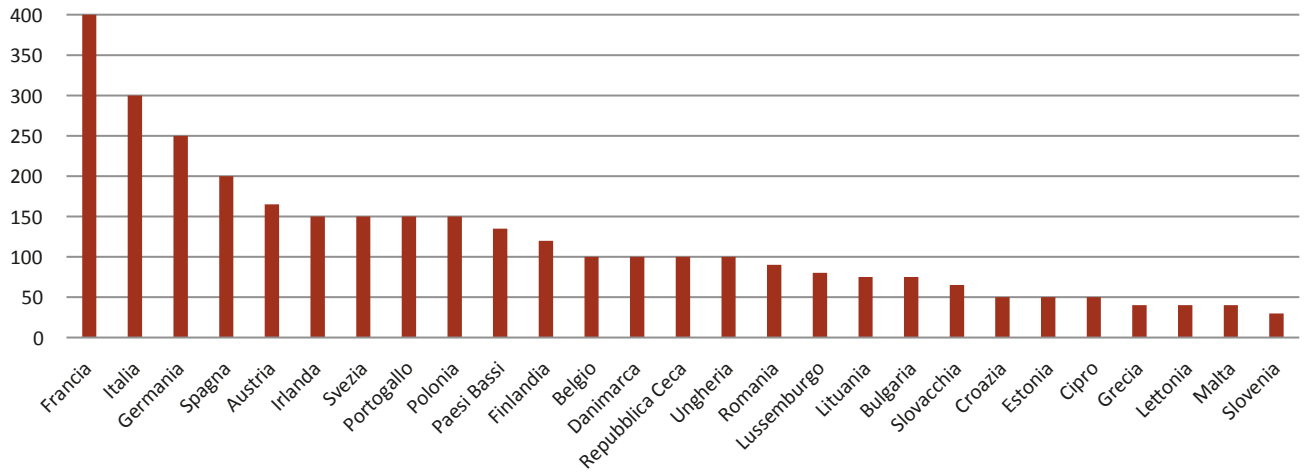
Fonte: ENISA, NIS Investments Report, novembre 2023



5 Si fa riferimento al valore mediano.
6 Si fa riferimento al valore mediano.

Fig. 1.12: Budget per la formazione in cybersecurity (in migliaia) degli OES/DSP in ogni Stato membro

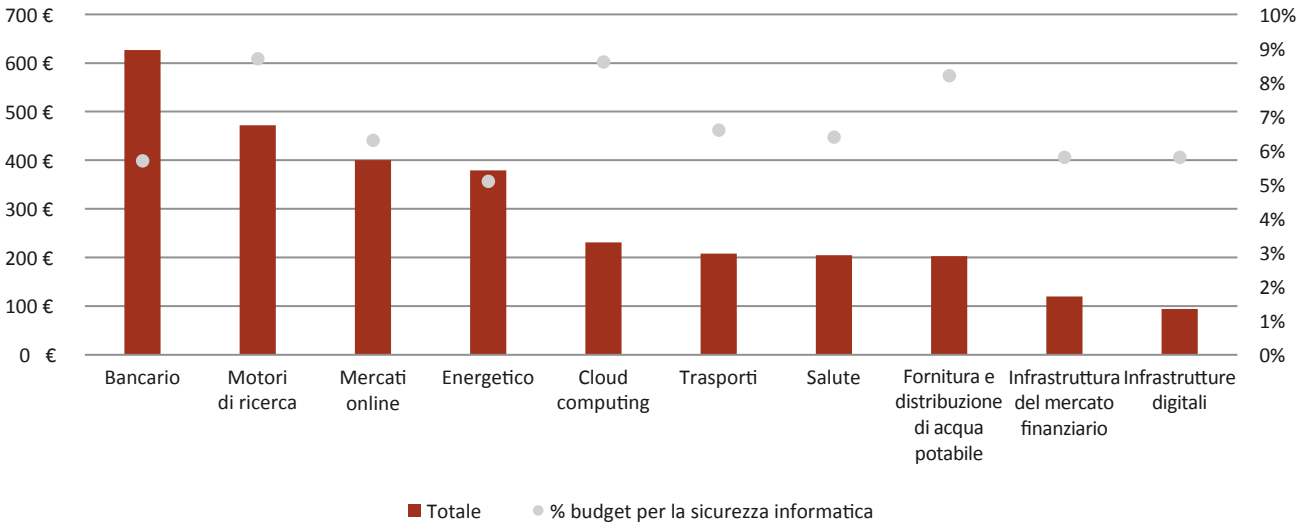
Fonte: ENISA, NIS Investments Report, novembre 2023



Valutando la formazione in cybersecurity per settore (Fig. 1.13), **nel 2022 quello più propenso a dedicarvi attenzione economica è stato il bancario che ha disposto mediamente €627 mila, corrispondenti al 5,7% del budget totale per la sicurezza informatica.** A seguire vi sono i motori di ricerca, con €472 mila, che costituiscono l'8,7% del budget in cybersecurity e i mercati online (€400 mila; 6,3% del budget). Anche in questo caso le infrastrutture del mercato finanziario e quelle digitali chiudono la classifica, avendo

Fig. 1.13: Budget per la formazione in cybersecurity (in € migliaia) degli OES/DSP per settore

Fonte: ENISA, NIS Investments Report, novembre 2023



messo a disposizione, in ordine, una media di soli €120 mila e €94 mila del proprio budget per la formazione necessaria a rendere le imprese del proprio settore pronte a gestire incidenti cyber. Queste somme, in entrambi i casi, corrispondono a una media del 5,8% delle risorse dedicate alla sicurezza informatica. Per comprendere il grado di maturità delle organizzazioni comunitarie in materia di rilevamento e risposta agli incidenti cibernetici (Fig. 1.14), l'ENISA – attraverso il rapporto NIS Investments – ha richiesto alle imprese appartenenti ai settori NIS di autovalutare le proprie competenze sul punto, dovendo riconoscersi in uno dei cinque livelli di maturità proposti: "Assente"; "Limitata"; "Basilare"; "Buona" e "Alta". Le risposte hanno permesso di comprendere che:

- Il 49% delle organizzazioni dichiara di avere capacità di rilevamento e risposta buone o alte;
- Solo il 18% afferma di avere capacità limitate o assenti;
- I settori che ritengono di essere in possesso di capacità elevate sono: il sanitario, il bancario, i trasporti e l'energetico, dove oltre il 50% delle organizzazioni ha scelto le opzioni buona o alta;
- I settori con le capacità di rilevamento e risposta ai cyberattacchi più limitate o nulle sono quello delle infrastrutture dei mercati finanziari (38%), i motori di ricerca online (35%) e le infrastrutture digitali (33%);
- A prevalere è un grado di maturità basilare, che coinvolge il 33% delle imprese, tra cui quello dei motori di ricerca (49%), del cloud computing e della fornitura di acqua potabile (47%).

Gli investimenti in cybersecurity sono inevitabilmente legati alle dimensioni delle singole organizzazioni; pertanto, per comprenderne la portata è necessario tener conto di questa peculiarità. Va innanzitutto evidenziato che nel settore dei motori di ricerca (Fig. 1.15) la percentuale più elevata è attribuita alle PMI, che sono l'86%, mentre le Grandi Imprese (GI) corrispondono al 14%. Le PMI primeggiano anche nelle infrastrutture digitali (64%), viceversa sono in carenza nel settore energetico e

Fig. 1.14: Maturità delle organizzazioni in materia di rilevamento e risposta agli incidenti

Fonte: ENISA, NIS Investments Report, novembre 2023

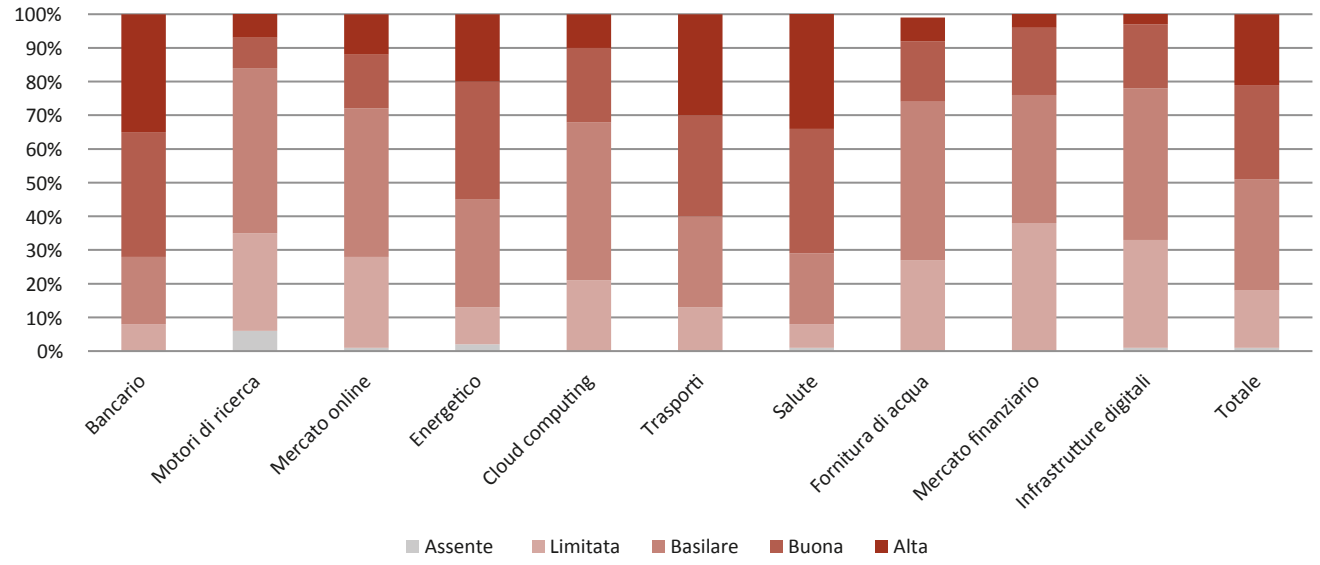
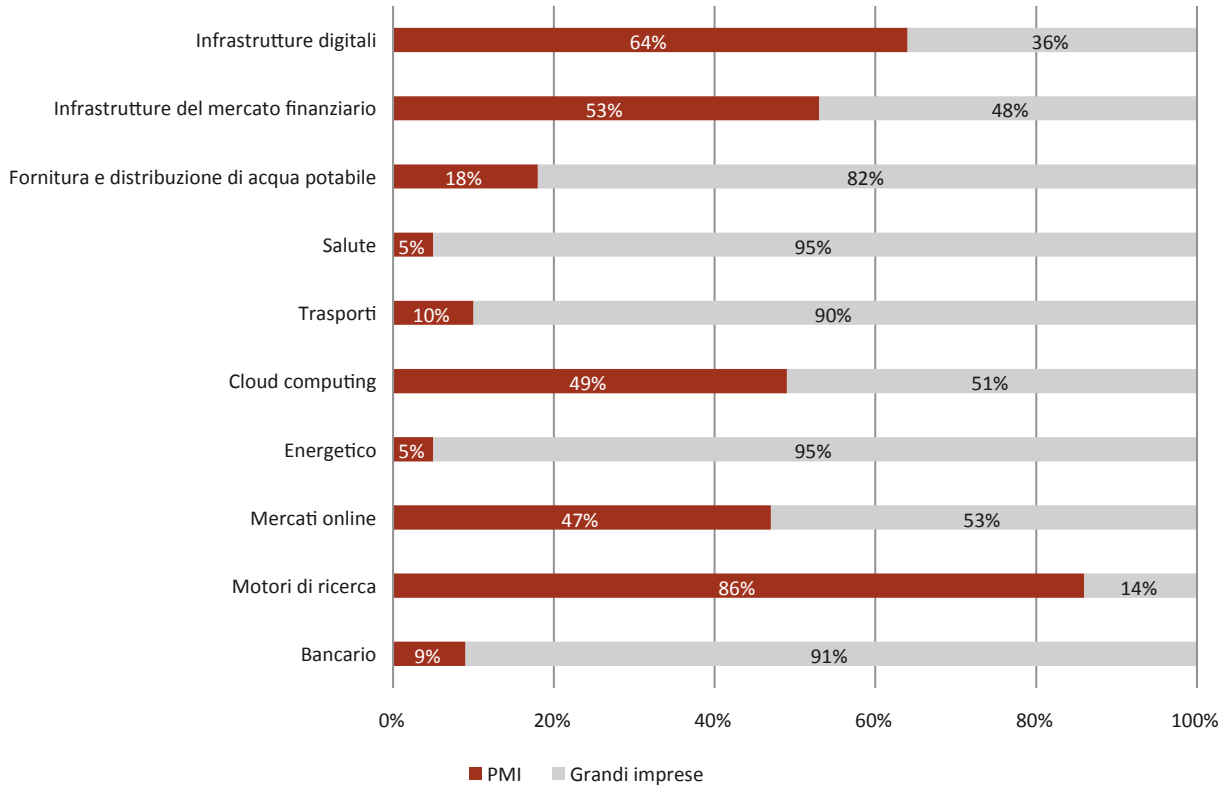


Fig. 1.15: Distribuzione delle PMI e delle grandi imprese, per settore NIS

Fonte: ENISA, NIS Investments Report, novembre 2023



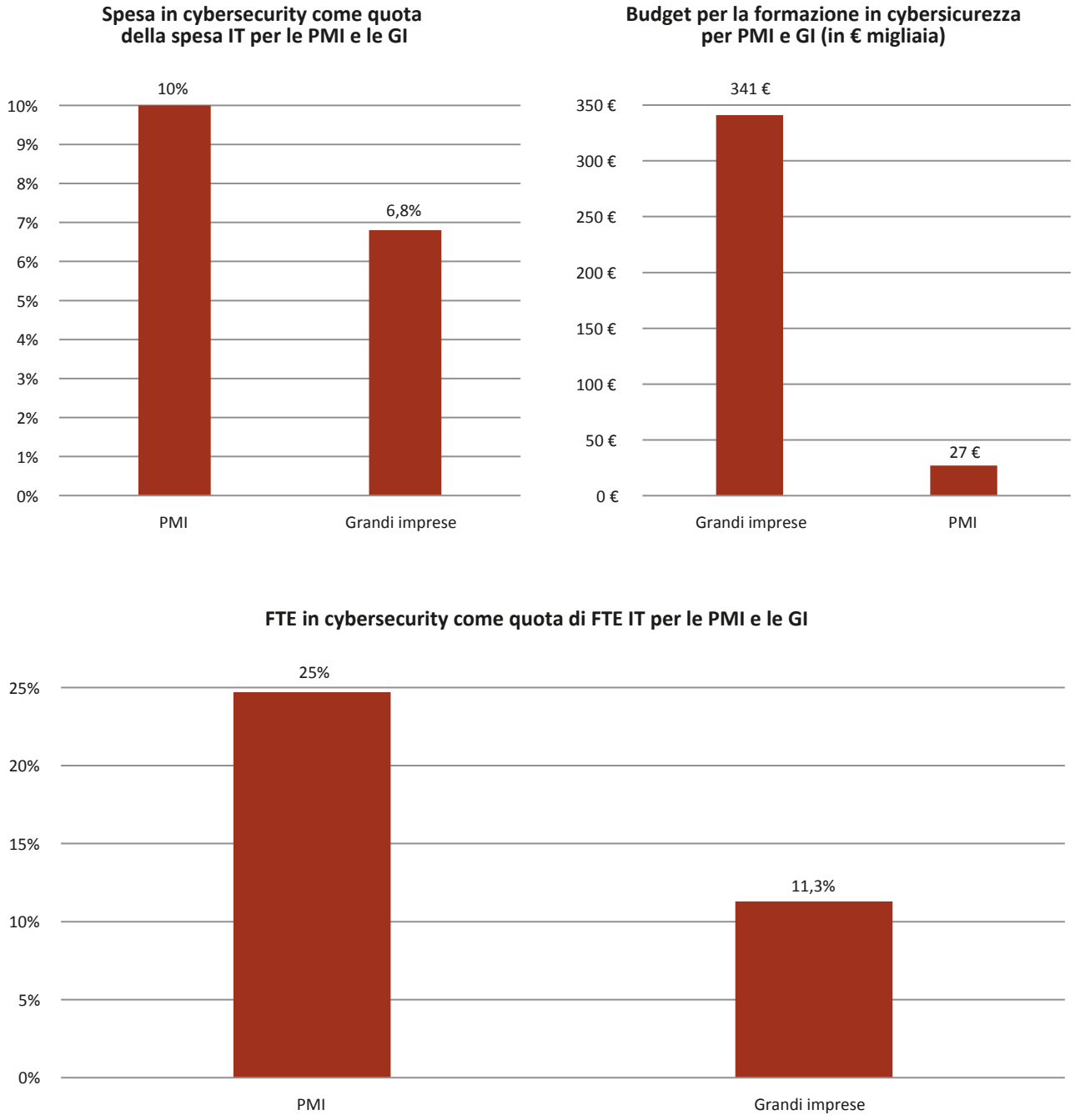
sanitario (dove si riscontra il 95% di GI), in quello bancario (91% GI) e dei trasporti (90% GI). Percentuali quasi alla pari sono individuate nelle infrastrutture del mercato finanziario (53% PMI e 48% GI), nell'ambito del cloud computing (51% GI e 49% PMI) e dei mercati online (53% GI, 47% PMI).

Pertanto, per comprendere che ruolo giocano nel panorama della cybersecurity le PMI e le grandi imprese, è possibile osservare (Fig. 1.16)[7] che la spesa in sicurezza informatica nelle prime costituisce il 10% della spesa IT, mentre nelle seconde il 6,8%. Il rapporto succitato specifica come la quota maggiore caratterizzante le PMI sia legata non alle dimensioni aziendali ma, piuttosto**, alla necessità che queste imprese hanno avuto nel 2022 di eseguire alcuni investimenti di base**. Tra essi, va menzionato quello inerente la formazione in cybersecurity del personale, che nelle grandi imprese ha visto impiegati €341 mila, ossia €114 mila in più rispetto alle PMI, che hanno riservato per tale prerogativa €27 mila del proprio budget interno. Infine, vi è un'importante differenza tra le due categorie di imprese anche in merito alla percentuale di FTE in cibersicurezza come quota del personale IT a tempo pieno. Questo indicatore è superiore nelle PMI (25%), mentre nelle grandi imprese raggiunge l'11,3%.

7 I valori fanno riferimento alla media.

Fig. 1.16: Investimenti in cybersecurity delle PMI e delle grandi imprese

Fonte: ENISA, NIS Investments Report, novembre 2023



icom
istituto per la competitività

CAPITOLO 2

L'ECOSISTEMA NORMATIVO SULLA CYBERSECURITY

2.1. L'APPROCCIO ALLA CYBERSECURITY. EU VS CINA E STATI UNITI

In un contesto socioeconomico sempre più incentrato sull'offerta di servizi digitali è irrinunciabile per gli Stati apprestare misure normative ed organizzative che siano in grado di far fronte ai rischi della digitalizzazione, predisponendo tutele efficaci per le risorse (umane, finanziarie e tecnologiche) a disposizione di enti pubblici e imprese da un lato, e per i diritti e le libertà fondamentali degli individui, dall'altro. In questo senso, al fine di salvaguardare opportunamente tutti gli interessi in gioco in ambito nazionale o – ancor di più – regionale ed affrontare in maniera adeguata e consapevole le sfide presenti e future del cyberspazio, risulta cruciale, in ottica di cyber-resilienza sistemica, la definizione di una strategia che individui in maniera chiara ed armonica le minacce e gli strumenti di prevenzione e contrasto (anche in termini di riduzione del relativo impatto).

L'Unione Europea si è mossa in tal senso a partire dal 2013, anno in cui si è dotata della prima strategia sulla *cybersecurity,* per poi proseguire con una serie di interventi normativi protesi a rendere l'ecosistema digitale quanto più sicuro possibile (come si dirà meglio *infra)*, in cui un ruolo centrale è affidato all'Agenzia dell'UE per la sicurezza informatica (ENISA).

Se si rivolge lo sguardo sul contesto globale, **nel mese di dicembre del 2016, anche la Cina ha pubblicato una propria strategia nazionale, nella quale è rinvenibile un riferimento interessante circa l'importanza del dominio cibernetico**, secondo cui esso costituirebbe un mezzo attraverso il quale promuovere la salvaguardia della pace mondiale e, al contempo, la sicurezza e gli interessi di sviluppo nazionale.

Ciò sarebbe realizzabile approfondendo la cooperazione con gli altri Paesi e riformando la governance globale di Internet. Più nel dettaglio, **la strategia cinese poggia su tre pilastri** fondamentali: I) **assicurare la sovranità dello Stato anche nel cyberspazio**, ricorrendo a qualsiasi mezzo – scientifico, tecnologico, legale, diplomatico o militare – necessario, sulla scorta del fatto che i Paesi dovrebbero avere un ruolo paritario nella governance del cyberspazio; II) **proteggere le infrastrutture informative critiche e i dati sensibili**, al fine di tutelare prodotti, servizi e imprese, soprattutto se correlate alla sicurezza nazionale, garantendo comunque un mercato trasparente e aperto alle aziende straniere; III) puntare sulla **cooperazione internazionale** tramite *policy*, leggi, tecnologie, standard e infrastrutture, coinvolgendo anche i paesi in via di sviluppo, in particolare quelli africani. Per quanto riguarda il lato più prettamente normativo, la cibersicurezza in Cina è regolamentata da tre atti principali: la ***Cybersecurity Law* (2017)**, che funge da legge generale per garantire gli obiettivi sopra menzionati, attraverso la definizione di regole per assicurare un'adeguata sicurezza delle reti e dei sistemi di trattamento dei dati; la ***Data Security Law* (2021)**, che si concentra sulla sicurezza nel trattamento di dati personali e non personali; la ***Personal Information Protection Law* (2021)**, in cui il focus è sulle regole per il trattamento dei soli dati personali. Queste tre leggi principali, essendo complementari tra di loro, saranno armonizzate nella *Regulations on Network Data Security Management*. Inoltre, vi sono normative settoriali e maggiormente specifiche, tra cui la *Cryptography Law* (2020) inerente l'utilizzo della crittografia per la tutela delle informazioni commerciali, l'*Internet Information Service Algorithmic Recommendation Management Provisions* (2022) – che ha lo scopo di promuovere il corretto utilizzo degli algoritmi da parte dei fornitori di servizi di informazione online – e il *National Cyber Incident Response Plan* (2017) concernente il miglioramento della risposta agli incidenti di *cybersecurity,* secondo un'ottica di prevenzione e riduzione del relativo impatto, e la protezione dell'interesse pubblico, della sicurezza nazionale e dell'ordine sociale.

Anche gli USA si sono attivati già da diverso tempo nella definizione di una propria strategia di cibersicurezza. In particolare, **gli Stati Uniti hanno puntato molto su una politica estera in ambito cyber, la quale – naturalmente – si è evoluta col tempo**. Infatti, se durante i primi anni dell'amministrazione Obama, si è tentato principalmente di tutelare un utilizzo di Internet che fosse quanto più aperto, gratuito e sicuro possibile, ricorrendo a limitate sanzioni e a iniziative diplomatiche volte a stabilire norme internazionali sul comportamento degli Stati nel cyberspazio, successivamente, con l'amministrazione Trump, si è cercato di attuare un approccio più attivo, nel senso di anticipare preventivamente le minacce cyber, penetrando i sistemi e le reti dell'avversario.

A marzo 2023, anche l'amministrazione Biden ha chiarito la strategia di cybersecurity[8] – il cui piano di implementazione è stato pubblicato a luglio 2023[9] – che guiderà gli USA per i prossimi anni e che appare focalizzata su cinque macro-obiettivi: I) **difendere le infrastrutture critiche**, in cui un ruolo cruciale viene affidato alla condivisione di informazioni tra le diverse agenzie federali competenti (sia civili che militari) e il settore privato; II) **contrastare gli attori delle minacce**, tramite il potenziamento delle attività di cyber-intelligence e di notifica delle vittime dei cyberattacchi, oltre che grazie all'aumento della collaborazione operativa tra pubblico e privato; III) **concepire la sicurezza come un vantaggio e non come un obbligo**, prevedendo – da un lato – forme di responsabilità in caso di insicurezza di software e servizi (ma non sui prodotti) e – dall'altro lato – incentivi federali e altre forme di investimento in cybersecurity; IV) **garantire una maggiore cyber-resilienza**, favorendo la ricerca in ambito cyber, implementando una strategia nazionale per rinforzare la forza lavoro specializzata e, inoltre, supportando lo sviluppo di un ecosistema di identità digitale; V) insistere sulla **cooperazione internazionale**, sia rinforzando la capacità di alleati e partner di contrastare le minacce nel dominio cibernetico, sia assicurando – soprattutto per i settori ICT – la cibersicurezza della *supply chain*.

Peraltro, lo scorso 30 ottobre il Presidente Biden ha adottato **l'*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, il quale accanto alla constatazione delle numerose opportunità offerte dai sistemi di IA, riconosce altresì i potenziali rischi connessi all'uso improprio di tali sistemi, con un focus dedicato anche alla cybersicurezza**. In particolare, viene posta l'attenzione sullo sviluppo di standard, strumenti e test per supportare la sicurezza e l'affidabilità dell'IA, che può essere sfruttata dagli attori malevoli e rappresentare una minaccia per le infrastrutture critiche anche dal punto di vista cibernetico. Altra priorità sul tema concerne la definizione di un programma avanzato di cibersicurezza per lo sviluppo di tecnologie di IA che possano rilevare e risolvere le vulnerabilità rinvenute in software e reti critiche.

Ad ogni modo, si possono individuare alcune normative – federali e statali – di primaria importanza, che si occupano di definire i requisiti di *cybersecurity*. Ad esempio – tra quelle federali – è opportuno menzionare: l'*Health Insurance Portability and Accountability Act* (**HIPAA – 1996**), che prescrive l'attuazione di misure di sicurezza per le informazioni personali di tipo sanitario; il ***Gramm-Leach-Bliley Act* (1999)**, concernente invece i dati trattati dalle istituzioni finanziarie; **l'*Homeland Security Act* (2002)**, che include il *Federal Information Security Management Act* (2002) inerente la cibersicurezza nelle agenzie federali (e relativi fornitori, con l'aggiornamento del 2014); il ***Cybersecurity Information Sharing Act* (2015)**, che contiene norme per garantire la protezione di quei soggetti che possono fornire informazioni utili al Governo sull'analisi delle minacce cibernetiche.

8 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
9 https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

Inoltre, **a marzo 2022 è stato approvato lo *Strengthening American Cybersecurity Act***, il quale prevede tre diversi disegni di legge che, fra l'altro, si occupano della segnalazione degli incidenti informatici e dell'avvenuto pagamento di *ransomware* da parte delle aziende considerate infrastrutture critiche, oltre che della sicurezza del *cloud*. Infine, un'ulteriore peculiarità del sistema statunitense può essere rintracciata nella governance della cybersecurity, dato che non vi è un'unica autorità (o agenzia governativa) a cui fare riferimento ma, in base alla normativa applicabile al caso di specie, sarà competente la *Federal Trade Commission* (FTC) oppure la *Securities and Exchange Commission* (SEC) o ancora la *Cybersecurity and Infrastructure Security Agency* (CISA).

2.2. L'EVOLUZIONE DEL FRAMEWORK EUROPEO SULLA CYBERSECURITY

2.2.1. Il Cybersecurity Package ed il nuovo scenario tracciato dalla NIS 2

Il 2020 rappresenta un anno particolarmente importante per le politiche europee 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)**.

Se la strategia, in particolare, ha declinato proposte concrete di iniziative politiche, di regolamentazione e di investimento per rafforzare resilienza, sovranità tecnologica e leadership, sviluppare capacità operative di prevenzione, dissuasione e risposta e promuovere un ciberspazio globale e aperto, all'esito di un ampio ed articolato dibattito, il 27 dicembre 2022 è stata pubblicata sulla G.U. 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 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 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 e un punto di contatto unico con funzioni di collegamento e obblighi di relazione alla Commissione, entro il **17 luglio 2028**, e successivamente ogni due anni, in merito alle notifiche ricevute e alle azioni intraprese.

Nella medesima data - **27 dicembre 2022** - è stata infine pubblicata la **Direttiva n. 2555/2022 (NIS2)**, entrata in vigore il 17 gennaio 2023 e da recepire entro il 17 ottobre 2024.

Tale direttiva, fa seguito all'adozione, nel 2016, della prima direttiva NIS[10] **(Direttiva NIS1)**, recepita in Italia con il d. lgs. n. 65/2018, tramite la quale l'Unione si è dotata per la prima volta di **misure organiche rivolte esplicitamente alla sicurezza delle informazioni e alla cybersicurezza**, prevedendo altresì un sistema di cooperazione tra Stati Membri grazie al **Gruppo di cooperazione NIS** e alla Rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (**rete CSIRT**).

Quanto all'ambito di applicazione, la Direttiva NIS1 individuava, in particolare, due categorie di soggetti: gli **operatori di servizi essenziali** (**OSE**)[11] e i ***digital service providers*** (**DSP**)[12]. Nell'implementazione di tale disciplina a livello nazionale, si è scelto di designare

10 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

11 Vi rientrano quei soggetti afferenti ad almeno uno dei seguenti settori: infrastrutture digitali, fornitura e distribuzione di acqua potabile, sanitario, bancario, infrastrutture di mercati finanziari, trasporti ed energia.

12 Vi rientrano le persone giuridiche con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale, che operino in almeno uno dei seguenti settori: cloud computing, motori di ricerca, e-commerce. In ogni caso, ai sensi del d. lgs. n. 65/2018, sono escluse le imprese di micro e piccole dimensioni (meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai €10 milioni).

molteplici **autorità competenti NIS**[13], sostanzialmente coincidenti con principali Ministeri, ognuno competente per i soggetti afferenti al proprio settore di riferimento, con il compito di valutare il rispetto da parte degli OSE degli **obblighi di sicurezza e di notifica** previsti dalla normativa ex art. 14, con il potere di richiedere tutte le informazioni necessarie a valutarne l'effettiva sicurezza – ricorrendo, eventualmente, ad **audit** e/o richiedendone la prova qualora siano stati compiuti da terze parti indipendenti – e, se del caso, di emanare **istruzioni vincolanti** per colmare le carenze individuate (art. 15).

Più nel dettaglio, l'art. 14 richiedeva di: i) adottare **misure tecniche e organizzative adeguate** e **proporzionate** alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi; ii) adottare **misure adeguate per prevenire e minimizzare l'impatto degli incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali; iii) **notificare**, senza indebito ritardo all'autorità competente o al **CSIRT**, gli incidenti aventi un impatto rilevante sulla continuità di tali servizi essenziali, tenuto conto del numero di utenti interessati, la durata e la diffusione geografica dell'incidente.

Peraltro, la NIS1 non ha previsto un meccanismo automatico di inclusione nel rispettivo ambito di applicazione per gli OSE, bensì ha rimandato agli Stati Membri – per il tramite del **punto di contatto unico** (in origine, per l'Italia, il **DIS – Dipartimento delle informazioni per la sicurezza**) – la loro individuazione mediante un'apposita comunicazione. Quanto ai DSP, oltre a quanto già previsto per gli OSE, si prescrive (art. 16) di adottare **misure tecniche e organizzative** adeguate rispetto al rischio inerente: a) la **sicurezza** di sistemi e impianti; b) il **trattamento degli incidenti**; c) la **gestione della continuità operativa**; d) il **monitoraggio, audit e test**; e) la conformità con **norme internazionali**. Inoltre, qualora un OSE abbia un DSP tra i suoi fornitori, con riferimento alla fornitura di un servizio indispensabile per le sue attività economiche e sociali fondamentali, allora è tenuto a notificare qualsiasi impatto rilevante per la continuità di tali servizi dovuto a un incidente a carico del DSP.

Ebbene, partendo da tale scenario, si è reso necessario adottare una versione aggiornata della precedente direttiva NIS per far fronte ad una serie di criticità applicative riscontrate negli oltre quattro anni di applicazione, tra cui: 1) **esclusione dall'ambito di applicazione** di settori che, già al tempo, erano caratterizzati da un buon livello in termini di digitalizzazione; 2) **inefficace supervisione** da parte delle autorità competenti circa una corretta attuazione delle disposizioni di legge; 3) **moltiplicazione delle misure di sicurezza** e degli **obblighi di reporting** predisposti dalle varie autorità competenti NIS, la cui compliance può divenire particolarmente gravosa, soprattutto per un'impresa con sedi in più SM; 4) la normativa è rimasta sostanzialmente **inapplicata** per i DSP in alcuni SM (Italia inclusa), in quanto essi non hanno mai ricevuto la notifica che – in effetti – non sarebbe prevista come nel caso degli OSE (si v. art. 18); 5) **condivisione limitata delle informazioni** tra gli Stati Membri.

Pertanto, la nuova direttiva NIS ha **ampliato l'ambito di applicazione soggettivo**, abbandonando la precedente distinzione tra OSE e DSP, in favore di una suddivisione tra **soggetti essenziali**[14] e

13 Attualmente, l'autorità competente è l'Agenzia per la Cybersicurezza Nazionale (ACN).

14 Settore energetico, trasporti, bancario e infrastrutture dei mercati finanziari, acqua potabile e acque reflue, infrastrutture digitali (fornitori di reti di distribuzione dei contenuti o fornitori di punti di interscambio internet, fornitori di DNS, ecc.), settore sanitario (laboratori, settore farmaceutico, ecc.), Pubblica amministrazione, Settore spaziale (operatori di infrastrutture terrestri possedute, gestite e operate dagli SM o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica).

soggetti importanti[15] (in cui rientrano anche le PMI), che ricomprende i soggetti originariamente inclusi nella NIS1 e le telecomunicazioni (precedentemente sottoposti a norme non dissimili dalla NIS1) ma che si estende anche ai soggetti pubblici che rientrano in una delle due categorie succitate. Più nel dettaglio, salvo le eccezioni previste dall'art. 2 di cui si dirà a breve, sono escluse quelle imprese che prestino i loro servizi o svolgano le loro attività all'interno dell'Unione e che congiuntamente non occupino più di 250 persone e abbiano un fatturato annuo non superiore a **€50 milioni** (o, in alternativa, un totale di bilancio annuo non superiore a **€43 milioni**).

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 – CER**[16].

Sono espressamente **esclusi** dall'ambito di applicazione della NIS2 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. Peraltro, agli SM è riconosciuta la facoltà di prevedere che la direttiva si applichi a enti della PA a livello locale e a istituti di istruzione, in particolare qualora questi ultimi svolgano attività di ricerca critiche. Ad ogni modo, spetterà comunque agli Stati membri stilare, entro il **17 aprile 2025**, anche attraverso le informazioni fornite dai soggetti interessati, un elenco dei soggetti essenziali e importanti, da aggiornarsi almeno ogni due anni.

Fermo restando l'apporto del legislatore italiano in fase di attuazione, è comunque possibile delineare i principali obblighi alla base della NIS2, in particolare:

1. **Adozione di misure tecniche, organizzative e operative adeguate e proporzionate** (art. 21), finalizzate alla tutela multirischio dei sistemi informatici e della rete e all'attenuazione dell'impatto in caso di incidenti, che comprendano almeno: 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

15 Settore dei servizi postali e di corriere, gestione dei rifiuti, fabbricazione/produzione/distribuzione di sostanze chimiche, produzione/trasformazione/distribuzione di alimenti ivi comprese le imprese della grande distribuzione, Organizzazioni di ricerca, Servizi di fabbricazione di: (i) dispositivi medici e di dispositivi medico-diagnostici in vitro, (ii) computer e prodotti di elettronica e ottica, (iii) apparecchiature elettriche, (iv) macchinari e apparecchiature n.c.a., (v) autoveicoli, rimorchi e semirimorchi, (vi) altri mezzi di trasporto, fornitori di servizi digitali (mercati online, motori di ricerca e piattaforme di servizi di social network).

16 Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio.

di emergenza protetti da parte del soggetto al proprio interno, se del caso;

2. **Obblighi di segnalazione in caso di "incidenti significativi"** (art. 23), ossia quegli eventi in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato ovvero di avere ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. In presenza di tali condizioni, i soggetti interessati devono trasmettere al proprio ***Computer Security Incident Response Team*** *(CSIRT)* o – se opportuno – alla propria autorità competente[17]: un **preallarme** senza indebito ritardo ed entro il termine di **24 ore** dalla conoscenza dell'incidente significativo (cioè da quando l'evento è stato effettivamente qualificato come tale); una **notifica** entro il termine di **72 ore** dalla conoscenza dell'incidente significativo, che aggiorni – se necessario – le informazioni del preallarme; un **report** intermedio se richiesto dall'autorità competente o dallo CSIRT; una **relazione finale** entro **un mese** dalla trasmissione della notifica, che includa l'analisi dell'incidente e la descrizione delle misure di mitigazione adottate, oppure – nel caso in cui l'incidente sia ancora in corso in tale occasione – **una relazione sui progressi** e una **relazione finale entro un mese** dall'avvenuta gestione dell'incidente;
3. **Sottoposizione a misure di vigilanza** (artt. 32-33) – in misura differente in base alla categoria a cui afferisce il soggetto obbligato (**essenziale o importante**) – tra cui ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati; audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente; scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato. Invece, per quanto concerne il quadro sanzionatorio (art. 34 ss.), la violazione delle misure di gestione dei rischi di *cybersecurity* o degli obblighi di segnalazione potrà arrivare a un massimo di **€10 milioni** (ridotti a €7 milioni 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;
4. **Adozione di misure per garantire la sicurezza della supply chain** da parte dei soggetti obbligati al rispetto della normativa in questione, con specifico riferimento al monitoraggio dei propri fornitori – anche a livello di governance – tramite verifiche costanti e puntuali che potranno interessare la qualità complessiva dei prodotti, le pratiche di cybersicurezza dei suoi diretti fornitori o fornitori di servizi (incluse le procedure di sviluppo sicuro), al fine di tenere conto delle relative vulnerabilità nelle attività di ***cyber risk management***.

Dal punto di vista operativo, la NIS2 (art. 16) mira a istituire la **Rete Europea dell'Organizzazione di Collegamento per le Crisi Informatiche (*Eu–CyClone*)**, che favorirà la gestione coordinata degli incidenti di sicurezza informatica su larga scala. Per di più, l'art. 19 introduce un importante meccanismo volontario di revisione tra pari – tramite l'ausilio di esperti di cibersicurezza (designati da almeno due SM, diversi dal Paese oggetto di revisione) – con l'obiettivo di trarre insegnamenti dalle esperienze

17 In tema di giurisdizione e territorialità (art. 26), la NIS2 riconosce la competenza all'autorità dello SM in cui il soggetto pubblico o privato è stabilito, salvo alcune eccezioni: in caso di servizi di rete elettronica, essi sono soggetti alla giurisdizione del Paese in cui si trovano i destinatari dei servizi, mentre i servizi online si affidano alla giurisdizione del Paese nel quale ha sede lo stabilimento principale.

condivise dell'UE, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cybersicurezza e migliorare le capacità e le politiche in cybersecurity degli SM.
Avendo sin qui delineato i passaggi più rilevanti delle direttive NIS1 e NIS2, la tabella che segue (Tab. 2.1) riassume e confronta le principali disposizioni ivi contenute, sia a carico dei soggetti rientranti nell'ambito di applicazione delle stesse, sia indirizzate agli Stati Membri e alle diverse entità nazionali ed eurounitarie coinvolte a vario titolo nella materia della cybersicurezza.

Tab. 2.1: Confronto tra le principali disposizioni delle direttive NIS1 e NIS2

Fonte: Dir. (UE) n. 1148/2016 – NIS1; Dir. (UE) n. 2555/2022 – NIS2

	DIRETTIVA NIS1 (2016)	**DIRETTIVA NIS2 (2022)**
Gestione del rischio	Nessun riferimento specifico	Organi di gestione dei soggetti essenziali e importanti chiamati ad approvare le misure di gestione dei rischi di cybersecurity e a supervisionarne l'attuazione (art. 20)
Requisiti di sicurezza	Adozione di misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi	Adozione di misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete, con indicazione delle misure "minime" da adottare (art. 21) e utilizzo dei sistemi europei di certificazione della cibersicurezza (art. 24)
Sicurezza della supply chain	Nessun riferimento	Valutazione delle vulnerabilità specifiche per ogni diretto fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza comprese le procedure di sviluppo sicuro (art. 22)
Segnalazione degli incidenti	Notifica senza indebito ritardo degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati (art. 14) o sulla fornitura di un servizio offerto nell'Unione (art. 16)	Notifica incidenti significativi scandita secondo diverse finestre temporali: da preallarme entro 24 ore, notifica entro 72 ore, report intermedio e report finale
Monitoraggio, gestione e risposta agli incidenti	Creare uno o più CSIRT in ogni SM dotati di risorse adeguate a svolgere efficacemente i compiti assegnati (art. 9). Essi compongono la rete CSIRT a livello UE (art. 12)	In aggiunta, i CSIRT possono stabilire relazioni di cooperazione con gli omologhi di paesi terzi e prendono parte al nuovo meccanismo di divulgazione coordinata delle vulnerabilità, che alimenta l'apposita banca dati europea tenuta dall'ENISA (art. 12)
Gestione delle crisi informatiche	Nessun riferimento	Ogni SM designa o istituisce una o più autorità di gestione delle crisi informatiche e adotta un piano nazionale per la risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, da presentare alla Commissione e alla neo-istituita EU-CyCLONe (artt. 9-16)
Enforcement	Designazione o istituzione autorità competenti e punto di contatto unico con risorse adeguate ai compiti, con la specifica di collaborare con le autorità competenti negli altri SM, il gruppo di cooperazione e la rete CSIRT (art. 8)	Designazione o istituzione autorità competenti e punto di contatto unico con risorse adeguate ai compiti, con l'ulteriore specifica di collaborare con l'ENISA e la Commissione (art. 8), nonché con gli organismi e le autorità previsti da altri atti dell'Unione (art. 12)
Revisione tra pari	Nessun riferimento	Introduzione del meccanismo volontario di revisione tra pari, condotto da esperti in cibersicurezza, per trarre insegnamenti dalle esperienze condivise dell'UE (art. 19)

2.2.1.1. I primi chiarimenti applicativi sulla direttiva NIS2

Il **14 settembre 2023** la Commissione europea ha pubblicato, con qualche mese di ritardo ("entro il 17 luglio 2023"), i **primi orientamenti** sull'applicazione di alcune norme fondamentali della Direttiva NIS2, ossia l'art. 4 (paragrafi 1 e 2)[18] e l'art. 3, paragrafo 4[19]. Quest'ultima norma, che ha una minore rilevanza per i soggetti ricompresi nell'ambito di applicazione della direttiva in esame, concerne la compilazione da parte degli Stati Membri di un elenco dei soggetti essenziali ed importanti, nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. In sostanza, gli orientamenti sul tema pubblicati dalla Commissione forniscono un modello utile agli SM per le informazioni da richiedere ai soggetti di cui sopra.

D'altro canto, invece, gli orientamenti chiariscono aspetti maggiormente significativi per coloro che saranno obbligati a adeguarsi alla NIS2, poiché riguardano il **raccordo con le attuali e future regolamentazioni settoriali circa le misure di gestione dei rischi di cybersicurezza e la segnalazione degli incidenti**, nell'ottica di armonizzare e semplificare gli adempimenti per le imprese. Difatti, ai sensi dell'art. 4 (paragrafi 1 e 2) della direttiva NIS2, è prevista la disapplicazione degli artt. 21 e 23 della stessa direttiva qualora un soggetto essenziale o importante sia già tenuto a adottare misure di gestione dei rischi e/o a notificare incidenti significativi in ottemperanza ad altri atti giuridici settoriali dell'Unione (allo stato attuale, solo il Regolamento DORA[20]), nella misura in cui gli effetti di tali obblighi siano "**almeno equivalenti**" a quelli di cui alla presente direttiva, escludendosi, di conseguenza, anche le disposizioni in materia di vigilanza ed esecuzione.

Più nel dettaglio, con riguardo alle misure di gestione dei rischi di cybersicurezza (art. 21), gli orientamenti della Commissione chiariscono che il soggetto sarà esentato dalla disposizione in oggetto unicamente quando abbia già implementato misure tecniche, operative e organizzative adeguate e proporzionate a gestire i rischi posti alla sicurezza dei sistemi informativi e di rete, le quali garantiscano anche la **prevenzione** o comunque la **riduzione al minimo dell'impatto** degli incidenti su tutte le operazioni e i servizi del soggetto interessato, quindi non solo alle risorse informatiche specifiche o a servizi critici forniti dallo stesso. Nel valutare l'equivalenza di tali obblighi, viene sottolineato dalla Commissione come le misure già adottate debbano tendere a un **approccio multirischio**, quale è richiesto dalla NIS2, e pertanto occuparsi anche della sicurezza fisica e dell'ambiente in cui questi sistemi si trovano, proteggendoli da guasti, errori umani, azioni malevoli o fenomeni naturali di vario genere.

Con riferimento, invece, agli **obblighi di segnalazione** degli incidenti (art. 23), l'equivalenza può sussistere quando l'altro atto giuridico settoriale preveda: a) **la notifica degli incidenti significativi**, secondo il medesimo significato attribuito nella direttiva NIS2; b) un approccio scandito in almeno tre momenti, ossia **preallarme**, **notifica** dell'incidente e **relazione finale**; c) il **contenuto minimo della segnalazione**, che consenta allo CSIRT di valutare adeguatamente l'incidente, nonché l'aggiornamento delle informazioni trasmesse; d) **l'accesso immediato allo CSIRT** alle notifiche trasmesse, anche tramite meccanismi di segnalazione automatica e diretta.

18 Orientamenti della Commissione sull'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva (UE) 2022/2555 (direttiva NIS2) – C(2023) 6068 final.

19 Orientamenti della Commissione sull'applicazione dell'articolo 3, paragrafo 4, della direttiva (UE) 2022/2555 (direttiva NIS2) – C(2023) 6070 final.

20 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

Ulteriore chiarimento di rilievo concerne le norme relative agli **organi di gestione dei soggetti essenziali e importanti** (art. 20), in quanto queste ultime sono strettamente collegate alle misure di gestione dei rischi di cui all'art. 21. Pertanto, nell'ipotesi in cui trovi applicazione un atto giuridico settoriale dell'Unione ai sensi dell'art. 4 della NIS2, non dovranno applicarsi nemmeno gli obblighi di gestione dei rischi di cibersicurezza di cui al citato art. 20 della stessa direttiva.
In definitiva, attraverso tali orientamenti, la Commissione ha inteso regolare non solo i rapporti tra la NIS2 e gli attuali atti giuridici settoriali dell'UE, bensì anche con le **future regolamentazioni eurounitarie** che trattino il vasto tema della cybersicurezza, cercando in tal modo di occuparsi preventivamente di **eventuali sovrapposizioni**, perseguendo così il fine ultimo di mitigare il più possibile l'impatto sulle attività di compliance dei soggetti che ne saranno obbligati.

2.2.2. Il Cybersecurity Act e le modifiche proposte

Se la direttiva NIS, oggi superata dalla NIS2, 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 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 cybersecurity 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 cibersicurezza. 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 NIS2). 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 nonchè 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 Regolamento prescrive, a livello organizzativo, la designazione, da parte degli Stati membri, di una o più autorità nazionali di certificazione della cybersecurity nel proprio territorio oppure, con l'accordo di un altro Stato membro, la designazione di una o più autorità nazionali di certificazione della cybersecurity stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante. 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. Se questo è il quadro generale introdotto dal regolamento, va annoverato che la Commissione ha lanciato una **proposta di regolamento** che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti. Tale proposta, in particolare, partendo dalla constatazione dell'importanza dei fornitori di servizi di sicurezza gestiti - considerati soggetti essenziali o importanti appartenenti a un settore ad alta criticità ai sensi della NIS2 - in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza,

nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi e della necessità, dunque, che soggetti essenziali e importanti esercitino una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti, ha introdotto importanti modifiche al regolamento. A tal fine, la modifica proposta punta a consentire, mediante atti di esecuzione della Commissione, l'adozione di **sistemi europei di certificazione della cibersicurezza per i "servizi di sicurezza gestiti", oltre ai prodotti della tecnologia e dell'informazione (TIC), ai servizi TIC e ai processi TIC, che già rientrano nelle prescrizioni della legge sulla sicurezza informatica**. I sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti, in particolare, sono progettati per conseguire una serie minima di obiettivi che riguardano la competenza, l'esperienza e l'integrità del personale responsabile della prestazione di tali servizi, il possesso di procedure interne idonee ad assicurare una qualità molto elevata del servizio ed un'adeguata tutela dei dati raccolti, trattati e conservati anche attraverso il rapido ripristino in caso di incidenti fisici o tecnici, la gestione di una politica di accesso ai dati rigorosa che assicuri l'accesso esclusivamente ai dati cui si ha diritto di accedere e che tenga traccia degli accessi e delle finalità perseguite e la garanzia che i prodotti TIC, i servizi TIC e i processi TIC avviati nella fornitura dei servizi di sicurezza gestiti siano sicuri fin dalla progettazione e per impostazione predefinita, non contengano vulnerabilità note e includano gli ultimi aggiornamenti connessi alla sicurezza. La Commissione è chiamata a **valutare periodicamente** - la prima volta entro dicembre 2023 e successivamente almeno ogni due anni - l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza. Specifici obblighi di cooperazione sono posti a carico delle autorità nazionali di certificazione tra loro e rispetto alla Commissione europea. La **Commissione per l'industria, la ricerca e l'energia** ha adottato una relazione nella quale il Parlamento viene sollecitato ad inserire una serie di modifiche al testo proposto nella logica di valutare i percorsi formativi esistenti, individuare l'attuale gap di competenze, formulare un elenco di proposte per affrontare le necessità dei lavoratori qualificati e prevedere specifiche forme di sostegno per le microimprese e le PMI. Viene inoltre suggerito di prevedere che entro il 28 giugno 2024, e successivamente ogni tre anni, la Commissione valuti l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue pratiche di lavoro, l'eventuale necessità di modificare il mandato dell'ENISA e le implicazioni finanziarie di tali modifiche. Tale valutazione dovrebbe concentrarsi su: a) **l'efficienza e l'efficacia delle procedure** che portano alla consultazione, alla preparazione e all'adozione dei sistemi europei di certificazione della cibersicurezza, nonché le modalità per migliorare e accelerare tali procedure; b) l'**eventuale necessità di individuare requisiti essenziali di cibersicurezza** per l'accesso al mercato interno al fine di impedire l'ingresso nel mercato dell'Unione di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che non soddisfano i requisiti fondamentali di cibersicurezza.

2.2.3. Il Cyber Resilience Act (CRA). Dalla proposta della Commissione allo stato della procedura

Sempre in attuazione di quanto previsto nella Strategia lanciata nel 2020 e partendo dalla constatazione della necessità, per assicurare un ecosistema europeo complessivamente sicuro, di garantire che i dispositivi utilizzati da cittadini, imprese e pubbliche amministrazioni rispondano a standard di sicurezza adeguati, il **15 settembre 2022** la Commissione 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.

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, nello specifico, 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. **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 inoltre 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 dall'analisi della proposta è la definizione di un articolato set di obblighi tesi a creare, di fatto, una catena di verifica e controllo reciproco molto robusta tra produttori, importatori e distributori.

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.

Sulla proposta della Commissione, Parlamento e Consiglio hanno raggiunto un **accordo provvisorio sul testo il 30 novembre scorso**. Il testo concordato, in particolare, pur mantenendo l'impianto generale proposto dalla Commissione che tuttavia aveva già subito diverse modifiche nel corso dell'*iter*, introduce una metodologia più semplice per la classificazione dei prodotti digitali, fissa in almeno 5 anni il periodo di sostegno per un prodotto digitale (esclusi i prodotti di cui sia previsto un periodo di utilizzo più breve), fissa obblighi di segnalazione relativi alle vulnerabilità attivamente sfruttate e agli incidenti innanzitutto nei confronti delle autorità nazionali competenti anche se è rafforzato il ruolo dell'ENISA, introduce ulteriori misure di sostegno per le piccole imprese e microimprese, comprese specifiche attività di sensibilizzazione e formazione, nonché il sostegno alle procedure di prova e di valutazione della conformità. Quanto al periodo di applicazione delle norme, nella logica di prevedere per i fabbricanti tempistiche di adeguamento idonee, esso è fissato in tre anni dall'entrata in vigore del regolamento.

2.2.4. Assicurare la resilienza operativa digitale del settore finanziario: il Digital Operational Resilience Act (DORA)

Con l'ambizioso obiettivo di rafforzare e armonizzare a livello europeo i principali requisiti di *cybersecurity* per le società finanziarie, tra cui banche, compagnie di assicurazione, società di servizi di criptovalute, istituzioni finanziarie e i loro fornitori critici, il 17 gennaio 2023 è entrato in vigore – ma si applicherà dal 17 gennaio 2025 – il **Reg. n. 2554/2022 (DORA)**. Quanto all'ambito di applicazione, esso **si rivolge a un'ampia varietà di entità finanziarie**, non soltanto di stampo tradizionale come banche, assicurazioni e imprese di investimento ma anche nuovi attori, tra cui, fornitori di servizi per le cripto-attività e fornitori di servizi ICT (es: fornitori di servizi cloud), nonché i fornitori critici di servizi per le aziende che sono obbligate al rispetto del presente regolamento.

Per quanto concerne gli adempimenti prescritti alle imprese, essi possono essere suddivisi in sei pilastri:

1. **Governance e organizzazione interna** (art. 5): le entità finanziarie dovranno dotarsi di un quadro organizzativo e procedurale per garantire una gestione efficace e prudente di tutti i rischi informatici, nell'ambito del quale la responsabilità finale viene riconosciuta ad un apposito Organo di gestione dell'entità finanziaria. Quest'ultimo avrà un ruolo fondamentale nell'attribuire responsabilità e ruoli per tutte le funzioni ICT, controllare e monitorare la gestione dei rispettivi rischi e, infine, allocare adeguatamente investimenti e formazione specialistica;
2. **Gestione dei rischi ICT** (artt. 6-16), che si traduce nella predisposizione di un ICT *Risk Management Framework* adeguatamente documentato e periodicamente aggiornato (almeno una volta l'anno), soprattutto in occasione di "gravi incidenti ICT" o a seguito di processi di audit (interni e/o esterni) o indicazioni e conclusioni delle competenti autorità europee di vigilanza (AEV)[21]. Tale quadro è funzionale all'istituzione e al mantenimento di strumenti e sistemi ICT resilienti (compresi quelli *legacy)* durante ogni fase del loro ciclo di vita con una visione *end-to-end* dei processi, attraverso: a) l'identificazione e la mappatura dei rispettivi rischi, nonché il rilevamento di minacce, con particolare attenzione sui quei processi dipendenti da fornitori di servizi ICT; b) la predisposizione di misure di protezione e prevenzione, nella forma di policy, procedure e prassi; c) l'implementazione di strategie di *business continuity* e piani di ripristino in caso di disastro *disaster recovery*; d) l'analisi da effettuarsi a seguito di un "incidente ICT", al fine di comprendere le cause della violazione e valutare un eventuale riesame delle misure di protezione e prevenzione; e) la gestione della comunicazione;
3. **Gestione degli incidenti e *reporting*** (artt. 17-23), che si sostanzia nell'attuazione di processi di monitoraggio, registrazione e classificazione degli incidenti connessi alle tecnologie ICT in base alla loro priorità, gravità e criticità dei servizi colpiti, al fine di notificarli alle autorità competenti. Su quest'ultimo punto, il DORA disciplina la segnalazione di incidenti gravi, prevedendo modalità e tempistiche differenziate (notifica inziale, relazione intermedia e relazione finale). Inoltre, le entità finanziarie possono, su base volontaria, notificare le "minacce informatiche significative" all'autorità competente qualora ritengano che siano rilevanti per il sistema finanziario, gli utenti dei servizi o i clienti;
4. **Test di resilienza operativa digitale** (artt. 24-27), ossia un vero e proprio sistema funzionale a identificare punti deboli, carenze e lacune della resilienza operativa digitale e conseguentemente attuare – in maniera tempestiva – misure correttive;
5. **Gestione dei fornitori terzi di servizi ICT** (artt. 28-44) a cui è dedicata una parte corposa di norme all'interno del Regolamento, in virtù del fatto che il rapporto con i fornitori ed eventuali subfornitori è un aspetto cruciale. In sostanza, si richiede – da un lato – l'identificazione, la classificazione e la documentazione di tutti i processi dipendenti da fornitori terzi di servizi legati alle tecnologie ICT e – dall'altro – l'imposizione di obblighi contrattuali, da riesaminare periodicamente, per tutte le fasi

21 L'art. 16 introduce una serie di semplificazioni per quelle imprese esentate dagli obblighi rafforzati, senza escludere l'implementazione di misure base di mappatura e gestione del rischio ICT.

chiave del contratto (stipula, esecuzione, estinzione, post-contrattuale), al fine di garantire un adeguato monitoraggio delle attività svolte, nonché la possibilità di svolgere verifiche documentali, *audit* e ispezioni da parte dell'operatore finanziario;

6. **Condivisione delle informazioni** (art. 45), tramite l'istituzione di un programma denominato comunità fidate di entità finanziarie – su base volontaria e tramite protocolli di *information sharing* – che consenta agli attori finanziari di prevedere accordi per lo scambio reciproco di informazioni sulle minacce informatiche (***cyber threat intelligence***), con lo scopo di rafforzare la cooperazione tra gli Stati Membri e cercare di sopperire alla mancanza di comunicazione tra le varie entità del settore finanziario all'interno dell'UE.

In ultimo, va evidenziato che le entità finanziarie soggette al Regolamento DORA fanno capo a tre diverse **autorità europee di vigilanza (EBA, EIOPA ed ESMA)** – ciascuna competente per una o più categorie di soggetti – che, fra l'altro, **si occupano della normativa tecnica di dettaglio** che, a seguito dell'adozione da parte della Commissione europea, integra a tutti gli effetti quanto previsto dal presente regolamento. Ebbene, il 19 giugno 2023 è stata avviata la consultazione pubblica per il primo set di queste norme, la cui versione definitiva è stata emanata lo scorso 17 gennaio[22]. In particolare, questo primo pacchetto contiene gli standard tecnici in merito al quadro di gestione del rischio ICT, la classificazione degli incidenti, le policy sui servizi ICT che supportano funzioni critiche o importanti, nonché il registro delle informazioni. Inoltre, lo scorso 8 dicembre è stata avviata la consultazione sul secondo set di norme tecniche, che proseguirà fino al prossimo 4 marzo[23].

2.3. L'ECOSISTEMA NORMATIVO NAZIONALE SULLA CYBERSECURITY

2.3.1. L'ACN ed il nuovo modello di governance cyber. Gli obiettivi della strategia e del piano di implementazione

Considerati i maggiori rischi derivanti dall'estensione dei confini del dominio cibernetico, il **Piano nazionale di ripresa e resilienza** (PNRR), ha dedicato specifica attenzione alla cibersicurezza che figura tra i 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 successivo, 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

22 https://www.eiopa.europa.eu/publications/set-rules-under-dora-ict-and-third-party-risk-management-and-incident-classification_en
23 https://www.esma.europa.eu/press-news/esma-news/esas-launch-joint-consultation-second-batch-policy-mandates-under-digital

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 che ha visto la luce 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). Si tratta dell'inizio di una nuova era per la cybersicurezza a livello nazionale, una nuova fase che vede attribuire ad un unico soggetto la grandissima parte delle competenze in materia e definitivamente superare la precedente frammentazione di competenze che tanta complessità ed incertezza aveva creato.

Il D.L. in questione, infatti, 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 cybersicurezza 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 cybersicurezza**, ad assicurare, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, il **coordinamento tra i soggetti pubblici coinvolti** in materia di cybersicurezza a livello nazionale, 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 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.

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 cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Il Comitato, in particolare, è chiamato a proporre al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di

cybersicurezza nazionale, esercitare l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza, promuovere l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza ed infine esprimere il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza. nazionale.

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

Alla stessa ACN sono attribuite importantissime funzioni anche rispetto all'***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) i cui componenti - attualmente in fase di nomina - 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), competente a 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**.

Nell'esercizio delle proprie funzioni, il 25 maggio 2022 l'ACN ha lanciato la **strategia nazionale di cybersicurezza 2022-2026 ed il relativo piano di implementazione.** 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 cybersicurezza 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 cybersicurezza 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 macrotemi 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 cybersicurezza 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 cybersicurezza, 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 cybersicurezza, 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.

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.

2.3.2. Il recepimento della direttiva NIS2 in Italia

L'apporto del legislatore nazionale nel recepimento della direttiva NIS2 – da finalizzarsi, si ricorda, entro il 17 ottobre 2024 – potrà essere più o meno ampio, in considerazione del fatto che per certi versi l'ordinamento giuridico italiano è già ben strutturato con riguardo alla materia della cybersicurezza (si pensi

alla disciplina sul Perimetro di Sicurezza Nazionale Cibernetica, che si richiamerà in seguito). A parte questo, molto dipenderà dall'attenzione che le istituzioni, col supporto imprescindibile degli stakeholders, porranno sulla discussione del decreto di attuazione, in particolare per cogliere le peculiarità dell'ecosistema Paese, il quale è fortemente contraddistinto da piccole e medie imprese anche nell'ambito cibersicurezza.
Ripercorrendo brevemente le tappe a livello nazionale, lo scorso 27 luglio è stato presentato alla Camera il **disegno di legge recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023"** (Atto Camera 1342), che all'art. 3 si occupa specificamente dei principi e dei criteri per l'esercizio della delega per il recepimento della direttiva NIS2. **Il ddl è stato assegnato, naturalmente, alla XIV Commissione Politiche UE in sede referente lo scorso 5 settembre** e il 20 dicembre è stato approvato dalla Camera. Il disegno di legge è attualmente al vaglio del Senato.
Entrando nello specifico, il testo approvato dalla Camera fissa i principi e criteri direttivi che il Governo, sentita l'ACN, è chiamato ad osservare nell'esercizio della delega, affidando innanzitutto al **decreto legislativo di attuazione l'individuazione dei criteri in base** ai quali un ente pubblico possa essere considerato pubblica amministrazione ai fini dell'applicazione della direttiva NIS2, prevedendo – secondo principi di gradualità, proporzionalità e adeguatezza – di ricomprendere comunque anche i comuni e le province, oltre agli enti dell'amministrazione centrale e regionale (lett. a). Sono da escludere, invece, dall'ambito di applicazione delle disposizioni della NIS2 gli enti della PA indicati dall'art. 2.7 della direttiva stessa, ossia quelli che svolgono 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, ivi compresi gli organismi di informazione per la sicurezza ai quali si applica la **legge n. 124/2007**. In terzo luogo (lett. c), viene precisato che l'Italia si intende avvalere della facoltà prevista dall'art. 2.8 della direttiva, che consente di esentare alcuni soggetti specifici che svolgono le loro attività nei settori appena menzionati o che forniscono servizi esclusivamente agli enti della PA. Ciò dovrà avvenire con o uno più DPCM, adottati su proposta delle Amministrazioni competenti per settore.
Senza alcuna sorpresa, il testo (lett. d) conferma la distinzione già presente nel **d. lgs. n. 65/2018** di attuazione della NIS1 (come modificato dal **d.l. 82/2021**) tra l'ACN, in qualità di autorità nazionale competente e punto di contatto unico, e le Amministrazioni di settore operanti negli ambiti delineati dalla direttiva. **Viene inoltre confermata la presenza dello CSIRT Italia** all'interno dell'ACN (lett. e), con l'ulteriore precisazione di prevedere una più ampia collaborazione tra tutte le strutture pubbliche coinvolte in eventi malevoli legati alla sicurezza informatica (ossia i CERT – Computer Emergency Response Team), in attuazione dell'art. 10 della direttiva. Di assoluta rilevanza (lett. f), la previsione per cui vada **definito un regime transitorio per i soggetti già sottoposti alla disciplina di recepimento della NIS1**, al fine di consentire un agevole passaggio al nuovo impianto normativo, per cui in Commissione è stato esplicitato di garantire termini congrui di adeguamento per tali soggetti. Di assoluta rilevanza (lett. f), la previsione per cui vada definito un **regime transitorio per i soggetti già sottoposti alla disciplina di recepimento della NIS1**, al fine di consentire un agevole passaggio al nuovo impianto normativo, per cui in Commissione è stato esplicitato di garantire termini congrui di adeguamento per tali soggetti. Inoltre (lett. g), viene evidenziata la **necessità di dotarsi di meccanismi ad hoc per la registrazione dei soggetti essenziali e importanti** – e a tal fine certamente saranno di supporto gli orientamenti della Commissione europea descritti supra – comprendendo altresì quelli che gestiscono servizi connessi o strumentali alle attività oggetto delle disposizioni

della direttiva, con specifico riferimento al settore della cultura, così come emendato in sede referente. A seguito dell'esame in Commissione è stata introdotto il principio (lett. h) per cui dovrà essere **individuata un'autorità amministrativa responsabile per l'identificazione delle tecnologie necessarie ad assicurare l'effettiva attivazione delle misure di gestione dei rischi di cybersicurezza**, indicate all'art. 21 della NIS2. Peraltro, tale autorità curerà anche l'aggiornamento degli strumenti adottati, di pari passo con lo sviluppo tecnologico. Altro aspetto rilevante (lett. i) concerne la **modifica della legislazione vigente**, anche in materia penale, per consentire il recepimento a livello nazionale del nuovo meccanismo di divulgazione coordinata delle vulnerabilità, che rivede un ruolo centrale in capo agli CSIRT e all'ENISA, secondo quanto stabilito dall'art. 12 della direttiva. Il ddl in esame si preoccupa anche della **differenziazione delle competenze tra l'AgID e l'ACN** (lett. l), dato che la NIS2 impatta parzialmente anche sulle attività previste dal Reg. UE n. 910/2014 (meglio noto come eIDAS, che peraltro è attualmente in corso di approvazione nella sua versione 2.0). Si prevede inoltre (lett. m) di **individuare criteri oggettivi e proporzionati per garantire gli obblighi informativi nei confronti dei destinatari dei servizi erogati dai soggetti essenziali e importanti**, i quali si rendono necessari nel momento in cui tali destinatari siano potenzialmente interessati da una minaccia informatica significativa. La ratio è quella di consentire tempestivamente l'adozione di qualsiasi misura o azione correttiva in risposta a tale minaccia. Proseguendo nell'analisi dei principi e dei criteri direttivi, la lett. n) prescrive di **rivedere il sistema sanzionatorio, nonché quello di vigilanza ed esecuzione previsto dal decreto di attuazione della prima direttiva NIS**, disponendo in particolare di introdurre sanzioni che siano effettive, proporzionate e dissuasive rispetto alla gravità degli obblighi violati, richiamando altresì strumenti deflattivi del contenzioso e confermando che gli introiti derivanti dall'irrogazione delle sanzioni siano versati dapprima nel bilancio dello Stato per poi essere assegnati al MEF, che a sua volta incrementerà la dotazione del bilancio dell'ACN. Dato che la direttiva NIS2 costituisce uno dei (principali) tasselli della nuova legislazione eurounitaria in ambito cybersecurity, la lett. o) chiarisce che dovrà essere oggetto del decreto di attuazione anche il **coordinamento con le disposizioni relative alla direttiva CER, al regolamento DORA e alla direttiva n. 2556/2022** in materia di servizi finanziari, oltre che con riguardo alle disposizioni emanate in attuazione dell'articolo sin qui esaminato.

Posto che l'iter parlamentare è ancora in corso è opportuno, in una logica sistematica, svolgere qualche riflessione in merito a quanto già stabilito nell'ambito della disciplina sul Perimetro di Sicurezza Nazionale Cibernetica (PSNC), ovviamente tenendo in debita considerazione le dovute differenze, prima fra tutte la natura dei due framework normativi.

Difatti, **la direttiva NIS2 si focalizza sull'assicurare la continuità operativa dei soggetti essenziali e importanti**, mentre **il PSNC pone la sua attenzione su aspetti maggiormente legati alla sicurezza nazionale**. Per di più, **il complesso puzzle normativo del PSNC ruota attorno all'elenco di beni ICT che viene comunicato (e aggiornato) dai soggetti perimetro all'ACN**, sostanziandosi in un approccio più puntuale, che si interessa prettamente di quelle reti, sistemi informativi e servizi informatici connessi all'erogazione di un servizio essenziale o da cui dipende una funzione essenziale dello Stato; diversamente, come specificato anche nei recenti orientamenti della Commissione europea, **le misure di gestione dei rischi di cybersicurezza richieste ai soggetti essenziali e importanti debbono prevenire o comunque ridurre al minimo l'impatto degli incidenti su tutte le operazioni e i servizi del soggetto interessato**. Altra differenza rilevante è **il numero dei soggetti che sono ricompresi nelle due normative a livello nazionale**, ossia poche centinaia per il PSNC

e in ordine di migliaia per la NIS2 – con una quota elevata di PMI – essendo quest'ultima estesa a molti più settori rispetto alla prima.
Nonostante questi innegabili punti di divergenza, è evidente che attraverso la disciplina del perimetro molti degli obiettivi fissati dalla NIS2 sono centrati ed è dunque auspicabile che si faccia tesoro dell'esperienza applicativa di questi anni, anche per evitare sovrapposizioni di adempimenti, in particolar modo per quegli operatori che saranno obbligati al rispetto di entrambe le discipline. Ad esempio, **si può immaginare che le misure di sicurezza di natura tecnica e organizzativa delineate nell'allegato B del DPCM 14 aprile 2021, n. 81 siano quantomeno prese in considerazione per delineare nel dettaglio i requisiti di sicurezza a norma dell'art. 21 della direttiva NIS2**.
Nonostante questi innegabili punti di divergenza, è possibile immaginare che si cercherà di fare tesoro dell'esperienza applicativa di questi anni, anche per evitare sovrapposizioni di adempimenti, in particolar modo per quegli operatori che saranno obbligati al rispetto di entrambe le discipline.
Seguendo il medesimo ragionamento, le categorie di incidenti richiamate nell'allegato A del DPCM summenzionato, così come pure nella Determina del Direttore Generale dell'ACN del 3 gennaio 2023, recante "**Tassonomia degli incidenti che debbono essere oggetto di notifica",** potrebbero essere di notevole supporto nella specificazione degli "incidenti significativi" da notificare a norma dell'art. 23 della NIS2, soprattutto a favore delle imprese non incluse nel PSNC, bensì rientranti in uno dei nuovi settori della direttiva. Altro punto di contatto tra i due corpus normativi si rivede nella responsabilizzazione degli organi di gestione dei soggetti essenziali e importanti, similmente a quanto previsto per i soggetti perimetro.
È indispensabile, infatti, che le aziende italiane, già alle prese con un quadro economico intricato, possano avere certezze e tempi definiti per l'implementazione di normative che puntano - o quantomeno dovrebbero puntare - a semplificare e migliorare la sicurezza informatica.
In tale contesto, certificazioni, conformità, test continui e monitoraggio sono elementi fondamentali di questo processo, che deve essere garantito attraverso una cooperazione efficace tra le aziende che gestiscono sistemi Ict e reti.
Gli standard di sicurezza condivisi diventano cruciali per garantire la resilienza di apparati, reti e sistemi complessi. L'adozione di standard internazionali rappresenta sicuramente un importante passo avanti, garantendo cooperazione tra gli stakeholder, prevenendo rischi di interoperabilità e promuovendo competizione e innovazione tecnologica.
Nell'immaginare il futuro ecosistema normativo che sarà delineato a valle del recepimento della NIS2, sarà certamente importante l'adozione di una metodologia unica EU-CC che possa raccogliere importanti input relativi ad un efficientamento della metodologia di test finalmente comune in Europa ed applicabile agli asset strategici che possa traguardare una corretta e tempestiva gestione della variabilità delle versioni SW, la riusabilità delle certificazioni ed un tempo definito di esecuzione dei test ed un appropriato management delle vulnerabilità.

2.3.3. Il recepimento della direttiva CER in Italia

Nella medesima legge di delegazione europea all'esame del Senato, l'art. 5 definisce princìpi e criteri direttivi specifici per l'esercizio della delega per il recepimento della **direttiva CER** (2022/2557). Innanzitutto, questi prevedono l'**esclusione dall'ambito di applicazione** delle disposizioni di recepimento della direttiva, degli **enti della PA** 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, gli **Organismi di informazione per la sicurezza**, ai quali

si applicano le disposizioni di cui alla legge 3 agosto 2007, n. 124[24]. A ciò si aggiunge la possibilità di escludere anche specifici **soggetti critici** operanti nei suddetti settori o che forniscano servizi esclusivamente ai succitati enti della pubblica amministrazione, rimettendone l'individuazione a uno o più **decreti del Presidente del Consiglio dei ministri**, su proposta delle competenti Amministrazioni.

In relazione agli undici settori disciplinati dalla direttiva, si richiede di istituire o designare una o più **autorità competenti** ovvero, in caso di istituzione o designazione di un'unica autorità competente, un **punto di contatto unico** che garantisca la cooperazione transfrontaliera con i punti di contatto unici di altri Stati membri e con il gruppo per la resilienza dei soggetti critici. I princìpi direttivi prevedono anche **misure** atte a conseguire, ove necessario, un livello di **resilienza** più elevato per i soggetti critici del **settore bancario**, del settore delle **infrastrutture dei mercati finanziari** e di quelle **digitali**; **sanzioni penali e amministrative efficaci**, **proporzionate** e **dissuasive**, nonché **strumenti deflattivi** del contenzioso, tra cui la **diffida ad adempiere**. Altro principio di rilievo è quello che prescrive di assicurare il coordinamento delle disposizioni recanti il recepimento della direttiva CER con quelle di recepimento della **direttiva NIS2**, con il **regolamento DORA** e con le **disposizioni nazionali di adeguamento ad esso**. In ultimo, si richiede di **tutelare le attribuzioni** dell'**autorità giudiziaria** relativamente alla ricezione delle notizie di reato, del **Ministero dell'interno** in materia di garanzia dell'ordine e della sicurezza pubblica e di difesa civile, del **Ministero della difesa** in materia di difesa e sicurezza dello Stato, del **Dipartimento della Protezione civile** in materia di previsione, prevenzione e mitigazione dei rischi, del **Ministero delle imprese e del made in Italy** in materia di resilienza fisica delle reti di comunicazione elettronica, nonché dell'**ACN** in materia di cybersicurezza e resilienza nazionale nello spazio cibernetico, istituendo un **tavolo di coordinamento** tra il punto di contatto unico e la Commissione interministeriale tecnica di difesa civile in relazione alla formulazione e attuazione degli obiettivi di resilienza nazionale; e di favorire la **tutela dei lavoratori** che svolgono **attività critiche** o **sensibili**, anche prevedendo disposizioni speciali in tema.

2.3.4. Il Perimetro di Sicurezza Nazionale 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 (PSNC)** 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 e 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

24 Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto.

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** e ha declinato i **criteri con i quali i soggetti inclusi nel perimetro predispongono** (entro sei mesi dall'avvenuta inclusione nel Perimetro) **e aggiornano** (con cadenza almeno annuale) il c.d. **"elenco di beni ICT" di rispettiva pertinenza**, indicando le reti, i sistemi informativi e i servizi informatici di rispettiva pertinenza (comprensivo della relativa architettura e componentistica). Pertanto, tale decreto pone le basi normative per il PSNC da un punto di vista tecnologico, per cui i successivi decreti faranno riferimento, in merito agli obblighi prescritti, prettamente a tale elenco;

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[25]. Su quest'ultimo punto, il DPCM scinde gli adempimenti in due momenti: a) entro sei mesi dalla data di trasmissione dell'elenco di beni ICT, con riguardo alle misure di cui alla categoria A, appendice 2,

25 Le misure di sicurezza, ricomprese nell'allegato B del presente DPCM, riguardano i seguenti aspetti: 1) le politiche di sicurezza, la struttura organizzativa e la gestione del rischio; 2) la mitigazione e gestione degli incidenti, nonché la loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza; 3) la protezione fisica, logica e dei dati; 4) l'integrità delle reti e dei sistemi informativi; 5) la gestione operativa, ivi compresa la continuità del servizio; 6) il monitoraggio, i test e le procedure di controllo; 7) la formazione e la consapevolezza; 8) l'affidamento di forniture di beni, sistemi e servizi ICT, anche mediante definizione di caratteristiche e requisiti di carattere generale.

allegato B[26]; b) entro trenta mesi dalla stessa data, con riferimento all'adozione delle misure previste dalla categoria B, appendice 2, allegato B[27]. Tale distinzione temporale dipende da una maggiore complessità delle misure di sicurezza ricomprese nella categoria B. Inoltre, il decreto prevede un aggiornamento con cadenza almeno biennale delle stesse misure;

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 e 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

26 Ad esempio: a) censire i sistemi e gli apparati fisici dell'organizzazione; b) identificare i flussi di dati e comunicazioni inerenti l'organizzazione; c) definire e rendere noti i ruoli e le responsabilità inerenti la cybersecurity per tutto il personale e le terze parti rilevanti; d) identificare e rendere nota una policy di cybersecurity; e) identificare e documentare le vulnerabilità delle risorse, tra cui sistemi, locali e dispositivi dell'organizzazione; f) tenere conto delle minacce, delle vulnerabilità, nonché delle relative probabilità e conseguenti impatti derivanti dal loro sfruttamento nell'analisi del rischio.

27 A titolo esemplificativo: i) censire le piattaforme e le applicazioni software in uso nell'organizzazione; ii) identificare e prioritizzare le risposte al rischio; iii) identificare, prioritizzare e valutare i fornitori e i partner terzi di sistemi informatici, componenti e servizi utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber; iv) utilizzare i contratti con i fornitori e i partner terzi per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del piano di gestione del rischio della catena di approvvigionamento cyber.

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 privata 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 Italia 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[28].

Con **provvedimento del Direttore Generale dell'ACN**, **l'11 agosto 2022** sono state approvate le determinazioni tecniche previste dal Regolamento in materia di accreditamento dei laboratori di prova, fissando per le varie **aree di accreditamento** (Allegato 4), **i requisiti tecnici e logistici, le misure di sicurezza fisica[29],**

28 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.

29 Ad esempio: distruggi documenti, contenitori di sicurezza, sistema di allarme antiintrusione, di videosorveglianza e di controllo accessi.

procedurale[30] **e tecnica**[31] **per i LAP** (Allegato 1), **i requisiti di competenza ed esperienza per l'accreditamento dei LAP**, ivi comprese le modalità di redazione del curriculum professionale da presentare nella domanda di accreditamento (Allegato 2), nonché la **procedura di notifica delle limitazioni di operatività superiori a 24 ore e di comunicazione e raccordo tra il CVCN e i LAP**. Attualmente, è prevista un'unica area di accreditamento (**"*Software e network*"**), mentre i livelli di severità delegabili ai LAP sono basso, medio/basso e medio/alto (ossia dal mero *password cracking* sino a ***vulnerability assessment*** **e** ***penetration test*** con potenziale di attacco sino a ***enhanced-basic***). Inoltre, i LAP possono testare la maggior parte dei componenti di cui al DPCM 15 giugno 2021 sopra richiamato, ad eccezione di quelli inerenti la tecnologia 5G, all'IoT e all'***automotive***, oltre che con riferimento ai sistemi di intelligenza artificiale (ivi incluso il *machine learning*) funzionali alla gestione di reti e sistemi informatici.

È dunque giunto a completamento il complesso puzzle normativo sul Perimetro di Sicurezza Nazionale Cibernetica e 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, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro) dalle Amministrazioni competenti nei rispettivi settori, sono tenuti a **predisporre e aggiornare 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 Italia attivo presso la Presidenza del Consiglio. Tali soggetti, inoltre, sono tenuti – dal **30 giugno 2022** – a **comunicare al CVCN l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici"** (contenuti nell'elenco di beni ICT) e rientranti nelle categorie sopra descritte (DPCM 15 giugno 2021). A seguito di questa comunicazione (correlata da apposita documentazione)[32], prende inizio il **procedimento di verifica e valutazione dinanzi al CVCN, che si suddivide in tre macro fasi**, puntualmente descritte dal DPR n. 54/2021: i) **verifiche preliminari** (art. 5); ii) **preparazione all'esecuzione dei test** (art. 6); iii) **esecuzione dei test di hardware e software** (art. 7).

Più nel dettaglio, **la prima fase** si incentra sull'analisi della documentazione prodotta dal soggetto perimetro interessato, al fine di comprendere se il bene, il servizio o il sistema ICT che intende acquistare è ricompreso in una delle categorie di cui al DPCM 15 giugno 2021 e, inoltre, se lo stesso deve essere implementato su uno dei beni ICT presenti all'interno dell'elenco comunicato all'ACN. Tale fase deve concludersi entro **45 gg** dall'invio della comunicazione al CVCN, prorogabili un'unica volta per ulteriori **15 gg** in casi di "particolari

30 Tra cui: divieto di attività di test da remoto, inventario dei dispositivi, utilizzo e dismissione sicuri di supporti di memorizzazione, verifica aggiornamenti software, blocco e chiusura sessione.

31 Ad esempio: procedure di autenticazione multifattoriale e identificazione degli utenti in maniera univoca, configurazione di una scadenza sessione, predisposizione di diversi profili di autorizzazione, separazione della rete del laboratorio dall'esterno, audit dei sistemi operativi, strumenti per l'analisi degli eventi, prevenzione dei malware, aggiornamento dei sistemi, specifici requisiti per l'accesso al sistema operativo o a software applicativo, cifratura del disco.

32 La documentazione contenuta nella comunicazione di affidamento riguarda alcuni elementi inerenti l'oggetto della valutazione, tra cui: la sua descrizione generale; il relativo impiego, ovvero la destinazione d'uso; la rispettiva categoria di appartenenza; le informazioni e i servizi che deve trattare e le correlate modalità di gestione. Inoltre, è prevista l'allegazione di un documento di analisi del rischio dell'oggetto, considerato nel suo ambiente di impiego, nonché dei livelli di severità determinati sulla base di appositi modelli predisposti dal CVCN.

complessità"[33]. Decorso il termine stabilito, il silenzio del CVCN è da interpretarsi come assenso, per cui il soggetto perimetro può procedere con la procedura di affidamento. Ad ogni modo, la prima fase si conclude con l'individuazione del/i test da eseguire, nonché la definizione delle eventuali ed ulteriori condizioni e indicazioni, che possono riguardare anche il fornitore, attraverso l'imposizione di clausole che possono – sospensivamente o risolutivamente – condizionare il contratto al rispetto di tali condizioni e all'esito favorevole dei test. Ne deriva che si tratta di un passaggio cruciale per la programmazione delle attività di *procurement* del soggetto perimetro e del business del fornitore dell'oggetto da testare.

La seconda fase prevede che il fornitore interessato, la cui individuazione univoca deve essere resa possibile dal soggetto perimetro, metta a disposizione del CVCN l'oggetto della valutazione, il quale fissa data e sede di esecuzione dei test. Va sottolineato che tale fase è eventuale (art. 6), in quanto se il componente è stato già sottoposto a precedenti valutazioni, oppure queste siano già in corso, non si procederà con lo svolgimento del test. La terza ed ultima fase concerne l'esecuzione dei test presso i laboratori del CVCN, dei CV e i LAP, ovvero da parte del loro personale presso il fornitore o il soggetto perimetro interessato. Il termine previsto è di 60 gg dalla comunicazione di conclusione delle attività preparatorie. Il procedimento termina con l'elaborazione di un rapporto finale da parte del CVCN, che viene comunicato al soggetto perimetro e al fornitore interessati entro il suddetto termine, potendosi prospettare le seguenti soluzioni alternative: 1) si può **procedere all'acquisto e all'implementazione del componente valutato all'interno dell'elenco dei beni ICT senza alcun adempimento ulteriore**; 2) si può **procedere all'acquisto, ma è imposto al soggetto perimetro, al fornitore o a entrambi, il rispetto di determinate prescrizioni di sicurezza**; 3) viene attivata l'apposita **procedura per l'esercizio dei poteri speciali** di cui all'art. 1-*bis*, d. l. n. 21/2021 (**Golden Power**), qualora venga valutata la presenza di fattori di vulnerabilità che potrebbe compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano; 4) **non si può procedere all'acquisto**, in quanto sussistono motivi ostativi, i quali vanno comunicati al soggetto perimetro e al fornitore.

Va evidenziato come tale procedimento non conduca a una certificazione di prodotto, processo o servizio, come invece accade per le certificazioni volontarie di cybersicurezza a norma del **Cybersecurity Act (Reg. UE n. 881/2019)**. Infatti, **il componente hardware o software su cui vengono eseguiti i test non viene preso in considerazione principalmente per le sue caratteristiche intrinseche, ma è analizzato per l'utilizzo in uno specifico ambiente operativo**. Di conseguenza, nulla vieta che lo stesso possa essere valutato presso un altro soggetto o in un diverso contesto, purché non si applichi una delle ipotesi di esclusione già menzionate con riferimento all'**art. 6 del DPR n. 54/2021**. Quindi, pare potersi affermare che il quadro sin qui delineato può assumere un ruolo di primaria importanza per l'efficienza e l'efficacia di una data organizzazione, in particolare per quei soggetti inclusi nel PSNC che riscontrino la necessità di acquistare urgentemente tecnologie e servizi indispensabili per il prosieguo delle rispettive attività di impresa, nel momento in cui queste risultano connesse – direttamente o indirettamente – con la funzione o il servizio essenziali per cui sono stati inclusi nel Perimetro.

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

33 L'art. 4, co. 4, DPR n. 54/2021 riconosce la "particolare complessità" quando il componente da valutare: 1) sia costituito da beni, sistemi e servizi ICT integrati tra loro; 2) sia basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di test consolidate; 3) interagisce con ulteriori componenti che erogano altre funzioni o servizi essenziali.

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. Peraltro, sono 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. Infine, tra tali indicazioni rileva anche la possibilità di acquistare in urgenza, essendovi un vuoto normativo in tal senso, per cui il CVCN potrà effettuare controlli ex post sull'effettiva sussistenza di tale impellenza.

2.3.5. L'evoluzione della disciplina sul Golden Power

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.

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 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 un 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. 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 (c.d. 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 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.

Una novità rilevante per quanto concerne **l'ambito di applicazione della disciplina GP**, è stata introdotta con il **d. l. n. 104/2023 (c.d. Decreto Asset)**[34] che ha disposto, con l'art. 7, co. 1, la modifica dell'art. 2, co. 1-ter, aggiungendovi il seguente secondo periodo: "*Quando gli atti, le operazioni e le delibere hanno ad oggetto attivi coperti da diritti di proprietà intellettuale afferenti l'intelligenza artificiale, i macchinari per la produzione di semiconduttori, la cibersicurezza, le tecnologie aerospaziali, di stoccaggio dell'energia, quantistica e nucleare, e sono disposti a beneficio di imprese collocate fuori dall'Unione europea, l'esercizio dei poteri speciali è consentito anche all'interno del medesimo gruppo, fermo restando il ricorrere del pericolo e dei pregiudizi di cui al primo periodo*". Pertanto, **la novella autorizza l'applicazione del golden power a tecnologie particolarmente critiche, inclusi l'IA, la cybersecurity e i macchinari per la produzione di chip**.

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, 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 sono passate da **342 a 608 in soli due anni** (2020-2022). 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/

34 D. l. 10 agosto 2023, n. 104, recante "Disposizioni urgenti a tutela degli utenti, in materia di attività economiche e finanziarie e investimenti strategici".

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 anche tenendo conto delle segnalazioni degli enti territoriali ai fini del 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.

2.3.5.1. Esercizio dei poteri speciali e andamento delle notifiche

Risulta confermata la tendenza incrementale delle **notifiche ai sensi del decreto-legge 21/2012**[35].

35 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 2022, Camera dei Deputati, presentata dal Sottosegretario di Stato alla Presidenza del Consiglio dei ministri Mantovano e trasmessa alla Presidenza il 30 giugno 2023.

Fig. 2.1: 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 (2022)

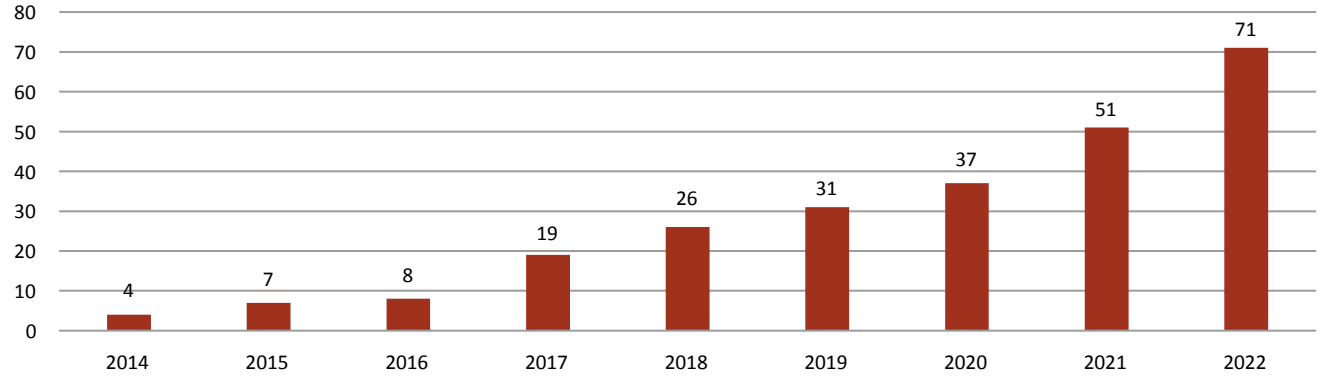
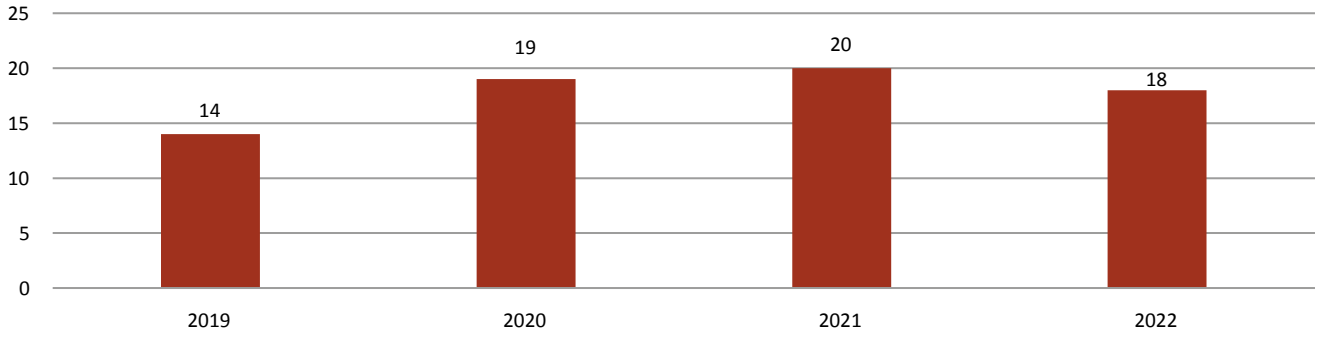


Fig. 2.2: Tecnologia 5G: il trend delle notifiche

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 (2022)



Infatti, **nel 2022 il numero totale di informative presentate è pari a 608**, in aumento di circa il **23%** rispetto all'anno precedente. Il trend è decisamente crescente per i settori difesa e sicurezza nazionale (art. 1, d. l. n. 21/2012), così come per energia, trasporti, comunicazioni e nuovi settori del Regolamento (UE) 2019/452 (art. 2), mentre è in lieve diminuzione per la tecnologia 5G (art. 1-*bis*)

Per quanto riguarda il comparto difesa e sicurezza nazionale, nel 2022 le notifiche pervenute sono 71, in crescita di circa il 39% rispetto all'anno precedente (Fig. 2.1).

In merito alla **tecnologia 5G**, le notifiche ai sensi dell'art. 1-*bis* hanno iniziato ad essere presentate dal 2019. Nel 2022, il loro numero è pari a **18**, in discesa di due unità rispetto all'anno precedente (Fig. 2.2).

Infine, rispetto alle altre macrocategorie, si evidenzia un incremento significativamente maggiore delle notifiche pervenute ai sensi dell'art. 2, dovuto principalmente all'ampliamento di tale categoria, la quale

comprende, ora, anche i settori indicati nel Reg. (UE) 2019/452**. Nel 2022, le notifiche in tale comparto rappresentano circa l'85% del totale**, superando di oltre sette volte il settore difesa e sicurezza nazionale e registrando una crescita del 22% rispetto al 2021 e di oltre l'81% rispetto al 2020 (Fig. 2.3).
Nel 2022, la maggior parte delle notifiche (**218 su 608**) è stata assegnata al **Ministero delle imprese e del made in Italy** (MIMIT), coerentemente con la progressiva estensione dell'ambito di applicazione della disciplina sul golden power nei settori ricompresi nell'art. 2. Si può osservare anche un notevole coinvolgimento del MEF e del **Ministero della Salute**, rispettivamente con **119 e 112** operazioni di istruttoria curate (Fig. 2.4).

Fig. 2.3: 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 (2022)

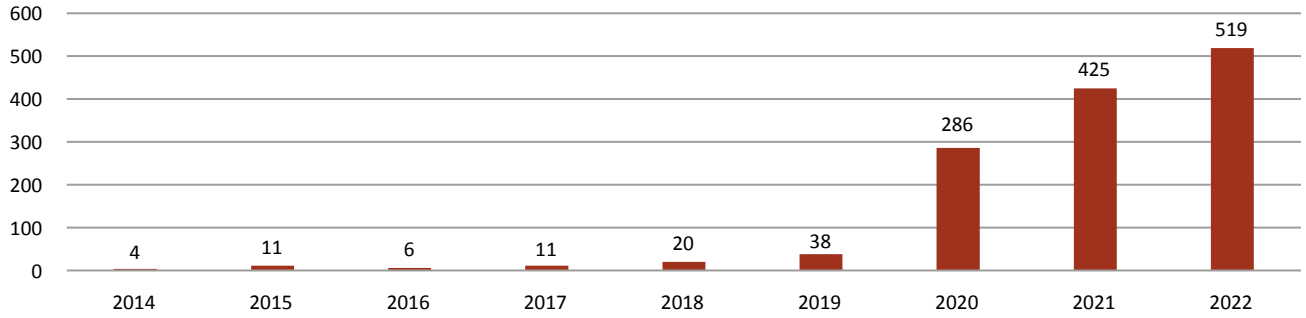
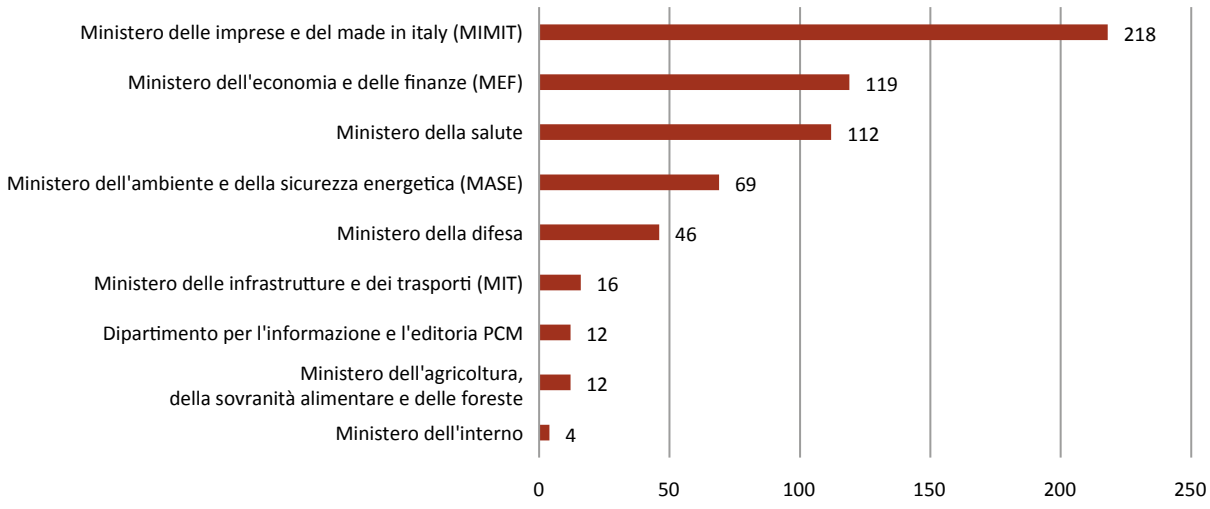


Fig. 2.4: La responsabilità istruttoria delle notifiche (2022)

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 (2022)



All'esito dell'istruttoria, delle **608 notifiche pervenute nel corso del 2022**, per 21 di esse sono stati esercitati i poteri speciali (Fig. 2.5). In particolare (Fig. 2.6):

Fig. 2.5: Esercizio e non esercizio dei poteri speciali (2022)

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 (2022)

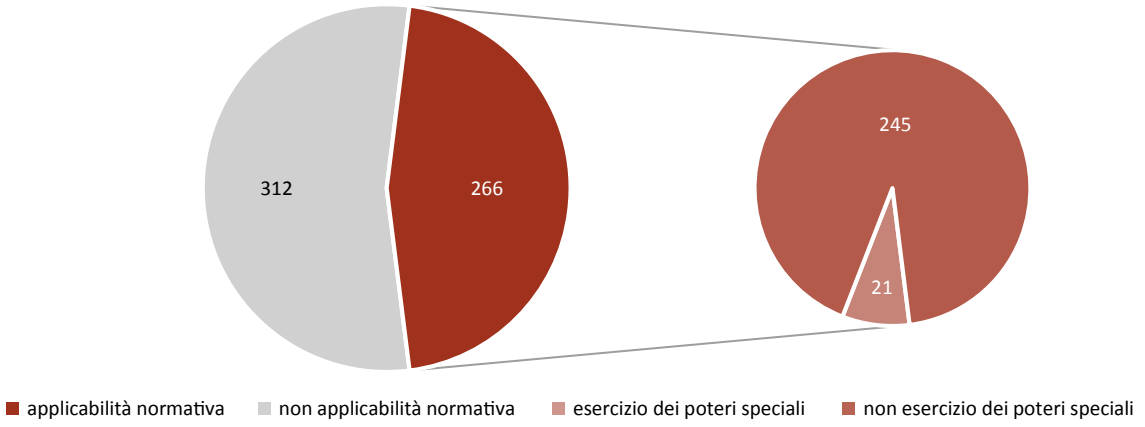
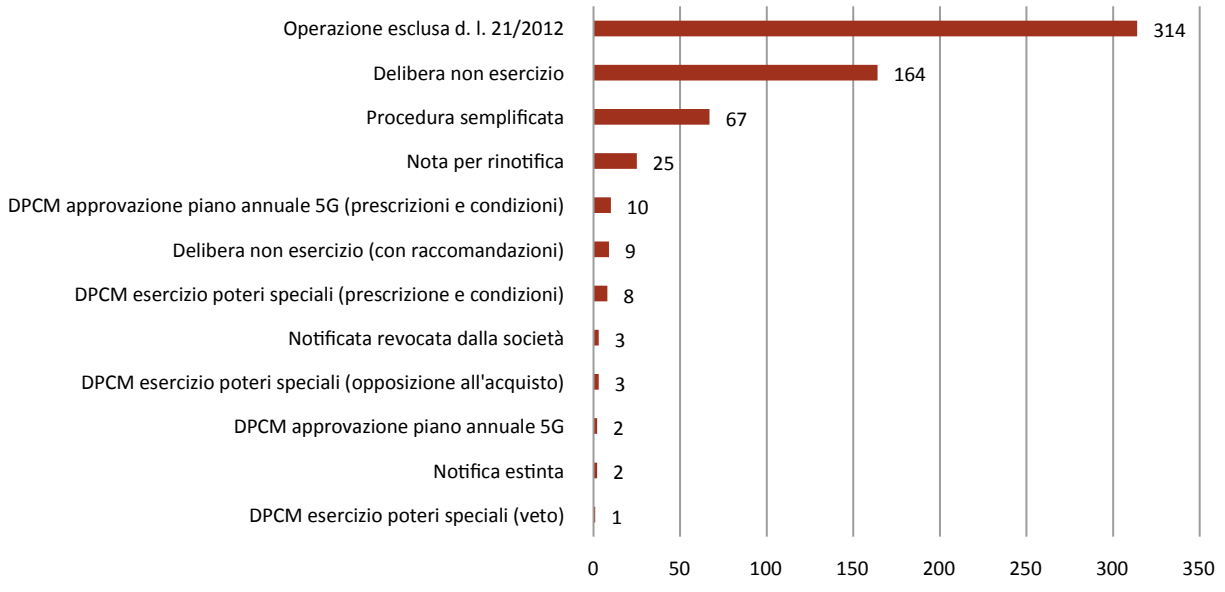


Fig. 2.6: Esito dettagliato della trattazione delle notifiche (2022)

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 (2022)



- **8 notifiche** sono state oggetto di esercizio dei poteri speciali mediante imposizione di specifiche condizioni e prescrizioni;
- per **3 notifiche** è stato esercitato il potere di opposizione all'acquisto;
- per **1 notifica** è stato esercitato il potere di veto.

Al contrario, per **245 notifiche non sono stati esercitati i poteri speciali**:

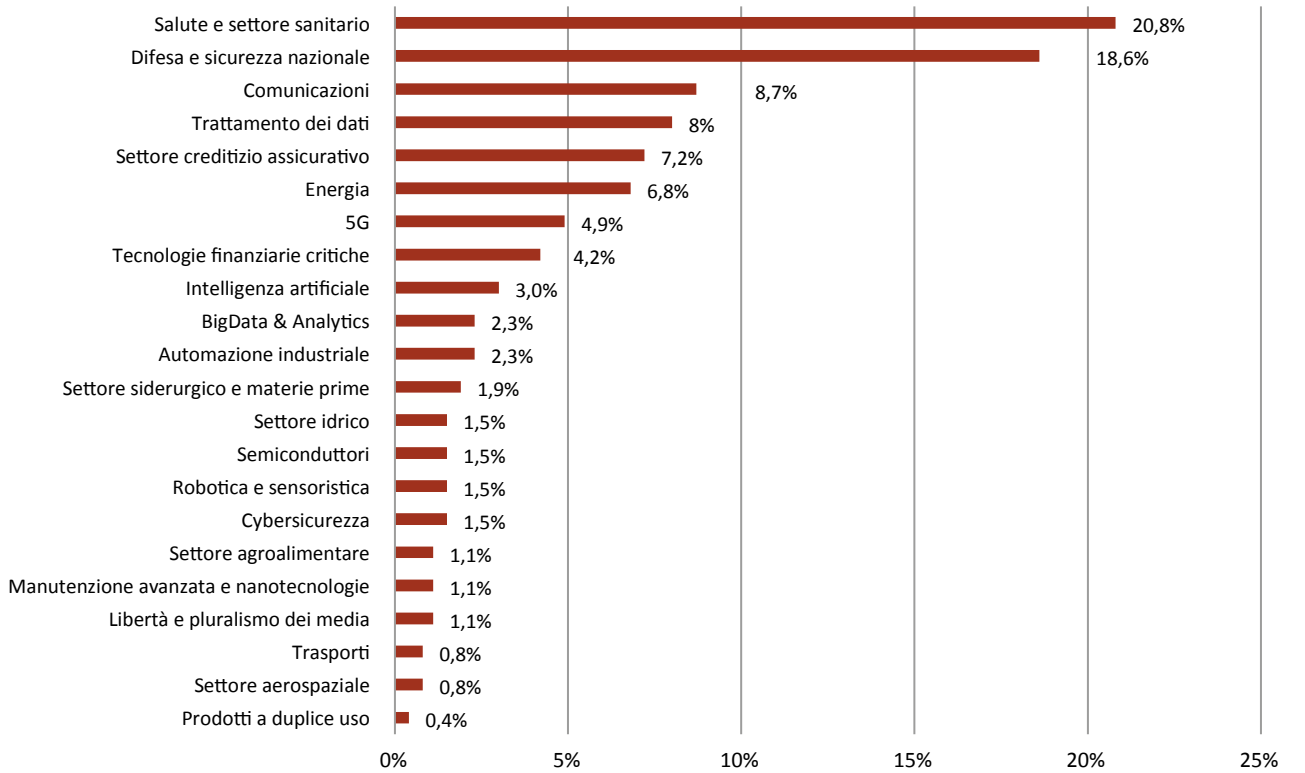
- **per 164** è stata adottata una delibera di non esercizio dei poteri speciali;
- **per 67** è stato disposto il non esercizio dei poteri speciali con procedura semplificata prevista dall'art. 1, co. 1-*bis*, e dall'art. 2, co. 1 e 1-*ter*, d. l. n. 21/2012, in quanto riguardanti operazioni infragruppo per le quali non è stata rilevata la minaccia di grave pregiudizio per gli interessi nazionali;
- **per 9 notifiche**, la delibera di non esercizio dei poteri speciali ha previsto delle raccomandazioni rivolte al soggetto notificante.

Inoltre, **312 notifiche** sono state ritenute non rientranti nella disciplina Golden Power, pari al **54%** del totale, evidenziandosi un utilizzo spesso cautelativo dello strumento della notifica.

Considerando le sole operazioni rientranti nell'ambito di applicazione del Golden Power (Fig. 2.7), spiccano quelle relative al **settore della salute e sanitario** per oltre il **20%**, seguite dal comparto difesa e sicurezza

Fig. 2.7: Notifiche per settore strategico (2022)

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 (2022)



nazionale (**18,6%**) e comunicazioni (**8,7%**). Quanto ai settori strategici correlati alle nuove tecnologie rilevanti ai sensi dell'art. 9, DPCM n. 179/2020, le notifiche raggiungono circa il **13% del totale**, suddivise così come segue: **intelligenza artificiale (3%)**, **automazione industriale (2,3%)**, ***Big Data* & *analytics* (2,3%)**, **cybersicurezza (1,5%)**, **robotica e sensoristica (1,5%)**, **semiconduttori (1,5%)**, **manifattura avanzata e nanotecnologie (1,1%)**.

In ultimo, è opportuno sottolineare che l'istituto della prenotifica è divenuto operativo dal 24 settembre 2022, data di entrata in vigore del già menzionato DPCM n. 133/2022, facendo registrare ben **43 prenotifiche**, quasi totalmente riconducibili ai settori di cui all'art. 2 (**86%**), mentre il restante **14%** afferisce al comparto difesa e sicurezza nazionale[36]. Nel **93%** dei casi non è stata richiesta alcuna notifica formale dell'operazione, potendosi affermare che, almeno in questa prima fase applicativa, la prenotifica stia assolvendo la ratio di semplificare l'intero procedimento.

2.3.6. *Gli scenari in discussione. Il disegno di legge sulla cybersicurezza*

In un contesto ad elevata complessità in cui la procedura di recepimento della NIS2 è in corso e la disciplina sul perimetro di sicurezza nazionale cibernetica vive le prime stagioni applicative, continua ad essere alta l'attenzione del Governo sui temi della cibersicurezza e ferma la volontà di contrastare il cybercrime. Secondo le notizie apprese e gli annunci pubblicati, il **25 gennaio scorso**, in particolare, il Consiglio dei Ministri avrebbe approvato un nuovo disegno di legge sulla cybersicurezza al fine espresso di rafforzare la normativa attuale per riuscire a contrastare l'avanzata offensiva del cybercrimine in Italia. Si tratta di un'iniziativa importante che da un lato **inasprirebbe pene e sanzioni** per gli hacker e, dall'altro, **allargherebbe il perimetro di soggetti tenuti a dotarsi di sistemi di cybersicurezza** includendovi espressamente le regioni e le province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali. Tali soggetti, in particolare, dal punto di vista organizzativo, sarebbero chiamati ad individuare, laddove non presente, **un referente per la cybersicurezza** che tra le varie funzioni eserciti anche quella di punto di contatto unico dell'amministrazione con l'ACN e, per quanto concerne gli ambiti più operativi, a segnalare senza ritardo ad ACN, e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze ottenute e ad inviare entro settantadue ore a decorrere dal medesimo momento, una notifica completa di tutti gli elementi informativi disponibili, un incidente riconducibile a una delle tipologie individuate. A corredo di tale obbligo, sarebbe previsto, nel caso di reiterata inosservanza dell'obbligo di notifica, una sanzione amministrativa pecuniaria **da euro 25.000 a euro 125.000**.

Dovrebbe essere assente dal DDL, probabilmente in considerazione dell'imminente approvazione dell'AI Act, l'intelligenza artificiale.

36 Con riguardo alla tecnologia 5G, tale istituto non risulta applicabile ai sensi dell'art. 7 del decreto succitato.

icom
istituto per la competitività

CAPITOLO 3

L'EVOLUZIONE DELLE CERTIFICAZIONI A LIVELLO EUROPEO

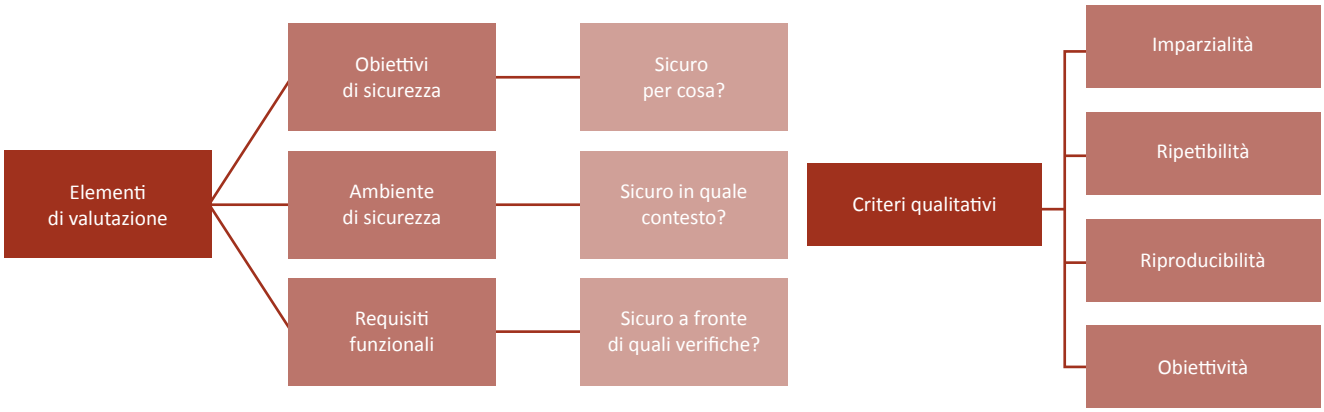
3.1. IL FUNZIONAMENTO E LE TENDENZE DI UTILIZZO DEI *COMMON CRITERIA*

È 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**. 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. 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. 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.

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

Fig. 3.1: I *Common Criteria*: elementi di valutazione e criteri qualitativi

Fonte: elaborazioni I-Com su varie



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").

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[37], tra cui i requisiti di sicurezza (SFR) e di garanzia (SAR), che risultano determinanti per misurare quantitativamente il grado di sicurezza del TOE stesso[38]. 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 (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*. È indicato nei casi di minaccia medio-alta ed è il livello più richiesto dai committenti (Fig. 3.2).

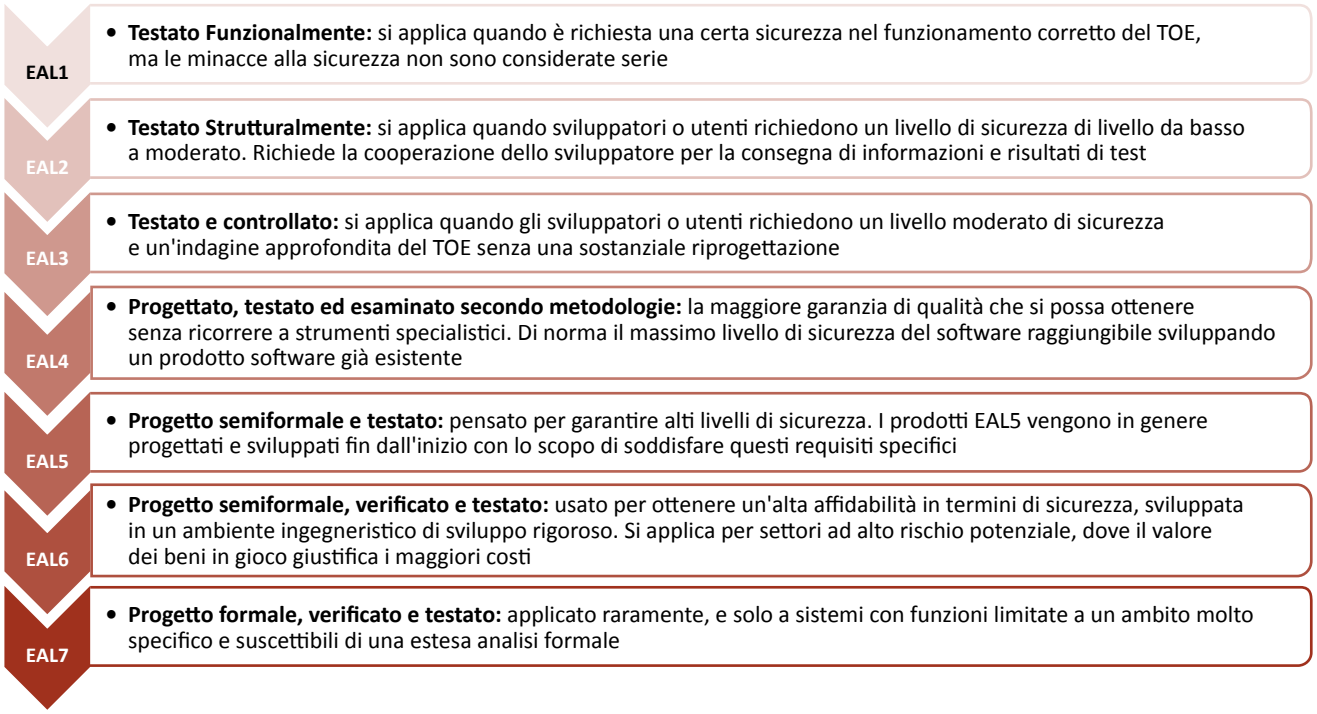
Per quanto concerne le richieste di certificazione ricevute e le certificazioni rilasciate, **nel 2021 – secondo lo studio Jtsec – si è raggiunto il valore più alto**

37 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.

38 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. 3.2: I 7 livelli di sicurezza EAL

Fonte: elaborazioni I-Com su varie



della storia[39], rafforzando un trend in forte crescita, particolarmente marcato soprattutto dal 2013, anche se va evidenziato che nel 2022 si è registrato un lieve rallentamento in tal senso, in quanto sono stati certificati 370 prodotti, a fronte dei 399 dell'anno precedente e dei 383 del 2020 (Fig. 3.3).

Le ragioni di questo leggero decremento potrebbero essere riconducibili a: l'incapacità di laboratori ed enti di certificazione di gestire un numero elevato di certificazioni; l'indisponibilità di alcuni produttori di farsi carico del processo di certificazione per motivi di tempo, costo o altro; la creazione di nuovi standard di cibersicurezza e/o una maggiore diffusione di quelli già esistenti; la posticipazione della certificazione nell'ottica di verificare la pubblicazione degli EUCC (si v. *infra*, par. 3.2).

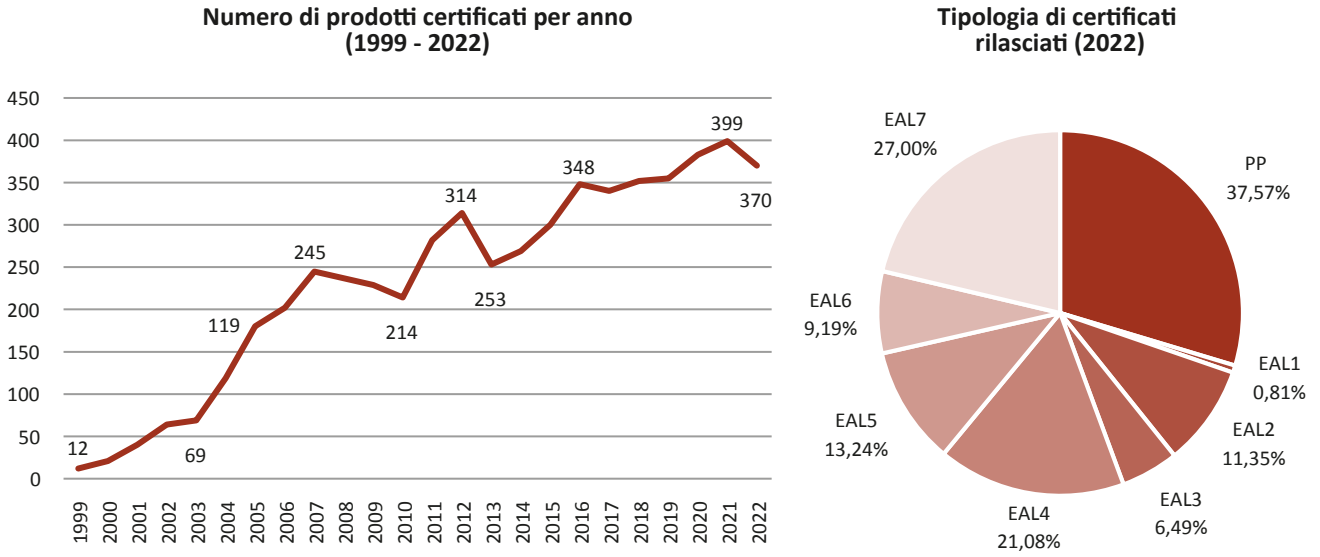
Ciò detto, vi sono sia vantaggi che criticità nell'utilizzo dei *Common Criteria*. Tra i primi, rileva sicuramente la competitività sul mercato: difatti, il prodotto ICT certificato gode di maggiore fiducia da parte dei consumatori e pertanto di maggiore domanda rispetto ai prodotti non certificati.

Inoltre, **in presenza di uno standard comune di valutazione, i consumatori 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

39 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 399 attestazioni registrate. Dati Jtsec – "Common Criteria Statistics Report for 2022" (marzo 2023).

Fig. 3.3: Tendenze dei certificati *Common Criteria*

Fonte: Jtsec – "Common Criteria Statistics Report for 2022", marzo 2023



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.

Tra le criticità, invece, si evidenziano i costi elevati del processo di certificazione poiché – oltre al tempo impiegato – la valutazione richiede l'utilizzo di risorse specializzate, costituendo una potenziale barriera all'ingresso (o alla permanenza) nel mercato, per gli operatori piccole-medie dimensioni.

Altro elemento di difficoltà è rappresentato dai lunghi tempi di esecuzione della valutazione e per il rilascio delle certificazioni, ritenuti non conformi al dinamismo e alla velocità di evoluzione del settore digitale; difatti – a differenza dei livelli EAL1 e EAL2 – i livelli dal terzo in poi possono impiegare un orizzonte temporale di vari mesi, esponendo il prodotto/servizio al rischio di divenire obsoleto prima della conclusione dell'iter di certificazione. Ciò troverebbe conferma nell'esiguo numero di prodotti assicurati nello scorso anno pari a 370 a livello mondiale. 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.

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, cioè 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 obbligatorie 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.

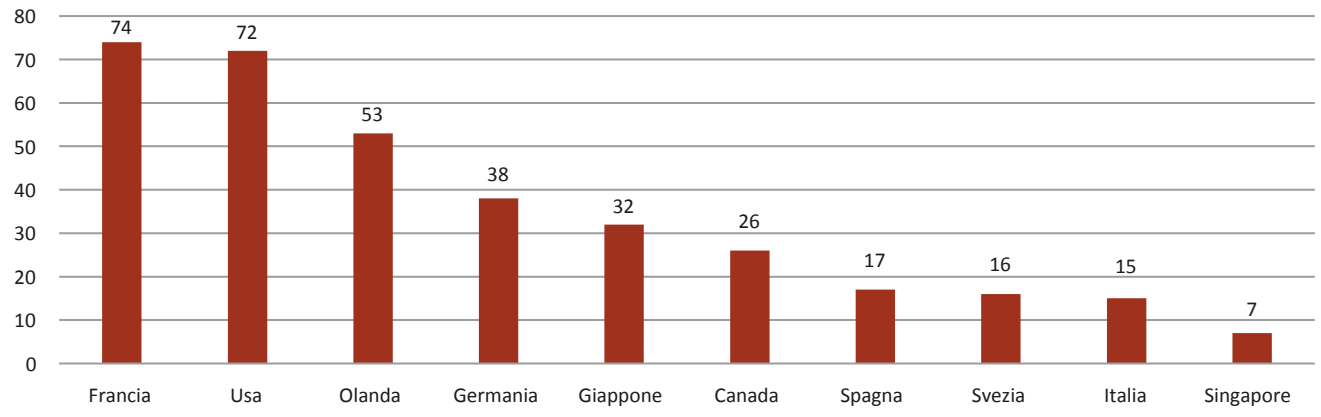
Per concludere, è opportuno fare riferimento ai dati Jtsec circa i primi 10 Paesi nel mondo che hanno certificato prodotti con i *Common Criteria* (Fig. 3.4). **Si può osservare come l'Italia rientri in questa classifica, mantenendo il nono posto a livello globale con 15 certificazioni** (nel 2021 erano state solo 11). Inoltre, si può notare come la Francia abbia superato gli USA al primo posto, con uno scarto di 2 prodotti certificati, e che Singapore abbia sorpassato la Corea del Sud (rispetto all'anno precedente). In termini percentuali, la top 3 (Francia, USA e Olanda) rappresenta il 54% delle certificazioni totali, mentre i successivi 3 paesi (Germania, Giappone, Canada) costituiscono il 26%. Sempre a livello UE, anche la Spagna (17) e la Svezia (16) si posizionano nella Top 10 globale, mentre l'Austria si trova nelle ultime posizioni con sole 4 certificazioni.

3.2. VERSO GLI EUROPEAN *COMMON CRITERIA*

Nel 2019 l'ENISA, in osservanza di quanto previsto dall'art. 48.2 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio (c.d. *Cybersecurity Act* – CSA), ha istituito un gruppo di lavoro ad hoc[40] per supportare la stesura dei *Common Criteria* Europei, detti EUCC (*Common Criteria based European candidate cybersecurity certification scheme*). **La versione attualmente disponibile di tali meccanismi di certificazione (Versione 1.1.1) si fonda su un modello ispirato agli schemi ISO/IEC 15408 e ISO/IEC 18045 e**

Fig. 3.4: Top 10 Paesi per certificazione prodotti con *Common Criteria* (2022)

Fonte: Jtsec – "Common Criteria Statistics Report for 2022", marzo 2023



40 Esso prende il nome di "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.

ha lo scopo di creare un progetto comunitario volto a sostituire i singoli schemi nazionali, anch'essi basati sui *Common Criteria*, che operano sotto l'accordo di mutuo riconoscimento SOG-IS MRA[41].

L'attuale versione degli EUCC[42] è il risultato di un processo di consultazione di tutti gli stakeholder interessati avviato nel maggio del 2020 dall'ENISA, conformemente alle prescrizioni dell'art. 49.3 del CSA[43]. **Il punto di arrivo auspicato è quello di stabilire una certificazione uniforme in grado di raggiungere i due livelli di garanzia di sicurezza più alti previsti dall'art. 52 del CSA, ovverosia quello "sostanziale" e quello "alto", coinvolgendo autorità nazionali e prendendo in considerazione valutazioni di terze parti indipendenti**. È escluso dagli EUCC il livello "base" indicato nel CSA, poiché si tratta di un requisito di sicurezza inferiore e, quindi, inadatto per il sistema in esame, che presenta esigenze maggiori dal punto di vista tecnico e procedurale. Alla stregua di quanto previsto per i *Common Criteria*, il livello di garanzia è riconosciuto tenendo conto del livello identificato nel *Vulnerability Assessment* ed è riportato con classificazione AVA, dove 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". Inoltre, gli EUCC dovrebbero includere la possibilità di certificare i *Protection Profiles*, che permetterebbero una definizione armonizzata di requisiti di sicurezza associati a categorie specifiche di prodotti.

Per quanto concerne il rilascio delle certificazioni, questo avverrà da parte di enti accreditati e riconosciuti (ISO/IEC 17065), che potrebbero differenziarsi da quelli presenti attualmente a livello nazionale. Le certificazioni di livello "alto" dovranno essere rilasciate con una procedura più rigorosa, per cui è prevista l'obbligatorietà dell'autorizzazione delle corrispondenti autorità nazionali di certificazione per la sicurezza informatica, o degli organismi di certificazione da essi autorizzati. In merito ai processi di valutazione della sicurezza dei prodotti, essi saranno affidati a laboratori accreditati interni o esterni all'organismo di certificazione di riferimento[44]. Quest'ultimo punto risulta conformarsi alla disciplina descritta nei già riconosciuti *Common Criteria*.

Gli attori che possono far uso degli EUCC vengono distinti in quattro categorie: a) i produttori o fornitori che vogliono valutare la qualità della sicurezza dei loro prodotti ICT con una certificazione rilasciata da terzi; b) i fornitori di servizi/processi/prodotti ICT che desiderano beneficiare dell'evidenza di sicurezza dei propri prodotti a favore dei loro clienti; c) le autorità attive nel settore della regolamentazione del mercato; d) gli utenti finali che possono beneficiarne in termini di affidabilità e sicurezza del sistema digitale. **È importante evidenziare che gli EUCC, differentemente dai *Common Criteria* applicati a livello nazionale, tentano di superare determinati aspetti che possono collidere con le dinamiche di mercato, soprattutto l'allungamento dei tempi e l'incremento dei costi**. In particolare, si intendono adottare nuove procedure armonizzate per la gestione delle criticità non previste al momento del rilascio e una procedura di valutazione rapida per le successive modifiche dei prodotti. In questa direzione si muove il *Patch Management*, ossia la possibilità di risolvere le vulnerabilità di sicurezza, nonché aggiornare e ottimizzare le prestazioni di un programma. **Gli EUCC prevedono il "*testing once principle*", per cui al produttore è consentito includere un previo meccanismo di gestione delle *patch* già ad origine, da analizzare durante le procedure di certificazione del prodotto**.

41 Senior Officials Group – Information Systems Securit. Mutual Recognition Agreement.
42 ENISA – Cybersecurity Certification: Candidate EUCC Scheme V1.1.1. 25th May 2021.
43 Esso prevede che: "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".
44 IT Security Evaluation Facilities, ITSEF.

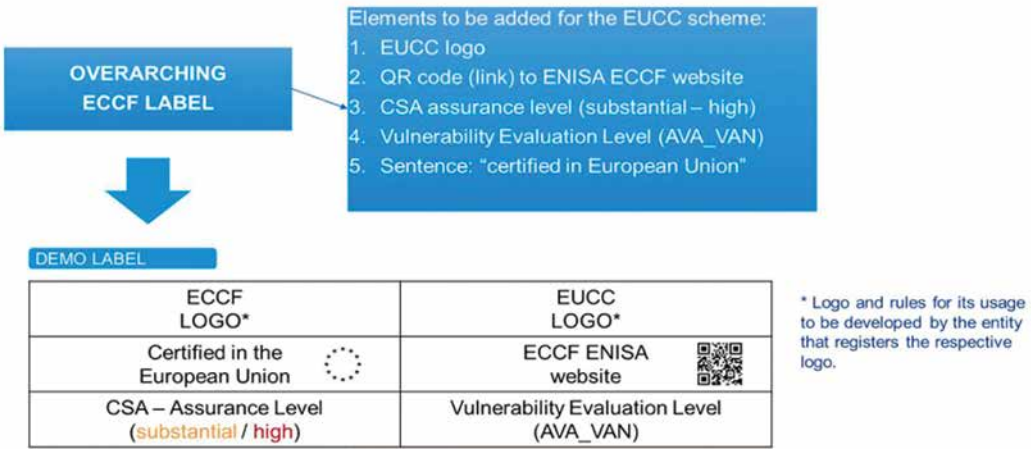
In questo modo, è possibile evitare percorsi di certificazione ripetuti anche per componenti del prodotto/servizio che non hanno subito aggiornamenti, pertanto il prodotto sarà costantemente patchato pur mantenendo lo stato di certificazione originale[45]. La validità di quest'ultimo per la sua intera durata dovrà essere confermata attraverso nuovi criteri armonizzati volti a rafforzare il mantenimento dei certificati nel tempo, mediante revisioni da parte dell'ente di certificazione ed eventuali valutazioni specifiche da parte dei laboratori indipendenti. **Un'importante novità è che il 19 marzo 2023 è stato lanciato dall'ENISA un sito web[46] contenente lo status delle certificazioni di cybersicurezza, per promuovere e diffondere informazioni relative, fra l'altro, agli EUCC**. Peraltro, per aumentare la trasparenza, si vuole far uso di un'etichetta 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 (Fig. 3.5).

In base a quanto esposto, è evidente che gli EUCC comporterebbero una serie di benefici significativi, primo fra tutti il miglioramento della sicurezza dei prodotti connessi e delle infrastrutture critiche, oltre a garantire una maggiore adeguatezza rispetto alle esigenze derivanti dalle dinamiche di mercato. In particolare, la creazione di un approccio standardizzato dovrebbe ridurre la richiesta di misure aggiuntive di certificazione a livello nazionale, evitando di ripetere le procedure già svolte in altri Paesi europei.

Nel maggio del 2021, l'ENISA ha svolto delle consultazioni con gli stakeholder del mercato digitale, da cui si possono tirare le somme relativamente alle intenzioni da parte di tali soggetti di far uso del sistema di certificazione comunitario. **Il 33% dei produttori, degli sviluppatori e delle organizzazioni commerciali ha indicato di voler certificare i propri prodotti/servizi ICT con il sistema EUCC, 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**

Fig. 3.5: L'etichetta EUCC

Fonte: ENISA

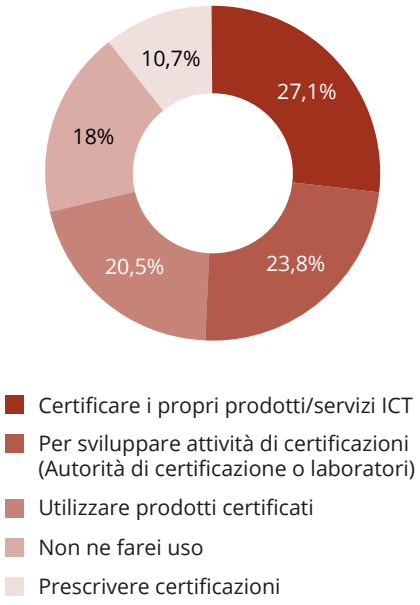


45 Questo aspetto risulta essere innovativo rispetto all'attuale sistema dei Common Criteria, che prevede, salvo eccezioni, ad ogni modifica del prodotto/servizio, di dover avviare nuove procedure di verifica che lo coinvolgano per intero e non nelle singole parti oggetto di variazione (si v. supra, par. 3.1).

46 https://certification.enisa.europa.eu/

Fig. 3.6: Intenzione di usare gli EUCC (% dei rispondenti)

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



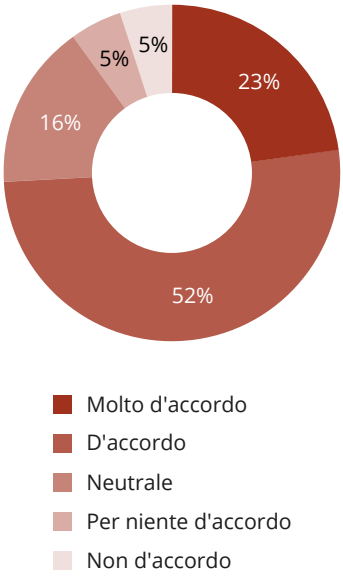
25% prevede di fare uso degli EUCC come utilizzatore finale o cliente (Fig. 3.6).

In merito all'impatto positivo degli EUCC sulle condizioni del mercato digitale europeo, risultano favorevoli il 52% dei rispondenti e molto favorevoli un ulteriore 23% degli intervistati, in quanto tali meccanismi di certificazione sono dotati di particolare trasversalità, flessibilità e autorevolezza a livello mondiale (Fig. 3.7).

Il 31 gennaio 2024, la Commissione europea ha adottato l'*Implementing Act* – in realtà, previsto entro il quarto trimestre dell'anno scorso[47] – ossia il regolamento di esecuzione con cui gli EUCC possono finalmente diventare ufficialmente parte della legislazione europea. Parallelamente, l'ENISA ha pubblicato una serie di documenti tecnici a supporto dell'*Implementing Act* (*state-of-the-art documents*[48]), i quali specificano metodi di valutazione, tecniche e strumenti applicabili alla certificazione di prodotti ICT o a requisiti di sicurezza riferiti a una categoria generica di prodotti ICT, al fine di armonizzare i criteri di valutazione o i profili di sicurezza. Tali documenti potranno essere sottoposti a revisione da parte dei titolari di schemi di certificazione EUCC. **Una piena attuazione del sistema richiederà probabilmente nuove discussioni in sede comunitaria e la stesura di linee guida per facilitare il periodo di transizione (12 mesi, che aumentano a 24 se il processo di certificazione prende inizio entro i 12 mesi dall'entrata in vigore *dell'Implementing Act*), al termine del quale le certificazioni nazionali dovrebbero cessare di operare per lasciare spazio agli EUCC.**

Fig. 3.7: Impatto positivo degli EUCC sulle condizioni del mercato UE (% di rispondenti)

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



47 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en

48 https://certification.enisa.europa.eu/#documentation

icom
istituto per la competitività

CAPITOLO 4

IL QUADRO REGOLATORIO EUROPEO E NAZIONALE IN CYBERSICUREZZA E LA PERCEZIONE DELLE IMPRESE

4.1. NOTA METODOLOGICA E ANALISI DEL CAMPIONE

Al fine di **verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity, con particolare riferimento al Perimetro di Sicurezza Nazionale Cibernetica (PSNC)**, l'Istituto per la Competitività (I-Com) ha condotto un'indagine, avvalendosi anche del sostegno di alcune delle principali associazioni di categoria, che ha coinvolto **145 imprese appartenenti a vari settori**: utilities (acqua, rifiuti ed energia), trasporti, TLC/digitale, ecc.
La survey si è svolta in modalità completamente online tra l'8 agosto e il 3 ottobre 2023 ed è stata condotta mediante la predisposizione di un questionario, testato e migliorato tramite interviste qualitative condotte con esperti del settore, e la successiva somministrazione della versione finale del medesimo, costituito da 20 domande.
Osservando la distribuzione dei rispondenti per settore (Fig. 4.1) è possibile notare come **la maggioranza delle imprese (58,62%) rientri tra le utilities**, mentre le aziende del comparto Ict corrispondono al 15,86% del campione, seguite da trasporti (7,59%) e Tlc (6,21%). Per di più, oltre l'11% dei rispondenti appartiene ad altri settori, di cui ben 6 afferiscono a quello finanziario.
Analizzando il campione dal punto di vista dimensionale (Fig. 4.2), **si osserva la netta prevalenza delle grandi aziende** (oltre le soglie della media impresa), che corrispondono al 61,38%, seguite dalle medie (meno di 250 dipendenti con fatturato non superiore ai €43 milioni) con il 24,14% e, infine, dalle piccole imprese (meno di 50 dipendenti con fatturato non superiore ai €10 milioni), le quali occupano il 14,48% del totale.

Fig. 4.1: Distribuzione dei rispondenti per settore

Totale rispondenti: 145 su 145
Fonte: Elaborazioni I-Com

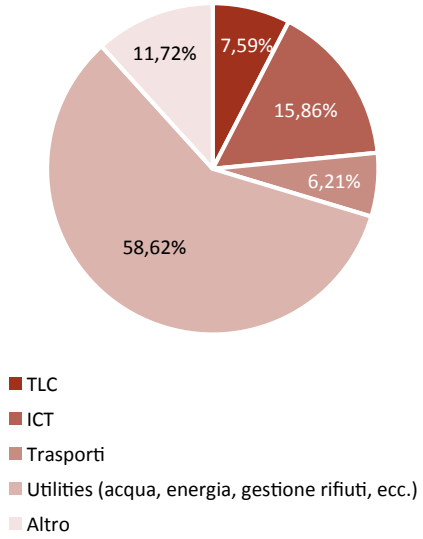
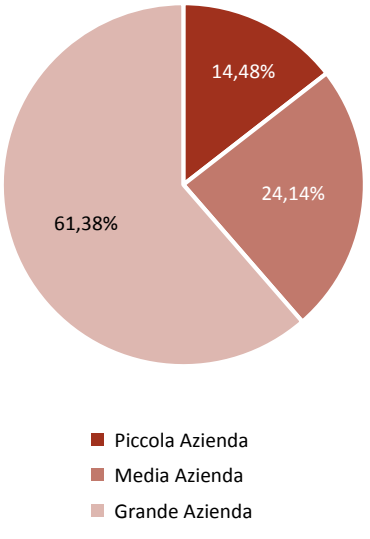


Fig. 4.2: Distribuzione dei rispondenti per dimensione aziendale

Totale rispondenti: 145 su 145
Fonte: Elaborazioni I-Com

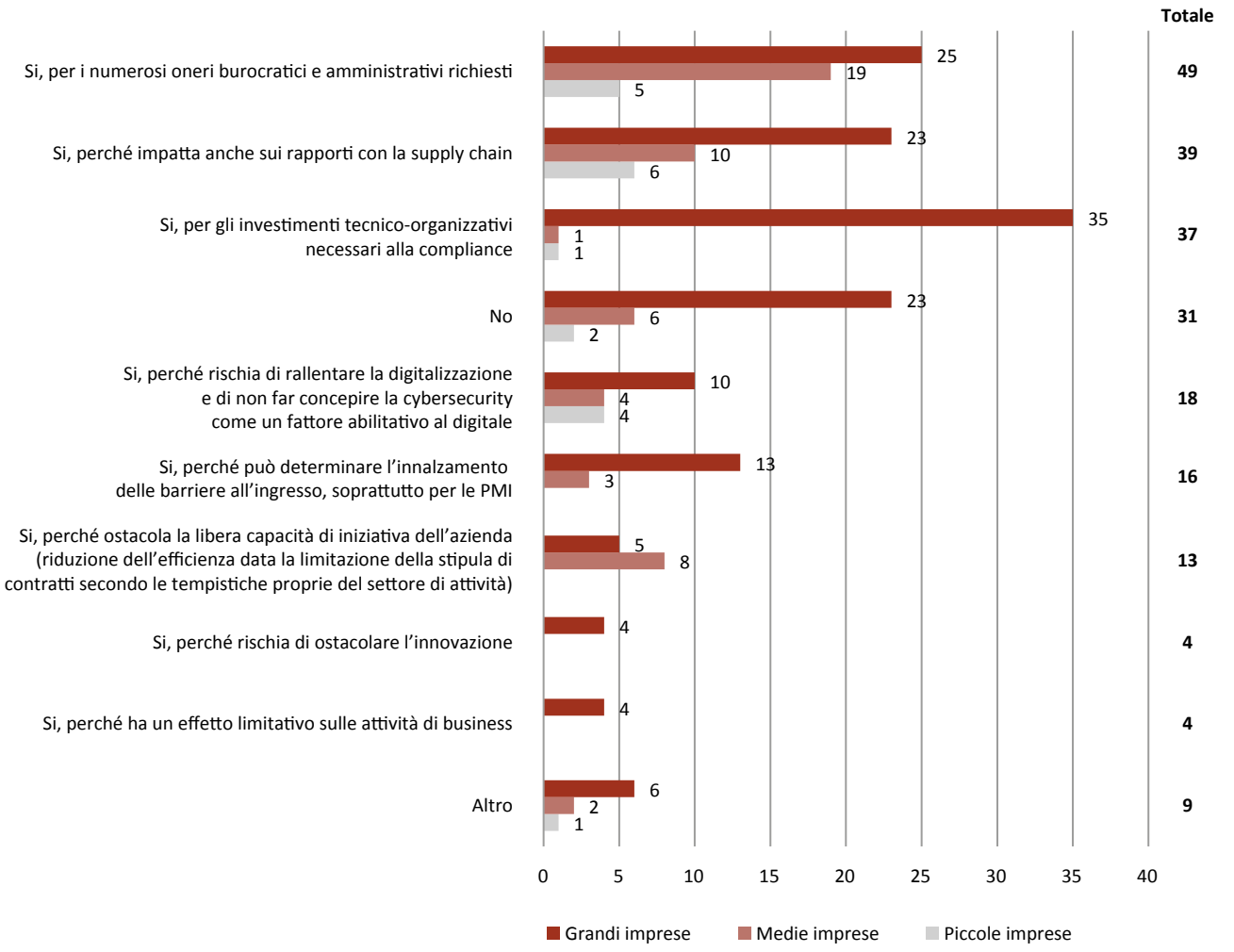


4.2. ANALISI DEI RISULTATI

La seconda sezione dell'analisi mira ad approfondire, tramite domande a risposta multipla, temi quali la compliance, l'*awareness* e gli investimenti in cybersicurezza, nonché le certificazioni di cybersecurity e, infine, alcune considerazioni sul rapporto con i fornitori e sulle attività del CVCN. La quasi totalità delle risposte pervenute sono state suddivise per dimensione aziendale – e in alcuni casi anche per settore – al fine di poter comprendere meglio le eventuali differenze che possano emergere in virtù della specificità del contesto in cui operano le imprese del campione.

Fig. 4.3: Ritiene che il crescente numero di adempimenti richiesti dalle normative in cybersicurezza possa impattare sulla competitività aziendale?

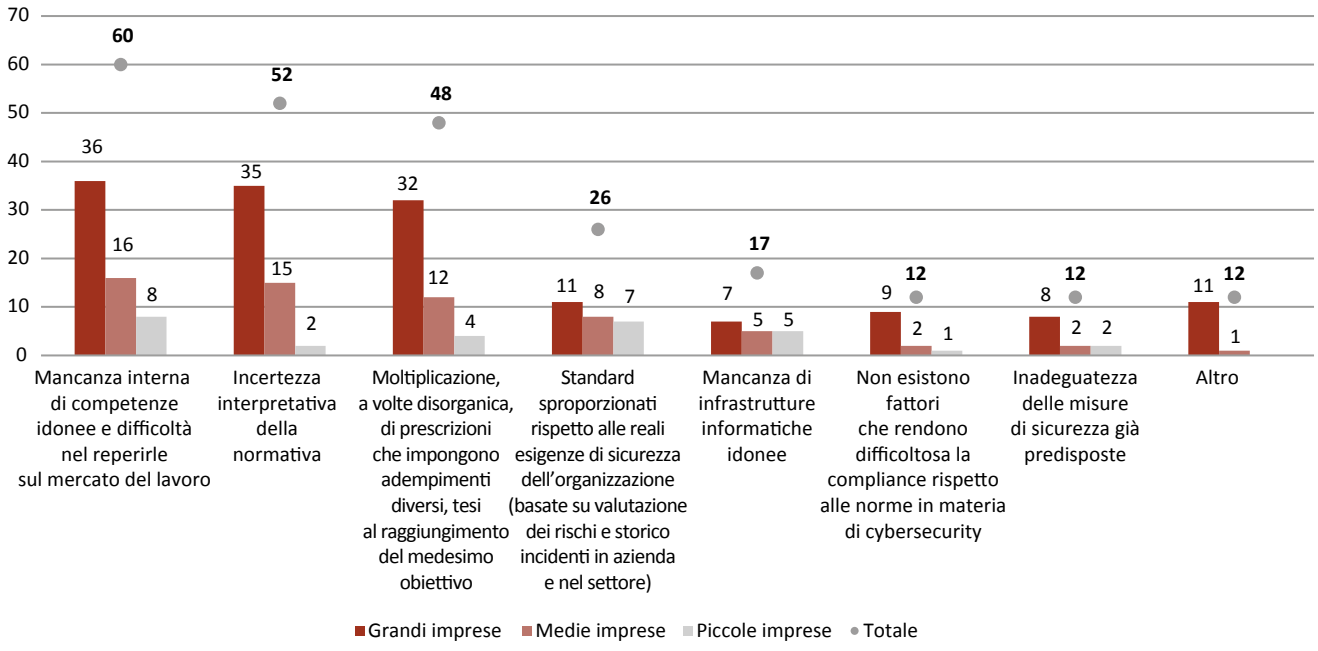
Note: Possibilità di più risposte
Totale dei rispondenti: 119 su 145
Fonte: Elaborazioni I-Com



Innanzitutto, ai soggetti partecipanti è stato chiesto di fornire una valutazione circa l'impatto degli adempimenti prescritti dalle normative in cybersicurezza sulla competitività aziendale (Fig. 4.3).
Per il 39% delle grandi imprese la principale criticità è legata agli investimenti tecnico-organizzativi necessari alla compliance, mentre il 54% delle aziende di medie dimensioni si concentra prettamente sulla numerosità degli oneri burocratici e amministrativi richieste e, infine, il 29% delle piccole imprese si preoccupa prioritariamente dell'impatto sui rapporti con la supply chain.
Anche considerando unitamente tutte le classi dimensionali, i tre motivi appena citati sono i più ricorrenti tra i rispondenti. Viceversa, gli adempimenti previsti da normative in ambito cibersicurezza vengono più limitatamente ritenuti come ostacoli rispetto alla libera capacità di iniziativa dell'azienda (13 risposte in totale), all'innovazione (4) e sulle attività di business (4). Inoltre, alla voce "altro" (9 risposte) ricorre, per un verso, la difficoltà, soprattutto per le PMI, di far fronte a tali adempimenti, dovuta in parte alla **mancanza di adeguate professionalità interne che riescano ad analizzare e implementare il quadro regolatorio vigente**; per altro verso, le prescrizioni normative in ambito cybersecurity vengono percepite come un acceleratore della competitività.
Successivamente, è stato chiesto alle imprese intervistate di indicare nello specifico i fattori che rendono più difficoltosa la **compliance rispetto alle norme in materia di cybersecurity** (Fig. 4.4) ed è emerso che ciò sarebbe dovuto alla **mancanza di competenze idonee**

Fig. 4.4: Quali sono i fattori che rendono più difficoltosa la compliance rispetto alle norme in materia di cybersecurity?

Note: Possibilità di max. 4 risposte
Totale dei rispondenti: 117 su 145
Fonte: Elaborazioni I-Com



sia internamente, sia sul mercato del lavoro (60 risposte in totale), seguito dall'incertezza interpretativa della normativa (52 risposte) e alla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (48 risposte). Invece, tra le opzioni meno selezionate rileva, con 12 preferenze espresse, l'assenza di fattori che rendono difficoltosa la compliance. Nella voce "altro" è interessante osservare come venga annoverata più volte sia **la mancante (o insufficiente) consapevolezza dei livelli apicali per quanto riguarda l'ambito cybersecurity, sia l'aspetto rigido e prescrittivo di alcune normative di settore, il che comporterebbe una gestione più costosa e meno efficace nel medio-lungo periodo**.

Come si evince dal grafico successivo (Fig. 4.5), **quasi i due terzi delle imprese rispondenti assegnano meno del 5% del budget IT alla cybersecurity**. Non sorprende che figurino solo grandi (27) e medie imprese (4) fra chi dedica tra il 5 e il 15% delle risorse economiche a disposizione per l'IT alla cybersicurezza, così come nel caso – estremamente limitato (6 in totale, di cui 5 grandi imprese) – di un'allocazione superiore al 15% del budget IT a disposizione.

La figura successiva (Fig. 4.6) mostra come tra i rispondenti vi sia un minimo ricorso al ruolo del ***Customer Security Manager***. Difatti, **tale figura è presente solo nel 16,8% delle aziende** partecipanti, prevalendo in tal senso le grandi imprese (16), seguite dalle medie (3) e, infine, da un'unica piccola impresa.

Agli operatori economici intervistati è stato chiesto di dichiarare **la vita media dei rispettivi strumenti di sicurezza hardware e software** (Fig. 4.7). Oltre **il 66% delle imprese rispondenti dismette tali strumenti mediamente dopo 5 anni**, mentre quasi il 28% dopo 3 anni di utilizzo. Solo un'unica grande impresa esegue l'aggiornamento delle proprie tecnologie dopo 12 anni. Nella voce "altro" è apparsa come ricorrente la risposta per cui la vita media della soluzione hw o sw dipenda dalla specifica tipologia di prodotto, nonché dal contesto esterno.

In merito alle **risorse umane specificamente assegnate alla cybersecurity** rispetto agli FTE (*Full-Time Equivalent*, una misura funzionale a comprendere quanto personale a tempo pieno sia necessario per svolgere una determinata attività) impiegati in ambito IT (Fig.

Fig. 4.5: A quanto ammontano le risorse economiche assegnate alla cybersecurity rispetto al budget IT nella sua impresa?

Note: Possibilità di un'unica risposta
Totale dei rispondenti: 119 su 145
Fonte: Elaborazioni I-Com

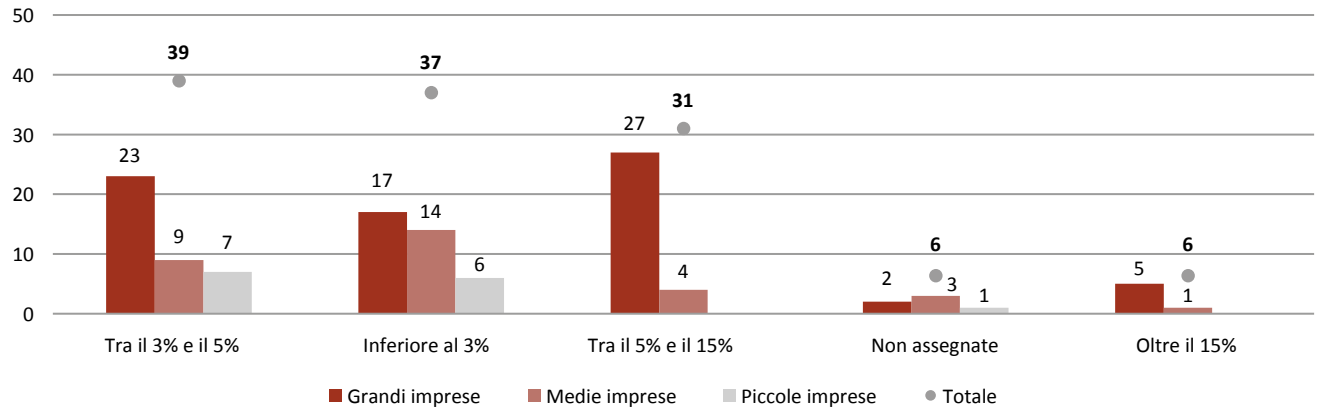


Fig. 4.6: Esiste presso la vostra azienda un Customer Security Manager?

Note: Possibilità di un'unica risposta
Totale dei rispondenti: 119 su 145
Fonte: Elaborazioni I-Com

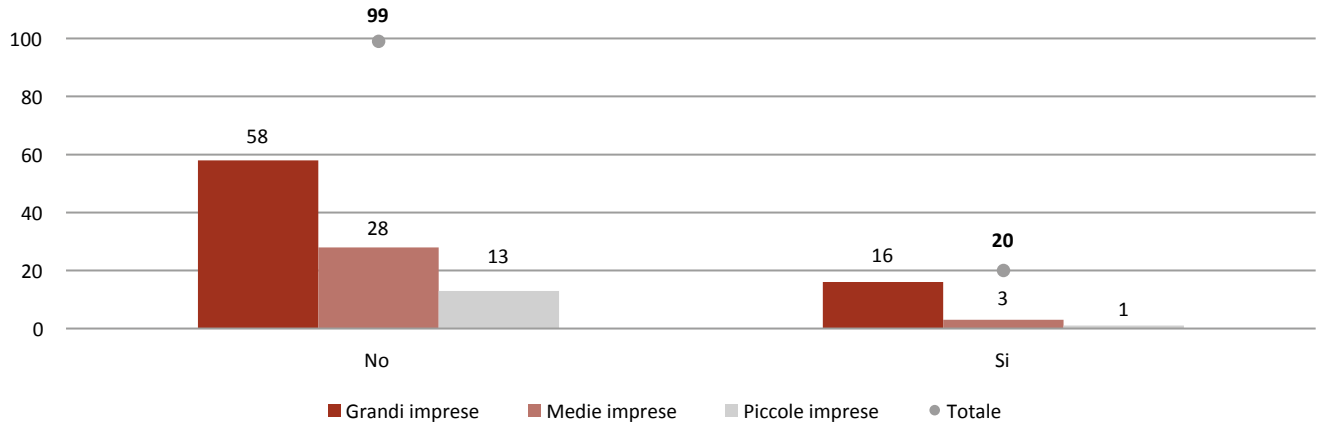
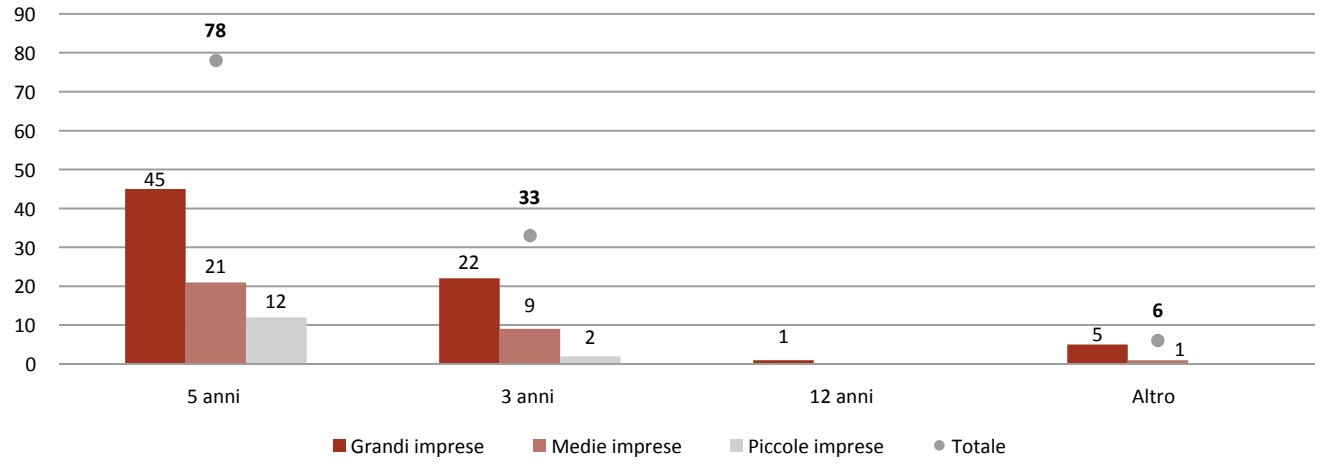


Fig. 4.7: Qual è la vita media dei vostri strumenti di sicurezza (hardware e software)?

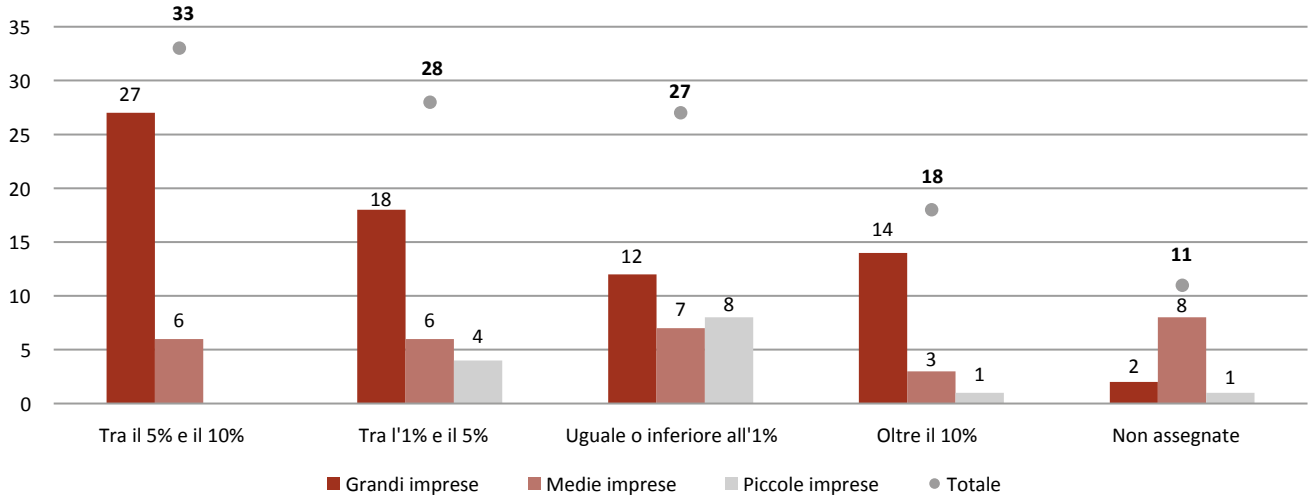
Note: Possibilità di un'unica risposta
Totale rispondenti: 118 su 145
Fonte: Elaborazioni I-Com



4.8), i feedback pervenuti sono piuttosto diversificati. **Tra le piccole imprese prevale la risposta che vede l'assegnazione di lavoratori appositamente dedicati alla cibersicurezza uguale o inferiore all'1%** rispetto alla quota di personale IT a tempo pieno dell'impresa. Fra le medie imprese rispondenti, vi è sostanzialmente una parità di scelta rispetto alle diverse opzioni a disposizione, con una leggera preponderanza per

Fig. 4.8: A quanto ammontano le risorse umane assegnate alla cybersecurity rispetto agli FTE impiegati in ambito IT nella sua impresa?

Note: Possibilità di un'unica risposta
Totale rispondenti: 117 su 145
Fonte: Elaborazioni I-Com



la non assegnazione di personale ad hoc. In ultimo, **le grandi imprese tendono maggiormente a destinare tra il 5% e il 10% degli FTE impiegati in ambito IT a compiti inerenti la cibersicurezza**.

Considerando l'aggravarsi dello scenario, sia in termini numerici che di impatto, circa le attività malevole a danno delle infrastrutture critiche anche in Italia, nonché dei maggiori adempimenti previsti dalle direttive NIS2 e CER, le quali si applicheranno a partire dal 18 ottobre 2024, è stato chiesto alle aziende partecipanti di fornire indicazioni su un **eventuale incremento delle risorse destinate alla cybersecurity** (Fig. 4.9). Sul punto, si può osservare come **il 51,2% dei rispondenti stia ancora valutando tale eventualità. Diversamente, il 36,1% delle imprese ha già deciso di aumentare gli investimenti in cybersicurezza, mentre il restante 12,6% non stanzierà ulteriori risorse**.

Il grafico successivo (Fig. 4.10) mostra **le modalità più diffuse per la valutazione del livello di cibersicurezza**. In tal senso, **spicca il ricorso a test tecnici come i *vulnerability assessment* e i *penetration test*, che sono eseguiti da oltre il 62% dei rispondenti**, seguito dalla pianificazione di audit interni (poco più del 39%) ed esterni (35%), e dall'utilizzo di strumenti per la simulazione di attacchi (34%), tra cui si possono annoverare le campagne di phishing. Ulteriori tipologie comunque prese in considerazione dalle imprese in maniera rilevante riguardano lo svolgimento di test per verificare il rispetto delle policy interne (27%) e la previsione di determinati KPI (quasi il 19%). **Risulta interessante anche il dato relativo all'utilizzo di tutte le modalità di valutazione sin qui richiamate, che interessa il 30% delle imprese**. In ultimo, **è preoccupante notare come 5 rispondenti (1 grande impresa, 2 medie imprese e 2 piccole imprese) non stiano valutando in concreto il livello di cybersecurity della propria organizzazione**.

Con riferimento ai principali **investimenti delle imprese in termini di cybersecurity** (Fig. 4.11), è emerso che oltre **il 67% dei rispondenti è dotato sia di**

Fig. 4.9: In considerazione del crescente numero e impatto di attacchi informatici, nonché dei maggiori adempimenti previsti dalla NIS2 e dalla direttiva CER che entreranno in vigore nel 2024, è previsto un incremento delle risorse destinate alla cybersecurity?

Note: Possibilità di un'unica risposta
Totale rispondenti: 119 su 145
Fonte: Elaborazioni I-Com

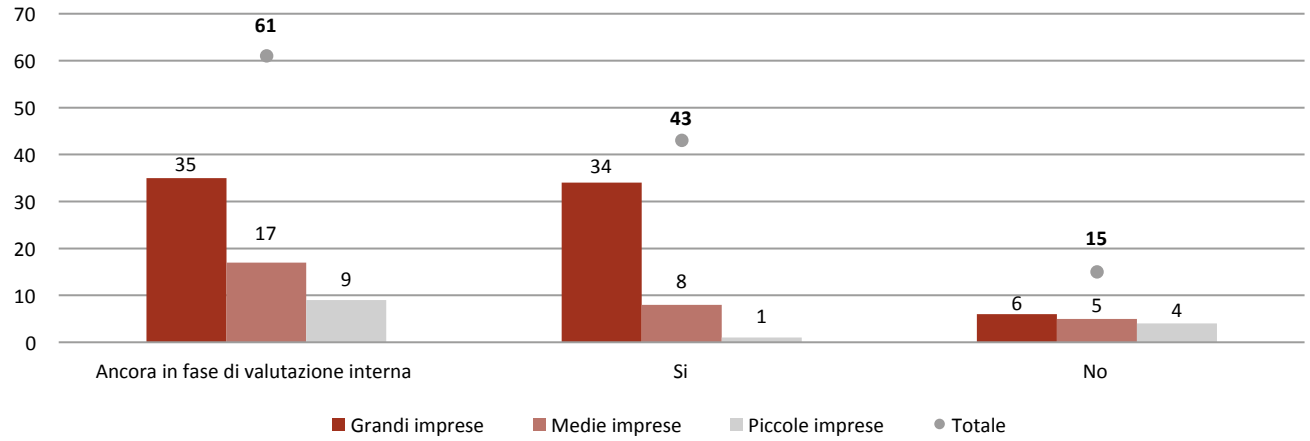


Fig. 4.10: Come viene valutato in concreto il livello di sicurezza informatica interno all'organizzazione?

Note: Possibilità di più risposte
Totale rispondenti: 117 su 145
Fonte: Elaborazioni I-Com

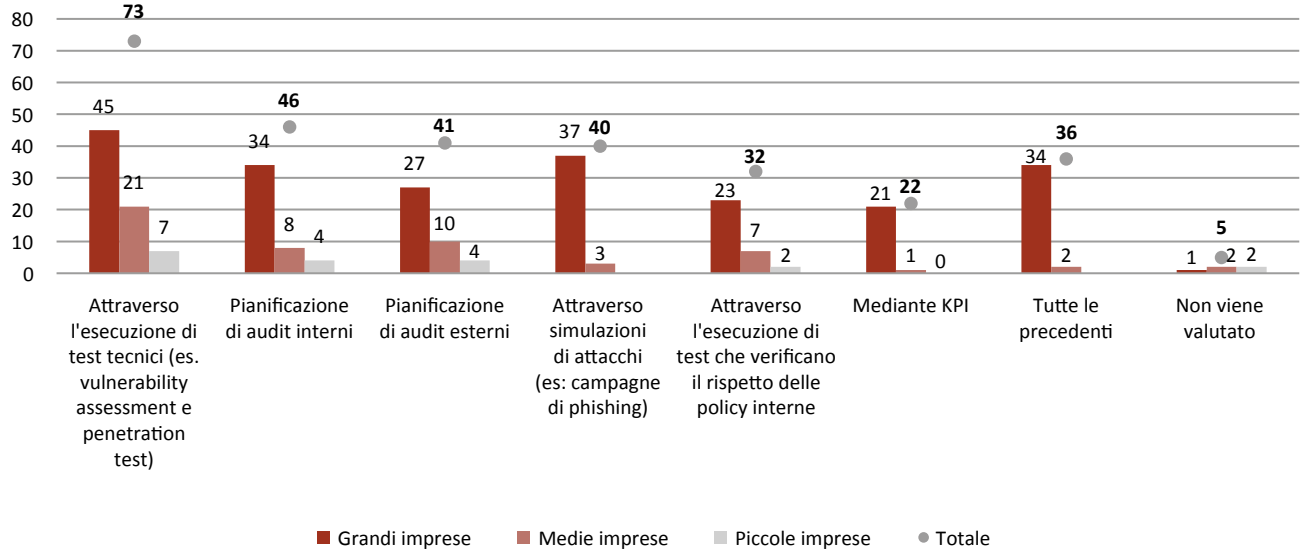
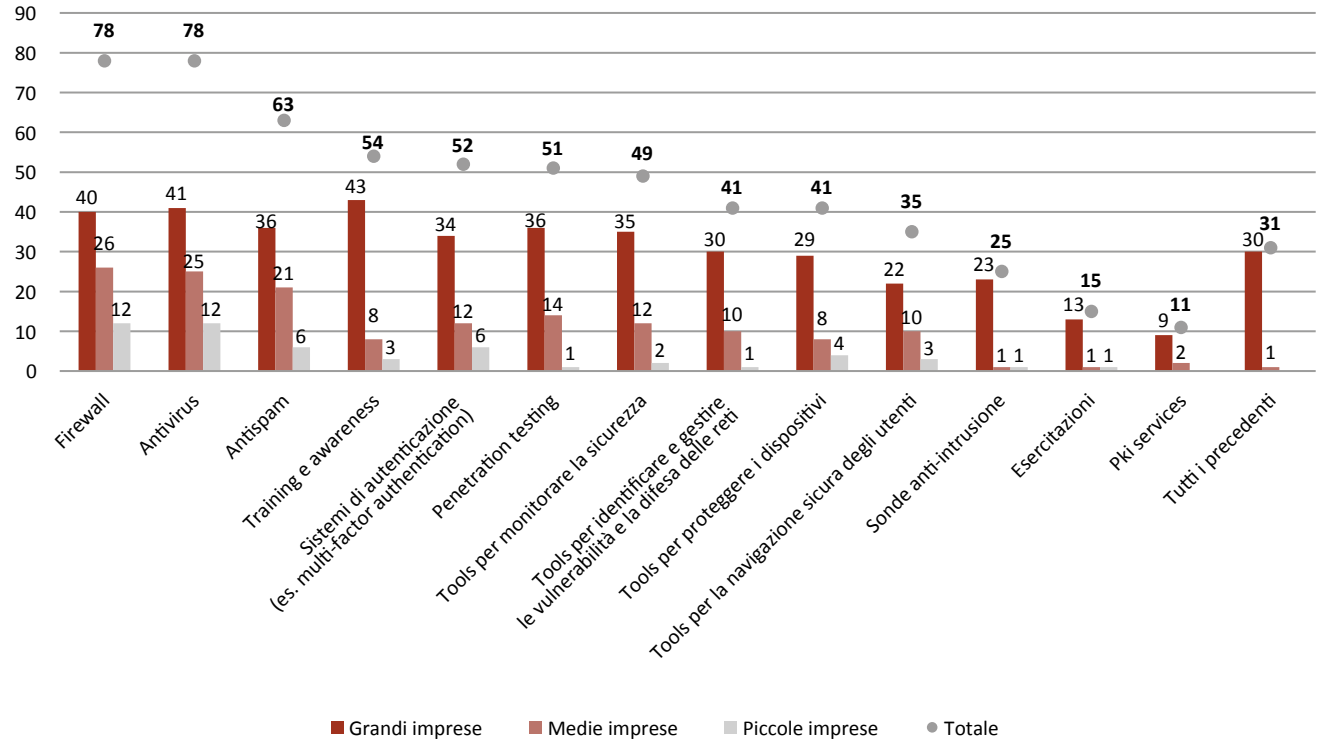


Fig. 4.11: Su quali investimenti si è concentrata la sua impresa in termini di cybersecurity?

Note: Possibilità di più risposte
Totale rispondenti: 116 su 145
Fonte: Elaborazioni I-Com

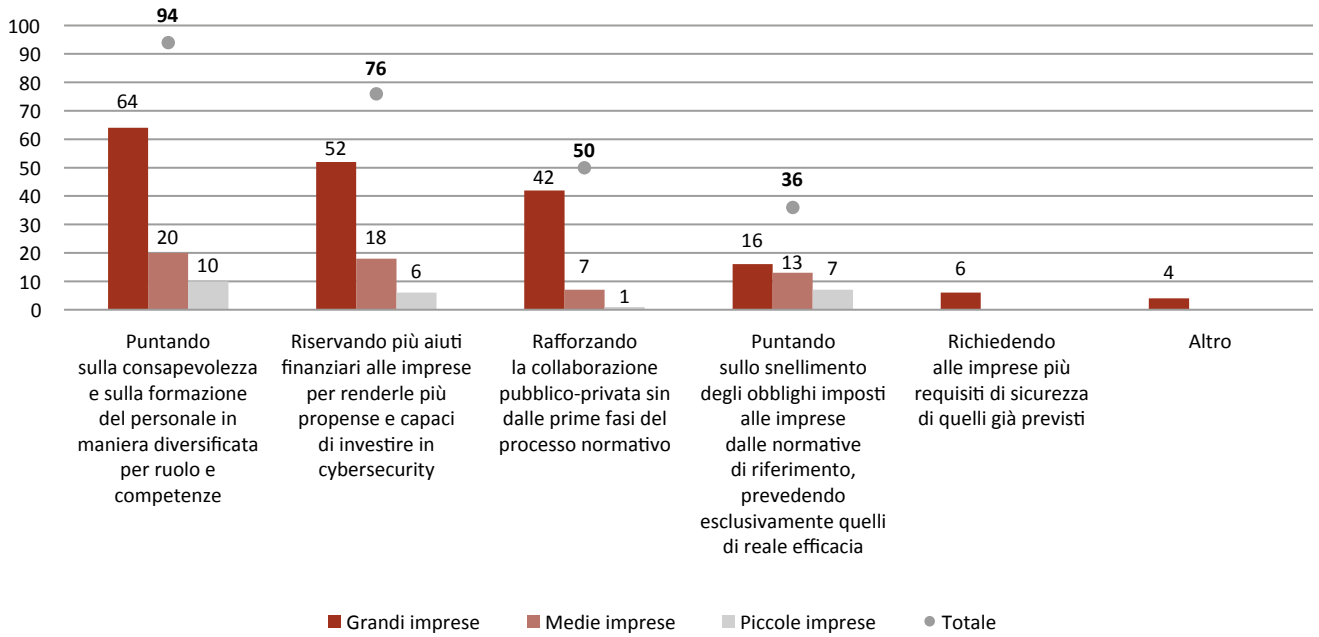


firewall che di antivirus. A seguire, il 54% utilizza un filtro antispam, mentre il 44%-46% ha investito in sistemi di autenticazione multifattoriale, *training* e *awareness*, oltre che *penetration testing*. Viceversa, fra gli ambiti di investimento meno selezionati spiccano le sonde anti-intrusione (21,5%), le esercitazioni di cybersicurezza (quasi il 13%) e i *pki services* (circa il 9%). Analizzando più nel dettaglio i feedback pervenuti, si può osservare come questi ultimi tre strumenti citati, nonché i *penetration test* e i tools per identificare e gestire le vulnerabilità e la difesa delle reti, siano pressoché inutilizzati dalle piccole imprese e – per alcuni di questi (sonde anti-intrusione ed esercitazioni) – anche dalle medie imprese.

Analizzando le risposte pervenute con riguardo alle **modalità con cui poter migliorare i livelli di sicurezza informatica** (Fig. 4.12), **l'81% delle imprese ritiene che si debba puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze**. Tale opzione è risultata la più selezionata da tutte e tre le classi dimensionali considerate, a conferma del fatto che si tratta di un aspetto particolarmente sentito a livello aziendale. **La seconda scelta (65,5%) è ricaduta sul riservare più aiuti finanziari alle imprese, in quanto ciò è ritenuto necessario per stimolare gli investimenti in cybersecurity, mentre il 43% dei rispondenti sostiene che si debba rafforzare la collaborazione pubblico-privata sin dalle prime fasi**

Fig. 4.12: In che modo ritiene possibile migliorare i livelli di sicurezza informatica?

Note: Possibilità di max. 3 risposte
Totale rispondenti: 116 su 145
Fonte: Elaborazioni I-Com



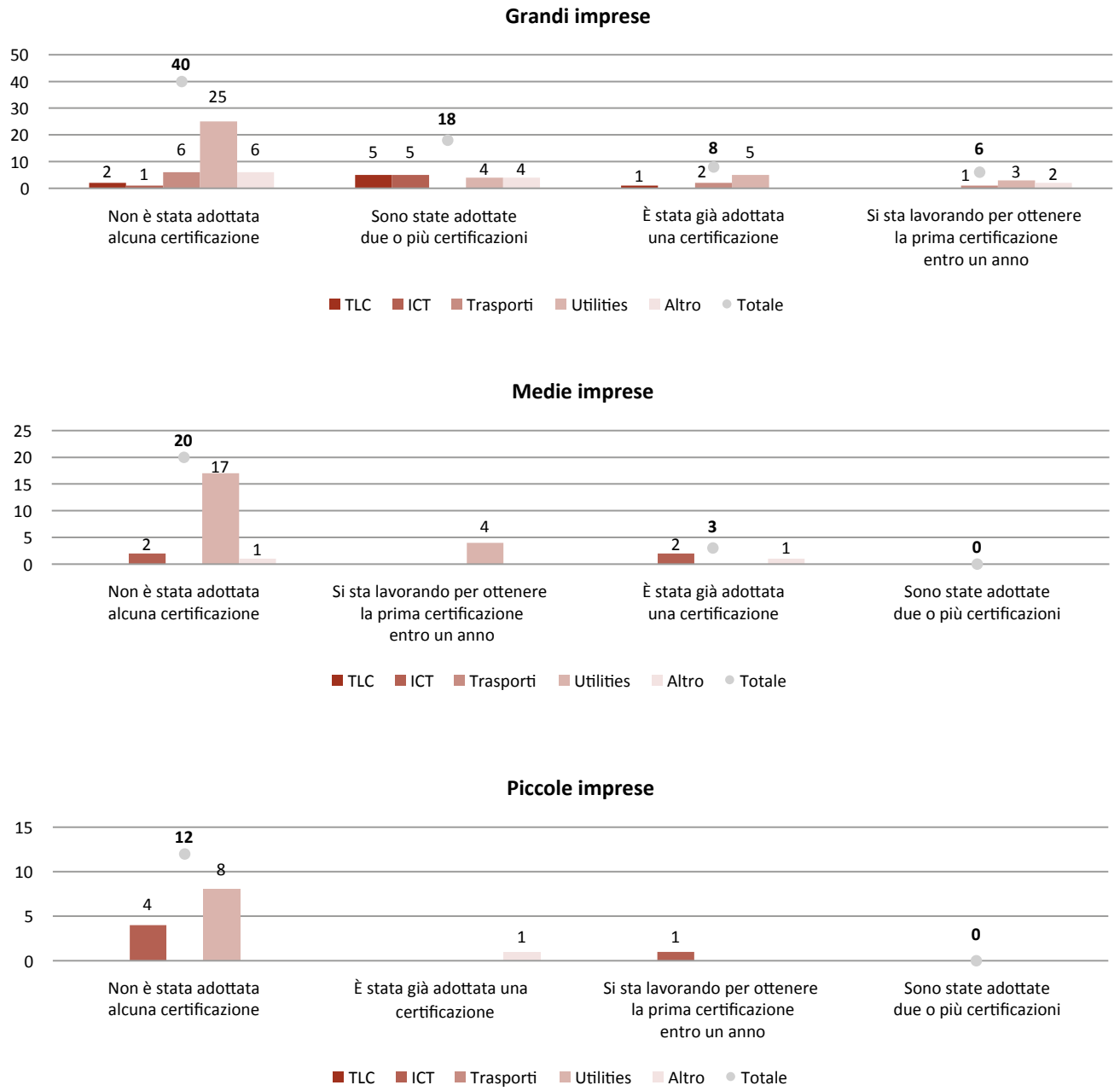
del processo normativo. Quest'ultima opzione non è stata particolarmente selezionata dalle PMI, che piuttosto hanno insistito sullo snellimento degli obblighi imposti dalle normative di cybersicurezza. La riposta meno gettonata (5%) – e che riguarda unicamente grandi imprese – è stata quella di richiedere più requisiti di sicurezza di quelli già previsti.

In merito all'adozione di una o più **certificazioni volontarie di cybersicurezza** (Fig. 4.13), si può osservare che **la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione**. Tuttavia, **considerando solo le grandi imprese rispondenti, il 36% delle stesse ha già adottato una o più certificazioni di cybersecurity, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno**. Di converso, tra le medie imprese i risultati sono ben diversi, in quanto un mero 11% ha acquisito almeno una certificazione, mentre il 14% intende ottenere la prima certificazione entro un anno. Quanto alle piccole imprese, solo 1 ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno.

Analizzando anche lo spaccato settoriale, **le utilities spiccano per numero tra le grandi imprese che hanno adottato una o più certificazioni (9); viceversa, le aziende dei trasporti chiudono la classifica con 2 soggetti**, i quali hanno adottato un'unica certificazione. Con riferimento alle medie imprese, quelle del settore ICT sono le più numerose con una certificazione, mentre è interessante notare che – al pari delle piccole imprese – nessuna abbia ottenuto due o più certificazioni.

Fig. 4.13: Qual è la posizione della sua impresa circa le certificazioni volontarie di cybersicurezza (es: Common Criteria/NESAS)?

Note: Possibilità di un'unica risposta
Totale rispondenti: 113 su 145
Fonte: Elaborazioni I-Com



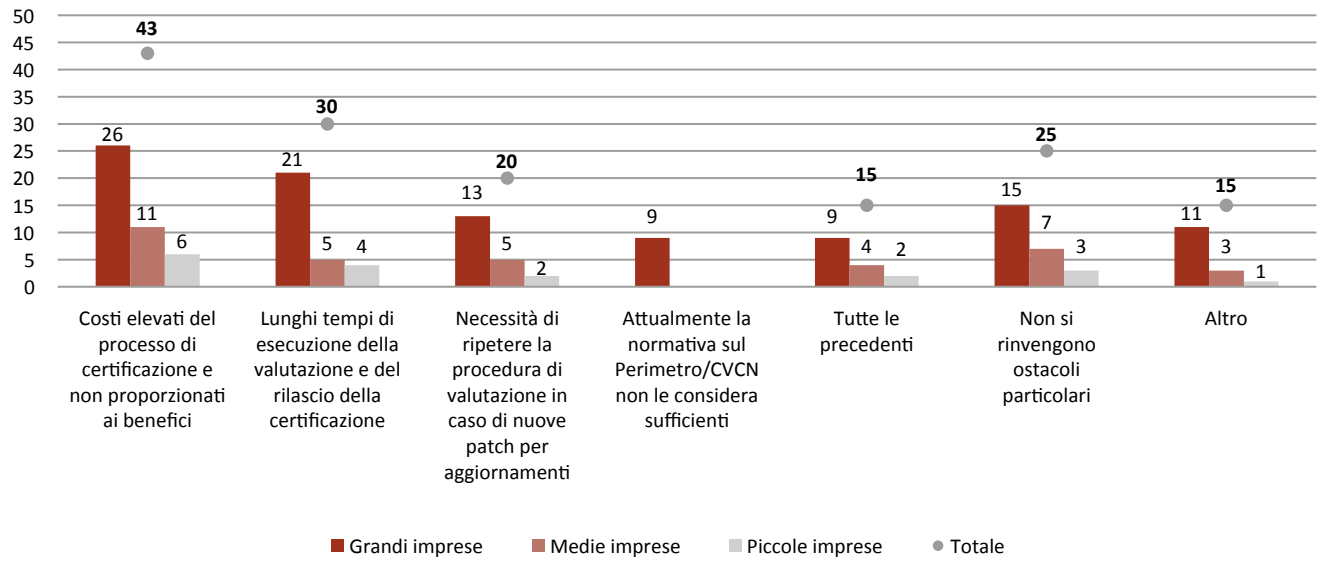
Con riguardo al tipo di certificazioni adottate, prevale nettamente la ISO27001, che interessa sostanzialmente tutti i rispondenti che hanno ottenuto almeno una certificazione, talvolta accompagnata da altre appartenenti alla famiglia delle ISO27000 – in particolar modo 27017 e 27018 – e dalla ISO23301. Altre tipologie indicate sono CSA Star Level One, SECAM e SOC 2.

I risultati della domanda precedente possono trovare una motivazione negli **ostacoli che sono percepiti dalle imprese con riguardo all'ottenimento di una certificazione volontaria di cybersecurity** (Fig. 4.14). In primo luogo, **il principale intralcio (38% dei rispondenti) risiede nei costi elevati del processo di certificazione, che non sono percepiti come proporzionati ai benefici** che ne possono conseguire. In secondo luogo, quasi **il 27% sostiene che i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi**. In terzo luogo, circa il 18% ritiene che la necessità di ripetere la procedura di valutazione in caso di nuove *patch* per aggiornamenti sia uno degli aspetti che limitano il perseguimento di una certificazione di cybersicurezza.

È interessante notare come il fatto che le certificazioni volontarie non siano considerate sufficienti dalla normativa sul PSNC e, in particolare, nell'ambito della procedura di *testing* dinanzi al CVCN, sia percepito come un ostacolo solo dall'8% dei rispondenti, tutti afferenti alle grandi imprese. Diversamente, il 22% delle imprese non rinviene difficoltà particolari nell'ottenimento di una certificazione. Nell'ambito della voce "Altro" è piuttosto ricorrente la mancanza di competenze e personale appositamente dedicato a curare l'intero processo di certificazione, così come pure rileva il caso in cui la scelta aziendale sia di perseguire certificazioni solo per il *core business* (*client facing*).

Fig. 4.14: Quali ritiene siano i principali ostacoli con riferimento al perseguimento di una certificazione volontaria di cibersicurezza?

Note: Possibilità di più risposte
Totale rispondenti: 112 su 145
Fonte: Elaborazioni I-Com



Tra coloro che hanno dichiarato di **aver adottato almeno una certificazione, i principali effetti direttamente riconducibili ad essa sono stati** (Fig. 4.15): un **miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders** (45% dei rispondenti), una **maggiore consapevolezza dei dipendenti e dei collaboratori esterni** (39,7%) e **più possibilità di partecipare a bandi di gara pubblici o** privati (29,5%). Peraltro, è interessante evidenziare come oltre il 15% dei rispondenti non abbia valutato effetti direttamente riconducibili all'ottenimento della certificazione. Inoltre, si può osservare come solo le grandi imprese abbiano registrato un impatto degli incidenti di sicurezza più contenuto per le attività di impresa successivamente all'adozione di una certificazione di cybersecurity.

Dalla domanda successiva (Fig. 4.16) emerge che, indipendentemente dal fatto che l'impresa abbia adottato o intenda adottare una certificazione di cybersicurezza, **il 70% dei rispondenti è parzialmente o totalmente d'accordo in merito al fatto che standard comunitari – come gli *European Common Criteria-based cybersecurity certification scheme* (EUCC)**, attualmente in fase di consultazione pubblica sino al prossimo 31 ottobre – **possano incentivare il ricorso a tali strumenti**. Non sorprende che le imprese silenti sul tema raggiungano quasi il 23%, con una prevalenza di quelle di medie e piccole dimensioni.

Tra le motivazioni correlate alle risposte pervenute e che accolgono con favore standard di certificazione a livello comunitario, viene sottolineato che – **se questi ultimi condividono una base comune di requisiti**

Fig. 4.15: Qualora la sua organizzazione abbia adottato almeno una certificazione di cybersecurity, quali sono stati i principali effetti direttamente riconducibili ad essa?

Note: Possibilità di max. 4 risposte
Totale rispondenti: 78 su 145; chi ha risposto "altro", ha precisato esclusivamente di non aver acquisito alcuna certificazione
Fonte: Elaborazione I-Com

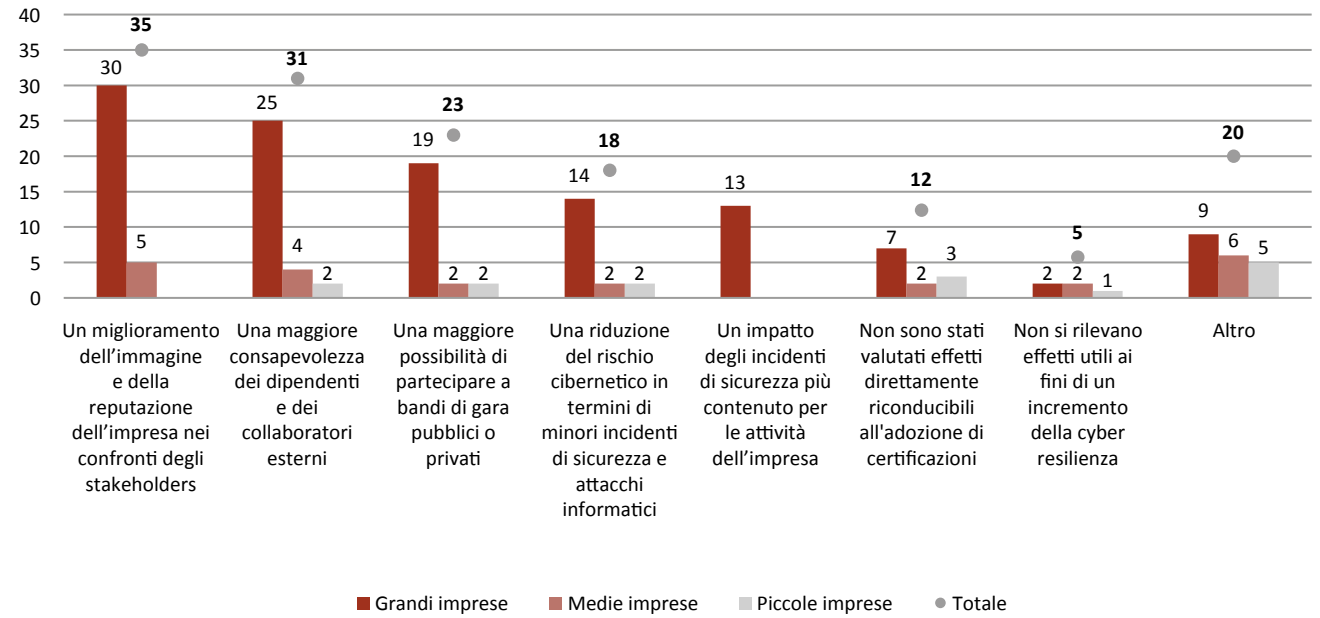


Fig. 4.16: Indipendentemente dal fatto che la sua organizzazione ha adottato o intenda adottare una certificazione di sicurezza informatica, ritiene che standard comunitari (es: EUCC) possano incentivare il ricorso a tali strumenti?

Note: Possibilità di un'unica risposta
Totale rispondenti: 114 su 145
Fonte: Elaborazione I-Com

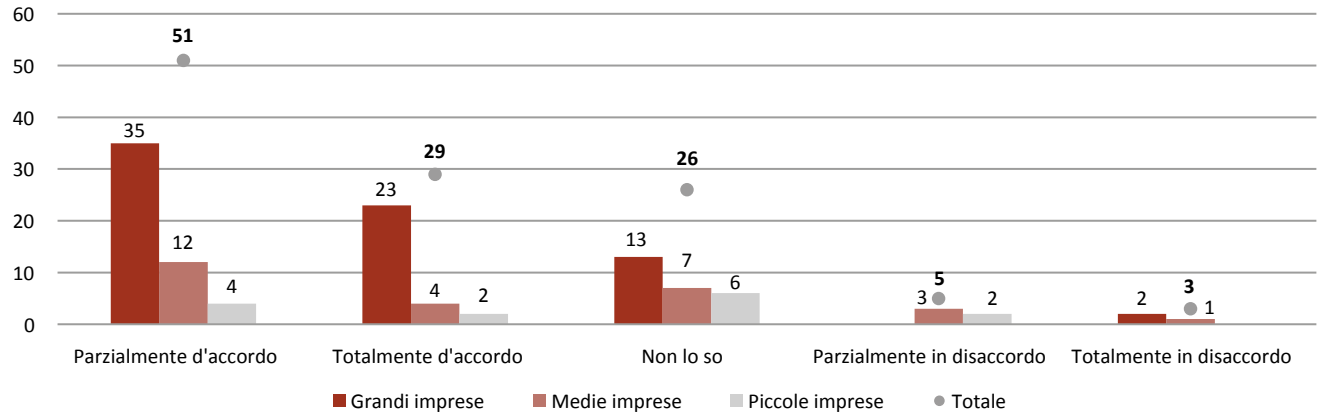
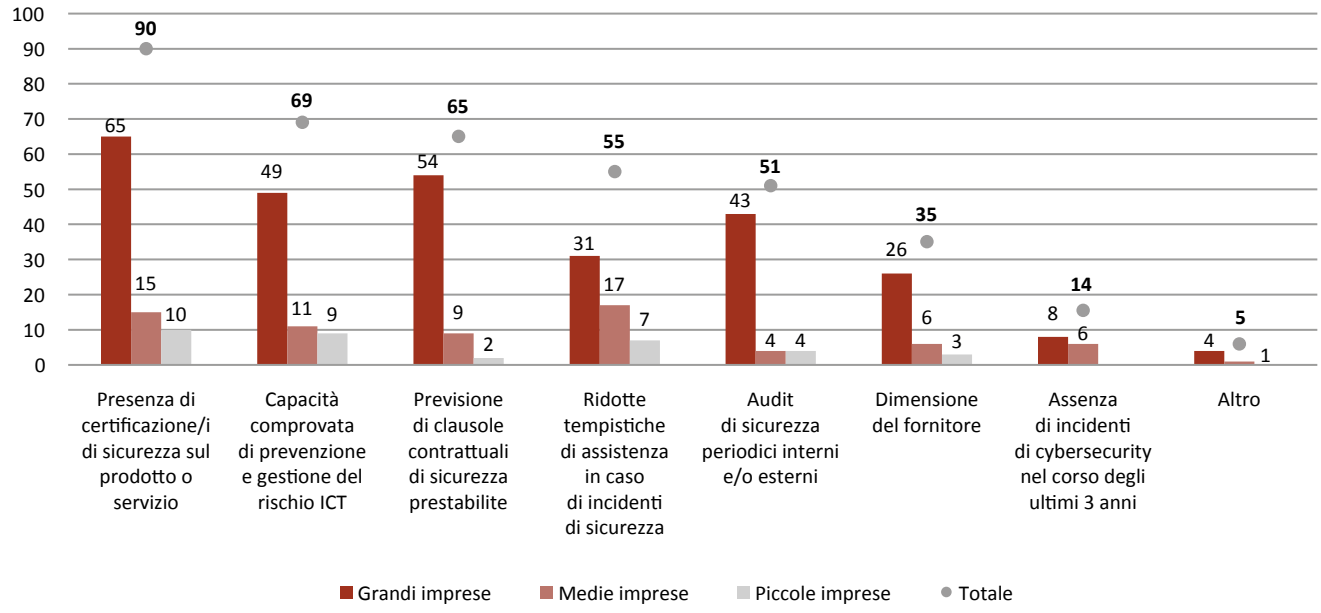


Fig. 4.17: Nella scelta di un fornitore che eroghi servizi o fornisca prodotti Ict, la sua organizzazione ne valuta la rispettiva affidabilità secondo quali parametri?

Note: Possibilità di più risposte
Totale rispondenti: 113 su 145
Fonte: Elaborazione I-Com

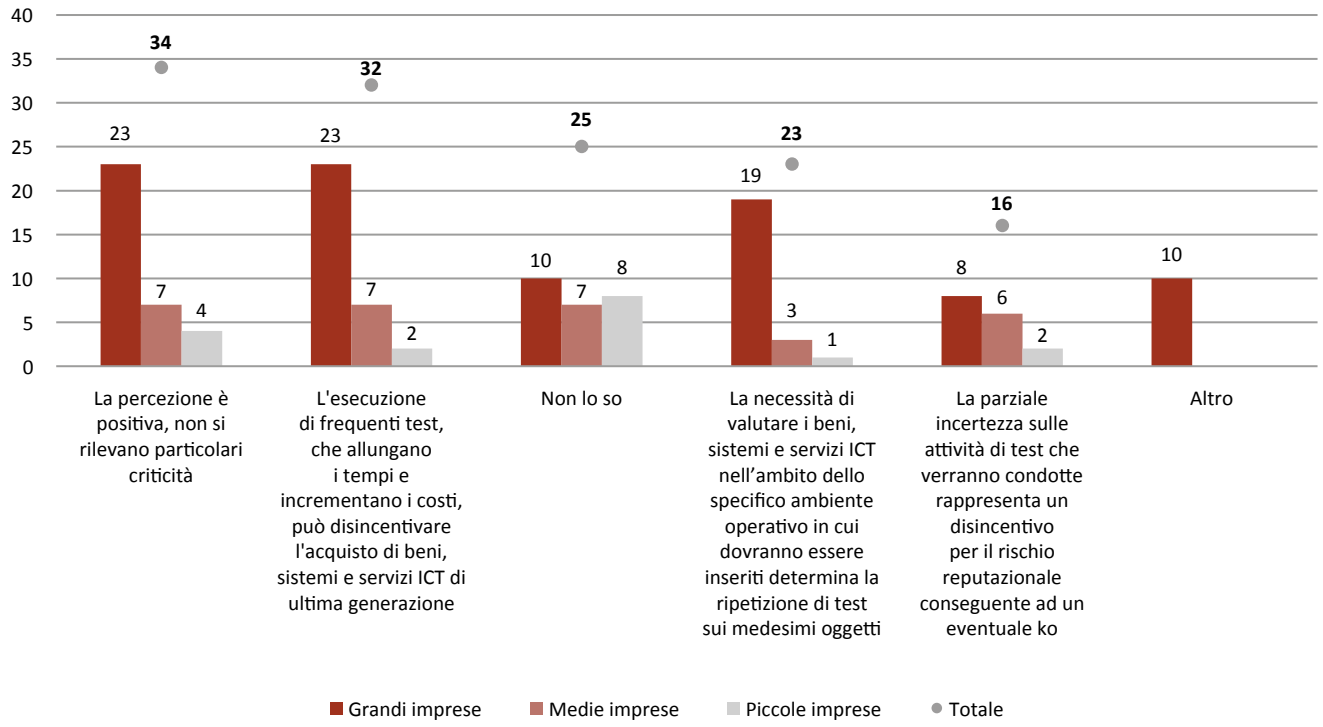


– possono comportare una serie di vantaggi inerenti, fra l'altro, una più corretta gestione delle scelte aziendali, che passa anche per una maggiore proceduralizzazione dei processi interni, oltre a uniformare e chiarire in modo trasparente e pubblicamente accessibile i requisiti di sicurezza comuni. Di converso, è stato segnalato che la complessità del procedimento per ottenere e mantenere nel tempo i Common Criteria possa rendere più difficile la creazione di una cultura aziendale, per cui si ritengono maggiormente adeguati gli standard della famiglia ISO 27000.

Inoltre, agli intervistati è stato chiesto di indicare i **principali parametri che prendono in considerazione nella scelta di un fornitore che eroghi servizi o fornisca prodotti Ict** (Fig. 4.17). A riprova dell'importanza della standardizzazione in tale ambito, **il 79,6% dei rispondenti valuta la presenza di certificazioni di sicurezza sul prodotto o servizio, seguita dalla capacità comprovata di prevenire e gestire il rischio Ict (61%) e dalla previsione di clausole contrattuali di sicurezza prestabilite (57,5%)**. Diversamente, per le medie imprese intervistate rilevano maggiormente tempistiche ridotte di assistenza in caso di incidenti di sicurezza, opzione selezionata dal 48,6% del totale dei rispondenti, di cui il 63% sono aziende di medie dimensioni. Il parametro meno considerato per la scelta di un

Fig. 4.18: Ai sensi della disciplina sul Perimetro di Sicurezza Nazionale Cibernetica, il CVCN può prescrivere dei test per valutare la sicurezza di beni, sistemi e servizi Ict dei soggetti inseriti nell'ambito del perimetro stesso. Quale è la vostra attuale percezione?

Note: Possibilità di max. 3 risposte
Totale rispondenti: 110 su 145
Fonte: Elaborazione I-Com



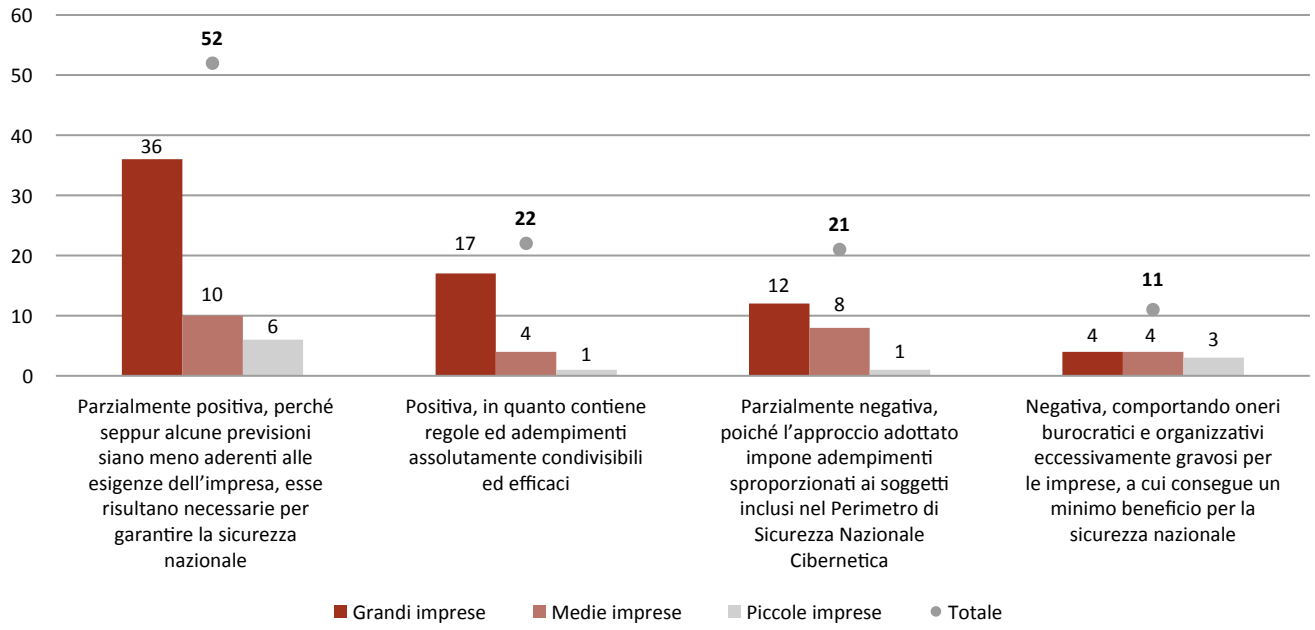
fornitore Ict (12,4%) concerne l'assenza di incidenti di cybersecurity nel corso degli ultimi 3 anni.

L'ultima sezione della presente indagine riguarda più nello specifico alcuni aspetti connessi al Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e alle attività del Centro di Valutazione e Certificazione Nazionale (CVCN). Più nel dettaglio, la prima domanda chiede alle imprese la loro **percezione rispetto ai test prescritti dal CVCN sui beni, sistemi e servizi Ict** di rispettiva pertinenza (Fig. 4.18) ed è emerso che **per il 30% dei rispondenti non si rilevano particolari criticità in tal senso, mentre il 22,7% non ha espresso un'opinione in merito**. La restante quota di feedback pervenuti evidenzia, invece, alcune problematiche: **32 soggetti ritengono che l'esecuzione di frequenti test, che allungano i tempi e incrementano i costi, possa disincentivare l'acquisto di "beni Ict" di ultima generazione; 23 aziende convengono che la necessità di esaminare tali beni Ict nel relativo ambiente operativo determini la ripetizione di test sugli stessi beni; 16 imprese si preoccupano che la parziale incertezza sulle attività di valutazione possa rappresentare un disincentivo dato il rischio reputazionale conseguente a un eventuale ko**.

Il grafico successivo (Fig. 4.19) riassume le diverse posizioni dei rispondenti con riferimento a una **valutazione complessiva della disciplina sul PSNC**. Più nel dettaglio, è possibile osservare come **il 20,7%, soprattutto grandi imprese, si ritenga assolutamente soddisfatto dalle regole e dagli adempimenti previsti nell'ambito del Perimetro**. Parallelamente, poco **più del 10% considera tale normativa come eccessivamente gravosa**,

Fig. 4.19: La disciplina sul Perimetro di Sicurezza Nazionale Cibernetica è ormai giunta a completamento e sono partite le attività del CVCN, in attesa dell'accreditamento dei LAP. Qual è la vostra percezione attuale?

Note: Possibilità di un'unica risposta
Totale rispondenti: 106 su 145
Fonte: Elaborazione I-Com



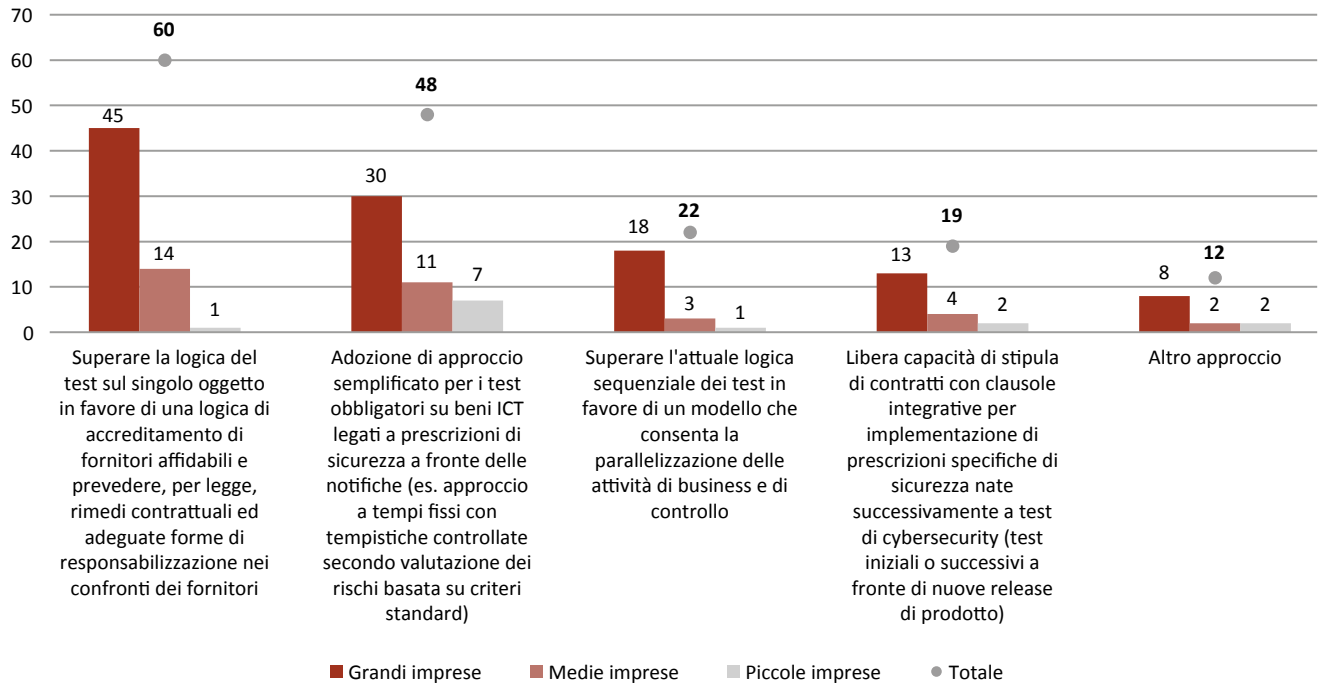
recando solo un minimo beneficio per la sicurezza nazionale. Invece, **il restante 68,8% si colloca nel mezzo**. Il maggior numero, 52 imprese, ha una percezione parzialmente positiva, poiché ritiene che gli adempimenti richiesti – seppur meno aderenti alle esigenze aziendali – siano funzionali a garantire la sicurezza nazionale. Di converso, 21 rispondenti hanno denunciato che l'approccio adottato impone adempimenti sproporzionati ai soggetti inclusi nel Perimetro.

L'ultima domanda del questionario richiede agli intervistati di proporre alcuni **aspetti su cui insistere per migliorare l'ecosistema della cibersicurezza in Italia** (Fig. 4.20). Sul punto, **60 rispondenti ritengono sia opportuno superare la logica del test sul singolo oggetto in favore di una logica di accreditamento dei fornitori affidabili, prevedendo rimedi contrattuali per legge e adeguate forme di responsabilizzazione nei confronti dei fornitori stessi**. Anche la semplificazione dei test obbligatori sui beni ICT, introducendo – ad esempio – un approccio a tempi fissi con tempistiche controllate secondo una valutazione dei rischi basata su criteri standard, ha incontrato un importante consenso tra i rispondenti, precisamente 48, di cui ben 7 piccole imprese.

Con riguardo agli altri approcci proposti dalle imprese intervistate, pare opportuno fare riferimento **all'armonizzazione dei requisiti delle normative in materia di cybersicurezza, a una maggiore considerazione delle certificazioni a norma del Cybersecurity Act per la procedura di valutazione dinanzi al CVCN, oltre che a un effettivo riconoscimento sul mercato del costo necessario per garantire un elevato livello di cibersicurezza dei prodotti e servizi ICT**.

Fig. 4.20: Quali ulteriori aspetti andrebbero considerati per migliorare lo stato della cybersecurity in Italia?

Note: Possibilità di più risposte
Totale rispondenti: 108 su 145
Fonte: Elaborazione I-Com



4.3. CONCLUSIONI DELL'INDAGINE

L'aggravarsi dello scenario relativo all'evoluzione delle minacce cibernetiche nel corso degli ultimi anni sta avendo impatti negativi a livello globale, europeo e nazionale, con innegabili ripercussioni sulla sicurezza dello Stato e sulle attività di business delle imprese. Ciò vale in particolar modo per le PMI, che spesso non hanno né le necessarie risorse umane, finanziarie e tecnologiche per fronteggiare adeguatamente tali minacce, né per ottemperare ai numerosi, e a volte eterogenei, adempimenti posti dal legislatore europeo e italiano per garantire un elevato livello di cybersicurezza delle reti, dei sistemi e dei servizi Ict.
L'indagine condotta dall'Istituto per la Competitività ha evidenziato, innanzitutto, che **la maggior parte dei rispondenti ritiene che il crescente numero di adempimenti previsti dalle normative in cybersicurezza può impattare sulla competitività aziendale** principalmente a causa degli oneri burocratici e amministrativi richiesti, nonché per gli investimenti tecnico-organizzativi necessari alla compliance, il che **può avere ripercussioni anche sui rapporti con la supply chain, con l'ulteriore conseguenza – evidenziata da 18 rispondenti tra grandi, medie e piccole imprese – che vi sia il rischio di rallentare la digitalizzazione e non far concepire la cybersicurezza come un fattore abilitativo al digitale**.
Le imprese partecipanti hanno anche indicato i principali fattori che rendono difficoltoso il processo di compliance, con specifico riferimento alla **mancanza di competenze idonee sia internamente, sia sul mercato del lavoro** (60 risposte in totale), seguito dall'incertezza interpretativa della normativa (52 risposte) e alla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (48 risposte). Pertanto, alcune imprese ritengono utile un maggiore sforzo, fra l'altro, a supporto delle PMI e verso l'accrescimento del grado di consapevolezza in materia cyber dei livelli apicali e di indirizzo strategico. **Interessante la proposta di un "Codice della Sicurezza Digitale" che funga da compendio per le diverse regolamentazioni di settore, da aggiornarsi progressivamente**. Altro dato di fondamentale rilievo riguarda le risorse economiche dedicate specificamente alla cybersicurezza, per cui è emerso che **quasi i due terzi dei rispondenti assegnino meno del 5% del budget IT alla cybersecurity**. Inoltre, appare rilevante evidenziare che circa il 57% delle piccole imprese riconosca una quota di personale appositamente dedicato alla cyber uguale o inferiore all'1% rispetto agli FTE impiegati in ambito IT. Per di più, nonostante lo scenario non sia propriamente ottimistico e considerando che le direttive NIS2 e CER siano ormai in vigore da mesi e che tra un anno saranno pienamente applicabili (dal 18 ottobre 2024), **il 51,2% delle imprese rispondenti sta ancora valutando se incrementare le risorse destinate alla cibersicurezza e il 12,6% ha deciso di non stanziare ulteriori risorse**.
Una parte corposa dell'indagine si è soffermata sulle certificazioni volontarie di cybersecurity ed è emerso che **il maggior numero di imprese afferenti alle tre classi dimensionali considerate non ha conseguito alcun tipo di certificazione**. Ad ogni modo, tra le imprese che hanno adottato almeno uno standard di questo tipo quasi tutte hanno optato per la famiglia delle ISO27000, in particolare la ISO27001, 27017 e 27018, talvolta affiancate dalla ISO23301. Simili risultanze sarebbero giustificate – secondo il 38% dei rispondenti – dai costi elevati del processo di certificazione, che non sono percepiti come proporzionati ai benefici, nonché dai tempi troppo dilatati per giungere al rilascio della certificazione stessa (27%). Piuttosto rilevante sul punto è il segnale lanciato da alcuni soggetti intervistati, per cui uno scarso ricorso a tali strumenti sarebbe influenzato dalla mancanza di competenze interne e, in alcuni casi, dalle scelte aziendali di perseguire certificazioni solo per il *core business*, poiché *client facing*. **Appare incoraggiante, invece, che il 70% dei rispondenti sia d'accordo in merito al fatto che standard comunitari (es. EUCC)**

possano incentivare le imprese a certificarsi.

Peraltro, **nella scelta di un fornitore che eroghi servizi o fornisca prodotti ICT il 79,6% dei rispondenti valuta la presenza di certificazioni di sicurezza sul prodotto o servizio**. È interessante notare come tra gli altri parametri indicati dai partecipanti vi sia la conoscenza del contesto, la postura di cybersicurezza, nonché l'*expertising* nel campo delle infrastrutture critiche e la conformità a normative europee di settore. Uno degli aspetti più interessanti dell'indagine riguarda i modi con cui gli intervistati ritengono sia possibile migliorare lo stato della cibersicurezza in Italia. Sul punto, sono state poste due domande: la prima più generale e la seconda maggiormente focalizzata sul Perimetro di Sicurezza Nazionale Cibernetica e i test dinanzi al CVCN. Quanto alla prima, **l'81% dei rispondenti sostiene che si debba puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze**. Tale opzione è risultata la più selezionata da tutte e tre le classi dimensionali considerate, a conferma del fatto che si tratti di un aspetto particolarmente sentito nel Paese.

Tra le altre proposte avanzate dai partecipanti vi è quella **di incentivare la collaborazione internazionale e rafforzare la sinergia con il CSIRT Italia per realizzare un servizio nazionale di *threat intelligence***, che possa essere alimentato anche dai soggetti privati, al fine di avere una quanto più ampia consapevolezza situazionale possibile. Di rilievo, anche il suggerimento circa l'assegnazione della responsabilità ai *vendor* e ai produttori di hardware e software, affinché garantiscano il supporto ai prodotti per periodi di tempo adeguati a consentire alle aziende la gestione del ciclo di vita degli stessi. Più nel dettaglio, la cosiddetta *End of Sale* (EoS) dovrebbe essere almeno 5 anni prima della *End of Maintenance* (EoM).

Con riguardo alla seconda domanda in tema, partendo dal presupposto che poco più del 20% dei rispondenti, in larga parte grandi imprese, si è dichiarato assolutamente soddisfatto dalle regole e dagli adempimenti previsti per i soggetti inclusi nel PSNC, **per oltre il 55% dei rispondenti sarebbe opportuno superare la logica dei test obbligatori dinanzi al CVCN in favore dell'accreditamento dei fornitori di fiducia**, prevedendo, al contempo, rimedi contrattuali per legge, nonché adeguate forme di responsabilizzazione nei confronti dei fornitori stessi, oppure – come espresso dal 44% – optare per un approccio semplificato con tempistiche controllate secondo una valutazione dei rischi basata su criteri standard.

Appaiono particolarmente interessanti anche gli spunti che evidenziano **come l'esecuzione di frequenti test, che allungano i tempi e incrementano i costi, possa avere effetti negativi sul *time-to-market* delle imprese**, come complicare la programmazione circa l'acquisto di soluzioni tecnologiche aggiornate e più performanti anche in termini di sicurezza, oltre che poter causare un danno di immagine alla concezione che hanno gli operatori della cybersecurity, la quale potrebbe essere percepita come un fattore ostativo e non abilitante alla digitalizzazione e all'innovazione. Meritevole di attenzione anche la proposta di **incentivare l'utilizzo di certificazioni della cybersicurezza di prodotti ICT ai sensi del Cybersecurity Act, prevedendo una semplificazione della procedura di valutazione del CVCN**, qualora l'operatore acquisti un prodotto già certificato.

In conclusione, dai risultati dell'indagine si può affermare che la cybersicurezza, ad oggi, rappresenti sempre più un elemento imprescindibile nei processi decisionali delle imprese. Queste ultime si muovono in un panorama costituito da minacce e strumenti per combatterle, di natura legislativa oltre che tecnica, per cui al fine di affrontare al meglio le nuove sfide del cyberspazio appare necessario puntare sull'aumento delle competenze e della consapevolezza, senza sottovalutare l'importanza dell'istaurazione di un continuo dialogo partecipato tra privati e istituzioni, affinché le prassi e le prescrizioni normative non diventino un ostacolo, ma un ombrello protettivo per i destinatari delle stesse.

icom
istituto per la competitività

CAPITOLO 5

LA CYBERSICUREZZA ALLA BASE DELLA COOPERAZIONE TRA PUBBLICO E PRIVATO

5.1. IL PARTENARIATO PUBBLICO-PRIVATO (PPP) APPLICATO ALLA SICUREZZA INFORMATICA: VANTAGGI E CRITICITÀ

Il Partenariato Pubblico-Privato (PPP) è richiamato dalla Strategia Nazionale di Cybersicurezza 2022-2026 e dal relativo Piano di Implementazione come elemento traversale agli obiettivi di protezione, risposta e sviluppo, nonché ai fattori abilitanti della formazione, della promozione della cultura della cybersicurezza e della cooperazione. Difatti, secondo un approccio c.d. "*whole-of-society*" che caratterizza la Strategia, il settore pubblico è tenuto a collaborare con quello privato, il mondo accademico e della ricerca, i media e i cittadini al fine di rafforzare la resilienza cibernetica dell'intero sistema Paese. Peraltro, i prodotti e i servizi ICT sono realizzati o erogati principalmente da soggetti privati, per cui la collaborazione strutturata e costante tra pubblico e privato è oggigiorno imprescindibile.

Sulla base di tali premesse, il Piano di implementazione succitato si riferisce esplicitamente al PPP all'interno della misura #64, dove prescrive che vadano previsti incentivi per lo sviluppo di startup operanti nel settore della cybersecurity e partenariati con aziende del settore a conduzione femminile, oltre che con riferimento alle iniziative in tema di cybersecurity *awareness* e di sviluppo della ricerca.

Il Codice dei Contratti Pubblici, riformato di recente attraverso il d. lgs. n. 36/2023, contiene una disciplina organica del partenariato pubblico-privato, che era del tutto assente nel d. lgs. n. 163/2006 e meno strutturata nella precedente normativa in materia, ossia il d. lgs. n. 50/2016. In sostanza, l'istituto del PPP è l'insieme di modelli di collaborazione tra il settore pubblico e privato e può essere utilizzato in tutti quei casi in cui il primo intenda realizzare un progetto che coinvolga un'opera pubblica o di pubblica utilità, la cui progettazione, realizzazione, gestione e finanziamento – in tutto o in parte – vengano affidati al settore privato.

Più nel dettaglio, con l'ultima riforma è stata introdotta una nuova nozione di partenariato (art. 174) nell'ambito della quale lo si definisce, innanzitutto, come un'operazione economica e non più avente necessariamente la forma contrattuale. Ciò è di fondamentale importanza sul piano applicativo, anche in ottica dell'attuazione delle misure previste dal PNRR, in quanto agevola il ricorso a questo istituto senza dover per forza di cose formalizzare un contratto tra le parti.

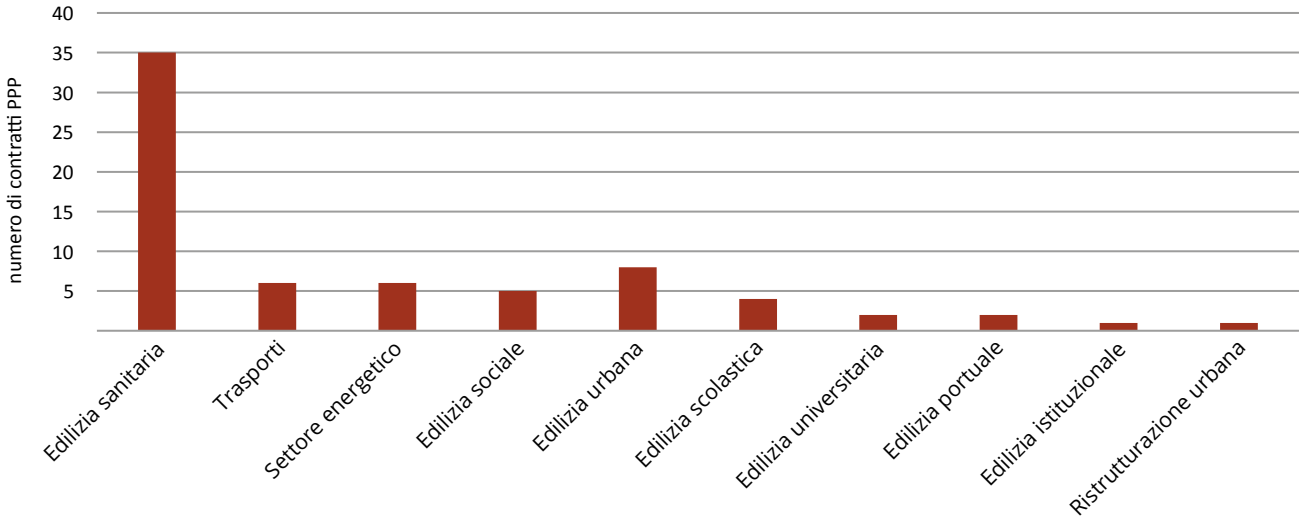
Inoltre, affinché un'operazione economica possa essere ricompresa nella definizione di PPP devono ricorrere le seguenti condizioni: a) l'instaurazione di un rapporto contrattuale di lungo periodo tra un ente concedente[49] e uno o più operatori economici privati, al fine di raggiungere un risultato di interesse pubblico; b) le risorse finanziarie connesse alla realizzazione del progetto provengono – in misura significativa – dalla parte privata; c) la parte privata ha il compito di realizzare e gestire il progetto, mentre quella pubblica definisce gli obiettivi e ne verifica l'attuazione; d) il rischio operativo è allocato in capo al soggetto privato.

In Italia, il Dipartimento per la programmazione e il coordinamento della politica economica (DIPE) si occupa di coordinare una raccolta di dati di monitoraggio dell'adozione di contratti di partenariato, condotta con ISTAT. Nell'edizione di luglio 2023, si monitorano le caratteristiche e l'esito di PPP nel periodo 2010-2022. In undici anni, sono stati siglati 70 accordi di partenariato, di cui la metà nel settore dell'edilizia sanitaria.

49 Amministrazioni aggiudicatrici o enti aggiudicatori di cui all'articolo 1 della direttiva 2014/23/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014.

Fig. 5.1: Numero di contratti PPP monitorati da ISTAT per settore economico prevalente (2010-2022)

Fonte: DIPE



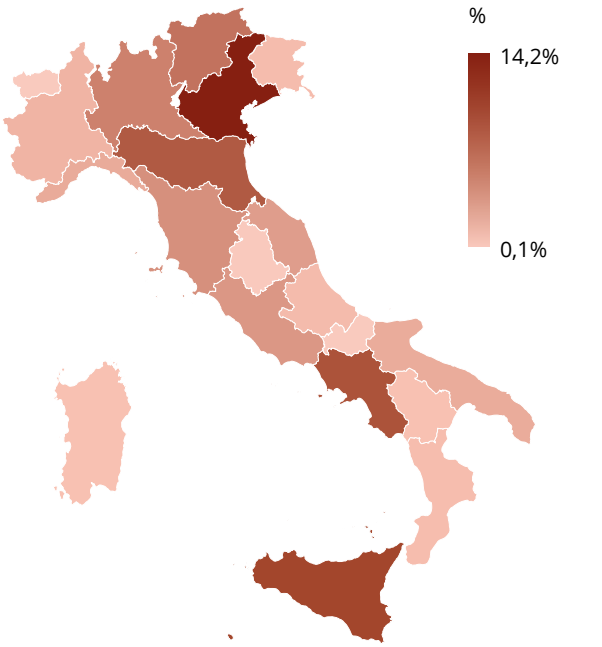
Il valore totale dei 70 contratti è pari a circa €11,2 miliardi, mentre il valore medio di ciascun contratto si attesta sui €162 milioni. Sebbene l'edilizia sanitaria sia il settore con più contratti di PPP all'attivo, è il settore dei trasporti ad aver assorbito più della metà dell'importo complessivo stanziato tramite PPP. Solamente cinque progetti afferenti al settore del trasporto urbano hanno mobilitato circa €4,4 miliardi di investimenti in undici anni, mentre l'unico progetto nel settore del trasporto extra-urbano ha avuto un valore di €2,3 miliardi. I 35 contratti di edilizia sanitaria hanno invece generato investimenti di poco inferiori a €4 miliardi di euro, con un valore medio per progetto di circa €110-115 milioni. In riferimento ai soggetti concedenti, prevalgono le Aziende Sanitarie Locali (ASL), Unità Socio-Sanitaria Locale (USSL) e aziende ospedaliere (44%); seguono i Comuni (38%) e le Regioni (10%).

Esaminando la distribuzione regionale delle risorse mobilitate con contratti di PPP nel periodo 2002-2021, le regioni Veneto, Sicilia e Campania risultano le destinatarie degli investimenti più sostanziosi. Fra le tre macroaree del paese, prevale il Settentrione per risorse mobilitate (43% delle risorse totali destinate a PPP in 19 anni), mentre il Centro appare la destinazione dove si sono attivati contratti per valore complessivo minore (13%). Al Meridione sono state destinate il 27% delle risorse, mentre a progetti di interesse strategico nazionale che riguardano diverse regioni è stato destinato il 16% degli importi complessivi dei contratti PPP.

Le tempistiche totali di avvio del contratto di PPP si calcolano partendo dalla richiesta di dati da parte dell'operatore economico fino ad arrivare all'aggiudicazione della gara pubblica. Le tappe intermedie a questo processo sono: la predisposizione della proposta di PPP (in capo all'operatore economico interessato), la valutazione della proposta di PPP (compito della PA), l'indizione della gara pubblica (PA), l'elaborazione delle offerte pervenute (PA) e l'aggiudicazione della gara (PA). Dall'esperienza di operatori economici, in media, nel periodo 2016-2022, lo svolgimento dell'intero processo ha richiesto circa due anni e tre mesi.

Fig. 5.2: Distribuzione territoriale dei contratti PPP per valore economico regionale rapportato al numero di operazioni regionali (2002-2021)

Fonte: DIPE



Sebbene si rilevi un progressivo miglioramento, le tempistiche di attuazione di alcune fasi risultano ancora troppo lunghe, specialmente in relazione alla valutazione delle proposte e all'indizione della gara. Tempi troppo prolungati rischiano di disincentivare gli operatori privati a presentare proposte di PPP, riducendo il potenziale di questo strumento. Proprio per tali ragioni, il 19 maggio 2022 è stata emanata un'apposita circolare del Presidente del Consiglio dei Ministri con cui si sono definite nuove modalità per comunicare l'avvenuta stipula di operazioni di PPP ed è stato abilitato l'utilizzo di un portale web dedicato per i soggetti aggiudicatori[50], riducendo in tal modo l'onere di trasmissione a carico delle amministrazioni aggiudicatrici.

Il DIPE stesso ha riassunto i vantaggi e le criticità per le Pubbliche Amministrazioni che si riscontrano dall'adozione dei PPP.

Fra i vantaggi, si cita:

- l'incremento del potenziale di dotazione infrastrutturale a parità di risorse pubbliche impiegate;
- l'ottimizzazione della gestione delle diverse attività riguardanti il progetto attraverso il coinvolgimento di soggetti specializzati;
- il miglioramento dell'efficacia della fase di programmazione degli interventi;
- la razionalizzazione del processo di identificazione degli investimenti;
- la ripartizione dei rischi e dei ricavi secondo le possibilità e le esigenze dei partecipanti al progetto;
- il maggiore coinvolgimento dei soggetti finanziatori al successo dell'iniziativa.

Le criticità individuate sono invece:

- la complessità del procedimento di identificazione e corretta allocazione dei rischi tra le parti;
- i maggiori costi di strutturazione dell'operazione;
- l'assenza di preliminari verifiche sulla reale convenienza del ricorso al PPP;
- la scarsa capacità delle amministrazioni pubbliche nel confrontarsi con la controparte privata.

Se questi sono i risultati del monitoraggio del DIPE sul partenariato pubblico-privato nel nostro Paese, è evidente che vi sia un'assenza importante: la cybersicurezza. Difatti, nonostante sussistano alcuni esempi rilevanti di PPP in ambito cybersecurity soprattutto nel contesto dei Centri di Competenza riconosciuti dal MISE (si v. *infra*), questi non sono stati tenuti in considerazione nel monitoraggio appena descritto, in parte perché sono state considerate

50 https://ppp.rgs.mef.gov.it/ppp.

unicamente le opere pubbliche dato che per queste ultime l'assegnazione del CUP[51] è tendenzialmente obbligatoria, mentre è facoltativa per le altre classi di investimenti pubblici[52].

Per altro verso, la motivazione di fondo potrebbe essere più ampia, ossia essere riconducibile a un problema culturale non limitato esclusivamente al tema della cibersicurezza, ma che si estende alla collaborazione tra pubblico e privato. Pertanto, appare utile fare riferimento in merito a un report dell'OSCE di marzo 2023[53], che si focalizza sulle pratiche emergenti in tema di PPP e altre forme di collaborazione in ambito cybersecurity.

Lo studio in questione si basa sulla misura n. 14 della decisione n. 1202/2016 dell'OSCE, secondo cui gli Stati partecipanti promuovono – su base volontaria – forme di partenariato pubblico-privato e sviluppano *best practice* comuni per rispondere alle sfide di sicurezza correlate all'utilizzo delle ICT. Il report summenzionato è il prodotto di una survey lanciata nel 2021 da un gruppo di sei Stati (tra cui figura l'Italia) per comprendere il livello di aderenza a questa specifica misura da parte dei membri dell'OSCE (ad oggi, 57 Paesi), i cui risultati sono stati suddivisi in quattro macro-aree: 1) *Purpose*; 2) Policy; 3) *Process*; 4) *People*.

Nella prima area, si pone l'accento sulla chiara e precisa finalità della collaborazione tra pubblico e privato per fronteggiare le sfide presenti e future correlate alla cybersicurezza. In particolare, se da un lato emerge che il ruolo dei soggetti privati è ritenuto molto importante poiché sono questi ultimi a sviluppare la maggior parte dei prodotti, servizi e tecnologie ICT utilizzate poi dalla compagine pubblica e governativa, dall'altro si registra una certa discrepanza di intenti da ambo le parti, a cui consegue una limitata fiducia reciproca. Tuttavia, solo da una più ampia comprensione dell'ecosistema nazionale di cibersicurezza (e quindi dei rispettivi punti di forza e di debolezza) è possibile garantire la resilienza, in particolar modo, delle PMI.

Per quanto concerne la seconda area (policy), se per un verso si osserva un crescente numero di Stati che si sono dotati di una strategia nazionale per la cybersicurezza in cui viene richiamata l'importanza del PPP (e, in alcuni casi, come svilupparlo nello specifico), è vero anche che si incontra una certa resistenza da parte di alcuni settori industriali di condividere regolarmente informazioni, tra cui risalta la segnalazione degli incidenti sulle reti e i sistemi di propria pertinenza.

In merito alla terza area (*process*), si fa riferimento alla previsione di una struttura di governance e all'implementazione di modalità ben precise per la collaborazione pubblico-privata, la cui fonte può essere direttamente la strategia nazionale o il relativo piano di implementazione, come nel caso dell'Italia, che rimandano a una serie di iniziative ad oggetto dei paragrafi successivi. Tuttavia, a differenza di altri Stati OSCE, l'Italia – come evidenziato dal monitoraggio del DIPE sui contratti di partenariato – non effettua una rilevazione sistematica e costante delle iniziative di PPP in ambito cybersicurezza, nonostante la riconosciuta importanza del tema da qualche anno a questa parte.

In ultimo, la quarta area (*people*) si concentra sulle *best practice* circa quali soggetti devono essere coinvolti e per quali finalità. Sul punto, viene menzionata l'Italia con la riforma degli ITS Academy (si v. *infra*) nell'ambito della quale viene riconosciuto un ruolo centrale alla cooperazione tra istituzioni nazionali e regionali, il mondo della scuola e dell'università, nonché dell'industria.

51 Il Codice Unico di Progetto (CUP) è il codice che identifica un progetto d'investimento pubblico ed è lo strumento cardine per il funzionamento del Sistema di Monitoraggio degli Investimenti Pubblici (MIP).

52 Cfr. "Relazione sull'attività svolta dal DIPE nell'anno 2021", DIPE (2022), p. 27.

53 Cfr. "Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States", OSCE (2023).

In definitiva, il report dell'OSCE qui brevemente descritto consente di affermare che il coinvolgimento del settore privato nella cybersecurity è un tema di primaria importanza per gli Stati intervistati, ma contestualmente vi sono una serie di ostacoli da superare in merito, ad esempio, a misure per incentivare partenariati pubblico-privati e il loro monitoraggio. Da questo punto di vista, l'obiettivo può essere raggiunto solo con un costante dialogo tra tutti gli stakeholder, incluse PMI, istituti di ricerca e soggetti che si occupano, in particolar modo, di infrastrutture critiche.

5.1.1. Le principali iniziative di PPP in ambito nazionale

Attraverso una ricognizione effettuata da I-Com nel **gennaio 2024**, è possibile segnalare le principali iniziative di PPP in cybersecurity che sono state avviate in Italia negli ultimi anni. Innanzitutto, va menzionato il **Polo Strategico Nazionale (PSN)**, ossia l'infrastruttura che ha l'obiettivo di dotare la PA di tecnologie e sistemi cloud che possano beneficiare di elevate garanzie di affidabilità, resilienza e indipendenza. Esso è gestito da un operatore economico selezionato attraverso l'avvio di un partenariato pubblico-privato ad iniziativa di un **soggetto proponente**[54]. La sua attivazione risale a **dicembre 2022** nelle sedi di Acilia e Pomezia nel Lazio, Rozzano e Santo Stefano Ticino in Lombardia. Il PSN ha permesso il completamento della **Missione 1, componente 1, investimento 1.1 Infrastrutture digitali del PNRR**, prevedendo come obiettivo di portare circa il **75% delle PA italiane** a utilizzare **servizi cloud** entro il 2026. Con **Decreto direttoriale n. 29/2023**, adottato dall'ACN d'intesa con il Dipartimento per la trasformazione digitale, sono state tracciate le tappe che definiscono le nuove modalità che imprese e amministrazioni devono seguire per avviare il nuovo percorso di qualificazione cloud.

In particolare, dal **19 gennaio 2023** la qualificazione dei servizi cloud per la PA è divenuta di **competenza dell'ACN**, che è subentrata all'**AgID**. L'Agenzia ha previsto un **regime transitorio fino al 31 luglio scorso**, durante il quale era possibile, nell'ambito del processo di vigilanza, revocare la qualifica al venir meno dei requisiti. Il 1° agosto ha avuto avvio il **regime ordinario** assieme al nuovo regolamento e alla procedura di qualificazione online, che prevede anche controlli sistematici per le qualifiche più elevate di sicurezza. Inoltre, sono stati promossi vari eventi su scala nazionale per rafforzare la consapevolezza e lo scambio di idee, come richiamato dal Piano di Implementazione dell'ACN. Tra essi vi è **Itasec**, la principale **conferenza nazionale sulla sicurezza informatica**, organizzata dal Cybersecurity National Lab del **CINI** (Consorzio interuniversitario nazionale per l'informatica). Il programma dell'anno scorso si è concentrato sui temi della sicurezza informatica, dell'IA, del *Quantum Security* e delle Tecnologie *Distributed Ledger*, mentre **l'edizione 2024** si terrà dall'8 all'11 aprile a Salerno. Altra iniziativa dello stesso genere è **CyberSec**, un evento promosso da **Cybersecurity Italia**, quotidiano online nato per aziende ed esperti interessati alla crescita coerente del sistema di sicurezza del Paese, delle PA e delle imprese, con l'obiettivo di interloquire con istituzioni, decisori politici, autorità regolamentari, addetti ai lavori, mondo dell'università e della ricerca. **La prossima conferenza avverrà a marzo 2024 e verterà particolarmente sul ruolo della cybersecurity nell'era dell'AI**.

Il **MUR** ha selezionato **quattordici** grandi **Partenariati estesi** alle università, ai centri di ricerca, alle aziende sul territorio, con l'obiettivo di finanziare - grazie a **€1,61 miliardi** all'interno della **Componente 2 "Dalla ricerca all' impresa" della Missione 4 "Istruzione e ricerca" del PNRR** - progetti per rafforzare le filiere della ricerca a livello nazionale e promuovere la loro

54 Il soggetto è composto da TIM, Leonardo, CDP Equity e Sogei.

partecipazione alle catene di valore strategiche europee e globali.

Nelle linee guida del MUR sono state previste **14 tematiche** su cui si sono incentrate, singolarmente, le proposte di Partenariato. Tra esse rinveniamo il tema dell'IA e quello della Cybersecurity, nuove tecnologie e tutela dei diritti, in cui è stata avanzata una proposta progettuale, da parte dell'Università degli Studi di Salerno (UNISA), dal titolo **"SEcurity and RIghts In the CyberSpace" (SERICS)**. Quest'ultima definisce un'ampia agenda di ricerca che abbraccia questioni tecniche, legali e sociali relative alla sicurezza e alla privacy, includendo i migliori ricercatori accademici e industriali con competenze significative per far crescere il settore. I progetti SERICS si articolano in **10 *spoke*** che si incentrano sui temi della cybersecurity in merito agli **aspetti umani, sociali e legali** (1); **disinformazione** (2); **attacchi e difese** (3); **sicurezza dei sistemi operativi e della virtualizzazione** (4); **crittografia e sicurezza dei sistemi distribuiti** (5); **sicurezza del software e delle piattaforme** (6); **sicurezza delle infrastrutture** (7); **gestione del rischio e governance** (8); **trasformazione digitale** (9) **protezione dei dati** (10). Ogni progetto è capeggiato da un proprio leader (tra questi primeggiano le Università) ed è supportato da alcuni affiliati, elencati nella tabella successiva (Tab. 5.1).

Tab. 5.1: Descrizione, leader e affiliati dei progetti Serics divisi in 10 Spoke

Fonte: FONDAZIONE SERICS - SEcurity and RIghts In the CyberSpace

Spoke	Descrizione	Leader	Affiliati
1 - Aspetti umani, sociali e legali	L'obiettivo è quello di studiare come creare un cyberspazio affidabile e sicuro combinando sistemi tecnologici solidi con comportamenti umani appropriati	CNR	UNIFI, UNICA, UNI GE, UNIBO, UNIMI, SSSUP
2 - Disinformazione e Fake News	Mira a progettare e sviluppare soluzioni innovative per identificare e gestire le minacce al sistema informativo che si manifestano attraverso le fake news e la loro diffusione	UNISA	CNR, Scuola IMT Alti Studi Lucca, CNIT, UNICA, UNIVE, UNIMI, UNI ROMA 1, ENI S.p.A.
3 - Attacchi e difese	Analizza le metodologie di attacco emergenti e sviluppa metodi avanzati per la rilevazione e la gestione di attacchi	UNICA	SSSUP, CNR, UNIBA, UNI GE, UNICAL, UNI ROMA 1, UNISA, UNIVE, ENI S.p.A., Leonardo S.p.A., Telsy S.p.A.
4 - Sicurezza dei Sistemi Operativi e della Virtualizzazione	Si occupa di sviluppare servizi di sicurezza automatici di alto livello nonché metodologie innovative di valutazione e garanzia della sicurezza per supportare lo sviluppo *secure-by-design* e la verifica di applicazioni cloud, *edge computing* e 5G	UNI GE	CINI, CNIT, CNR, Scuola IMT Alti Studi Lucca, Fondazione Bruno Kessler, Fondazione Ugo Bordoni, UNISA, UNICAL, UNI ROMA 1, Fincantieri, Leonardo S.p.A.
5 - Crittografia e sicurezza dei sistemi distribuiti	Si occupa di attività di ricerca nei domini della crittografia e della sicurezza dei sistemi distribuiti	UNICAL	Fondazione Bruno Kessler, UNISA, CNR, UNICA, PoliTO, Deloitte, Intesa Sanpaolo S.p.A
6 - Sicurezza del software e delle piattaforme	Il primo obiettivo è fornire un ecosistema in cui gli sviluppatori di software possano facilmente ragionare sulla sicurezza del software. Il secondo obiettivo è fornire soluzioni innovative per proteggere la catena di fornitura del software, compresi i processi di gestione e sviluppo	UNIVE	UNISA, UNICA, Deloitte, UNIBA, UNIFI, UNI ROMA 1, Scuola Imt Alti Studi Lucca
7 - Sicurezza delle infrastrutture	Ha come obiettivo generale lo sviluppo di tecnologie di sicurezza per le infrastrutture	PoliTO	CINI, CNR, Fondazione Ugo Bordoni, Scuola IMT Alti Studi Lucca, Scuola Superiore Sant'Anna Di Pisa, UNICA, UNI GE, Deloitte, Leonardo S.p.A., Telsy S.p.A.

Spoke	Descrizione	Leader	Affiliati
8 - Gestione del rischio e governance	Intende contribuire alla resilienza informatica dei futuri sistemi e servizi caratterizzati da componenti digitali sempre più interconnessi e intrinsecamente vulnerabili, come richiesto dall'UE attraverso NIS e NIS2, nonché dall'ACN.	UNIBO	CNIT, CNR, UNIBA, UNIFI, UNI GE, UNITO, UNIMI, Deloitte
9 - Mettere in sicurezza la trasformazione digitale	L'obiettivo principale è di studiare nuovi approcci, metodologie, soluzioni e strumenti in grado di fornire adeguate garanzie di sicurezza per i nuovi scenari applicativi.	UNI ROMA 1	CNR, UNIBA, UNICA, UNI GE, UNIMI, UNISA, Telsy S.p.A., Intesa Sanpaolo S.p.A
10 - Governance e protezione dei dati	Punta a garantire ai vari attori coinvolti nella condivisione dei dati e la disponibilità di strumenti e scenari per il controllo dei loro dati, per supportare la condivisione dei dati in modo selettivo e sicuro, garantendo allo stesso tempo funzionalità, efficienza e scalabilità.	UNIMI	UNI ROMA 1, UNIFI, UNICA, UNISA, Leonardo S.p.A.

Tra le attività volte a creare forza lavoro nazionale specializzata in cybersicurezza, coinvolgendo giovani talenti dai **18 ai 24 anni**, abbiamo ***CyberChallenge***, anch'essa richiamata dal **Piano di Implementazione Nazionale**. Si tratta della principale iniziativa italiana per identificare, attrarre, reclutare e collocare la prossima generazione di professionisti della sicurezza informatica. Dal 2017 al 2023, le richieste di partecipazione di studenti provenienti da scuole e Università sono aumentate in maniera esponenziale. Difatti, si è passati da un numero totale di **683 registrazioni a una quota pari a 4.720**. Di conseguenza, si è assistito a un incremento delle sedi e delle scuole coinvolte e, soprattutto, della percentuale di soggetti ammessi al progetto. Il programma si compone di **12 settimane di training**, gestite autonomamente da ogni sede, principalmente sugli ambiti della crittografia e della sicurezza in ambito hardware, reti, software e web.

La **Fondazione SERICS e il CINI** organizzano due corsi gratuiti e aperti ai giovani, dal nome ***OliCyber*** e ***CyberTrails***, che hanno l'obiettivo di rafforzare le conoscenze digitali e favorire l'avvicinamento di ragazzi e ragazze al mondo della sicurezza informatica. In particolare, ***Olicyber*** è la **prima competizione nazionale sulla cybersicurezza** rivolta a studentesse e studenti delle scuole superiori, ai quali è offerta l'opportunità di accedere a un esclusivo programma di formazione che include tutte le principali conoscenze necessarie a destreggiarsi nel mondo delle minacce digitali. ***CyberTrials*** è invece una **scuola rivolta a tutte le studentesse degli istituti di secondo grado**, che coinvolge anche chi non ha conoscenze pregresse in informatica. Le partecipanti sono guidate da esperti di altissimo livello sulla strada dei principi non tecnici del mondo digitale, dall'individuazione di una minaccia alle principali tecniche di indagine forense.

Il **19 giugno 2023**, **Enel** – insieme a **Planven Entrepreneur Ventures** e **Nozomi Networks** – ha presentato ***"Cyber Harbour"***, un laboratorio di innovazione volto a diffondere la consapevolezza sulla cybersecurity delle infrastrutture critiche, delle tecnologie dell'informazione e dell'industria mediante un approccio che promuova la ricerca e la nascita di **start-up**. Si tratta di un centro di eccellenza che unisce i maggiori esperti sulla materia, le aziende, gli investitori e il mondo accademico.

L'Università degli Studi di Roma Tor Vergata, attraverso il **CREeSEC** (**Centro di Ricerca e Sviluppo sull'E-Content**), ha promosso un PPP per la realizzazione di un Piano di formazione nazionale in materia di cyber security, cyber threat e privacy. Lo scopo è di ampliare il bagaglio conoscitivo, la ricerca e lo sviluppo e di creare professionalità con competenze multidisciplinari ai tre settori indicati precedentemente. Tutto ciò

è reso possibile grazie all'estensione della collaborazione ad altre Università e centri di ricerca (nello specifico UNISA e CNR), enti e aziende (tra cui Leonardo, Formiche.net e Cloud for Defence), istituzioni (Camera dei deputati, Garante per la protezione dei dati personali, AgID, Ministero della Difesa e Guardia di Finanza) e associazioni (ad esempio, l'Istituto Italiano Privacy).

Per concludere, ulteriore esempio di PPP è il **Primo dottorato nazionale in cybersicurezza**, interamente in lingua inglese e della durata di 3 anni, realizzato dalla **Scuola IMT Alti Studi di Lucca in collaborazione con il Laboratorio nazionale di Cybersecurity del CINI** (Consorzio Interuniversitario Nazionale per l'Informatica). Il dottorato beneficia del sostegno dell'ACN – con cui ha sottoscritto apposita convenzione il 13 febbraio 2023 – e ciò consentirà di collaborare su studi e ricerche sul tema della sicurezza delle infrastrutture informatiche, su programmi e progetti di ricerca nazionale e internazionale, nonché ad altre iniziative funzionali alla promozione e diffusione della cultura della cybersicurezza.

5.1.2. I Competence Center per l'orientamento e la formazione in cybersecurity

I centri di competenza sono partenariati pubblico-privati che hanno avuto origine nel 2019 con il compito di svolgere attività di orientamento e formazione alle imprese, in particolare le PMI, rispetto a tematiche correlate a Industria 4.0, supportandole verso la trasformazione digitale. I *Competence Center* sono stati istituiti dal MISE e co-finanziano progetti di innovazione mediante appositi bandi. Attualmente, gli **otto centri di competenza riconosciuti** sono: 1) **CIM 4.0 - *Competence Industry Manufacturing* 4.0**; 2) **MADE - *Competence Center* Industria 4.0**; 3) **BI-REX - *Big data Innovation-Research EXcellence***; 4) **ARTES 4.0 - *Industry 4.0 Competence Center on Advanced Robotics and enabling digital TEchnologies & Systems* 4.0**; 5) **SMACT - *Competence Center***; 6) **MediTech - *Mediterranean Competence Centre 4 Innovation***; 7) **START 4.0 - Sicurezza e ottimizzazione delle Infrastrutture Strategiche Industria 4.0**; 8) **CYBER 4.0 - *Cybersecurity Competence Center***. Il decreto

Tab. 5.2: Elenco *Competence Center* con relativo focus tematico

Fonte: Siti web dei *Competence Center*

Competence Center	Focus
CIM 4.0	Tecnologie di Industria 4.0
Cyber 4.0	Cybersecurity
Start 4.0	Sicurezza delle infrastrutture
SMACT	Supporto nella trasformazione digitale delle imprese
Artes 4.0	Robotica
BI-REX	Big Data
MADE	Tecnologie di Industria 4.0
MediTech	Tecnologie di Industria 4.0

ministeriale del **10 marzo 2023** rifinanzia le attività degli otto centri fino al **2025**, con uno stanziamento pari a **€113,4 milioni** a valere sulle risorse messe a disposizione per l'investimento del PNRR **"Potenziamento ed estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di industria" (Missione 4, componente 2, Investimento 2.3)**. Esso, inoltre istituisce anche la **Cabina di regia** che ha il compito di monitorare l'attuazione dell'attività e di promuovere il coordinamento tra i diversi soggetti coinvolti, la cui composizione e funzioni sono normate dal **Decreto direttoriale 7 settembre 2023**.
Ogni Competence Center ha un focus specifico e nasce dall'iniziativa di prestigiose Università del Paese (Tab. 5.2).
Cyber 4.0 è il *Competence Center* con sede a Roma che ha come missione accompagnare *policy maker*, imprese e PA in un percorso di crescita verso una digitalizzazione sicura mediante la formazione, l'orientamento e l'innovazione in ambito cybersecurity. Esso si rivolge a imprese con un focus particolare su ***Automotive, Aerospace e-Health*** e attraverso due bandi realizzati ha sostenuto 15 progetti di ricerca e innovazione[55], per l'80% presentati da PMI. A titolo di esempio, tra questi possiamo individuare "**Con Tecnology Inteligent**", che ha come partner Leonardo ed è incentrato sulla *threat intelligence* e "**KEEPCALM**", coordinato da SOGEI, mirato a studiare e implementare metodi e strumenti per prevenire le violazioni di una specifica infrastruttura tecnologica. Di recente, è stata avviata una **collaborazione con il Clusit**, Associazione Italiana per la Sicurezza Informatica, che ha l'obiettivo di promuovere attività di orientamento e formazione verso le imprese su tematiche relative alla transizione digitale e all'adozione sicura delle nuove tecnologie. I servizi in cybersecurity di Cyber 4.0 si differenziano in varie categorie: ***Cyber Risk***, **Protezione dei dati**, **Protezione sistemi informatici**, **monitoraggio e rilevamento minacce**, **gestione degli incidenti**, **certificazioni di sicurezza e consulenza**. Inoltre, il centro eroga formazione di carattere manageriale, giuridico e tecnico con percorsi rivolti a manager, imprenditori, esperti cyber e operatori informatici. "***CyberX – Mind4Future***" è il progetto di formazione evoluta ed esperienziale su temi di cybersecurity, organizzato in collaborazione con Leonardo. L'iniziativa è rivolta agli studenti delle università associate al centro di competenza[56], iscritti all'ultimo anno triennale e magistrale delle lauree del settore dell'informazione, dell'ingegneria industriale e dell'informazione, e delle lauree in Matematica, Fisica, *Data science*, *Management & Computer Science*. Il progetto si incentra su un modello didattico che coniuga la **formazione tradizionale** con **attività laboratoriali e di gaming**, per creare un percorso esperienziale e immersivo che permetta l'adozione di *hard skills* in ambito sicurezza, promuovendo anche lo sviluppo di competenze trasversali, ossia *soft skills*. Altra collaborazione importante è quella con la **Regione Lazio** per lo sviluppo dell'Accademia **Cybersicurezza Lazio (ACL)**, rivolta agli allievi delle scuole superiori, diplomati e laureati. Questa prevede 4 percorsi formativi di livello di specializzazione incrementale e ha visto il suo avvio a settembre 2023 con il corso di "***Cybersecurity Technician***", intento a preparare gli studenti ad attività di analisi di vulnerabilità e di rischio, di supporto per il team, di monitoraggio dei sistemi informativi e gestione di eventuali incidenti. Peraltro, a **luglio 2023** sono stati previsti **due nuovi bandi** destinati a co-finanziare progetti innovativi, per un totale di 5,1 milioni di euro, nel biennio **2023-25**. Il primo, è stato lanciato a luglio, per un valore complessivo di 2,5 milioni di euro, mentre il secondo è previsto per **gennaio 2024** (valore 2,6 milioni di euro).

55 Per un elenco dei progetti si veda: https://www.cyber40.it/progetti-finanziati/.
56 Sapienza Università di Roma, Università di Tor Vergata, Roma Tre, LUISS Guido Carli, Campus Biomedico, Università della Tuscia, Università di Cassino e del Lazio Meridionale, Università dell'Aquila.

Il progetto **CIM 4.0** del Politecnico di Torino, dell'Università di Torino e ventiquattro aziende private, presenta un focus su alcune delle tecnologie che abilitano l'Industria 4.0[57]. Esso dispone di due percorsi d'azione, uno sulla **fabbrica digitale** e l'altro sull'***Additive Manufacturing*** e organizza corsi di specializzazione anche attraverso la sua **Academy**. Tra questi, nel **catalogo 2024** spiccano singoli insegnamenti in Cybersecurity inerenti specifici temi, come: *Industrial security*; *Information security*; Blockchain; impatto di GDPR compliance su processi produttivi; *embedded security-security by design*; impatto delle pratiche di cybersecurity sul business ed evoluzione delle legislazioni.

Bi-Rex è un consorzio pubblico-privato nato nel 2018 che ha sede a Bologna e riunisce in partenariato **60 player** tra Università, Centri di Ricerca ed imprese. Con riferimento ai percorsi in sicurezza informatica, quello denominato ***"Cyber Security & Blockchain"***, presenta sedici insegnamenti, in parte specializzati sulla materia e in parte volti a declinare la cibersicurezza alla protezione dei sistemi industriali e dei servizi, delle reti e dei dati personali, comprendendola anche tra gli obiettivi del corso "investimenti in innovazione".

MADE, con sede a Milano, è il *Competence Center* incentrato intorno ai temi e le **tecnologie di Industria 4.0** e con un particolare focus su sostenibilità e digitale. Nella programmazione per il 2024 della **Scuola di competenze 4.0**, nata con lo scopo di sviluppare corsi di formazione per l'aggiornamento e la riqualificazione delle competenze aziendali nell'ambito delle transizioni gemelle, vengono presentati cinque corsi teorici in cybersecurity: **Cyber and industrial security**; **Cyber security awareness**; **Programmazione sicura dei sistemi a controllo numerico** e **dei sistemi di automazione**; **Cybersecurity industriale**.

Artes 4.0 situato a Pontedera, in provincia di Pisa, ha un focus specifico sulla **robotica** ed ha adottato un modello che abbraccia 13 macroaree con struttura hub & spoke, coinvolgendo otto regioni. Tra i corsi a catalogo in Cybersecurity vi sono[58]: "Cybersecurity, gestione e protezione dati"; "*Smart work*-cybersecurity"; "Master in Cybersecurity"; "Cybersecurity 4.0"; "Soluzioni tecnologiche per la sicurezza digitale della tua azienda".

SMACT ha come focus quello di mettere a sistema le competenze in ambito 4.0 della ricerca, dei provider di tecnologie e delle **imprese *early adopter***. Nasce e opera nel Triveneto, cooperando con stakeholder con capacità ed esperienza nella trasformazione digitale. Tra i corsi formativi teorici a catalogo sul tema della sicurezza informatica vi è "**Nuove sfide della Cyber Security: gli aggiornamenti dal mondo della ricerca**", dedicato a IT Manager e tecnici esperti che vogliono rimanere aggiornati sugli ultimi aggiornamenti dal mondo della ricerca e principalmente sulla sicurezza dei sistemi industriali, nonché sui principali nuovi rischi legati alle infrastrutture industriali, le tecniche di attacco e difesa in fase di studio.

Altro corso, di tipo esperienziale, è "Cyber Security: principi fondamentali e tecniche di difesa"[59], rivolto a sviluppatori, IT manager e ingegneri al fine di conoscere le basi della cybersecurity, acquisire una visione sulle maggiori sfide di sicurezza per le aziende e apprendere le migliori strategie di difesa. Inoltre, SMACT ha instaurato una collaborazione con l'ITS Meccatronico Veneto per il corso in "**Industrial Cyber Security**".

57 Additive Manufacturing e laser-based manufacturing; Smart grid, smart meters ed efficientamento energetico; Industrial IoT, piattaforme HW-SW, sensoristica, cloud e connectivity; Intelligenza Artificiale, data analytics e cyber-security.

58 La Cybersecurity è richiamata come tecnologia abilitante in corsi come: "Emissioni da sorgente convogliata: normativa tecnica e nazionale"; "La convergenza IT/OT"; "Introduzione all'uso dell'open source intelligence in ambito aziendale", ecc.

59 Il corso in questione non è ancora attivo.

MediTech è il *Competence Center* attivo in Campania, Puglia e Basilicata che conta sulla collaborazione di cinque Università della Campania, tre Università della Puglia e 21 player industriali. Il suo focus concerne le tecnologie di **Industria 4.0** e si è sviluppato seguendo una strategia incentrata sulla loro integrazione verticale ed orizzontale. Di rilievo è il Progetto ***"European Digital Innovation Hubs - Project Hubshsl (Heritage Smartlab)"***, sostenuta dalla Regione Basilicata e dal Comune di Matera, finalizzato alla creazione del più grande ***Digital Innovation Hub* europeo** (con sede in Basilicata e due *spokes* in Campania e Puglia). Importante iniziativa su cui fa leva tale progetto è la ***Talent's Academy***, ossia una piattaforma formativa avanzata e multidisciplinare che sarà ulteriormente specializzata sull'applicazione di conoscenze tecniche, tra cui **Cybersecurity e Intelligenza Artificiale**, con l'obiettivo di attrarre talenti, aggiornare e riqualificare il personale, creare una nuova generazione di professionisti con forti e aggiornate competenze digitali.

START 4.0 è un centro di competenza situato a Genova e ha un focus particolare sulla sicurezza delle infrastrutture. Il *Competence Center* prevede un'offerta formativa basata su **13 corsi in cybersecurity** che si sviluppano incentrandosi su aspetti differenti della stessa materia, ad esempio il tema dell'*awareness*, quello dei contratti commerciali, delle certificazioni, dei dati personali anche in merito al trasferimento extra-UE, della mobilità elettrica, del *Crisis Management* e della *Business Continuity*. Appare interessante la scelta di incentrare un insegnamento sul pagamento del riscatto a seguito di *ransomware* a causa dei continui attacchi perpetrati negli ultimi tempi a discapito delle imprese.

5.2. LE START-UP DI CIBERSICUREZZA E IL *CYBER INNOVATION NETWORK* DELL'ACN

In tema di collaborazione tra pubblico e privato, vengono in considerazione anche le **start-up innovative**. La normativa di riferimento contenuta nel d. l. n. 179/2012 (c.d. "Startup Act") e ss. mm. ne prescrive i requisiti: a) società di capitali, anche in forma cooperativa; b) costituita da non più di 5 anni (60 mesi)[60]; c) residenza in Italia (o in altro Paese SEE, ma con sede produttiva o filiale in Italia); d) fatturato annuo inferiore a €5 milioni; e) non quotata in un mercato regolamentato o in una piattaforma multilaterale di negoziazione; f) non distribuisce e non ha distribuito utili; g) l'oggetto sociale riguarda in maniera esclusiva o prevalente lo sviluppo, la produzione e la commercializzazione di un prodotto o servizio ad alto valore tecnologico; h) non è il risultato di fusione, scissione o cessione di un ramo di azienda.

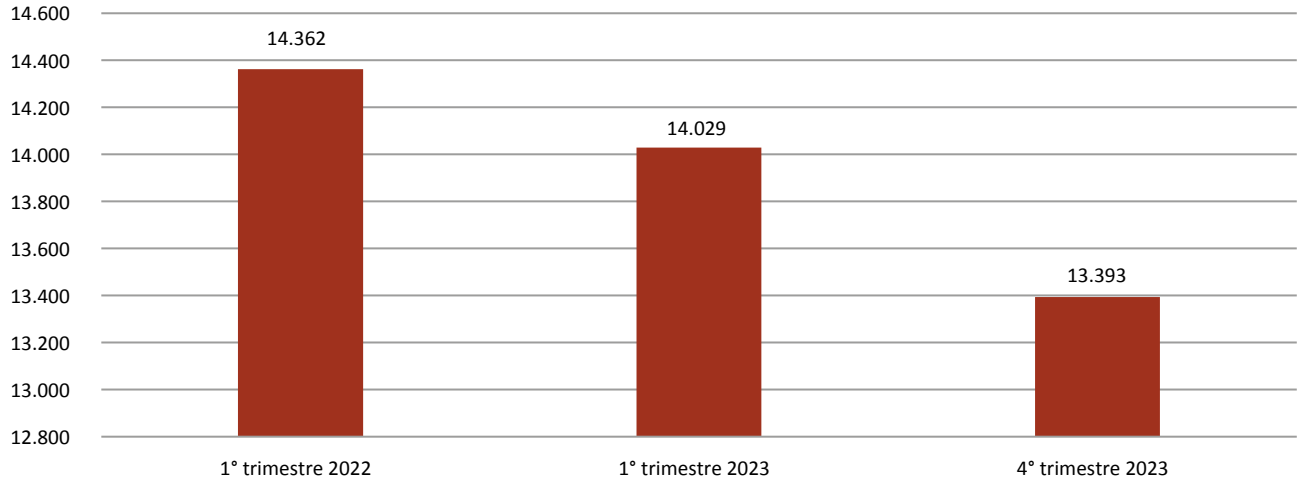
Inoltre, è necessario rispettare almeno uno dei seguenti requisiti soggettivi: 1) le spese in R&S sono maggiori o uguali al 15% del maggiore valore tra costo e valore totale della produzione; 2) la presenza di personale altamente qualificato (almeno 1/3 dottori di ricerca, dottorandi o ricercatori, oppure almeno 2/3 con laurea magistrale); 3) la società è titolare, depositaria o licenziataria di almeno un brevetto o titolare di un software registrato.

Al rispetto di tutte le caratteristiche sin qui richiamate, è possibile richiedere l'iscrizione nell'apposita **sezione speciale del registro delle imprese** e, di conseguenza, beneficiare di una serie di agevolazioni e incentivi fiscali, tra cui l'accesso gratuito al Fondo di Garanzia per le PMI e allo strumento di finanziamento *Smart&Start* Italia. Pertanto, le start-up possono essere intese come quelle imprese giovani, ad alto

60 Il "Decreto Rilancio" (d. l. n. 34/2020) ha disposto, in via eccezionale, la proroga di un anno della permanenza nella sezione speciale del Registro delle imprese delle start-up innovative, limitatamente alle imprese iscritte alla sezione speciale alla data del 19 maggio 2020.

Fig. 5.3: Start-up innovative inscritte alla sezione speciale del registro delle imprese

Fonte: Monitoraggio trimestrale start-up innovative (MIMIT)



contenuto tecnologico e con forti potenzialità di crescita, che rappresentano uno dei punti chiave della politica industriale italiana.

Come emerge dagli ultimi dati pubblicati sul portale dedicato alle start-up del registro delle imprese, aggiornati al 4° trimestre 2023, si registrano **poco meno di 14mila start-up innovative sull'intero territorio nazionale** (Fig. 5.3). Osservando l'andamento del numero di start-up nel corso degli ultimi due anni possiamo notare come la numerosità di questa tipologia di imprese si sia ridotta del 7%.

Se questi sono i dati per le start-up innovative in generale, I-Com ha svolto un monitoraggio su quelle che si occupano di cybersicurezza, osservandone **121 sull'intero territorio nazionale**[61]. Per quanto concerne l'anno di costituzione (Fig. 5.4), è possibile notare un andamento in costante crescita fino al 2019, a cui è seguito un rallentamento importante nel 2020 – causa pandemia da covid-19 – che è stato successivamente recuperato l'anno seguente, in cui si sono costituite il maggior numero di start-up in cybersicurezza su base annua (35). Tuttavia, nel 2022 si è assistito a una contrazione altrettanto significativa, con sole 11 start-up in tale ambito, **tendenza calante continuata nel 2023 in cui se ne rilevano appena 4**.

In merito alla loro distribuzione geografica (Fig. 5.5), **la Lombardia (34) e il Lazio (21) si confermano ai primi due posti anche per start-up specializzate in cibersicurezza**, seguite dalla Toscana (13) e da Piemonte e Campania (entrambe a quota 10). Invece, **sono ben 3 le regioni (Valle d'Aosta, Abruzzo, Molise) in cui non vi è alcuna start-up di questo tipo**. Fra le tre macro aree del Paese, **prevale il Settentrione (56)**, seguito dal Centro (43) e, con un importante distacco, il Sud (22).

In merito alle caratteristiche principali delle start-up di cibersicurezza (Fig. 5.6), innanzitutto rileva la **classe di addetti**, in quanto **prevalgono nettamente imprese che hanno tra i 0 e i 4 addetti (47)**, mentre solo 2 start-up hanno dichiarato di avere tra i 20 e i 49 dipendenti. Di conseguenza, si potrebbe desumere che in questo settore le start-up sono maggiormente di piccole dimensioni, anche se il dato in esame è stato pubblicato

61 Il monitoraggio è stato eseguito mediante una ricerca mirata per tag sul portale online del registro delle imprese – sezione speciale start-up.

Fig. 5.4: Numero di start-up in cybersicurezza per anno di costituzione

Fonte: Registro delle imprese – sezione speciale start-up

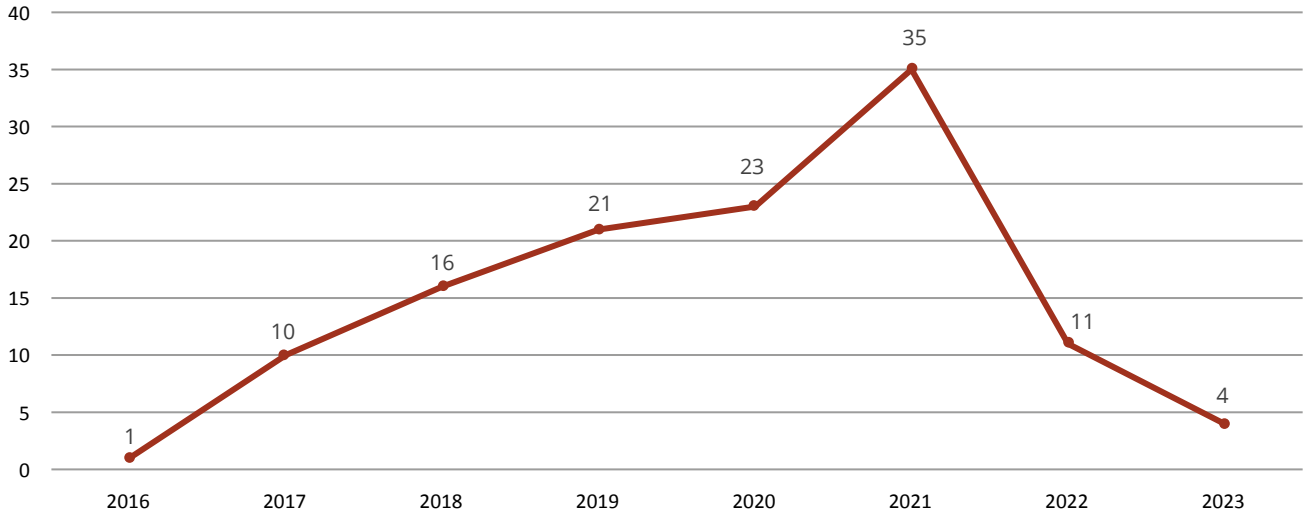
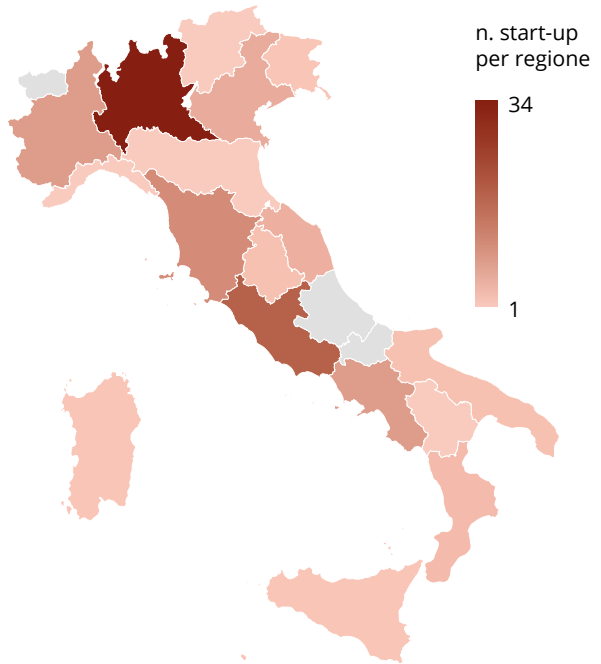


Fig. 5.5: Numero di start-up in cybersicurezza per regione

Fonte: Registro delle imprese – sezione speciale start-up



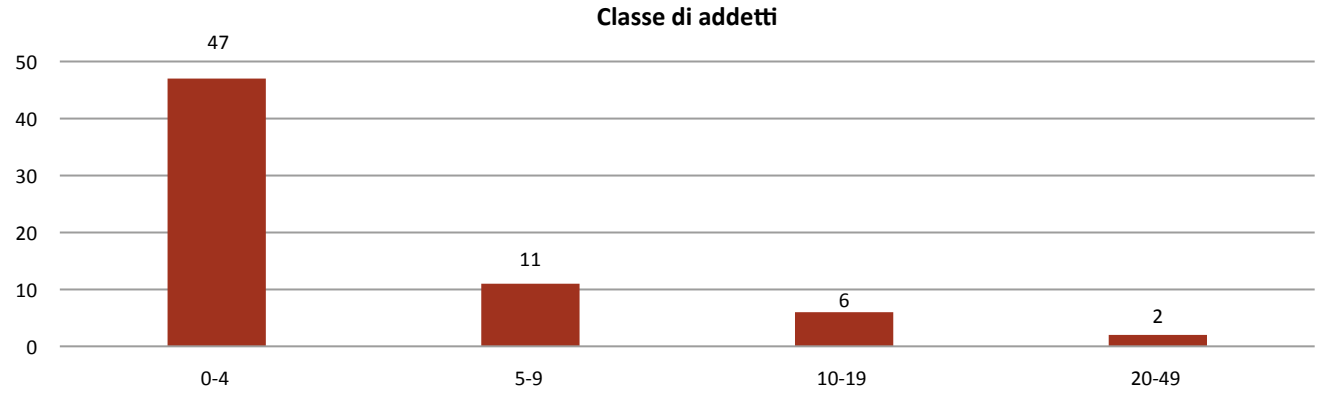
da poco più della metà delle società iscritte alla relativa sezione speciale del registro delle imprese.

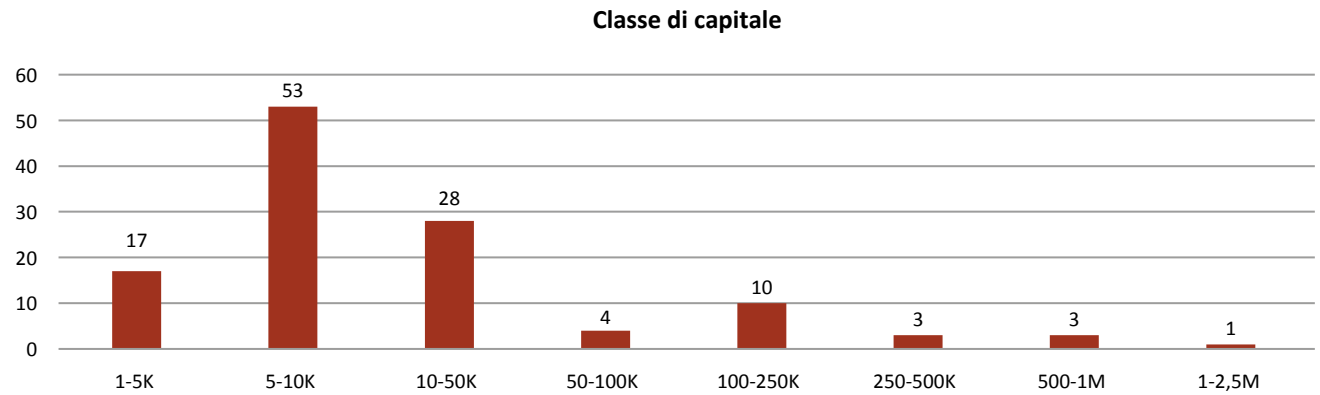
Quanto alla classe di **capitale sociale**, invece, tutte le start-up monitorate hanno comunicato i propri dati, potendosi affermare che **la quasi totalità non supera i €50mila di capitale sociale (98)**, con una maggiore concentrazione nella fascia €5-10mila (53), mentre **vi è una sola società che supera il milione di euro**. L'ultimo dato riportato riguarda il **valore di produzione** per cui oltre la metà delle imprese che hanno dichiarato questa informazione (93) **non raggiunge la soglia dei €100mila (51)**, mentre 5 società superano il milione di euro, di cui **ben 4 rientrano nella fascia €2-5 milioni**.

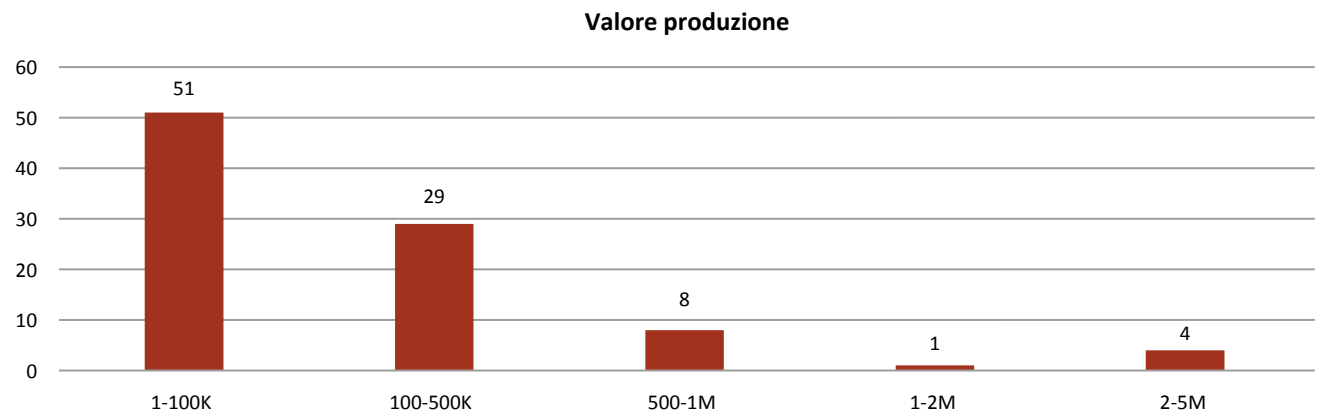
Pertanto, dai dati sin qui presentati è possibile affermare che – a parte poche eccezioni – **è necessario un maggiore impegno affinché le start-up operanti in ambiti correlati alla cybersicurezza possano apportare un contributo significativo al sistema produttivo nazionale** e, non meno importante, alla protezione di sistemi, tecnologie e dati in possesso delle pubbliche amministrazioni e dei cittadini.

Fig. 5.6: Classificazione start-up in cibersicurezza per caratteristiche principali

Note: Non tutte le start-up hanno reso disponibili i dati relativi a classe di addetti, classe di capitale e valore di produzione.
Fonte: Registro delle imprese – sezione speciale start-up







Infatti, **il primo avviso dell'ACN dedicato allo sviluppo di nuova imprenditorialità per progetti di cibersicurezza** che sfruttano tecnologie emergenti persegue tali finalità[62]. Più nel dettaglio, il programma fa parte della Strategia Nazionale e mira alla creazione del ***Cyber Innovation Network***, ossia una rete di collaborazioni per favorire lo sviluppo delle start-up dedicate a tecnologie emergenti che siano connesse (anche in maniera non esclusiva) all'ambito della cybersecurity, tra cui blockchain, robotica, *data science*, intelligenza artificiale, IoT e crittografia.
Come da determina del direttore generale del 1° giugno 2023, sono stati presi in considerazione 24 soggetti (incubatori e/o acceleratori di start-up) rispetto alle 28 candidature presentate. Lo scorso 18 luglio sono stati individuati, tramite apposita graduatoria, i primi 6 operatori a cui l'ACN ha proposto un accordo di collaborazione per avviare nuovi programmi o adeguare quelli già avviati, avendo come obiettivo l'estensione del numero di operatori partecipanti al *Cyber Innovation Network*. L'iniziativa prevede anche che **le start-up selezionate ricevano contributi economici di vario tipo, inclusi eventualmente finanziamenti a fondo perduto**. Per di più, essi potranno beneficiare della rete istituzionale dell'Agenzia ed essere sottoposti a un sistema di monitoraggio con specifici KPI (*Key Performance Indicator*).

5.3. ALTRE FORME DI COLLABORAZIONE TRA PUBBLICO E PRIVATO

Nei paragrafi precedenti sono state individuate le principali forme di cooperazione pubblico-privato, tra cui, per ragioni di completezza, vanno annoverati alcuni **accordi di collaborazione con l'ACN** nell'ambito delle proprie funzioni di impulso. Tra questi vi è quello stipulato con il **Consiglio Nazionale delle Ricerche** (CNR), volto a incentivare iniziative riguardanti attività didattiche, di ricerca scientifica, di sviluppo tecnologico, di formazione della cultura della sicurezza, nell'ambito di aree disciplinari di reciproco interesse. Le macroaree afferenti alle iniziative di collaborazione sono: 1) attività di **formazione**, anche in forma congiunta; 2) **collaborazioni** per **studi**, **ricerche** e **sviluppi tecnologici** relativi ai temi di interesse; 3) **partecipazione** a bandi, programmi e progetti di ricerca nazionali e internazionali; 4) **collaborazioni** volte allo **scambio di dati** di natura tecnica; 5) organizzazione di **conferenze**, **dibattiti** e **seminari** funzionali alla promozione e diffusione della cultura della sicurezza.
Anche **Microsoft** ha stabilito una collaborazione con l'ACN con il duplice obiettivo di promuovere l'**accesso** a tecnologie e strumenti avanzati per garantire la sicurezza di organizzazioni pubbliche e private e incentivare la **diffusione** di **competenze** in ambito di sicurezza informatica. In particolare, ha annunciato l'ingresso dell'ACN nel ***Microsoft Government Security Program***, un'iniziativa che fornisce le risorse e le competenze di Microsoft a oltre **novanta autorità e agenzie** che operano in ambito sicurezza in **quarantacinque Paesi** del mondo per accrescere la loro consapevolezza sulle minacce e vulnerabilità e sul valore di strumenti tecnologici in grado di proteggere organizzazioni e cittadini. L'obiettivo è creare con l'Agenzia un quadro di **collaborazione** che consenta di **agire in maniera preventiva** e di **mitigare i rischi** legati all'aumento della criminalità informatica. Altro scopo è quello di sviluppare un **programma di formazione**, volto a diffondere competenze in ambito cybersecurity con un focus particolare su **PA**, **PMI** e **scuole** per far fronte alla carenza di figure professionali del settore.
La **Banca d'Italia** e l'ACN hanno instaurato un'**intesa**[63] al fine di scambiarsi informazioni e creare una sinergia per proteggere i rispettivi settori dalla minaccia

62 L'avviso è stato aperto in data 18 gennaio 2023 e si è chiuso, a seguito di proroga, il 13 marzo seguente.
63 La data di stipula risale al 12/12/2022.

cyber, secondo il paradigma della **difesa partecipata**. Ciò avverrà mediante il **CERT Istituzionale** (**CERTBI**) che ad oggi ha raggiunto un livello elevato di maturità, riconosciuto a livello nazionale e internazionale, nelle attività di *cyber threat intelligence* applicate alla **difesa preventiva**, **proattiva** e **reattiva**.

Anche nel settore finanziario non sono mancati **concordati** come quelli precedentemente indicati, nello specifico quello con il CERTFin, ***Computer Emergency Response Team*** **del settore Finanziario Italiano**. Il protocollo è in linea con gli obiettivi fissati dalla **Strategia Nazionale di Cybersicurezza 2022-2026**, tiene conto della sempre maggiore digitalizzazione del settore finanziario italiano, da un lato, e della crescente diffusione degli attacchi cibernetici, dall'altro. L'accordo prevede la collaborazione anche sul fronte della **sensibilizzazione** di utenti e imprese sui temi della cybersicurezza, attraverso la realizzazione di **campagne di comunicazione** dedicate ed esercitazioni e simulazioni finalizzate a potenziare le capacità di prevenzione e reazione agli incidenti informatici.

Il **19 ottobre 2022** è stato firmato il **Protocollo d'Intesa**, con durata triennale, tra l'ACN, **Confindustria e Generali** che inserisce tra le principali iniziative la creazione del ***"Cyber Index Pmi"*** (presentato a ottobre 2023), un rapporto che fotografa lo stato di consapevolezza in materia di cyber security all'interno delle organizzazioni aziendali di piccole e medie dimensioni. Il *Cyber Index PMI* rappresenta, anche a livello metodologico, il primo tassello del futuro Cyber Index italiano, così come previsto dalla Strategia Nazionale di Cybersicurezza, che andrà a sua volta ad alimentare il Cyber Index europeo. Inoltre, nell'ottica di implementare la conoscenza e la consapevolezza dei rischi legati a queste minacce, sono previsti **incontri di formazione** e **workshop** su base territoriale destinati alle imprese associate di Confindustria.

Con il patrocinio dell'Agenzia per la Cybersicurezza Nazionale, **Google** ha lanciato in Italia la ***Google.org Impact Challenge*****:** ***Tech for Social Good***, un invito aperto a organizzazioni no profit, istituzioni accademiche e di ricerca, enti civici e imprese sociali del nostro Paese, che potranno ricevere supporto tecnico e finanziamenti pro bono per progetti incentrati sull'uso della tecnologia per risolvere problemi complessi e contribuire a creare una società digitale più sicura. Le organizzazioni hanno l'opportunità di rientrare nel programma di sostegno allo sviluppo tecnologico previsto dalla Strategia Nazionale di Cybersicurezza di ACN, in particolare su temi come la **sicurezza dei dati** e la **privacy**, la gestione delle **minacce cibernetiche**, la sicurezza dei **software**, delle **piattaforme**, delle **infrastrutture digitali** e gli aspetti sociali e di **governance** connessi.

Agli inizi del mese di **febbraio 2023**, **Amazon Web Services** (**AWS**) ha annunciato l'avvio della collaborazione con l'ACN nell'ambito del ***Government Cybersecurity Program*** (GCSP), un programma che mira a condividere le migliori pratiche nel campo della sicurezza informatica, incluse le informazioni sulle minacce e i rischi in ambito cibernetico. L'obiettivo di AWS è quello di **condividere** tecnologie avanzate, servizi cloud sicuri e le proprie competenze con cittadini, aziende e autorità pubbliche italiane per potenziare i sistemi di prevenzione agli attacchi contro le infrastrutture nazionali.

Ulteriore Protocollo d'Intesa volto a rafforzare le misure di protezione del Paese è quello tra ACN e **Cisco**. Gli ambiti di collaborazione previsti riguardano la possibilità di intraprendere iniziative su temi come la formazione, la condivisione di best practice tecnologiche, la ricerca, la cooperazione e lo scambio di informazioni e metodologie di analisi in tema di *cyber threat intelligence*.

Lo scorso **12 gennaio**, il **MEF** e **Consip** hanno siglato un protocollo di intesa con l'ACN per garantire la cybersicurezza dell'intero ciclo di vita dei contratti pubblici. In particolare, l'obiettivo del protocollo è supportare l'Agenzia nello sviluppo di strategie per migliorare la protezione della **piattaforma di e-procurement nazionale**

e, più in generale, il patrimonio informativo di Consip, attraverso l'adozione di misure adeguate per la prevenzione e la mitigazione degli incidenti di sicurezza, in raccordo con lo CSIRT Italia.

All'interno del Piano di Implementazione dell'ACN tra le misure individuate per la Strategia Nazionale di cybersicurezza vi è quella di favorire le sinergie tra l'Agenzia e i **Cluster tecnologici per agevolare il trasferimento tecnologico verso le PMI**[64]. Questi consistono in reti di soggetti pubblici e privati che operano sul territorio nazionale in settori come la **ricerca industriale**, la **formazione** e il **trasferimento tecnologico**. Hanno la funzione di catalizzatori di risorse per rispondere alle esigenze del territorio e del mercato, coordinare e rafforzare il collegamento tra il mondo della ricerca e quello delle imprese. Ciascuna aggregazione fa riferimento a uno specifico ambito tecnologico e applicativo ritenuto strategico per il nostro Paese, di cui rappresenta l'interlocutore più autorevole per competenze, conoscenze, strutture, reti e potenzialità.

Nel 2012 il Miur ha promosso la nascita e lo sviluppo dei **primi otto cluster tecnologici nazionali**: **Aerospazio**, **Agrifood**, **Chimica verde**, **Fabbrica intelligente**, **Mezzi e sistemi per la mobilità di superficie terrestre e marina**, **Scienze della Vita**, **Tecnologie per gli ambienti di vita**, **Tecnologie per le Smart Communities**. Nel 2016 sono stati inclusi quattro nuovi cluster: **Tecnologie per il Patrimonio Culturale**, **Design**, **creatività e Made in Italy**, **Economia del Mare**, **Energia**.

Per comprendere come la cybersecurity sia stata coinvolta tra i principali obiettivi dei cluster, si può prendere in considerazione l'esempio di **Deloitte**, che nel 2020 ha aderito al Cluster Tecnologico Nazionale Fabbrica Intelligente come ***Pathfinder*** (partner tecnologico) al fine di condividere le sue competenze in tema di cybersecurity industriale collegata alla digitalizzazione dei processi manifatturieri. In particolare, Deloitte ha presentato benchmark, trend evolutivi e best practice di gestione delle piattaforme digitali e della loro sicurezza in ambito industriale, per affidare disponibilità, confidenzialità e integrità alle informazioni trattate negli ambienti produttivi attraverso metodologie e tecniche di ***identification***, ***prevention***, ***detection***, ***response*** & ***recovery***.

Per il Cluster Tecnologico Nazionale Aerospazio è stato approvato il progetto **CRUISE** che intende sviluppare e validare un ***CyberSec Test Range***, una infrastruttura tecnologica, associata all'aeroporto di Grottaglie, dove misurare la vulnerabilità e la resilienza degli UAS agli attacchi informatici.

Nell'ambito delle attività del Cluster Tecnologico Nazionale Tecnologie per le *Smart Communities* si è tenuto il progetto **Mobilità Intelligente Ecosostenibile**, che ha avuto come capofila la Divisione Cyber Security di Leonardo. Al progetto ha partecipato il CNR, accanto al Politecnico di Milano, al Politecnico di Torino, all'Università di Genova, a primari player aziendali e a cinque PMI.

Il Cluster Tecnologico Fabbrica Intelligente (CFI) ha sviluppato una **Roadmap per la Ricerca e Innovazione**, un documento fondamentale per orientare scelte strategiche e investimenti di imprenditori, industriali e manager. Lo scopo è quello di rendere omogeneo il livello tecnologico e digitale tra le PMI all'interno della filiera, identificando una serie di punti focali: a) **innovativi sistemi per il governo della cybersecurity** per la gestione del rischio in tutta la catena produttiva al fine di ottenere protezione, affidabilità e integrità dei dati, l'integrazione progressiva sicura e sostenibile di nuove tecnologie nella rete industriale, la definizione di contenuti per una efficace formazione sulla cybersecurity del personale; b) **soluzioni a supporto della resilienza** dei sistemi; c) protezione dei **flussi di comunicazione**; d) **monitoraggio di sicurezza** del mondo Cyber-Fisico.

Il 15 novembre 2023 si è aperto il bando ***Digital and***

64 Sul punto si v. Misura #47.

emerging technologies for competitiveness and fit for the Green Deal, del Programma di lavoro 2023-2024 del Cluster Digital, Industry and Space di **Horizon Europe**. Esso è costituito da 4 *topic*: *Open Source for Cloud/Edge to support European Digital Autonomy (RIA); Public recognition scheme for Open Source (CSA); Pilot line(s) for 2D materials-based devices (RIA); Quantum sensing and metrology for market uptake (IA)*. È previsto anche l'avvio di un nuovo bando intorno ad **aprile 2024**, che sarà pubblicato solo dopo l'adozione di un emendamento al Programma di lavoro da parte della Commissione europea.

icom
istituto per la competitività

CAPITOLO 6

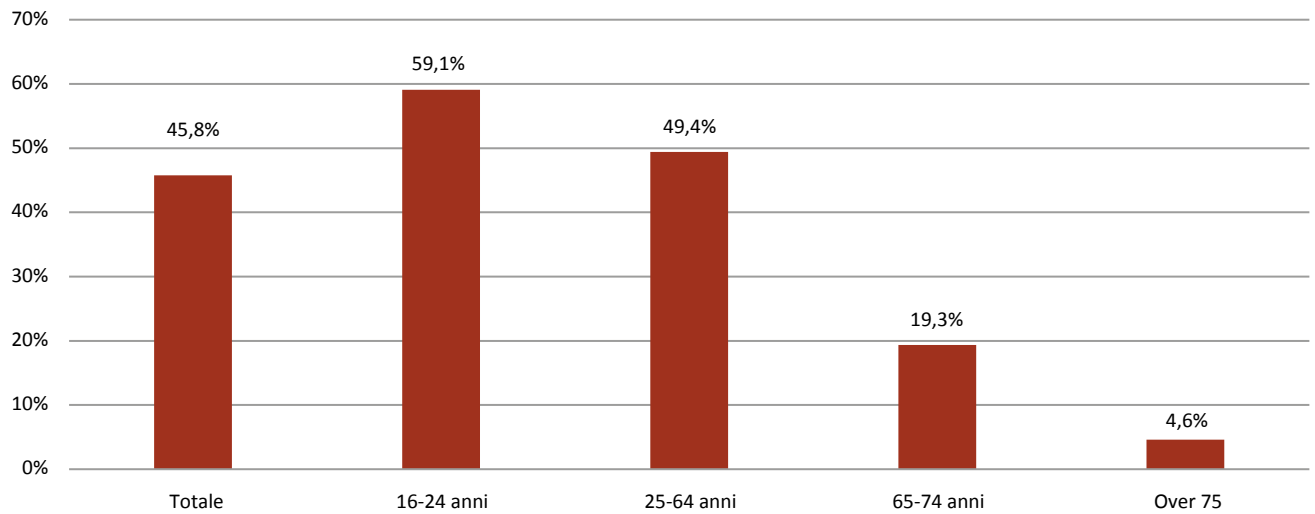
LE COMPETENZE IN CIBERSICUREZZA: A CHE PUNTO SIAMO E ATTIVITÀ IN CORSO

6.1. LA CYBERSICUREZZA PER I CITTADINI: 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, spingendo tutte le categorie di individui, anche quelli meno avvezzi all'utilizzo degli strumenti digitali, ad interfacciarsi con dispositivi elettronici, con conseguente esposizione a nuove minacce come il cybercrime.
Si tratta di rischi importanti e concreti ove si considerino i dati Eurostat sulle competenze digitali. Questi registrano una media nazionale particolarmente bassa (45,8%) (Fig. 6.1). Appaiono più confortanti gli stessi dati con riferimento alla fascia d'età 16-24 anni (59,1%), dopodiché si registra un calo nella fascia 25-64 al 49,4%. Sotto la media nazionale si posiziona la popolazione meno giovane con un 19,3% per il range 65-74 anni e un mero 4,6% negli over 75. Tali evidenze richiamano urgentemente la **necessità di attuare strategie inclusive in termini di digitalizzazione**, che consentano di guidare tutti i cittadini e dunque l'intero sistema Paese verso una trasformazione digitale più consapevole, omogenea e sicura.
Allo stesso tempo anche i dati relativi agli **individui che, per timori legati alla sicurezza, non utilizzano l'Internet of things** rilevano un interessante divario fra l'Italia e la media europea (Fig. 6.2). Infatti, **in tutte le fasce d'età e nella media totale la quota interessata di individui è minore rispetto al dato europeo** (la media nazionale è pari all'1% mentre quella UE al 7,5%), con il divario maggiore che si realizza nella fascia 25-64 anni (1,1% italiano contro l'8% europeo). Se a prima vista questo dato parrebbe evidenziare uno scenario favorevole per l'Italia, considerati i minori timori per la sicurezza, allo stesso tempo questi potrebbero dipendere dalle minori competenze in campo digitale, come precedentemente evidenziato. Dunque, **i dati suggeriscono un'ulteriore arretratezza da parte dell'Italia rispetto allo scenario europeo insieme alla necessità di maggiore formazione sui pericoli digitali**.

Fig. 6.1: Quota di individui con competenze digitali almeno di base (2023)

Fonte: Eurostat



Se si osserva la quota di computer infettati almeno una volta da malware nell'ambito dei principali partner europei del nostro Paese (Fig. 6.3), i dati raccolti da Comparitech e aggiornati al 2022 vedono l'Italia in seconda posizione con il 10,7% di computer infettati, dietro solo alla Spagna (11,6%)

Fig. 6.2: Quota di individui che non utilizza l'Internet of things per timori legati alla sicurezza (2022)

Fonte: Eurostat
(Dato europeo mancante per gli over 75)

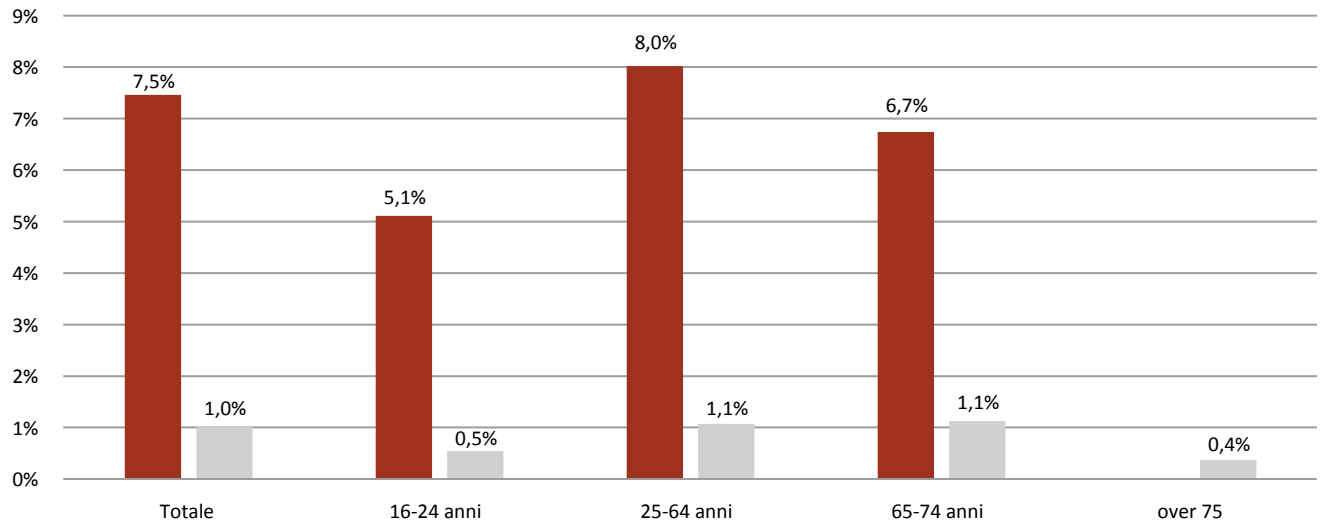


Fig. 6.3: Quota di computer infettati almeno una volta da software malevoli (2022)

Fonte: Comparitech

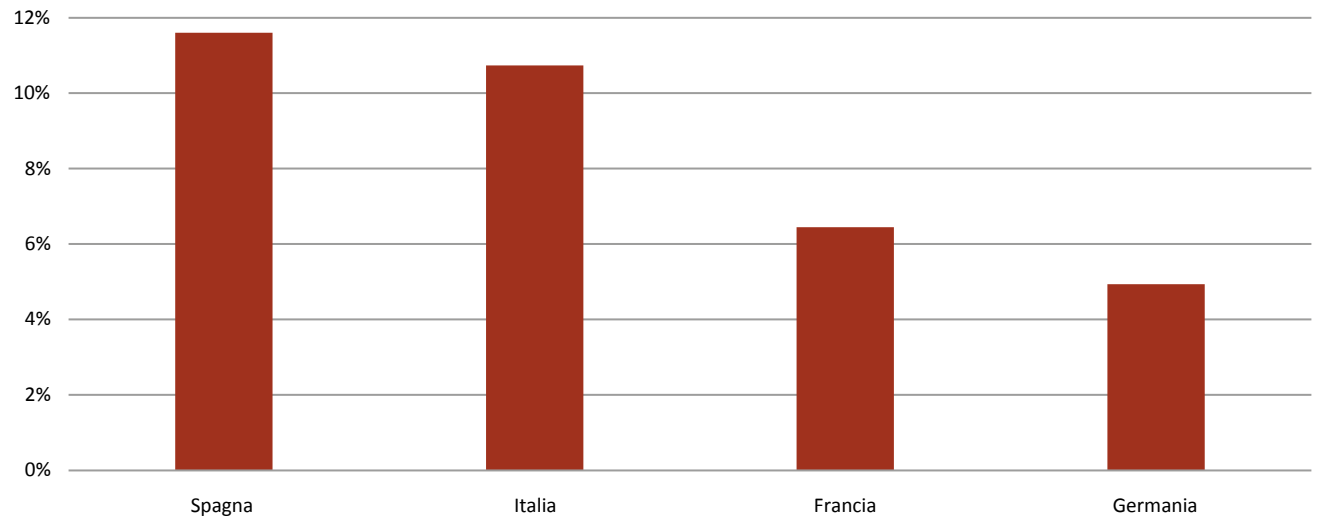
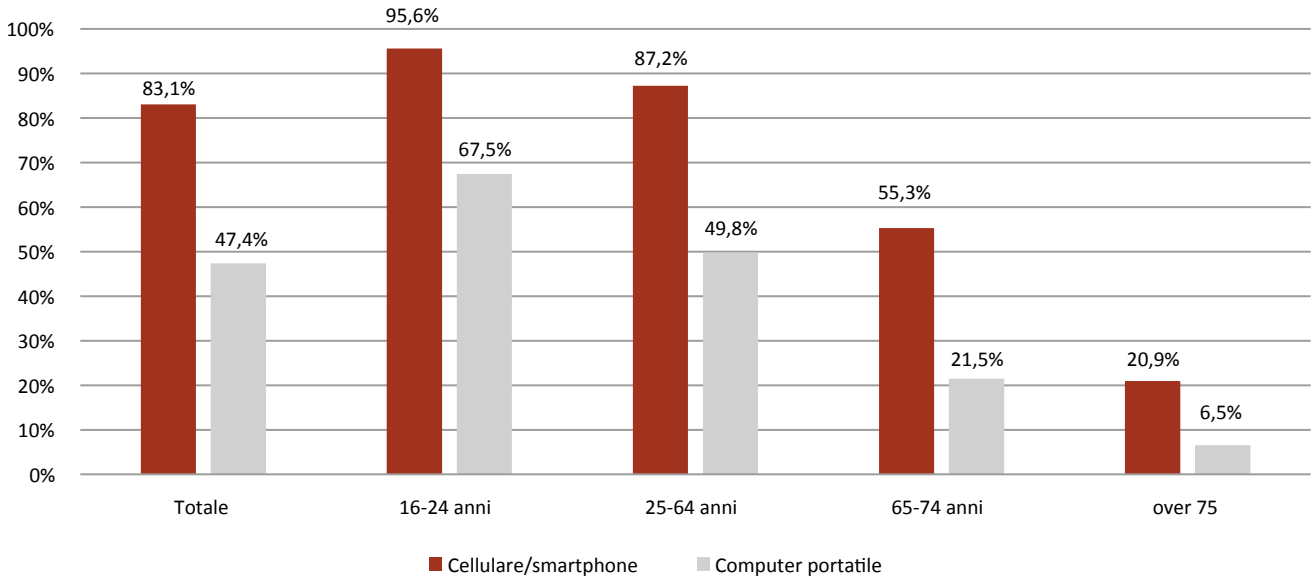


Fig. 6.4: Quota di individui per tipo di dispositivo utilizzato per l'accesso a Internet (2023)

Fonte: Eurostat



e seguita invece da Francia (6,5%) e, infine, dalla Germania (4,9%).

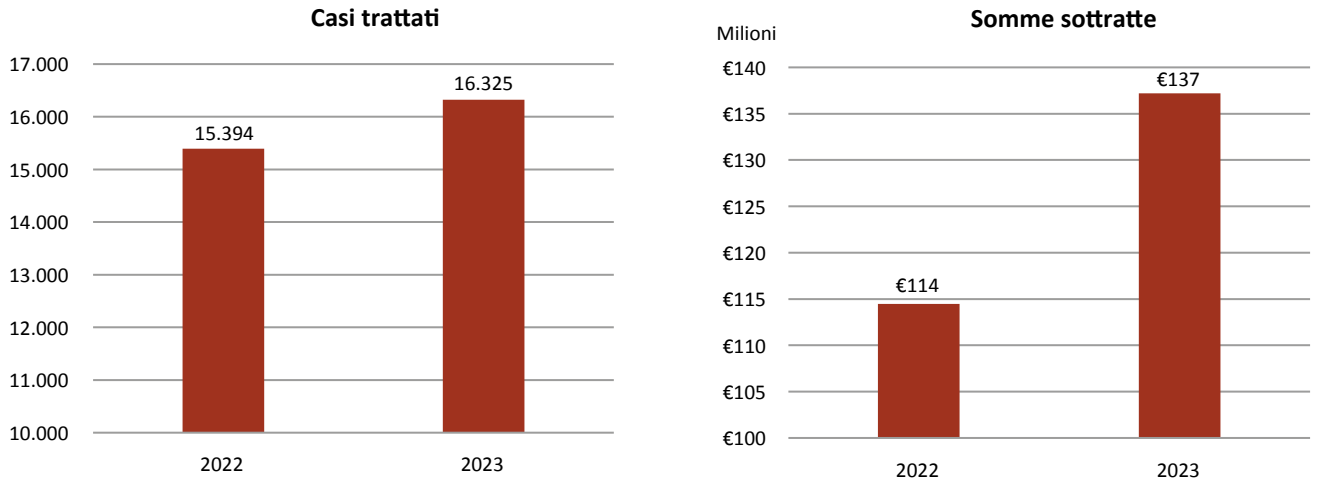
I dati sin qui presentati restituiscono un'immagine preoccupante del livello di cibersicurezza nazionale, con particolare riguardo alle fasce più anziane della popolazione, specialmente considerando le ultime rilevazioni di Eurostat per il tipo di dispositivi utilizzati per l'accesso a Internet in Italia. Infatti, lo smartphone è utilizzato dall'83,1% dei cittadini (78,3% nel 2021), mentre il computer fisso o portatile è utilizzato dal 47,4%, percentuale aumentata in maniera significativa dal 29% del 2021.

Le rilevazioni effettuate dalla Polizia Postale nell'ambito del resoconto delle rispettive attività, aggiornato al 27 dicembre scorso (Fig. 6.5), offrono una panoramica importante relativamente alle truffe online in Italia. Infatti, anche **nel corso del 2023, si è riscontrato un significativo incremento degli illeciti legati al fenomeno del falso trading online**. Più in generale i casi trattati sono stati 16.325 (15.394 nel 2022), conseguentemente sono state indagate 3571 persone (3511 nel 2022) vedendo sottratti €137.202.592 (€114.459.014 nel 2022). In queste circostanze l'attività investigativa prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, richiedendo il blocco delle somme versate e l'esecuzione di controlli sui flussi finanziari generalmente destinati all'estero.

Di conseguenza, è possibile desumere una stretta correlazione tra i dati raccolti dalla Polizia Postale con il basso livello di competenze digitali di base, l'adozione di misure di sicurezza elementari (come username e password) e la percentuale di smartphone e pc infettati da software malevolo, il cui **rimedio** non può che rivedersi in maggiori iniziative che puntino soprattutto sull'**accrescimento dell'*awareness* degli individui** e sull'offerta formativa, anche (ma non solo) specialistica, degli stessi, nonché sul ruolo cruciale della collaborazione tra pubblico e privato.

Fig. 6.5: Numero di casi trattati e somme sottratte (in milioni di euro) in relazione alle truffe online in Italia (2022-2023)

Note: i dati rilevati sono aggiornati al 27/12/2023.
Fonte: Resoconto attività 2023 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica



6.2. L'IMPEGNO DELLE IMPRESE PER LA SICUREZZA INFORMATICA

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 e uno dei principali canali di assistenza ai clienti, **il livello di competenze relative all'ambito ICT/IT all'interno delle imprese italiane**, soprattutto per il personale specializzato, **è sempre al di sotto della media UE**. Infatti, se il divario tra il nostro Paese e la media europea era di circa 13 punti percentuali nel 2016 e nel 2017 per la formazione del personale in ambito di *skill* ICT, esso è stato recuperato negli anni successivi (2018-2019), per poi tornare ad ampliarsi dal 2020 in poi. Nel 2022, infatti, a fronte di una media europea pari al 65,3% delle imprese del settore ICT, la percentuale italiana si ferma al 54,7%, con un distacco di oltre 10 p.p. (Fig. 6.6).

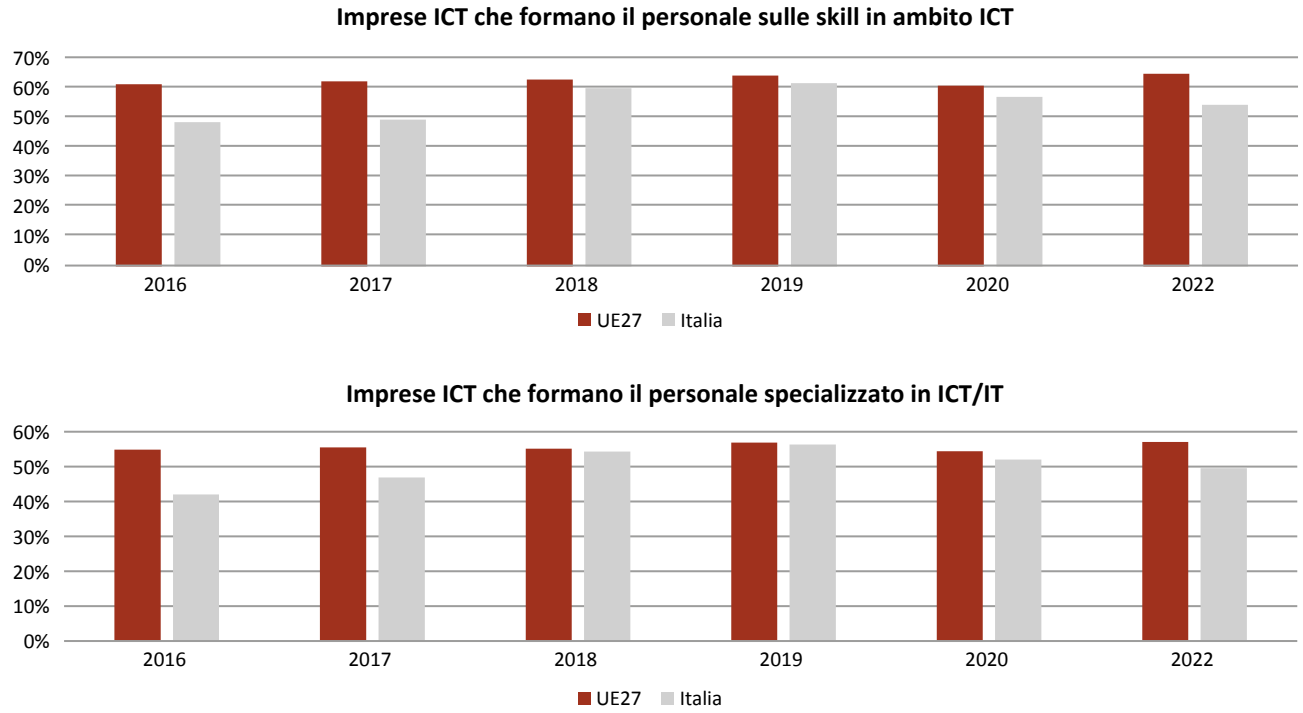
Con riguardo invece alla formazione avanzata per il personale specializzato in ambito ICT/IT, il livello medio europeo è inferiore rispetto alla formazione riferita al personale più in generale, attestandosi non oltre il 57% nel 2022 contro un 65%. Sul punto, nel nostro Paese si può osservare un andamento di costante avvicinamento al valore medio UE sino al 2019, arrivando a 7,6 punti percentuali in meno nel 2022 (57,1% UE vs 49,5% ITA).

Se si considera che gran parte delle azioni malevole subite 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.

In merito, nonostante i dati non propriamente ottimali sin qui esposti, **le imprese italiane non sembrano essere quelle che subiscono più incidenti di sicurezza in ambito comunitario**. Difatti, con riferimento a tipologie di attacchi cibernetici quali gli ormai (purtroppo) popolari *ransomware* e DDoS (*Distributed*

Fig. 6.6: Quota di imprese ICT con più di 10 addetti che erogano formazione al proprio personale (2016-2022)

Note: I dati riferiti all'anno 2021 non sono stati pubblicati nel database di Eurostat.
Fonte: Eurostat



Denial of Service) che causano l'interruzione di servizi ICT (Fig. 6.7), l'Italia si posiziona al di sotto della media UE27 (14,4% vs 20,1%), performando molto meglio rispetto a Germania (24,6%) e Francia (23,1%).
Ciò detto, **in Italia è meno diffusa rispetto alla media europea (16,4% vs 25%) la dotazione di un'assicurazione per gli incidenti di sicurezza ICT** (Fig. 6.8), nonostante gli attacchi e le minacce informatiche possano causare danni piuttosto seri alle imprese e alla rispettiva supply chain, non solo in termini di perdite finanziarie dirette (ad esempio, nel caso in cui si opti per il pagamento del riscatto per decriptare dispositivi e sistemi infettati dal ransomware o, più semplicemente, con riferimento all'interruzione della produzione o dell'erogazione di servizi), ma anche con riguardo al danno reputazionale o di immagine, oltre che alla potenziale propagazione delle conseguenze negative (anche, ma non solo, di natura contrattuale) dell'attacco verso i fornitori chiave e gli altri stakeholders. Viceversa, l'importanza delle assicurazioni contro il rischio cyber sembra essere stata colta maggiormente dalle aziende spagnole (21,9%), tedesche (32,3%) e soprattutto da quelle francesi (39,9%).
Peraltro, se si considera quanto siano ormai diventati fondamentali i dati nella società contemporanea, si può comprendere anche che ridurre al minimo l'impatto dato dalla loro esfiltrazione a causa di un attacco cibernetico sia di primaria importanza. Sul punto, IBM Security pubblica annualmente un report che offre una visione su come siano molteplici i fattori di rischio che possono influenzare i costi di una violazione di dati.

Fig. 6.7: Quota di imprese con più di 10 addetti che hanno subito un incidente di sicurezza che ha causato l'interruzione dei servizi ICT (2022)

Note: Interruzione dei servizi ICT (causata da: DDoS, ransomware, problemi hw o sw)
Fonte: Eurostat

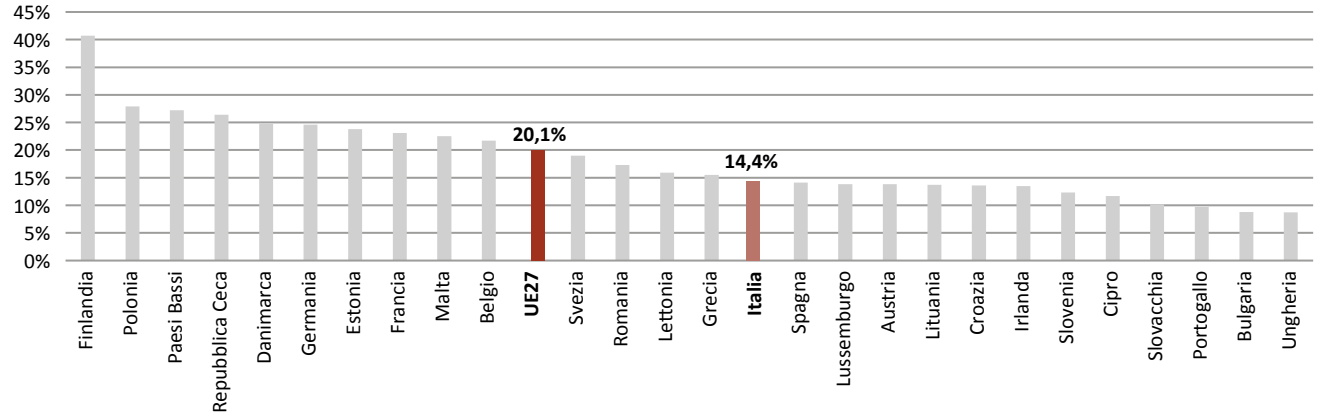
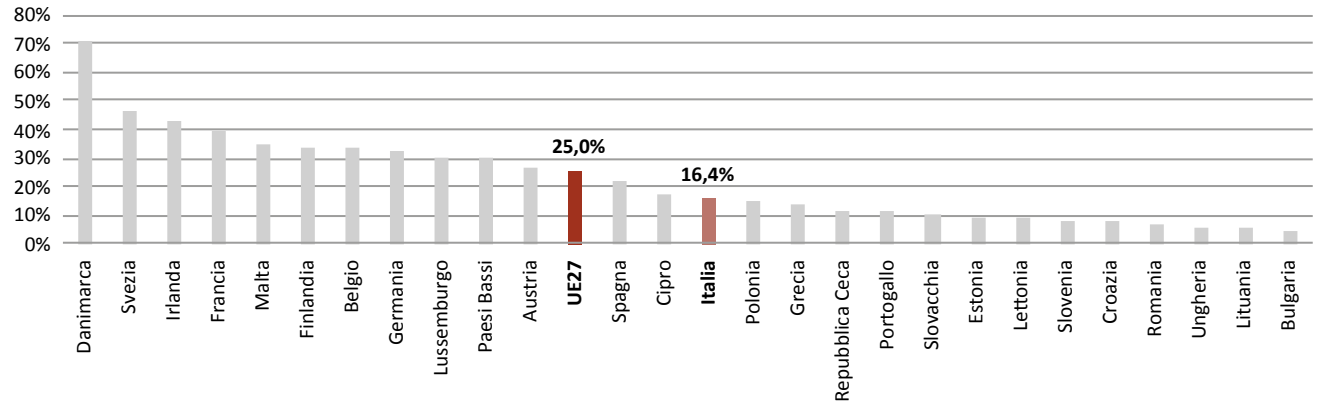


Fig. 6.8: Imprese con più di 10 addetti che hanno un'assicurazione per gli incidenti di sicurezza ICT (2022)

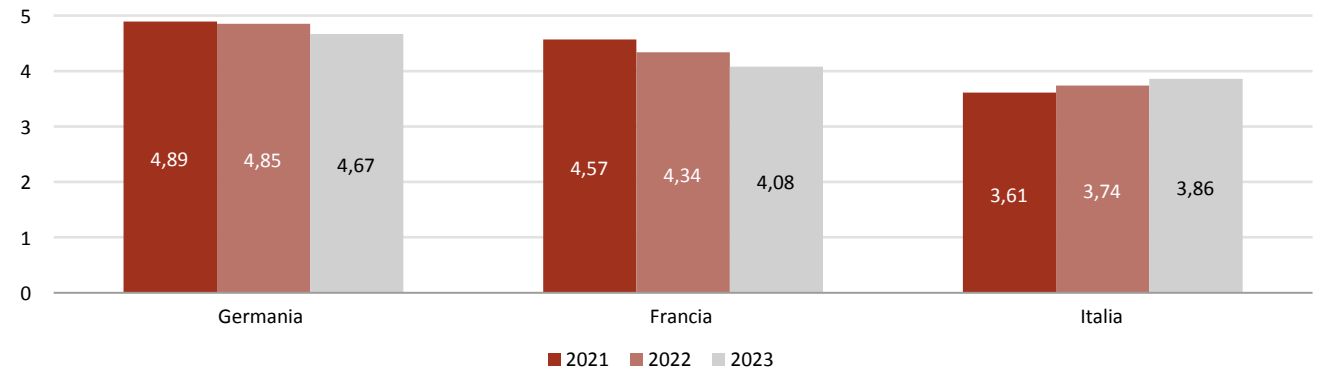
Fonte: Eurostat



Tra i dati più interessanti vi è che **per il 52% delle organizzazioni** prese in esame (appartenenti a 16 paesi e aree geografiche, tra cui l'Italia) **le conseguenze di un data breach si sono riversate sui consumatori, tramite un aumento dei prezzi** di beni e servizi offerti. Ciò non dovrebbe sorprendere se si considera il costo medio di una violazione di dati (Fig. 6.9). In merito, l'Italia ha fatto registrare valori inferiori, ma in controtendenza e quindi in aumento, rispetto alla Germania e alla Francia. Infatti, se negli altri due Paesi europei menzionati si può osservare un decremento rispetto al 2021 e al 2022, da 4,89 a 4,67 milioni di dollari per la Germania e da 4,57 a 4,08 milioni per la Francia, **nel nostro Paese si è apprezzato un incremento del costo medio di una violazione da 3,61 a 3,86 milioni.**

Fig. 6.9: Costo medio di una violazione di dati per Paese (in $ milioni)

Fonte: IBM Security, *Cost of a Data Breach Report 2023*



6.3. LE *BEST PRACTICES* PER LA FORMAZIONE ICT & CYBER

Lo *human factor*, come anticipato, rappresenta una delle maggiori cause di attacchi cyber, poiché quando il bersaglio è un individuo la possibilità di attuare frodi informatiche, mediante tecniche di persuasione, di manipolazione e di convincimento, produce effetti particolarmente distruttivi per l'intera organizzazione. Quanto detto è aggravato da fattori come la cattiva gestione delle password o dell'uso di internet, l'incapacità di distinguere tentativi di *phishing* tramite e-mail o chiamate telefoniche e l'assenza di policy aggiornate e adeguate.

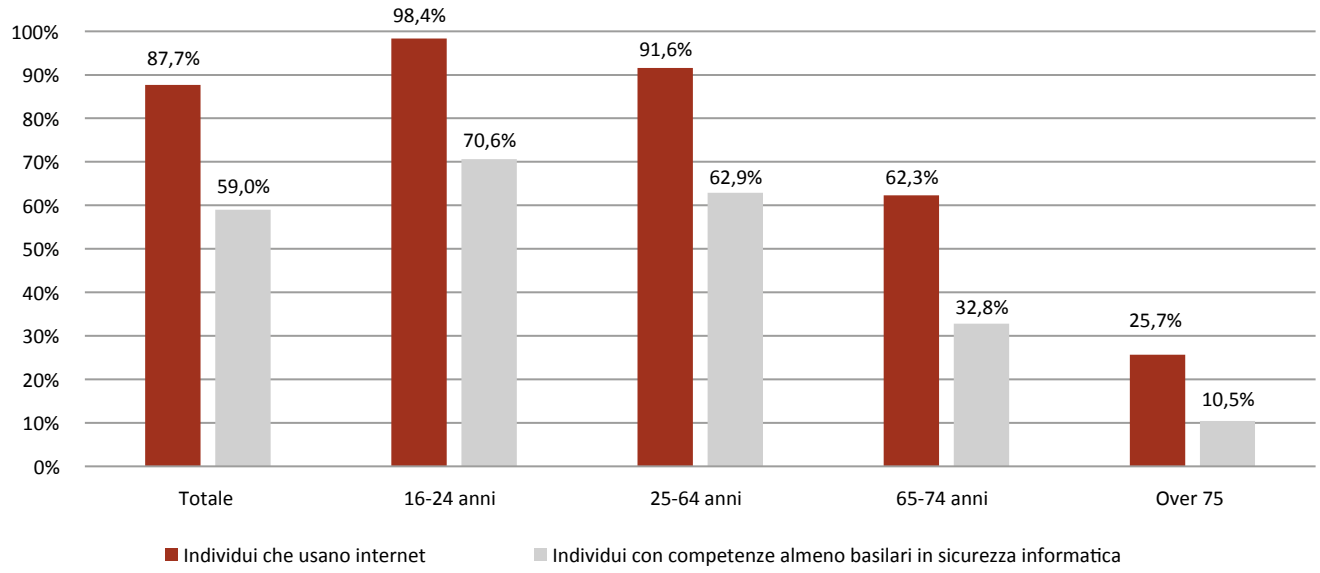
Pertanto, **per ridurre tali rischi è necessario puntare sull'aumento del livello di consapevolezza degli utenti**. Dall'analisi dei dati forniti da Eurostat con riferimento all'anno 2023 (Fig. 6.10), si evince che **solo il 59,0%** (59,8% nel 2022) **dei cittadini ha competenze almeno basilari in materia di sicurezza informatica**. Osservando la scomposizione demografica per età, viene confermato come la quota di persone impreparate in cibersicurezza cresce in maniera direttamente proporzionale all'età anagrafica. In particolare, analizzando i dati emerge come quasi due italiani su cinque tra i 25 e i 64 anni è carente di conoscenze di sicurezza informatica di base, quota che sale addirittura a sette su dieci se si considera la fascia di età 65-74 e a nove su dieci per gli over 75.

Perciò, **risulta necessario investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità, indipendentemente dal livello di alfabetizzazione digitale già in loro possesso**. Tra le proposte già attive vi è il progetto ***Safer Internet Centre* – Generazioni Connesse, che è co-finanziato dalla Commissione Europea nell'ambito del programma *Digital Europe***, ed è membro di una rete promossa dalla Commissione stessa, che si concretizza nella piattaforma online "*Better Internet for Kids*". Il progetto è coordinato dal MIUR con il partenariato di alcune delle principali realtà italiane che si occupano di sicurezza in rete, tra cui la Polizia di Stato. Il suo obiettivo è quello di fornire informazioni, consigli e supporto a bambini, ragazzi, genitori, docenti e educatori che hanno esperienze in Internet e di agevolare la segnalazione di materiale illegale online.

In quest'ambito rientra il ***Safer Internet Day***, l'edizione 2023 della Giornata mondiale per la sicurezza in Rete, istituita dalla Commissione per promuovere l'utilizzo positivo e consapevole del web. Il *claim* dell'evento è stato "*Together for a better internet*", un invito a cooperare insieme per migliorare l'ecosistema

Fig. 6.10: Quota di italiani che utilizzano internet e di individui che hanno almeno competenze basilari di sicurezza informatica (2023)

Fonte: Eurostat



online, sui temi della cybersicurezza, dell'economia della rete, del cyberbullismo, degli algoritmi, dell'intelligenza artificiale e della democrazia.

Per affrontare il problema dell'*awareness*, **l'*European Cybercrime Centre* (EC3) di Europol e la Federazione Bancaria Europea (EBF) hanno lanciato *Cyber Scams* 2.0**. Alcuni dei materiali della campagna, promossi dalle forze dell'ordine nazionali, dalle associazioni bancarie e da altri soggetti impegnati contro il crimine informatico sui principali social, hanno ad oggetto: le truffe del supporto tecnico, consigli aggiornati sul *Vishing*, furti di identità e SIM *swap*. In Italia, l'iniziativa è promossa dal CERTFin e dalla Polizia di Stato.

Il Centro di Competenza in Cybersecurity Toscano ha promosso un progetto per divulgare e sensibilizzare sui temi della cybersecurity, indirizzato alle PMI e alle pubbliche amministrazioni. Sono stati preparati articoli e brochure inerenti specifici topics differenziati in sei macroaree: principi della sicurezza digitale (crittografia, scambio delle chiavi crittografiche, tecniche di *hashing*); attacchi (*malware*, *ransomware*, *phishing*, DoS, *worm*, virus, *trojan, Sql injection*, *keyloggers* e attacchi ai processori); tecniche di difesa (prevenzione e rilevamento di intrusioni, uso di *firewall*); autenticazione e accesso ai sistemi (autenticazione biometrica, tramite password, da remoto e controllo degli accessi); nuove tecnologie (firma digitale, PEC, VPN, AI); steganografia; sicurezza nell'accesso alla rete. Tali contenuti sono stati pensati per un pubblico che ha una conoscenza basilare degli strumenti informatici e della rete; pertanto, utilizzano un approccio scevro da eccessivi tecnicismi.

Nell'ambito della consapevolezza situazionale alcune aziende italiane si sono impegnate con particolare attenzione, tra queste vi è **Cyber Guru**. Essa ha sviluppato una piattaforma per massimizzare l'efficacia dei processi di apprendimento e consolidare nel tempo la consapevolezza necessaria ad affrontare l'evoluzione delle tecniche utilizzate dal cybercrime. L'obiettivo principale dei processi formativi è quello di incidere

sui comportamenti degli utenti, sviluppando le tre principali caratteristiche difensive: conoscenza, percezione del pericolo e prontezza.
La piattaforma offre un training completo basato su tre percorsi metodologici, ossia quello cognitivo, induttivo ed esperienziale. Il primo programma didattico è il "*Cyber Guru Awareness*", il secondo è il "*Cyber Guru Channel*", che mediante uno schema narrativo tipico delle serie TV permette al discente di apprendere, identificandosi in situazioni reali. Il terzo programma didattico è il "*Cyber Guru Phishing",* un addestramento personalizzato sulla base delle esperienze individuali e del singolo livello di resistenza agli attacchi.
Il progetto ECHO, di cui è partner ACEA, è stato finanziato dall'UE nell'ambito della call H2020-SU-ICT-2018-2020, con lo scopo di creare una rete europea di centri di ricerca e competenza sulla cybersecurity mediante il coordinamento di un unico hub centrale. Quest'ultimo rivede tra i suoi obiettivi quello di definire i programmi di *education e training* sulla cybersecurity, che includono percorsi formativi e qualifiche trasversali e intersettoriali necessarie ai professionisti della materia, oltre alla creazione di sistemi di *training* e simulazione.
Al fine di accrescere la consapevolezza sui potenziali rischi della rete e sensibilizzare ad un uso positivo ed informato della tecnologia, **WindTre ha lanciato l'iniziativa "NeoConnessi", progetto di educazione digitale teso ad accompagnare scuole e famiglie nella fase in cui i bambini si approcciano al mondo digitale**. La quinta edizione è stata rivolta, nell'anno scolastico 2022/2023, al 41% delle scuole primarie italiane per complessivi 350.000 alunni di IV e V in 7.000 istituti. In continuità con tale progetto, la stessa WindTre ha presentato, nel febbraio 2023, il "Decalogo NeoConnessi: 10 passi per famiglie consapevoli e protette in Rete" che individua i principi chiave necessari per le famiglie per orientarsi nel momento in cui i bambini accedono al digitale, contiene una breve guida ed alcune pillole di "cyber saggezza" da seguire per una corretta educazione digitale.
Sempre con lo scopo di promuovere una maggiore consapevolezza sulla sicurezza digitale, il 7 febbraio 2023 **Huawei e Parole O_Stili hanno lanciato l'iniziativa "SmartBus", che ha ricevuto il patrocinio di Regioni, Comuni e associazioni di categoria**. Il progetto si è concluso a Napoli lo scorso 15 maggio e, all'insegna del motto #cybersicuriabordo, ha fatto tappa in 15 città di 5 regioni italiane coinvolgendo oltre 4500 studenti e studentesse delle scuole secondarie di primo guardo, con l'obiettivo di accrescere il loro livello di sicurezza su Internet e mostrare le opportunità e i rischi legati all'utilizzo degli strumenti digitali.
A partire da agosto 2021, Nokia invece ha dato il via a un corso di livello professionale sulla sicurezza delle reti 5G (denominato "*5G Secured networks*") nell'ambito dei ***Nokia Bell Labs***, al fine di consentire ai professionisti del settore ICT di conoscere processi, strumenti, tecnologie e risorse necessari per prevenire e gestire proattivamente le numerose minacce alla sicurezza del 5G in ambienti di rete, software e cloud.
Anche Fastweb offre percorsi di formazione specialistica sulla cybersecurity nell'ambito della ***Fastweb Digital Academy,*** adottando un approccio esperienziale accanto a lezioni teoriche. Ad esempio, il corso gratuito in "*Cyber Security Analyst"* punta a formare la figura omonima, ossia un professionista con forti competenze nel prevenire, individuare e gestire le minacce cibernetiche che possono impattare su software, hardware o reti. La peculiarità di tale corso è che consente ad alcuni discenti selezionati di concorrere per una posizione in un'azienda del network Fastweb.
Nel dicembre 2021, **Vodafone Business – insieme a Generali e Accenture – ha avviato una collaborazione volta a creare un'offerta di servizi di *cyber insurance* per supportare i clienti Corporate e le PMI nella prevenzione e nel contrasto alle minacce cyber**. L'iniziativa comprende simulazioni di *phishing* e programmi di formazione. In particolare, Vodafone Business si occupa di offrire alle imprese servizi di

risposta agli incidenti a seguito di intrusioni e gestendo le relazioni contrattuali con i clienti.

Ulteriore contributo in quest'ambito è offerto da **Ericsson**, per il tramite dei suoi tre centri di Ricerca e Sviluppo di Genova, Pisa e Pagani, i quali si affiancano agli ***Innovation Garage*** **istituiti nel 2020, ossia laboratori tecnologici aperti a studenti, start-up e imprese che si focalizzano su tematiche quali la cybersicurezza, industria 4.0 e 5G**.

Altra iniziativa è **l'*European Cybersecurity Month*** (Fig. 6.11), che vede la collaborazione tra Stati Membri, ENISA e Commissione Europea. Si tratta di una campagna annuale dell'UE volta a promuovere la sicurezza informatica tra i cittadini e le organizzazioni dell'UE e a fornire informazioni aggiornate sulla sicurezza online, attraverso attività di sensibilizzazione e condivisione di buone pratiche. In ambito nazionale, la competenza è stata affidata all'ACN che, nello specifico, ha pubblicato materiali e fornito consulenza di esperti su diversi argomenti di cybersicurezza per il pubblico degli Stati membri.

Fig. 6.11: Locandina del decimo anniversario dell'European Cybersecurity Month

Fonte: Sito web dell'iniziativa European Cybersecurity Month

Gli obiettivi principali della campagna 2023 sono stati: garantire che gli utenti finali e le organizzazioni siano ben informati sui potenziali rischi di sicurezza informatica e permettere che rimangano al sicuro online. I due temi portanti si sostanziano nel *Phishing* e nel *Ransomware*, a causa dei continui attacchi perpetrati durante gli ultimi anni che hanno sfruttato la pandemia da COVID-19. **Importante novità è che dall'edizione svoltasi nel 2023 le campagne informative di sensibilizzazione saranno continuative, differentemente dal passato in cui erano concentrate esclusivamente nel mese di ottobre**.

In ultimo, con il patrocinio dell'ACN, AIPSA, W4CI, ENISA e di altri soggetti di rilievo, è stato presentato alla Camera dei Deputati il "***Cybersecurity 5.0 – Career Day***", il primo *road show* nazionale che nel corso del 2023 ha coinvolto diverse Università del Paese in 6 città italiane (Bari, Firenze, Roma, Padova, Cosenza e Milano) e ha messo in contatto le aziende più competitive del settore e i rappresentanti di importanti realtà, nazionali e locali, con tutti coloro che sono interessati a intraprendere una carriera nel mondo della cybersicurezza. L'edizione 2023, che ha preso avvio il 23 giugno scorso nell'ambito dell'UniBa, si è incentrata proprio lo sviluppo delle abilità e competenze per affrontare le sfide del prossimo futuro.

6.4. L'OFFERTA FORMATIVA NAZIONALE IN MATERIA DI CIBERSICUREZZA

6.4.1. Corsi, Master e Dottorati di ricerca

A partire da 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. Per l'anno accademico

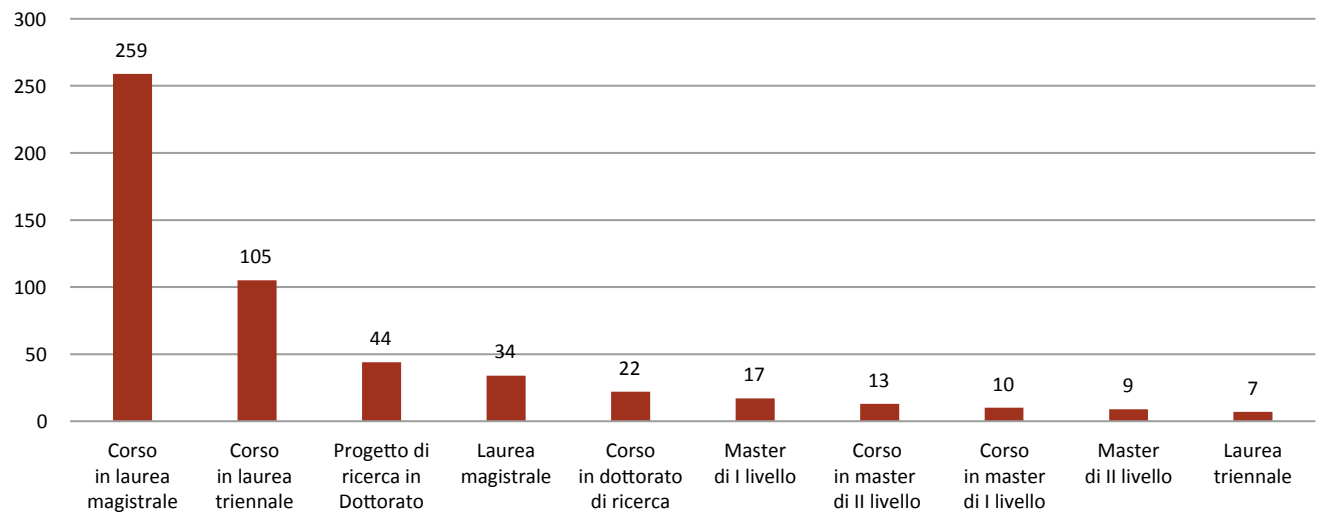
2023/2024[65], si registra la presenza di **520 corsi di formazione** universitaria, in notevole crescita rispetto ai 234 individuati a inizio 2023. I corsi analizzati includono sia insegnamenti singoli all'interno di corsi di laurea più generici[66] ("**offerta formativa non specializzata**"), sia corsi di laurea specifici sul tema, insieme a Master e Progetti di ricerca in Dottorato ("**offerta formativa specializzata**").

Nel dettaglio (Fig. 6.12), su un totale di 99 Università statali e non statali (private, straniere e telematiche) riconosciute dal Miur, il monitoraggio ha rilevato per l'anno accademico 2023/2024 un totale di 520 unità tra insegnamenti e corsi di studio sulla cybersecurity. Tra questi, sono stati osservati 259 insegnamenti singoli all'interno di corsi di laurea magistrale, 105 insegnamenti singoli all'interno delle lauree triennali, **44 progetti di ricerca in dottorati**[67], **34 lauree magistrali**, a fronte di 22 corsi all'interno di dottorati di ricerca, **26 master**, 23 corsi singoli all'interno di master di I e II livello e **7 lauree triennali interamente dedicate 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. Allo stesso tempo, è interessante notare come **le lauree specifiche sul tema della cibersicurezza siano in aumento, giunte a quota 41** (gennaio 2024) rispetto

Fig. 6.12: Offerta formativa specializzata e non specializzata in materia di cybersecurity per tipo (a.a. 2023-24)

Fonte: I-Com, gennaio 2024



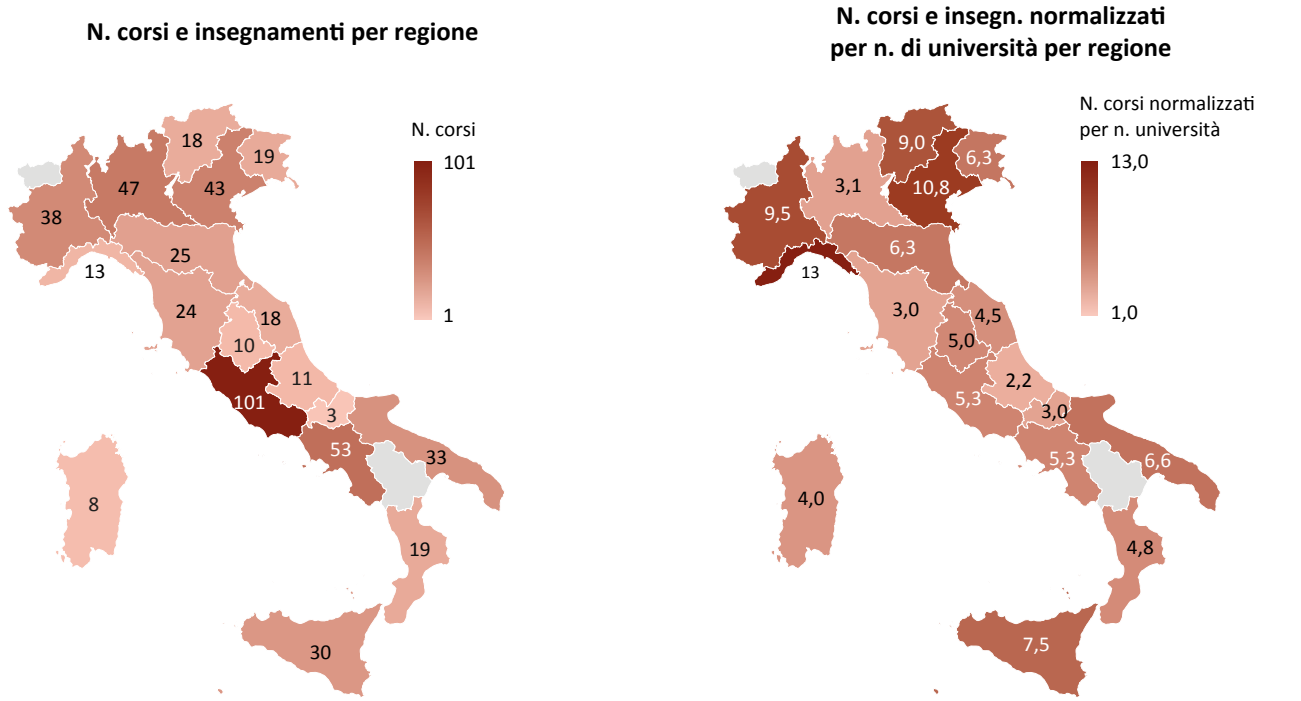
65 Il monitoraggio condotto nel 2022 è stato aggiornato e rimodulato all'inizio dell'anno in corso, includendo l'offerta formativa 2023-2024 disponibile sui siti web delle università statali e non statali, incluse quelle online.

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

67 L'elevato numero di progetti di ricerca in dottorato è dovuto all'attivazione del primo dottorato nazionale in cybersicurezza a partire dall'A.A. 2022- 2023.

Fig. 6.13: Offerta formativa sulla cybersecurity per regione (a.a. 2023-2024)

Note: non sono conteggiati i 7 progetti di ricerca di ricerca in Dottorato ospitati da enti non universitari
Fonte: I-Com, gennaio 2024



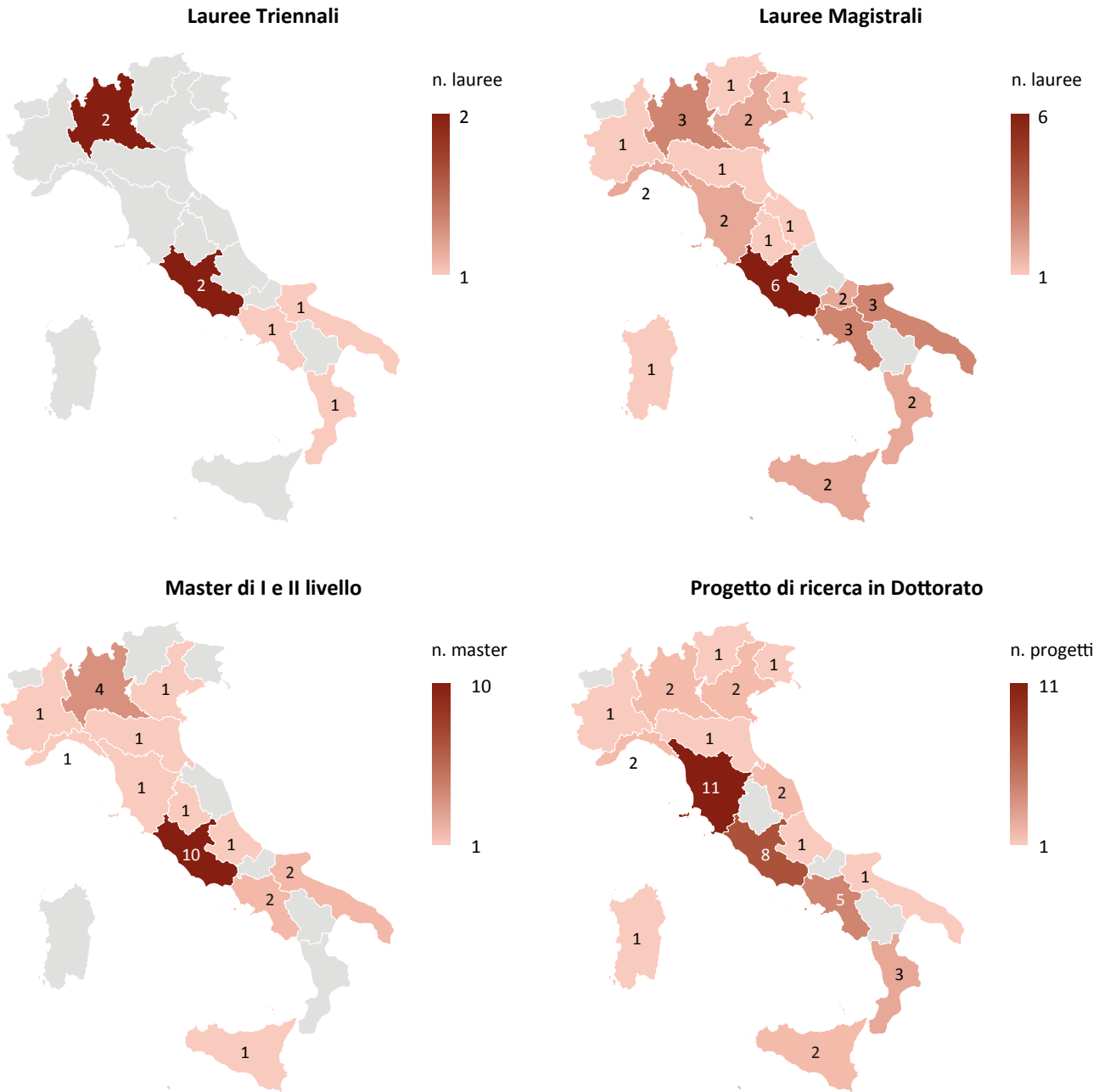
alle 26 rilevate a gennaio 2023). Tuttavia, queste appaiono ancora **relativamente poche e quasi tutte collocate, salvo rare eccezioni, nel ciclo magistrale**.

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** (si v. *infra*), 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 differenze in termini quantitativi abbastanza importanti, ovverosia **ben 70 corsi "specializzati" tra master e progetti di ricerca in dottorati** a fronte delle 41 tra lauree triennali e biennali dedicate. Pertanto, è importante notare come **la formazione specializzata in materia di cibersicurezza in Italia abbia raggiunto quota 111 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. 6.13), con una forte concentrazione nel **Lazio** (101 corsi), in **Campania** (53 corsi) e in **Lombardia** (47), seguite da Veneto (43) e Piemonte (38). La Liguria, in particolare, risulta nettamente prima in termini di corsi in cybersecurity normalizzati per il numero di università presenti sul territorio regionale (con un rapporto di 13:1), seguita da Veneto (10,8:1) e Piemonte (9,5:1). A livello regionale, a gennaio 2024 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere.

Fig. 6.14: Offerta formativa specializzata sulla cybersecurity per regione (a.a. 2023-24)

Note: L'offerta formativa specializzata comprende una Laurea Triennale, una Laurea Magistrale, un Master I Livello, un Master II Livello o un Progetto di ricerca in Dottorato incentrati sul tema della cybersecurity
Fonte: I-Com, gennaio 2024



Analizzando **la distribuzione geografica e universitaria dell'offerta formativa specializzata** (Fig. 6.14), **ossia quella che comprende corsi di studi interamente dedicati alla cybersecurity, il Lazio si conferma la regione più interessata con 26 percorsi complessivi**, catalizzando buona parte dell'offerta in termini di lauree dedicate (8 tra magistrali e triennali). Per quanto concerne la specializzazione post-laurea, invece, nel Lazio si registrano 8 progetti di ricerca in dottorato e 10 master, seguita dalla Toscana (11 progetti di ricerca in dottorato e 1 master) e dalla Campania (5 progetti di ricerca in dottorati e 2 master), mentre chiudono la classifica Friuli-Venezia Giulia (1 progetto di ricerca), Sardegna (1 progetto di ricerca), Trentino-Alto Adige (1 progetto di ricerca) e Umbria con un unico 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 26, **17 di I Livello e ulteriori 9 di II Livello**, di cui **10 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.

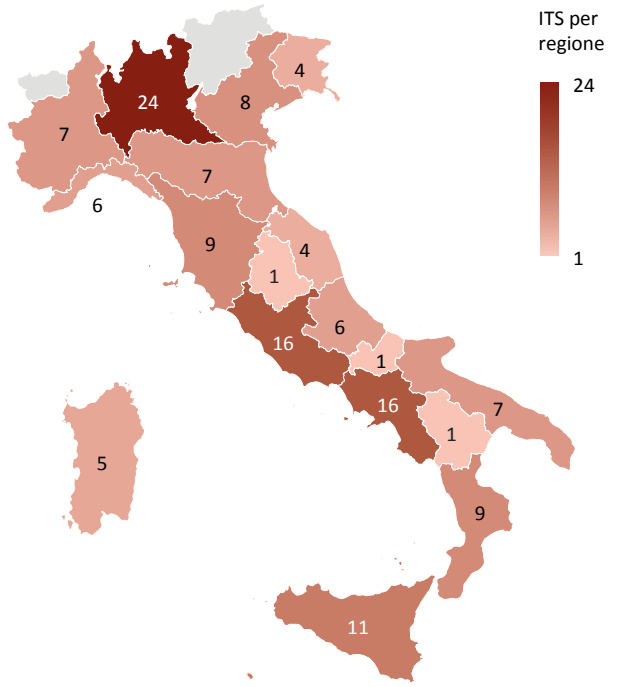
6.4.2. *Lo stato dell'arte e la riforma degli ITS*

Il Ministero dell'Istruzione italiano definisce gli **Istituti Tecnici Superiori 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 rapporto di monitoraggio, pubblicato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE), evidenzia che nel 2023 risultano presenti sul territorio nazionale **142 ITS** (Fig. 6.15). La regione che ospita il numero maggiore di istituti è la **Lombardia** (24), seguita dal Lazio e dalla Campania (16), mentre al terzo posto si trova la Sicilia (11). Al contrario, il Trentino-Alto Adige e la Valle d'Aosta non accolgono ITS, mentre la Basilicata si limita a un solo istituto.

La **Missione 4 del PNRR** sottolinea l'importanza della **riforma del sistema ITS**, attraverso il potenziamento del modello organizzativo e didattico, il consolidamento degli stessi nel sistema ordinamentale

Fig. 6.15: Distribuzione degli ITS per regione (2023)

Fonte: INDIRE



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 2022, della **L. n. 99 del 15 luglio 2022**. Si tratta della riforma degli ITS che 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**. I percorsi formativi vengono distinti in due livelli a seconda del quadro europeo delle qualifiche: il **5° livello EQF** di durata biennale, suddiviso in quattro semestri, con almeno 1.800 ore di formazione comprendenti ore di attività teorica, pratica e di laboratorio e il **6° livello EQF**, di durata triennale, suddiviso in sei semestri, con almeno 3.000 ore di formazione comprendenti attività teorica, pratica e di laboratorio. Il vero punto di forza della riforma risiede nel più forte **legame col mondo delle imprese**. 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. La legge, in una logica di rafforzamento degli ITS, ha istituito anche un **apposito Fondo presso il Ministero dell'Istruzione** con una dotazione di circa **€48 milioni annui** a decorrere dal 2022 da distribuire alle regioni (per il 2022 il riparto è stato disposto con decreto del 26 agosto) al netto di un 5% destinato alla realizzazione delle misure nazionali di sistema, tra le quali il monitoraggio e la valutazione. 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. 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. Al fine di dare attuazione alla legge n. 99/2022 sono stati adottati una serie di provvedimenti. Nello specifico, **il D.M. n. 87, 17/05/2023** si occupa di disciplinare il **Comitato nazionale ITS Academy**, ovverosia l'organo di consulenza del Ministro per lo sviluppo del sistema terziario di Istruzione tecnologica superiore. Tale organo fornisce proposte per l'aggiornamento delle aree tecnologiche e delle figure professionali, indica linee di indirizzo generali che verranno applicate ai piani triennali di programmazione regionali; propone azioni per favorire maggiore inclusione di genere e suggerisce indicazioni per lo sviluppo di forme di collaborazione fra gli ITS Academy. **Il D.M. n. 88, 17/05/2023** definisce la **composizione e il funzionamento** della **commissione per la valutazione delle prove di verifica finale del percorso ITS**; stabilisce la **tipologia delle prove e i punteggi** assegnati al termine della verifica finale; prevede il riconoscimento di **crediti per agevolare i passaggi da un percorso ITS ad altri percorsi ITS** e per valorizzare le esperienze acquisite in altri contesti, incluso quello lavorativo. La valutazione dell'allievo non sarà esclusivamente basata sulla prova finale, ma una parte del punteggio sarà attribuita in base alla **valutazione dell'intero percorso di studi**. Per gli **studenti con DSA** sono previsti **strumenti compensativi**, mentre per gli allievi con **disabilità** sono previste prove di verifica equivalenti, che assicurino comunque le competenze in uscita della futura figura professionale. Tale decreto si applica solo agli iscritti al primo anno dei percorsi ITS a partire dall'anno formativo 2023/24. **Il D.M. n. 89, 17/05/2023** fissa gli standard minimi dello **Statuto delle Fondazioni ITS Academy**, uno schema di regole cui le Fondazioni potranno ispirarsi per definire i loro singoli statuti. È stato innalzato il patrimonio minimo che le fondazioni dovranno avere in dote per poter operare, da €50mila a €100mila, elevabile ulteriormente in caso di ITS operanti su più aree tecnologiche, così da fornire maggiore solidità al sistema e garantire maggiormente gli studenti. **Il D.M. n. 144, 21/07/2023** concerne l'assegnazione delle risorse nazionali relative all'esercizio finanziario 2023, di cui al Fondo per l'istruzione tecnologica superiore e l'implementazione degli indirizzi di programmazione nazionale per la valorizzazione e il rafforzamento dei percorsi formativi degli ITS Academy. **Il D.M. n. 1385, 10/08/2023**, ripartisce le risorse del Fondo per l'istruzione tecnologica superiore agli ITS Academy per l'e.f. 2023; **il D.M. n. 191, 4/10/2023**, definisce i requisiti e gli standard minimi per il riconoscimento e l'accreditamento degli ITS Academy, nonché dei presupposti e delle modalità per la sospensione e la revoca dell'accreditamento; **il D.M. n. 203, 20/10/2023**, delinea le disposizioni concernenti le aree tecnologiche, le figure professionali nazionali di riferimento degli ITS Academy e gli standard minimi delle competenze tecnologiche e tecnico-professionali. **Il D.M. n. 217 del 15 novembre 2023**, richiama i criteri per autorizzare un ITS Academy ad operare in una o più aree tecnologiche; i tre **DM del MIUR (n. 227, n. 228, n. 229) del 30 novembre 2023** concernono aspetti rilevanti per la definizione degli indicatori di realizzazione e di risultato dei percorsi ITS Academy e il nuovo Sistema nazionale di monitoraggio e valutazione del sistema terziario di istruzione tecnologica superiore. Ulteriori otto decreti sono stati adottati nel

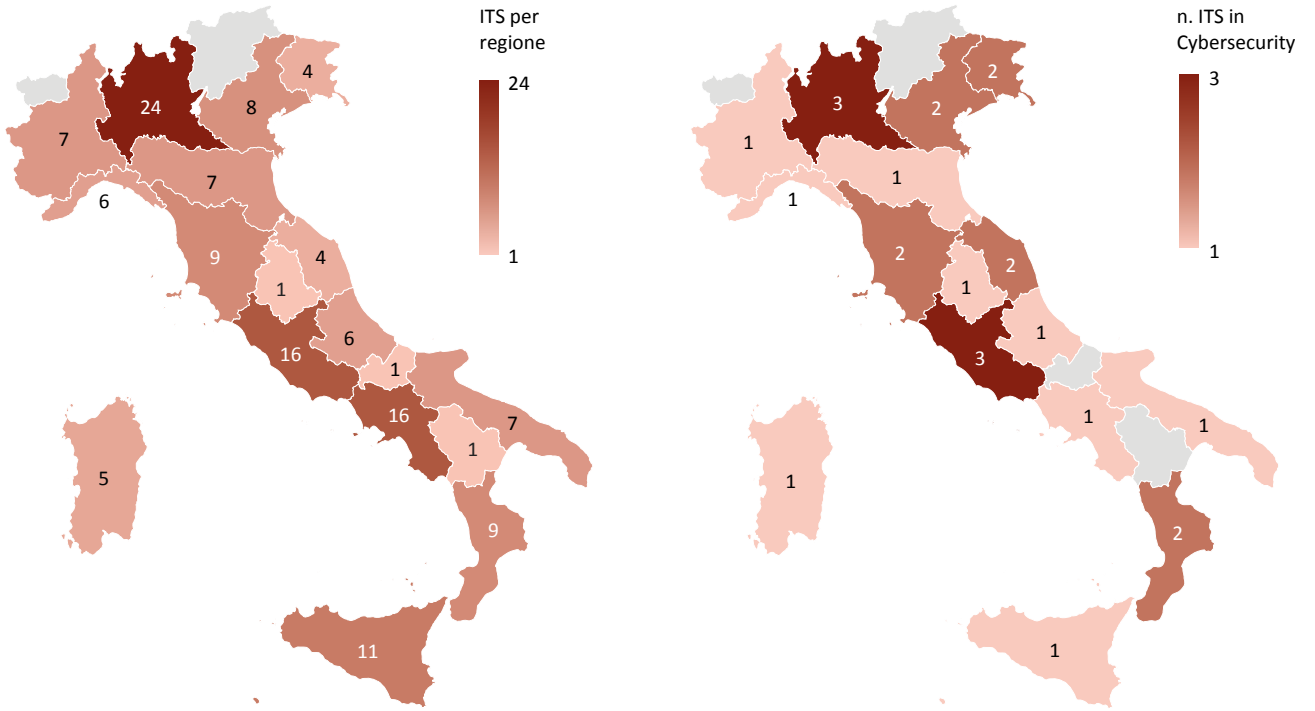
mese di dicembre, tra i quali assume particolare rilievo il **D.P.C.M del 29 dicembre 2023** in merito all'individuazione di figure professionali nazionali per i nuovi percorsi degli ITS Academy di sesto livello EQF e il più recente **D.M. n. 259**, che regolamenta la fase transitoria, della durata di tre anni, della legge n. 99 del 2022[68].

6.4.3. La sicurezza informatica nei corsi ITS

La costante diffusione degli ITS registratasi nell'ultimo anno e la particolare efficacia della loro offerta formativa sono andate di pari passo con le esigenze del mercato e con lo sviluppo tecnologico. Appare quindi evidente e necessario che gli Istituti si adoperino al fine di offrire curricula in cybersecurity al fine di formare i nuovi esperti del settore. Il **5 ottobre 2022** è stato firmato, al Ministero dell'Istruzione, l'**Accordo per la Rete di coordinamento nazionale per lo sviluppo di percorsi formativi specifici in Cybersecurity nell'ambito degli ITS Academy**. Detto atto sigla una serie di obiettivi di collaborazione fra Ministero dell'Istruzione, Regione Emilia-Romagna, Regione Lombardia, Regione Liguria, Regione Puglia, Regione Umbria, Ministero per l'innovazione tecnologica e la transizione digitale, ACN, Confindustria, Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa, Associazione Nazionale degli ITS e Fondazione Leonardo - Civiltà delle macchine. Lo scopo è quello di creare un ecosistema nazionale per la formazione delle nuove competenze digitali, supportare

Fig. 6.16: Comparazione tra il numero di ITS per regione e ITS che si occupano di Cybersecurity

Fonte: INDIRE (giugno 2023); I-Com (gennaio 2024)



68 Per un aggiornamento continuo sul tema consultare il sito: https://temi.camera.it/leg19/temi/la-riforma-degli-istituti-tecnici-superiori-its.html.

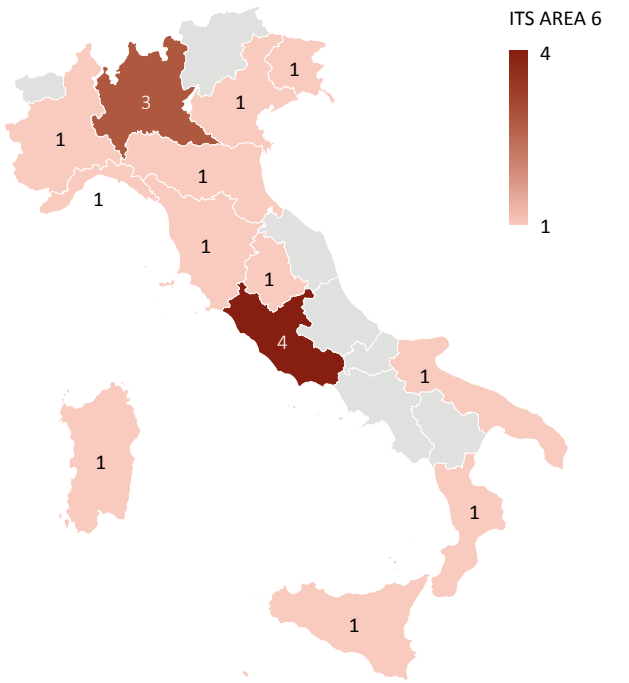
la valorizzazione delle migliori esperienze, anche in ambito **Cloud Computing e Cybersecurity**, sostenere la formazione di tecnologie altamente specializzanti, con possibilità di sbocchi a tutti i livelli, sia nella PA, che nel settore privato. L'accordo rientra nel **percorso di rafforzamento della formazione terziaria professionalizzante** che si è avuto con l'approvazione in Parlamento della riforma degli ITS. Secondo il Direttore Generale dell'ACN l'accordo è tra gli impegni chiave della Strategia Nazionale di Cybersicurezza, che vede nella formazione specialistica una priorità assoluta per assicurare la **trasformazione digitale** solida attraverso la creazione di un'adeguata **forza lavoro nazionale**, composta da soggetti con competenze in sicurezza informatica. Inoltre, egli sottolinea come lo strumento degli ITS rappresenti la migliore risposta a livello territoriale per garantire tecnici necessari alle imprese e alle amministrazioni italiane che affianchino gli ingegneri e gli informatici derivanti dalle Università nazionali. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-COM (Fig. 6.16), gli ITS che si occupano di cybersicurezza sono il **17,6%** rispetto al numero complessivo di quelli attivi. La **Lombardia** primeggia con 3 istituti su 24 totali, seguita dal Lazio che ne ha 3 su 16. Il Veneto, il Friuli-Venezia Giulia, la Toscana, le Marche e la Calabria registrano 2 istituti che si occupano di cyber, rispettivamente, su un numero di 8, 4, 9, 4 e 9 totali per regione.

La maggior parte di questi corsi fa capo agli ITS appartenenti all'**area delle Tecnologie dell'Informazione e della Comunicazione (area 6)** che generalmente offre percorsi su metodi e tecnologie per lo sviluppo di sistemi software, organizzazione e fruizione dell'informazione e della conoscenza, architetture e infrastrutture per i sistemi di comunicazione, nonché su gestione della supply chain digitale, Cyber security, *Cyber threat Intelligence*, gestione dei Big data, cloud e architetture digitali per Industria 4.0. Dalla mappa di seguito riportata (Fig. 6.17) si osserva che il Lazio ha il numero maggiore di ITS appartenenti all'area ICT, immediatamente seguito dalla Lombardia, anche se contestualmente sono lasciate scoperte sette regioni (Valle d'Aosta, Trentino-Alto Adige, Marche, Molise, Abruzzo, Campania e Basilicata).

L'area 6 non è l'unica coinvolta, in quanto la cibersicurezza risulta un tema altamente trasversale, una vera e propria garanzia per le attività di ogni settore. Pertanto, anche in aree come **"Nuove tecnologie per il Made in Italy"** o **"Mobilità Sostenibile"** si rinvengono corsi specifici tra cui **"Sistema cloud e cybersecurity"**[69] o "**Cybersecurity nel cluster marittimo portuale"**[70] e insegnamenti all'interno di corsi

Fig. 6.17: Numero degli ITS collocati nell'area 6 (Tecnologie dell'informazione e della comunicazione)

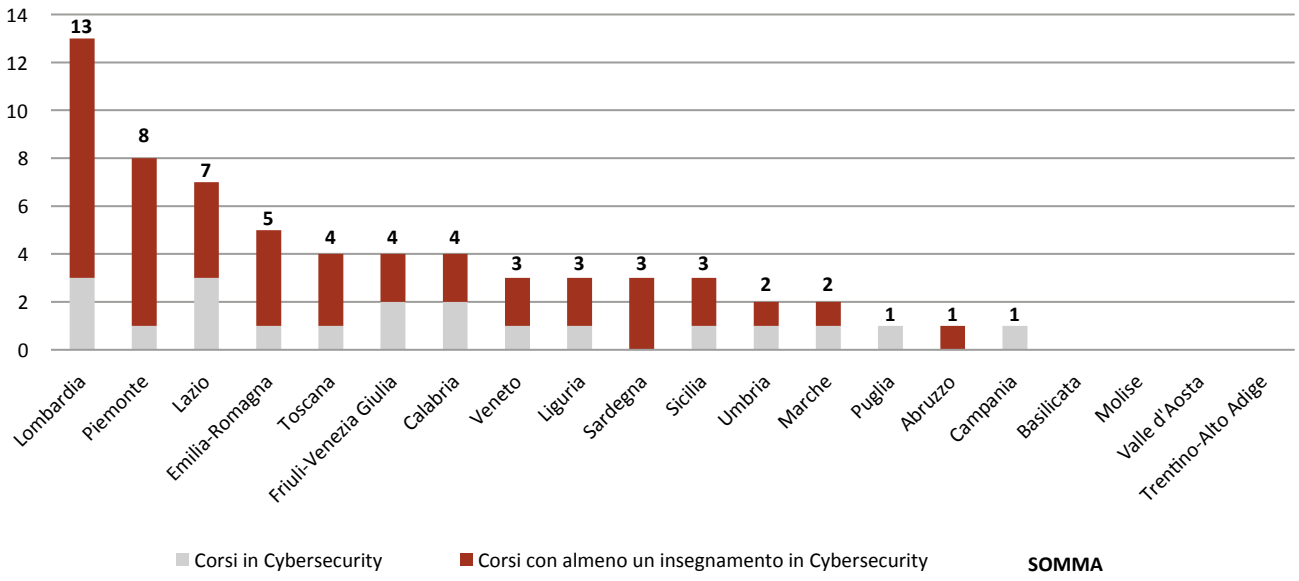
Fonte: INDIRE, 2023



69 Si fa riferimento nello specifico all'ITS "INCOM ACADEMY".
70 Si fa riferimento nello specifico all'Accademia Nautica dell'Adriatico.

Fig. 6.18: Distribuzione per regione corsi in Cybersecurity e corsi con almeno un insegnamento in Cybersecurity

Fonte: I-Com, 2024



incentrati su materie differenti, tra cui **"Intenet of Things"**[71], **"Cloud developer"**[72] e **"Tecnico Superiore per l'informatica nell'Industria 4.0"**[73].

È possibile distinguere i **corsi sulla sicurezza informatica** dai **corsi con almeno un insegnamento incentrato sul tema** (Fig. 6.18). La Lombardia presenta una relazione di 10 corsi specifici rispetto a 3 insegnamenti appartenenti alla seconda categoria, distribuiti in tutto il territorio regionale. A sua volta, il Piemonte è connotato da un rapporto di 7 a 1, seguito dal Lazio (4 a 3) e dall'Emilia-Romagna (4 a 1). Puglia e Campania hanno un unico corso in cybersecurity, mentre l'Abruzzo presenta un solo insegnamento legato a corsi non specifici in cyber. Inoltre, sono 4 le regioni (Basilicata, Molise, Valle d'Aosta e Trentino-Alto Adige) che non presentano alcun corso afferente alle due tipologie summenzionate.

Tra le figure professionali che potranno essere create mediante gli ITS va menzionata quella di **Tecnico Esperto nei processi di governance e compliance in ambito di sicurezza delle informazioni** che si occuperà di analizzare e monitorare il livello di sicurezza delle organizzazioni, le quali in tal modo risulteranno *compliant* a normative nazionali e internazionali in ambito Cybersecurity, privacy e Information Security. Inoltre, potranno diffondersi professioni come il **Tecnico Esperto nella ricerca e nell'analisi di informazioni da fonti aperte (OSINT)** che fornisce informazioni utili per incentivare il decisore competente all'adozione di specifiche strategie di cybersecurity. Egli sfrutta le fonti aperte, accessibili a tutti, e utilizza tool che agevolano l'attività di ricerca. Anche il **Tecnico Esperto in sicurezza delle reti, dei sistemi e dei servizi informatici** rientra nei futuri sbocchi

71 Si fa riferimento all'ITS "INCOM ACADEMY".
72 Ibidem.
73 Si fa riferimento all'ITS "Prime Web Academy".

occupazionali. Egli determina strumenti e metodologie efficaci per proteggere l'infrastruttura IT aziendale, valuta le vulnerabilità hardware e software mediante attività di *Vulnerability Assessment* e *Penetration Test* e predispone contromisure tecniche, tecnologiche e organizzative per garantire la resilienza di reti, sistemi e servizi informatici di organizzazioni pubbliche e private. In base al quadro sin qui delineato, si prospetta, conformemente a quanto previsto dall'accordo con l'ACN sopracitato, un aumento del numero degli ITS che forniranno percorsi in cybersecurity e l'implementazione di discipline in materia all'interno di corsi volti a professionalizzare esperti che, oltre alle mansioni afferenti al proprio settore, sapranno usare la rete e proteggersi dai pericoli che da essa ne derivino.

CONCLUSIONI

Alla crescente espansione del digitale si accompagna, inevitabilmente, un'estensione della superficie attaccabile e, dunque, la necessità di implementare strumenti e misure in grado di prevenire e contrastare gli attacchi informatici e le conseguenze degli stessi.

In questa sfida che globalmente interessa tutti gli stati e tutti i soggetti, siano essi individui, imprese e o PA, l'UE sta affrontando le sfide legate alla cybersecurity attraverso l'adozione di una serie piuttosto corposa di interventi normativi, molti dei quali regolamenti, nel tentativo di ridurre la frammentazione normativa e creare un ecosistema di sicurezza efficace, chiaro e *future-oriented.*

Un tassello cruciale di questo complesso ed articolato puzzle è rappresentato senza dubbio dalla NIS2 attraverso la quale si punta a superare l'attuale frammentazione normativa e di rispondere in maniera adeguata alle nuove minacce ed alle nuove criticità poste in materia di cibersicurezza. Si tratta di uno strumento straordinariamente importante che nella logica di rafforzare i presidi di sicurezza estende notevolmente il novero dei soggetti destinatari dei numerosi e complessi obblighi dalla stessa individuati fissando però delle soglie per quei soggetti pubblici o privati ricompresi nelle tipologie denominate "alta criticità" o "altri settori critici**"** che, in una logica di tutela e sviluppo della concorrenza, consente di non porre a carico di tali soggetti oneri sproporzionati con conseguenti inevitabili impatti anche sulla catena dei fornitori.

Nonostante questo rischio di carattere generale, la disciplina NIS2 prescrive l'adozione di misure tecniche, operative e organizzative ed obblighi di segnalazione stringenti in caso di incidenti significativi, chiamando gli organi di gestione dei soggetti rientranti nell'ambito applicativo della direttiva a garantire la sicurezza della rete e dei sistemi informativi, la compliance alla disciplina della direttiva ed un'attività di collaborazione con le autorità competenti in materia, imponendo un vero e proprio ripensamento dell'organizzazione e delle procedure aziendali.

Si tratta di una sfida straordinariamente complessa, come testimoniato **dalla survey condotta da I-Com** nel contesto italiano, nell'ambito della quale **la maggior parte dei partecipanti ritiene che il crescente numero di adempimenti previsti dalle normative in cybersicurezza può impattare sulla competitività aziendale** principalmente a causa degli oneri burocratici e amministrativi richiesti, nonché per gli investimenti tecnico-organizzativi necessari alla compliance, con possibili **ripercussioni anche sui rapporti con la supply chain.**

I principali fattori che rendono difficoltoso il processo di compliance sono: la **mancanza di competenze idonee (sia interne che sul mercato del lavoro)**, seguito **dall'incertezza interpretativa della normativa** e alla **moltiplicazione** – a volte disorganica – **di prescrizioni** che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo. Pertanto, alcune imprese ritengono utile un maggiore sforzo, tra l'altro, a supporto delle PMI e verso l'accrescimento del grado di consapevolezza in materia cyber dei livelli apicali e di indirizzo strategico**.**

Nonostante lo scenario di contesto non propriamente ottimistico e considerando che le direttive NIS2 e CER sono ormai in vigore da mesi e che dal 18 ottobre 2024 saranno pienamente applicabili**, il 51,2% delle imprese rispondenti sta ancora valutando se incrementare le risorse destinate alla cibersicurezza e il 12,6% ha deciso di non stanziare ulteriori risorse**.

Una parte corposa dell'indagine si è soffermata sulle certificazioni volontarie di cybersecurity ed è emerso che **il maggior numero di imprese afferenti alle tre classi dimensionali considerate non ha conseguito alcun tipo di certificazione**. Simili risultanze sarebbero giustificate dai costi elevati del processo di certificazione, che non sono percepiti come proporzionati ai benefici, nonché dai tempi troppo dilatati per

giungere al rilascio della certificazione stessa. Piuttosto rilevante sul punto è il segnale lanciato da alcuni soggetti intervistati, per cui uno scarso ricorso a tali strumenti sarebbe influenzato dalla mancanza di competenze interne e, in alcuni casi, dalle scelte aziendali di perseguire certificazioni solo per il *core business*, poiché *client facing*. **Appare incoraggiante, invece, che il 70% dei rispondenti sia d'accordo in merito al fatto che standard comunitari (es. EUCC) possono incentivare le imprese a certificarsi**.

Uno degli aspetti più interessanti dell'indagine riguarda i modi con cui gli intervistati ritengono sia possibile migliorare lo stato della cibersicurezza in Italia. Secondo **l'81% dei rispondenti si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze**. Tale opzione è risultata la più selezionata da tutte e tre le classi dimensionali considerate, a conferma del fatto che si tratti di un aspetto particolarmente sentito nel Paese. Di rilievo, anche il suggerimento circa l'assegnazione della responsabilità ai *vendor* e ai produttori di hardware e software, affinché garantiscano il supporto ai prodotti per periodi di tempo adeguati a consentire alle aziende la gestione del ciclo di vita degli stessi. Più nel dettaglio**, la cosiddetta *End of Sale* (EoS) dovrebbe essere almeno 5 anni prima della *End of Maintenance* (EoM)**. Per oltre il 55% dei rispondenti sarebbe opportuno **superare la logica dei test obbligatori dinanzi al CVCN in favore dell'accreditamento dei fornitori di fiducia**, prevedendo, al contempo, rimedi contrattuali per legge, nonché adeguate forme di responsabilizzazione nei confronti dei fornitori stessi, oppure – come espresso dal 44% – optare per un approccio semplificato con tempistiche controllate secondo una valutazione dei rischi basata su criteri standard.

Dalle risposte appare inoltre evidente come **l'esecuzione di frequenti test, che allungano i tempi e incrementano i costi, possa avere effetti negativi sul *time-to-market* delle imprese**, come complicare la programmazione circa l'acquisto di soluzioni tecnologiche aggiornate e più performanti anche in termini di sicurezza, oltre che poter causare un danno di immagine alla concezione che hanno gli operatori della cybersecurity, la quale **potrebbe essere percepita come un fattore ostativo e non abilitante alla digitalizzazione e all'innovazione**.

Se la NIS2 rappresenta il fulcro del nuovo sistema europeo della cybersecurity, la costellazione normativa europea è illuminata da numerosi altri atti tra cui la direttiva CER sulla resilienza dei soggetti critici, il Cybersecurity Act del 2019 attualmente in fase di revisione per i "servizi di sicurezza gestiti", il Cyber Resilience Act (CRA) sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, il Digital Operational Resilience Act (DORA) per la cybersecurity delle società finanziarie che, oltre alle singole e specifiche questioni oggetto di dibattito nell'ambito delle procedure legislative ancora in corso, pongono un tema più generale che è non più tanto quello dell'omogeneità degli obblighi che, attraverso i regolamenti, tende a ridursi fino ad azzerarsi, quanto piuttosto, quello del **coordinamento delle varie discipline**. È fin troppo evidente, infatti, la necessità di continuare ed anzi rafforzare l'opera già intrapresa dalle istituzioni europee nell'ambito delle varie proposte in discussione (rispetto, ad esempio, agli obblighi di segnalazione degli incidenti), di razionalizzazione del set di prescrizioni a vario titolo gravanti su soggetti che svolgono attività strategiche o comunque particolarmente sensibili al fine di rendere chiari e proporzionati gli obblighi a carico delle imprese nel tentativo, mai semplice, di trovare un efficace bilanciamento tra l'esigenza di rafforzare la sicurezza da un lato e di favorire l'innovazione dall'altro.

Se l'UE è impegnata a disegnare il proprio quadro normativo sulla sicurezza, l'Italia ha avviato l'iter di **recepimento della direttiva NIS2** prevedendo espressamente tra i principi e criteri direttivi l'esigenza di coordinamento con le altre le disposizioni

relative alla direttiva CER, al regolamento DORA e alla direttiva n. 2556/2022 in materia di servizi finanziari. Il recepimento di tale direttiva si tradurrà in un decreto legislativo che si innesterà in un contesto generale che, da una parte, vede continuamente rafforzare i poteri speciali ed estenderne gli ambiti di esercizio e, dall'altra, assiste alle prime stagioni applicative della normativa sul perimetro di sicurezza nazionale cibernetica che con non poche difficoltà è giunta a completamento. Nonostante le evidenti differenze tra la direttiva NIS2, che si focalizza sull'assicurare la continuità operativa dei soggetti essenziali e importanti e la disciplina sul PSNC, che pone la sua attenzione su aspetti maggiormente legati alla sicurezza nazionale, **è auspicabile che si faccia tesoro dell'esperienza applicativa di questi anni, anche per evitare sovrapposizioni di adempimenti, in particolar modo per quegli operatori che saranno obbligati al rispetto di entrambe le discipline**. Ad esempio, si può immaginare che le misure di sicurezza di natura tecnica e organizzativa delineate nell'allegato B del DPCM 14 aprile 2021, n. 81 siano quantomeno prese in considerazione per delineare nel dettaglio i requisiti di sicurezza a norma dell'art. 21 della direttiva NIS2. In tema di **certificazioni volontarie di cybersicurezza**, è auspicabile che l'iter conclusosi di recente sulla creazione degli *European Common Criteria* (EUCC) possa **stimolare e incentivare le organizzazioni e i laboratori nazionali a certificare un numero maggiore di prodotti e sistemi ICT**, dato che tali standard puntano a garantire **livelli di sicurezza elevati** e un'**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, consentendo di affrontare in maniera più efficace la dinamicità tipica della minaccia cibernetica. Naturalmente, ciò non può prescindere da un **lavoro di costante confronto e collaborazione** a livello europeo e nazionale per guidare al meglio tutti i soggetti coinvolti nella transizione verso questo nuovo paradigma, puntando innanzitutto sulla chiarezza per quanto riguarda il rapporto costi/benefici di tali certificazioni, avendo il fine ultimo di **irrobustire la postura di cybersicurezza nazionale**.

L'esigenza di rafforzare e innalzare il livello delle competenze in cybersecurity di cittadini e imprese trova un sostegno significativo nell'istituto del partenariato pubblico-privato. Il report dell'OSCE di marzo 2023 che si focalizza sulle **pratiche emergenti in tema di PPP e altre forme di collaborazione in ambito cybersecurity**, consente di costatare come questo genere di coinvolgimento rappresenti ad oggi un tema di primaria importanza per gli Stati intervistati. Contestualmente, non va sottovalutato che vi sono una serie di ostacoli da superare in merito, ad esempio, a misure per **incentivarne la nascita e il monitoraggio continuativo**. Difatti, mappare queste iniziative e tutte le **altre forme di partnership pubblico-privata che coinvolgono anche direttamente la stessa ACN**, risulta necessario per comprendere come il territorio nazionale stia rispondendo all'esigenza di aumentare l'awareness, la formazione e l'innovazione in sicurezza informatica. Appare evidente che per raggiungere questo obiettivo sia opportuno **instaurare un costante dialogo tra tutti gli stakeholder**, incluse le PMI, gli istituti di ricerca e i soggetti che si occupano, in particolar modo, di infrastrutture critiche.

Dai dati citati emerge una grave arretratezza da parte dell'Italia in materia di competenze e consapevolezza digitali. Infatti, **l'Italia performa peggio della media europea in quasi tutti gli ambiti rilevanti**, invero è addirittura quartultima per diffusione di competenze digitali almeno di base. Allo stesso tempo, tra le imprese italiane sembra esserci uno scarso livello di consapevolezza con riferimento ai rischi cibernetici, in quanto **soltanto il 16,4% delle aziende con più di 10 addetti ha un'assicurazione per problemi di sicurezza ICT** (contro il 25% della media UE). Definisce un ulteriore quadro allarmante l'ultimo rapporto della Polizia Postale sul 2023, il quale rileva un aumento

degli illeciti, passati da 15.394 a 16.325 su base annua, e un aumento dell'ammontare sottratto, da 114,5 milioni a 137,2 milioni di euro. Quest'ultimo dato viene anche affiancato da un costo medio delle violazioni dei dati che in Italia è in aumento rispetto a Paesi come Francia e Germania.

Sulla scorta di tali premesse, appare cruciale insistere sul **rafforzamento della cultura di base in cibersicurezza**, dato che le tecniche e le modalità degli attacchi cibernetici che singoli individui e organizzazioni pubbliche e private subiscono ancora oggi e che si ripercuotono in maniera anche piuttosto importante sulle rispettive attività quotidiane sono pressoché le medesime ormai da diversi anni. Pertanto, **è necessario investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità, indipendentemente dal livello di alfabetizzazione digitale già in loro possesso**. Ad oggi, molte delle iniziative già attive in questo campo nascono e si sviluppano anche grazie al settore privato, spesso in collaborazione e/o col patrocinio di enti pubblici. Appare dunque importante che queste forme di collaborazione pubblico-privato possano essere ulteriormente rafforzate e messe a sistema.

Inoltre, sarebbe opportuno puntare sulla **formazione in ambito ICT e specializzata in ambito cybersicurezza sin dai primi anni di scuola**, inserendo materie come il pensiero computazionale, la sicurezza informatica e la formazione digitale nei rispettivi curricula di studio, per poi proseguire con iniziative di **partnership strategica tra pubblico e privato per i successivi gradi di istruzione**. Allo stesso modo, non andrebbe sottovalutato il valore della **formazione continua, digitale e specializzata in cybersecurity per le imprese, soprattutto se di piccole e medie dimensioni**, anche in virtù del fatto che a breve saranno applicabili importanti normative dell'UE connesse a tale materia, il che comporterà nuove sfide per i soggetti che ricadono nel rispettivo campo di applicazione.

Dati piuttosto incoraggianti provengono dal versante della **formazione universitaria**. 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 520 tra corsi e insegnamenti offerti a gennaio 2024 rispetto ai 234 individuati a gennaio 2023. In particolare, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 111 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 (101 tra corsi e singoli insegnamenti), in Campania (53) e in Lombardia (47). Pertanto, ulteriori azioni potrebbero essere intraprese per incentivare una **maggiore capillarità a livello territoriale** di tale formazione, 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 della PA. In questo senso, anche nell'ottica di estendere il più possibile la formazione specialistica nell'ambito della cibersicurezza, assume particolare rilevanza la **Riforma degli Istituti Tecnici Superiori**, i quali possono fungere da ulteriore e fondamentale anello di congiunzione tra la realtà scolastica e quella lavorativa. Attualmente, la formazione garantita dai 142 ITS attivi sul territorio, seppur in aumento, viene ritenuta non sufficiente da parte del tessuto imprenditoriale. Di conseguenza, un aumento più consistente di questo tipo di Istituti e, in particolare, **l'incremento degli ITS che si occupano di tematiche connesse alla cibersicurezza** (a gennaio 2024, corrispondenti a un mero 17,6% rispetto al numero complessivo di quelli attivi) potrebbe costituire un ulteriore tassello in direzione della costruzione e del rafforzamento di un ecosistema maggiormente resiliente di fronte alle crescenti minacce provenienti dalla rete, anche in virtù dell'instabile scenario geopolitico attuale. Per permettere

l'avanzamento di tali Istituti sarà cruciale innanzitutto l'intervento del legislatore che, mediante i numerosi decreti attuativi della legge n. 99/2022, renderà realmente esecutive le previsioni della Riforma.
Peraltro, accanto a un'imprescindibile importanza circa gli investimenti per innalzare il livello di competenze tecnico-scientifiche in cybersecurity, anche grazie alle risorse finanziarie stanziate nell'ambito del PNRR, sarebbe opportuno puntare maggiormente su un **dialogo multidisciplinare in ambito cybersecurity**, attraverso un approccio cooperativo basato su una strategia efficace anche in ambito formativo, avendo cura di differenziare adeguatamente la consapevolezza di base in cybersicurezza, indirizzata a ciascun individuo in quanto tale, da quella pensata per quei soggetti che – in virtù del contesto in cui operano – possono entrare in contatto con una o più tipologie di rischi cibernetici e, pur non essendo esperti della materia, dovrebbero essere in grado di riconoscerli e comunicarli ai soggetti specializzati.

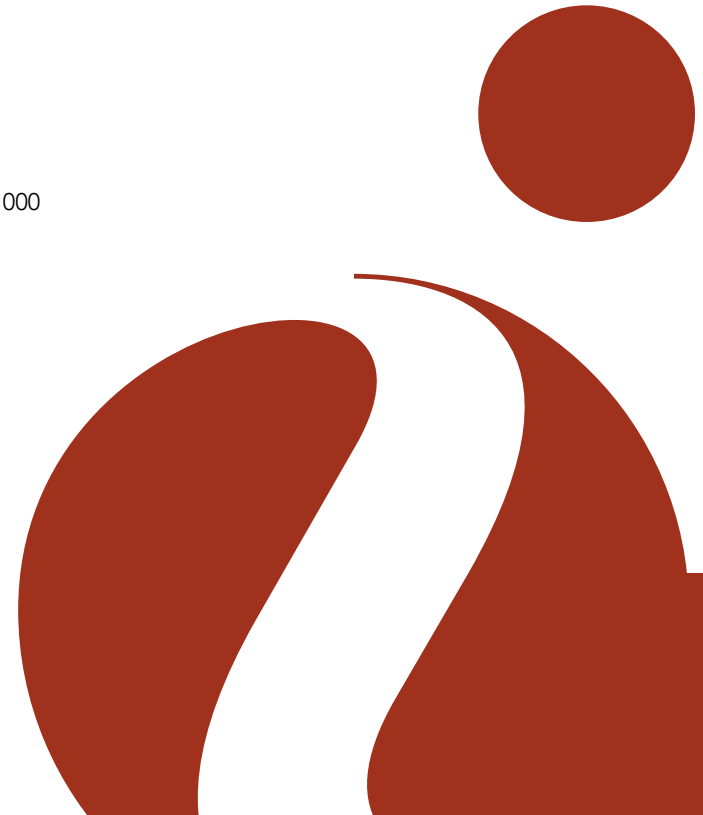
Si evidenzia inoltre che la presente pubblicazione contiene informazioni
di carattere generale. Prima di prendere decisioni o adottare iniziative che possano incidere
sui risultati aziendali, si consiglia di rivolgersi a un consulente
per un parere professionale qualificato. L'Istituto per la Competitività
è da ritenersi non responsabile per eventuali perdite subite da chiunque utilizzi
o faccia affidamento su questa pubblicazione.

Crediti fotografici:
Copertina – vska/Depositphotos.com

Impaginazione:
kreas.it

icom
cibersicurezza

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