icom 2005 25
istituto per la competitività

RAPPORTO OSSERVATORIO
SULLA CIBERSICUREZZA

COMPETITIVITÀ ALLA PROVA DELLA CYBERSECURITY

La sicurezza informatica in Italia e in Europa tra innovazione e regole

MARZO 2025

icom 2005 25
istituto per la competitività

RAPPORTO OSSERVATORIO
SULLA CIBERSICUREZZA

COMPETITIVITÀ ALLA PROVA DELLA CYBERSECURITY

La sicurezza informatica in Italia e in Europa tra innovazione e regole

MARZO 2025

CURATORI
Stefano da Empoli
Silvia Compagnucci
Domenico Salerno

AUTORI
Silvia Compagnucci
Alessandro D'Amato
Matteo Cassoli
Domenico Salerno

Il presente report è aggiornato alla data del 23 gennaio 2025

I-Com Edizioni

ISBN 9791280680167
Marzo 2025

INDICE

EXECUTIVE SUMMARY

CAPITOLO 1 – IL QUADRO EUROPEO E NAZIONALE DELLA SICUREZZA INFORMATICA

La **minaccia cibernetica** 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 cybersicurezza. Difatti**, siamo dinanzi ad attacchi sempre più gravi, numerosi e specializzati, che spingono i Paesi e le organizzazioni internazionali allo sviluppo di policy, strategie e normative che pongono al centro la tutela del cyberspazio per le cittadini, imprese e articolazioni statali.**

Secondo l'ultimo rapporto Clusit, pubblicato a novembre 2024, **a livello globale il primo semestre di quest'anno si configura come il peggiore di sempre, con 1.637 eventi malevoli rilevati,** registrando un incremento del 23% sul semestre precedente. Per quanto concerne l'analisi delle vittime classificate per categoria d'appartenenza, nel primo semestre di quest'anno **la maggioranza degli eventi ha colpito il settore sanitario (18%), seguito dalle Governativo/Militare/Law Enforcement (13%) e dal segmento finanza/assicurazioni (8%)**. Inoltre, il 16% degli attacchi rilevati non ha visto un destinatario specifico, bensì target multipli. Diversamente, i settori inerenti arti e intrattenimento, così come quelli dell'energia e delle telecomunicazioni hanno visto numeri decisamente inferiori (ciascuno al 2%), così come l'ospitalità, che si ferma all'1% a livello globale. Peraltro, è interessante segnalare come **l'ICT sia stabile in classifica rispetto al 2023 e faccia registrare una lieve flessione (-3%)**, similmente a finanza e assicurazioni. Se tale trend sarà confermato dai dati completi sul 2024, si potrà evidenziare che i segmenti di mercato più maturi in termini di cybersicurezza – anche per impulso della regolamentazione applicabile – sono proprio quelli che riescono a gestire e a reagire meglio agli attacchi in uno scenario che vede la minaccia cibernetica avanzare costantemente.

Procedendo con un'analisi specifica del contesto italiano, dal 2019 al primo semestre dell'anno in corso sono stati rilevati 777 incidenti noti di particolare gravità. Gli eventi relativi al H1 2024 sono leggermente diminuiti rispetto al medesimo periodo del 2023. Valutando la distribuzione delle vittime nel H1 2024, **la categoria merceologica per cui si rileva un maggior numero di attacchi è – per la prima volta – il manifatturiero, che fa registrare un importante incremento rispetto al 2023 raggiungendo una quota pari al 19% (+6%).** Le rilevazioni di quest'ultimo periodo, se lette congiuntamente con i dati a livello globale sopra richiamati, restituiscono una fotografia piuttosto chiara: **oltre un quarto (28%) delle imprese manifatturiere colpite da attacchi cyber gravi nei primi sei mesi del 2024 afferiscono alla filiera italiana.** Peraltro, similmente a quanto detto per lo scenario globale**, il settore ICT "guadagna" due posizioni in classifica rispetto al 2023, facendo altresì registrare una lieve flessione (-2%), che risulta ancor più mercata per il segmento finanza/assicurazioni (-6,7%).** Di conseguenza, se tale trend sarà confermato dai dati completi sul 2024, si potrà evidenziare che i segmenti di mercato più maturi in termini di cybersicurezza – anche per impulso della regolamentazione applicabile – sono proprio quelli che riescono a gestire e reagire meglio agli attacchi cibernetici gravi. In questo scenario, il recente **rapporto di Tinexta Cyber** ("*Risk Report 2024 H1*") fornisce un interessante spaccato sulle principali minacce informatiche a livello globale e nazionale. Guardando alla distribuzione della **minaccia cyber in Italia**, si può osservare come **la maggior parte delle aziende colpite nei primi sei mesi dell'anno in corso abbia meno di 50 dipendenti (53%; -5% sul semestre precedente),** che se considerate insieme a quelle con 51-100 di-

pendenti (20%; +9%), restituiscono una situazione piuttosto allarmante che vede una quota cospicua di attacchi rivolta verso le imprese di piccole e medie dimensioni. Analizzando il fatturato, il dato appare ancora più chiaro. Infatti, **l'86% delle aziende colpite afferisce alla fascia fino a 250 milioni di dollari, registrando un incremento pari al 77% rispetto al semestre precedente**.

T**ra le minacce cibernetiche più insidiose degli ultimi anni va annoverato l'attacco ransomware**. **Tra i paesi più colpiti nel primo semestre 2024 il primato è degli Stati Uniti,** che si confermano come bersaglio prioritario delle gang ransomware con oltre 1.170 vittime, mentre l'Italia occupa il quinto posto con 75 vittime. Rispetto alla **distribuzione geografica delle vittime nel nostro Paese**, gli ultimi dati di Tinexta Cyber mostrano **una maggiore concentrazione nelle regioni settentrionali, che raccolgono il 69% del totale, seguite da quelle del Centro (23%) e, infine, dalle regioni del Sud e le isole (8%)**. Si tratta di evidenze che riflettono quanto visto in precedenza rispetto a una più elevata concentrazione di attacchi, non solo di tipo ransomware, verso il settore manifatturiero, che è particolarmente presente nel Nord Italia.

In un contesto in cui i cyberattacchi sono sempre più gravi e numerosi, **gli investimenti** in cybersicurezza assumono un'importanza significativa in quanto rappresentano la prima risposta, in termini preventivi, alle esigenze che incombono su imprese e pubbliche amministrazioni e che derivano dalle nuove dinamiche del cyberspazio.

Secondo i dati contenuti nell'ultima versione del report "NIS Investments", pubblicato dall'ENISA a novembre 2024, **le organizzazioni francesi e tedesche sono quelle che spendono di più in valore mediano (€6 milioni), seguite da quelle italiane e spagnole (€5 milioni).**

L'edizione di quest'anno del report di ENISA contiene anche un utile spaccato **sulla preparazione dei soggetti intervistati rispetto all'implementazione della direttiva NIS2**, che è divenuta applicabile lo scorso 18 ottobre in tutti gli Stati Membri. Tuttavia, al 28 novembre, solo 4 Paesi hanno recepito questo importante atto normativo nei termini previsti (Italia, Belgio, Croazia e Lituania). Per tutti gli altri il ritardo si è tradotto nell'apertura di una procedura di infrazione da parte della Commissione europea.

In questo scenario**, il livello di awareness sulla NIS2 e sui rispettivi adempimenti varia significativamente tra gli Stati Membri e i settori**. Più nel dettaglio, si passa dal 100% di Francia e Finlandia al 82% della Croazia e al 80% di Malta, mentre **l'Italia si colloca in quinta posizione con il 96% di awareness**. Rispetto ai settori la disomogeneità è ancor più marcata, **7 settori su 12 raggiungono un valore pari o prossimo al 100%,** di converso, **lo spazio si colloca in ultima posizione col 57%, preceduto da acque reflue (60%), manifatturiero (62%) e PA (73%), evidenziando un urgente bisogno di aumentare la consapevolezza in questi settori.** Quanto detto vale ancor di più se si volge uno sguardo alle **variazioni di budget programmate per far fronte alla compliance richiesta dalla disciplina NIS2**. Infatti, considerando tutte le organizzazioni intervistate, **oltre il 38% ha dichiarato di non aver bisogno di ulteriore budget per implementare le disposizioni della direttiva e un ulteriore 14% non ritiene possibile procedere a un incremento delle risorse.**

Altro tema assolutamente centrale è rappresentato dal **coinvolgimento degli organi di gestione dei soggetti NIS2 nell'approvazione delle misure di gestione dei rischi di cybersicurezza**, dovendo altresì supervisionarne la conseguente attuazione e potendo essere destinatari di pesanti sanzioni in caso di violazioni. Per adempiere a queste nuove responsabilità viene previsto che i componenti di tali organi seguano una formazione specifica in materia di sicurezza informatica. Sul punto, **dai dati ENISA emerge che l'Italia è lo Stato Membro più virtuoso, in quanto il 70% delle organizzazioni intervistate a**

livello nazionale coinvolge i propri vertici nella formazione in cybersicurezza.
Dato che **la sicurezza della supply chain è un elemento centrale sia per la cybersicurezza in generale, sia nella direttiva NIS2**, specificamente nella parte in cui si prescrive di **valutare le vulnerabilità specifiche per ogni diretto fornitore di servizi**, nonché la **qualità complessiva dei prodotti e delle pratiche di cibersicurezza**, comprese le procedure di sviluppo sicuro, appare fondamentale per i soggetti pubblici e privati **stabilire policy chiare e adeguate atte a prevenire e gestire i rischi relativi alle terze parti** (come partner, vendor e fornitori). Sul tema, **le organizzazioni italiane fanno collocare il nostro Paese in prima posizione** insieme all'Irlanda (90%).

CAPITOLO 2 – L'ECOSISTEMA NORMATIVO SULLA CYBERSECURITY

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 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, al fine di aumentare la resilienza di soggetti che negli Stati membri sono fondamentali per la fornitura di servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno, 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. È scaduto lo scorso 17 ottobre 2024 il termine ultimo per il recepimento, da parte degli Stati membri, della **Direttiva n. 2555/2022 (NIS2)**, pubblicata il 27 dicembre 2022 ed entrata in vigore il 17 gennaio 2023. Tale direttiva fa seguito all'adozione, nel 2016, della prima direttiva NIS (recepita in Italia con il d. lgs. n. 65/2018) – con la quale per la prima volta sono state definite misure organiche rivolte esplicitamente alla sicurezza delle informazioni e alla cybersicurezza – di cui cerca di risolvere una serie di criticità applicative, 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.
Se il 14 settembre 2023, la Commissione europea ha pubblicato **i primi orientamenti sull'applicazione di alcune norme fondamentali della Direttiva NIS2, ossia l'art. 4** (paragrafi 1 e 2) e l'art. 3, paragrafo 4, fornendo un modello utile agli SM per le informazioni da richiedere ai soggetti NIS2, lo scorso 17 ottobre 2024 è stato invece pubblicato il **Regolamento di Esecuzione (UE) 2024/2690 che dettaglia le modalità di applicazione della Direttiva NIS2** per un sottoinsieme di soggetti critici, fornendo alcuni

primi spunti rispetto al contenuto delle misure di sicurezza e alle definizioni di incidenti significativi per i quali persiste obbligo di notifica.

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 questo contesto, 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.

Sebbene i principali obblighi si applicheranno a partire dall'11 dicembre 2027, lo scorso 10 dicembre 2024 è entrato in vigore un altro Regolamento di importanza particolare, il n. 2024/2847 (**Cyber Resilience Act**). Esso si inquadra nella cornice definita dalla Strategia lanciata nel 2020 e mira a rispondere all'esigenza, nella logica di assicurare un ecosistema europeo complessivamente sicuro, di garantire che i dispositivi utilizzati da cittadini, imprese e pubbliche amministrazioni rispondano a standard di sicurezza adeguati. La normativa dettata dal regolamento, in particolare, persegue il fine di 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.È attualmente è in fase di costituzione il Cyber Resilience Act Expert Group (CRA Expert Group), che assisterà e consiglierà la Commissione su questioni rilevanti per l'implementazione del CRA.

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, dal 17 gennaio 2025 è pienamente applicabile 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 di una serie di previsioni concernenti Governance e organizzazione interna, gestione dei rischi ICT, degli incidenti e reporting, test di resilienza operativa digitale, gestione

dei fornitori terzi di servizi ICT e condivisione delle informazioni. In attuazione del DORA, il 24 ottobre scorso è stato pubblicato il Regolamento delegato della Commissione che integra il regolamento (UE) n. 2022/2554 per quanto riguarda le norme tecniche di regolamentazione sull'armonizzazione delle condizioni per lo svolgimento delle attività di sorveglianza, mentre il 2 dicembre è stato adottato il Regolamento delegato della Commissione relativo alle norme tecniche di regolamentazione per specificare i criteri per determinare la composizione del gruppo di esame congiunto che garantisce una partecipazione equilibrata del personale delle AEV e delle autorità competenti interessate, la loro designazione, i compiti e le modalità di lavoro.

È stato pubblicato lo scorso 15 gennaio 2025 il **Regolamento UE n. 2025/38 (Cyber Solidarity Act)** che punta a definire misure volte a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi. Tale obiettivo è perseguito, in particolare, mediante l'istituzione di una rete paneuropea di poli informatici, un meccanismo per le emergenze di cibersicurezza ed uno di riesame degli incidenti di cibersicurezza.

Partendo dalla constatazione della centralità rivestita dalle reti di tlc per il processo di transizione digitale e per la competitività dell'UE, nel tentativo di comprendere le dinamiche di mercato e gli sviluppi tecnologici in atto, il 21 febbraio scorso è stato pubblicato dalla Commissione europea il Digital connectivity package, comprensivo del White Paper **"How to master Europe's digital infrastructure needs?"** e della Raccomandazione per la sicurezza e resilienza delle infrastrutture via cavo sottomarine. Il libro bianco, in particolare, oggetto di una consultazione pubblica conclusasi lo scorso 30 giugno 2024, si presenta come un documento ampio che affronta tematiche strategiche connesse alla convergenza tecnologica tra telecomunicazioni e cloud, al ruolo critico delle infrastrutture digitali nonché alle sfide presenti e future anche relative alla cybersecurity. Il 6 dicembre scorso Il Consiglio UE ha reso pubbliche le proprie conclusioni sul White Paper.

La Raccomandazione sulla sicurezza e la resilienza delle infrastrutture dei cavi sottomarini individua una serie di azioni a livello nazionale ed europeo attraverso le quali si punta a rafforzare la sicurezza e la resilienza dei cavi sottomarini attraverso un migliore coordinamento in tutta l'UE, sia in termini di governance che di finanziamento.

Se il White Paper sul Futuro dell'Infrastruttura digitale europea è un documento programmatico che ambisce fornire degli spunti di riflessione per la prossima Commissione sulle politiche da attuare per rafforzare il Mercato Unico europeo in ambito digitale, lo scorso 9 settembre è stato presentato il rapporto "***The future of European competitiveness*",** a firma di Mario Draghi su incarico dalla stessa Commissione europea. Si tratta, in questo caso, di un'analisi economica di ampio respiro sul livello di competitività dell'UE, che esamina le sfide affrontate dall'industria e dalle imprese nel mercato unico attraverso la disamina di numerosi settori che vanno dall'energia ai trasporti, dalle materie prime alla decarbonizzazione, fino alla space economy e alla difesa e che individua tre distinte aree di intervento per rilanciare la crescita sostenibile: la riduzione del divario di innovazione con gli Stati Uniti e la Cina, soprattutto nelle tecnologie avanzate, un piano congiunto per la decarbonizzazione e la competitività ed infine l'aumento della sicurezza e la riduzione delle dipendenze. Molta attenzione è dedicata al tema della sicurezza. Con riferimento ai settori delle apparecchiature per le telecomunicazioni e dei software, in particolare, il rapporto sottolinea come essi siano fondamentali per la resilienza informatica dell'UE, la sicurezza delle infrastrutture strategiche e la protezione dei dati dei cittadini e delle imprese ed affronta in maniera trasparente il tema della concorrenza proveniente dall'oriente nonché le

restrizioni messe in campo nei confronti di fornitori ad alto rischio da un numero certamente minoritario di SM per giungere a proporre il rafforzamento della sicurezza e dell'autonomia strategica aperta delle reti di comunicazione digitale dell'UE attraverso il sostegno ai fornitori di apparecchiature e software per le comunicazioni con sede nell'UE.

Se questo è il contesto europeo, a livello nazionale assistiamo alla definizione di un quadro normativo molto avanzato che vede nell'ACN uno dei principali protagonisti. Ed infatti, se da un lato l'Italia rientra tra i primi Paesi dell'Unione ad essersi dotato di un atto di recepimento della direttiva NIS2, ossia il d. lgs. 4 settembre 2024, n. 138, che è entrato in vigore il 16 ottobre scorso, dall'altro, tale intervento si inquadra nell'ambito di un ecosistema già molto ricco, che ruota intorno al Perimetro di Sicurezza Nazionale Cibernetica (PSNC) istituito con il decreto legge n. 105/2019, convertito con la legge n. 133/2019 (che punta ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale), la disciplina Golden Power, di cui al decreto-legge 15 marzo 2012, n. 21 (convertito, con modificazioni, in legge 11 maggio 2012, n. 56) così come successivamente modificato ed integrato e, da ultimo, la legge 28 giugno 2024, n. 90 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" (di seguito, "legge sulla cybersicurezza"), entrata in vigore lo scorso 17 luglio.

CAPITOLO 3 – LE CERTIFICAZIONI DI CYBERSICUREZZA

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 e i requisiti funzionali**. In numerosi paesi UE esistono attualmente diversi 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**.

L'apprezzamento per i sistemi condivisi di valutazione è cresciuto costantemente negli anni, difatti secondo l'ultima edizione dello studio Jtsec beyond IT security, **nel 2023 si è raggiunto il valore più alto della storia , rafforzando un trend in forte crescita, in quanto sono stati certificati 470 prodotti, a fronte dei 387 dell'anno precedente**. 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. In questo contesto, **i dati rilevati da Jtsec beyond IT security indicano per il 2023 l'avvenuta certificazione di 11 prodotti in Italia (nel 2022 erano stati 15)**.

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. A seguito di un lungo processo iniziato nel 2019 dall'ENISA, **il 31 gennaio 2024 la Commissione europea ha adottato il Regolamento di esecuzione (UE) 2024/482 con cui i Common Criteria Europei (Common Criteria based European candidate cybersecurity certification scheme – EUCC) sono diventati ufficialmente parte della legislazione europea e possono supportare la certificazione volontaria di un numero maggiore di prodotti e sistemi ICT**. La versione attualmente disponibile di tali meccanismi di certificazione si fonda su un modello ispirato agli schemi ISO/IEC 15408 e ISO/IEC 18045 e **consente di stabilire una certificazione uniforme in grado di raggiungere i due livelli di garanzia di sicurezza più alti previsti dall'art. 52 del Cybersecurity Act, ovverosia quello "sostanziale" e quello "elevato", coinvolgendo autorità nazionali e prendendo in considerazione valutazioni di terze parti indipendenti**. È escluso dagli EUCC il livello "base" – nonché l'autovalutazione della conformità – 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.

In questo contesto, è evidente **la necessità di garantire una risposta quanto più armonizzata possibile a livello eurounitario e dunque il contributo al raggiungimento di tale obiettivo che il ricorso a standard comuni di certificazione in tutti gli Stati Membri potrebbe offrire non solo per la creazione di un ecosistema digitale più sicuro e cyber-resiliente, ma anche per il rafforzamento della fiducia verso prodotti, servizi e processi ICT**. Naturalmente, ciò presuppone che tali strumenti siano strutturati per essere adeguatamente flessibili, così da stare al passo con l'evoluzione della minaccia cibernetica. Se è evidente l'opportunità offerta dalla certificazione di cybersicurezza **non può non considerarsi l'eventualità che, a livello unionale o nazionale, si opti per rendere mandatoria tale certificazione per alcuni prodotti, servizi e processi ICT e/o per determinate categorie di soggetti, a partire dalle infrastrutture critiche, come previsto – a titolo di esempio – dalla direttiva NIS2 e dal Cyber Solidarity Act (CSoA)**.

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

Al fine di **verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity**, l'Istituto per la Competitività (I-Com) ha riproposto e aggiornato un'indagine avviata a partire dall'anno scorso, avvalendosi anche del sostegno di alcune delle principali associazioni di categoria, che in questa edizione ha coinvolto 150 imprese appartenenti a vari settori: utilities (acqua, rifiuti ed energia), trasporti, TLC/digitale, ecc.

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 le grandi imprese rilevano maggiormente gli investimenti tecnico-organizzativi necessari alla compliance (32 risposte), così come per le aziende di medie dimensioni (11) e per le piccole imprese (14). Considerando unitamente tutte le classi dimensionali, altri due motivi ricorrenti tra i rispondenti si rivedono nella preoccupazione circa l'innalzamento delle barriere all'ingresso, soprattutto per le PMI (41 risposte in totale) e la numerosità degli oneri burocratici e amministrativi richiesti (35 risposte in totale).

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 (66 risposte in totale), seguito dalla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (63 risposte) e dall'incertezza interpretativa della normativa (54 risposte).**

Relativamente agli investimenti, **la maggioranza delle imprese rispondenti assegna meno del 3% del budget IT alla cybersecurity.** 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 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 42,11% dei rispondenti stia ancora valutando tale eventualità, il 9% in meno rispetto al 2023, mentre solo il 25,44% ha già deciso di aumentare gli investimenti in cybersicurezza, facendo registrare un sostanziale peggioramento su base annua (-11%)**.

In merito all'adozione di una o più **certificazioni volontarie di cybersicurezza**, si può osservare che **gran parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione**. Tuttavia, emergono **segnali moderatamente positivi se si confrontano i dati su base annua**. Difatti, mentre nell'edizione 2023 i rispondenti che dichiaravano ciò corrispondevano a oltre il 63%, **nell'ultima rilevazione sono scesi al 48%.** Tra questi, le piccole imprese sono quelle che hanno performato meglio rispetto all'anno scorso (-23,2%), seguite dalle grandi (-15,5%) e, infine, dalle medie (-13%). Tali risultati trovano una motivazione negli ostacoli che sono percepiti dalle imprese con riguardo all'ottenimento di una certificazione volontaria di cybersecurity. Similmente a quanto osservato per il 2023, il principale intralcio risiede nei **costi elevati del processo di certificazione**, che **non sono percepiti come proporzionati ai benefici** che ne possono conseguire (34,8% dei rispondenti). In secondo luogo, quasi il 19% sostiene che **i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi**. In terzo luogo, il 14,5% 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.

Tra coloro che hanno dichiarato di aver adottato almeno una certificazione, **i principali effetti positivi** direttamente riconducibili ad essa sono stati: un miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders (46,3% dei rispondenti), una maggiore consapevolezza dei dipendenti e dei collaboratori esterni (39%) e più possibilità di partecipare a bandi di gara pubblici o privati (28%).

Inoltre, il 74,5% 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) – possono incentivare il ricorso alle certificazioni (+4,5% rispetto al 2023)**. Posto che lo scorso 31 gennaio la Commissione europea ha adottato il Regolamento di esecuzione 2024/482 (Implementing Act) con cui gli EUCC sono diventati ufficialmente parte della legislazione europea, nell'ultima edizione della presente indagine è stato chiesto ai partecipanti di rendere noto il punto di vista della propria organizzazione circa l'eventualità di un approccio mandatorio o meno sull'adozione di schemi di certificazioni europei come, appunto, gli EUCC. Ebbene, **oltre il 70% dei rispondenti ha dichiarato che non si è ancora assunta una posizione sul tema**. Pertanto, la restante quota di imprese si divide tra chi ha optato per un **approccio volontario** (15,6%) e chi per quello **mandatorio** (12,8%).

L'ultima sezione dell'indagine riguarda più nello spe-

cifico alcuni aspetti connessi al **PSNC e alle attività del 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 27% dei rispondenti non si rilevano particolari criticità in tal senso, registrando un decremento del 3% rispetto a quanto osservato per il 2023, mentre il 20,7% non ha espresso un'opinione in merito (-2%).** La restante quota di feedback pervenuti evidenzia, invece, **alcune problematiche:** 43 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** (+9,7% su base annua); 26 aziende convengono che **la necessità di esaminare tali beni Ict nel relativo ambiente operativo determini la ripetizione di test sugli stessi beni** (+2,5%); 23 imprese si preoccupano che **la parziale incertezza sulle attività di valutazione possa rappresentare un disincentivo dato il rischio reputazionale conseguente a un eventuale ko** (+6,2%).

Relativamente alla valutazione complessiva della disciplina sul PSNC, **il 21,9% dei rispondenti (soprattutto grandi imprese) si ritiene assolutamente soddisfatto dalle regole e dagli adempimenti previsti nell'ambito del Perimetro**, percentuale leggermente aumentata rispetto al 2023 (+1,2%). Parallelamente, **poco più dell'8% nel 2024 e del 10% nell'anno precedente, considera tale normativa come eccessivamente gravosa**, recando solo un minimo beneficio per la sicurezza nazionale. Invece, **il restante 69,52% (68,8% nel 2023) si colloca nel mezzo**. **La maggioranza, 48 imprese (52 nel 2023), 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, **25 rispondenti (21 nel 2023) hanno denunciato che l'approccio adottato impone adempimenti sproporzionati ai soggetti inclusi nel Perimetro.**

Un ulteriore quesito ha posto luce sul punto di vista delle imprese circa la l. n. 90/2024 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" che si rivolge anche a un'ampia platea di soggetti privati, tra cui quelli già sottoposti ad altre discipline[1]. In particolare, si rileva **che quasi il 29% delle aziende ha dichiarato parere positivo, in quanto la normativa interviene sul tema della cybersicurezza nazionale in maniera assolutamente efficace.** Diversamente**, il 5,61% dei rispondenti mostra una valutazione negativa, in virtù della previsione di oneri burocratici ed organizzativi molto gravosi, aggravati dalla clausola di invarianza finanziaria**. Circa il 65% degli intervistati ha fornito risposte intermedie.

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**, il 60,75% dei rispondenti ritiene 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 (+4,5% su base annua). 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 il 44%, di cui ben 19 PMI.

CAPITOLO 5 – LE COMPETENZE IN CIBERSICUREZZA

La formazione degli individui riveste un ruolo fondamentale nell'ambito della cibersicurezza. Nel merito, l'Italia è più indietro rispetto alla media dei Paesi eu-

1 Si v. supra, par. 2.2.1.

ropei 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 italiana, a fronte di un 55,6% a livello UE**. 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 2024 si è riscontrato un significativo incremento degli illeciti legati al fenomeno delle truffe online nel nostro Paese**. Difatti, secondo gli ultimi dati della Polizia Postale sono aumentati 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 19,4% del 2019 al 17,9% del 2024**. Allo stesso tempo, sempre in Italia, il costo medio delle violazioni di dati è aumentato maggiormente rispetto a Germania e Francia, passando da 3,9 milioni di dollari nel 2021 a 4,7 nel 2024. 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**.

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 2025** presentava **774 tra corsi e insegnamenti relativi alla cibersicurezza, rispetto ai 520 individuati a inizio 2024, il che fa segnare un incremento di circa il 48% su base annua**. Nel dettaglio, l'analisi ha individuato 323 insegnamenti singoli all'interno di corsi di laurea magistrale, 158 insegnamenti singoli all'interno delle lauree triennali, 86 progetti di ricerca in dottorati, 69 corsi singoli in master di II livello e 54 in master di I livello, a fronte di 31 lauree magistrali, 30 master, 16 corsi all'interno di dottorati di ricerca, 11 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 38. 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 116 corsi "specializzati", ben 46 in più rispetto a quelli individuati a inizio 2024. Nel complesso, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 154 corsi di studio interamente dedicati, segnando un incremento pari al 38,7% su base annua. Per quanto riguarda **la distribuzione regionale della complessiva offerta formativa**, questa appare piuttosto disomogenea con una forte concentrazione nel Lazio (180 tra corsi e singoli insegnamenti), in Lombardia (119) e in Campania (70). Tuttavia, se si considerano i **dati normalizzati per il numero di Università presenti sul territorio regionale**, la classifica varia mostrando in prima posizione il Piemonte con un rapporto 13,5:1, seguito da Liguria (13:1) e Puglia (12,8:1). A livello regionale, a gennaio 2025 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 32 percorsi complessivi, catalizzando ben 5 lauree dedicate, oltre a 12 progetti di ricerca in dottorato e 15 master. In questo contesto, non sorprende che **oltre il 60% dell'offerta formativa universitaria in materia di cibersicurezza risulti erogata dai dipartimenti di ingegneria** (48,1%) **e informatica** (16,8%).

Inoltre, **l'elevato numero di master specifici sui temi della cibersicurezza (30) sembra suggerire un'elevata domanda di approfondimento post-laurea su questi temi**. Nell'ambito della formazione superiore, un ruolo di rilievo è rivestito certamente dagli ITS che hanno lo scopo di formare personale tecnico in aree strategiche per lo sviluppo del tessuto economico del Paese, tra cui spiccano l'area 6 "Tecnologie della informazione e della comunicazione". Il portale online curato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE) evidenzia che sul territorio nazionale risultano presenti 147 ITS. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-Com, **gli ITS che si occupano di cybersicurezza sono il 35,4% rispetto al numero complessivo di quelli attivi, una quota più che raddoppiata rispetto alla rilevazione precedente effettuata a inizio 2024**. In particolare, 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 2005 25
istituto per la competitività

CAPITOLO 1

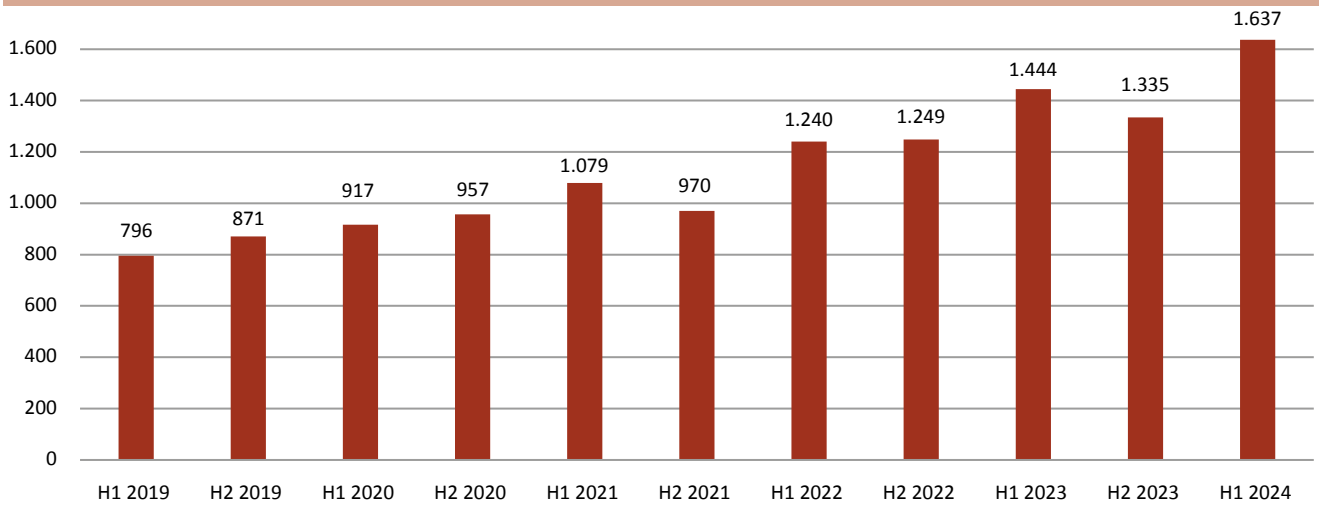
IL QUADRO EUROPEO E NAZIONALE DELLA SICUREZZA INFORMATICA

1.1. LO SCENARIO EUROPEO E NAZIONALE DEGLI ATTACCHI CIBERNETICI

La **minaccia cibernetica** 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 cybersicurezza. Difatti, siamo dinanzi ad attacchi sempre più gravi, numerosi e specializzati, che spingono i Paesi e le organizzazioni internazionali allo sviluppo di policy, strategie e normative che pongono al centro la tutela del cyberspazio per le cittadini, imprese e articolazioni statali.
L'ultimo rapporto dell'Associazione Italiana per la Sicurezza Informatica (Clusit), pubblicato a novembre 2024 e aggiornato con le evidenze rilevate nel primo semestre di quest'anno, fornisce una chiara panoramica di come **le minacce cibernetiche siano cresciute costantemente nel corso degli ultimi anni**. In particolare, lo studio ha ad oggetto l'analisi di 12.495 cyberattacchi che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali, o che comunque prefigurano scenari preoccupanti, registrati nel periodo tra gennaio 2019 e giugno 2024. Ebbene, **a livello globale il primo semestre di quest'anno si configura come il peggiore di sempre, con 1637 eventi malevoli rilevati, registrando un incremento del 23% sul semestre precedente** (Fig. 1.1).
Per quanto concerne l'analisi delle vittime classificate per categoria d'appartenenza (Fig. 1.2), nel primo semestre di quest'anno **la maggioranza degli eventi ha colpito il settore sanitario (18%), seguito dalle Governativo/Militare/Law Enforcement (13%) e dal segmento finanza/assicurazioni (8%)**. Inoltre, il 16% degli attacchi rilevati non ha visto un destinatario specifico, bensì target multipli. Diversamente, i settori inerenti arti e intrattenimento, così come quelli dell'energia e delle telecomunicazioni hanno visto numeri decisamente inferiori (ciascuno al 2%), così come l'ospitalità, che si ferma all'1% a livello globale. Peraltro, è interessante segnalare come **l'ICT sia stabile in classifica rispetto al 2023 e faccia registrare una lieve flessione (-3%)**, similmente a finanza e assicurazioni. Se tale trend sarà confermato dai dati completi sul 2024, si potrà evidenziare che i segmenti

Fig. 1.1: Andamento degli attacchi a livello globale, per semestre

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024



di mercato più maturi in termini di cybersicurezza – anche per impulso della regolamentazione applicabile – sono proprio quelli che riescono a gestire e a reagire meglio agli attacchi in uno scenario che vede la minaccia cibernetica avanzare costantemente.

In merito alla distribuzione geografica delle vittime (Fig. 1.3), **nel H1 2024 i numeri più elevati continuano a essere riconducibili al continente americano (41%), che tuttavia fa registrare una flessione pari al 3% rispetto all'anno scorso**. In questo panorama, **l'Europa – purtroppo – consolida la seconda posizione, attraendo il 29% dei cyberattacchi a livello globale (+6% sul 2023).** Gli attacchi inerenti le vittime europee sopravanzano anche quelli diretti verso obiettivi multipli, ossia inerenti organizzazioni situate in continenti diversi, che sono passati dal 21% del 2023 al 17% del primo semestre di quest'anno. L'ultimo posto è occupato dall'Africa, stabilmente all'1%, mentre peggiora anche l'Oceania che nell'ultimo periodo è stata vittima del 4% degli (+2).

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. Se **tra il 2022 e il 2023 si è instaurata una tendenza che ha visto aumentare gli attacchi con severity "critica"**, i quali hanno prodotto effetti dannosi importanti per le vittime, tra cui ingenti perdite economiche e di dati**, nel primo semestre 2024 questo trend – da confermarsi con i dati annuali – sembrerebbe aver subito una decisa flessione, segnando un -7% sul 2023** (Fig. 1.4). Diversamente, si registra un forte aumento per il grado "alto" della severity, che è associato alla maggioranza degli attacchi registrati nell'ultimo periodo di rilevazione, mentre rispetto agli anni precedenti si mantiene stabile il livello "medio" (19%) e in sostanza scompare la severity "bassa".

Procedendo con un'analisi specifica del contesto italiano, dal 2019 al primo semestre dell'anno in corso sono stati rilevati 777 incidenti noti di particolare gravità. Gli eventi relativi al H1 2024 sono leggermente diminuiti rispetto al medesimo periodo del 2023 (Fig. 1.5). Tuttavia, il report fin ora menzionato specifica che nel 2023 tra il primo e il secondo semestre si è registrata una crescita del 35%, per cui – anche in questo caso – appare opportuno verificare il trend su base annuale.

Fig. 1.2: Distribuzione della tipologia delle vittime (H1 2024)

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024

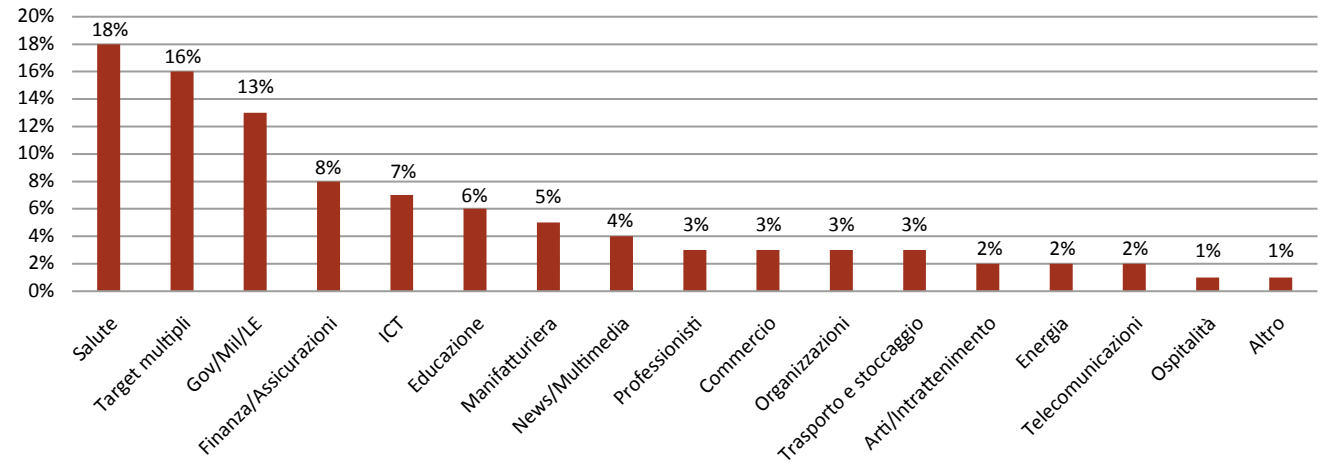


Fig. 1.3: Distribuzione geografica delle vittime (2023-H1 2024)

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, marzo 2024 (per dati 2023); Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024 (per dati H1 2024)

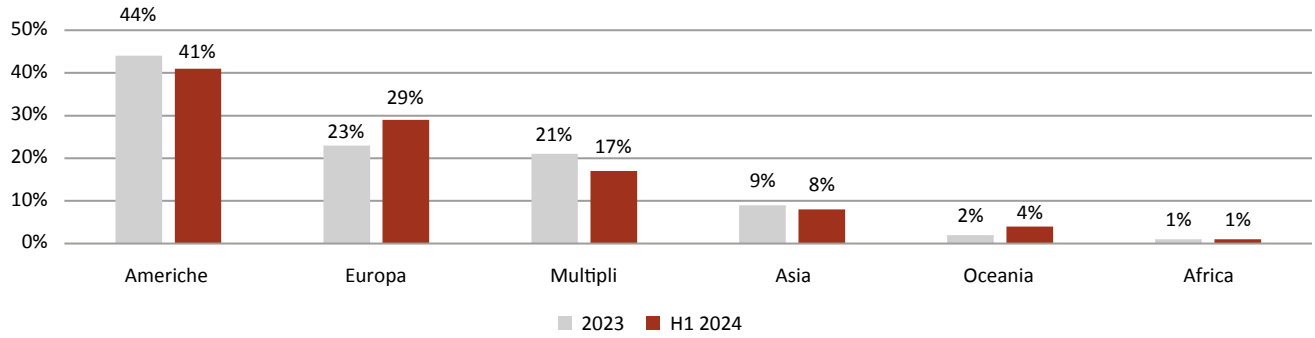


Fig. 1.4: Andamento della *severity* degli attacchi (2022-H1 2024)

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, marzo 2024 (per dati 2022-2023); Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024 (per dati H1 2024)

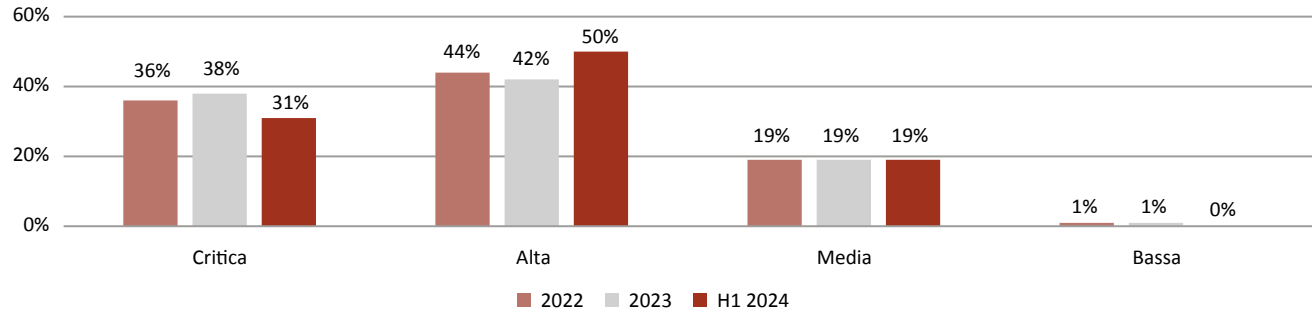
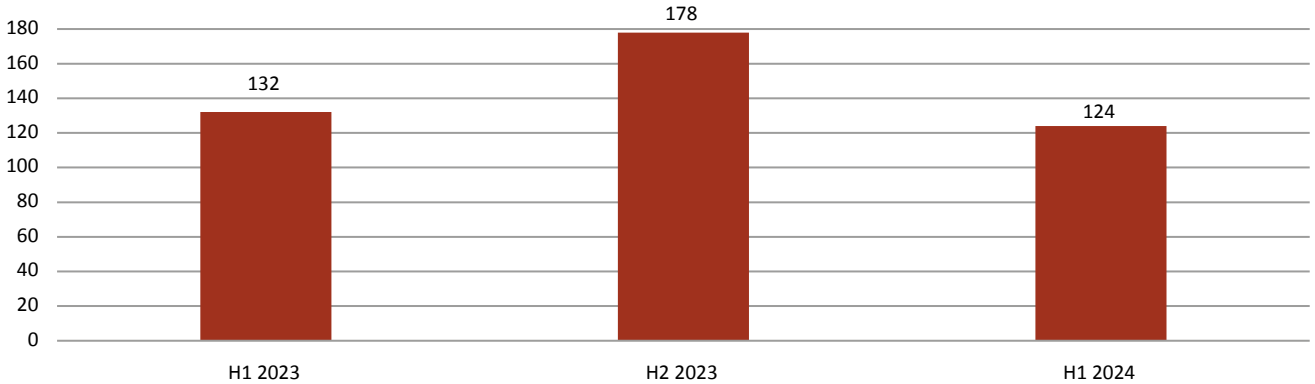


Fig. 1.5: Andamento degli attacchi in Italia, per semestre (H1 2023-H1 2024)

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024



Valutando la distribuzione delle vittime nel H1 2024 (Fig. 1.6), **la categoria merceologica per cui si rileva un maggior numero di attacchi è – per la prima volta – il manifatturiero, che fa registrare un importante incremento rispetto al 2023 raggiungendo una quota pari al 19% (+6%).** Le rilevazioni di quest'ultimo periodo, se lette congiuntamente con i dati a livello globale sopra richiamati, restituiscono una fotografia piuttosto chiara: **oltre un quarto (28%) delle imprese manifatturiere colpite da attacchi cyber gravi nei primi sei mesi del 2024 afferiscono alla filiera italiana.** Ad ogni modo, al secondo posto si collocano le imprese impegnate nel settore trasporto e stoccaggio (13%), seguite dalla categoria che comprende governativo/militare/law enforcement (11%). Anche nel nostro Paese gli eventi malevoli che hanno colpiti target multipli hanno interessato una porzione rilevante (11%). Di converso, in coda alla classifica vi sono la l'ospitalità, il settore delle costruzioni e news/multimedia, ciascuno all'1%.

Peraltro, similmente a quanto detto per lo scenario globale**, il settore ICT "guadagna" due posizioni in classifica rispetto al 2023, facendo altresì registrare una lieve flessione (-2%), che risulta ancor più mercata per il segmento finanza/assicurazioni (-6,7%).** Di conseguenza, se tale trend sarà confermato dai dati completi sul 2024, si potrà evidenziare che i segmenti di mercato più maturi in termini di cybersicurezza – anche per impulso della regolamentazione applicabile – sono proprio quelli che riescono a gestire e reagire meglio agli attacchi cibernetici gravi. Inoltre, **i dati sull'Italia mostrano come il settore del-**

Fig. 1.6: Distribuzione della tipologia di vittime in Italia (H1 2024)

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024

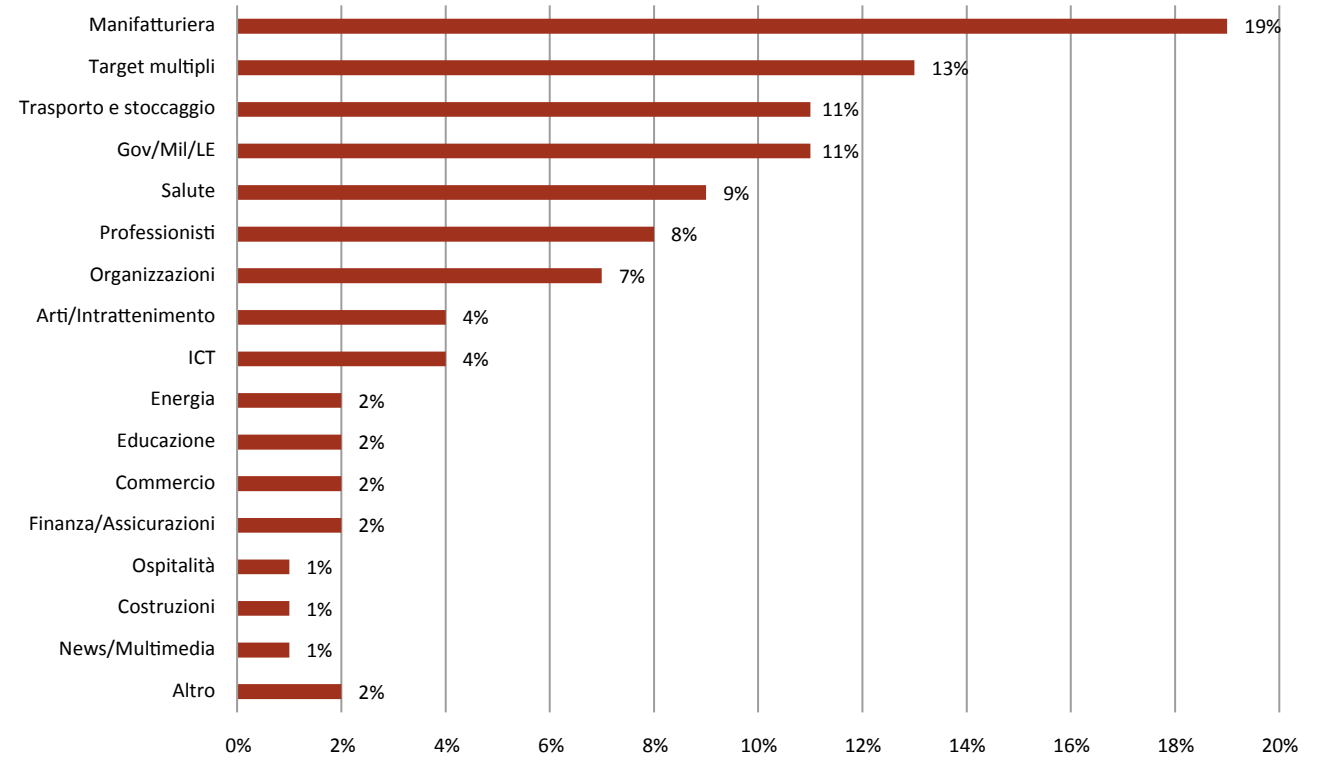
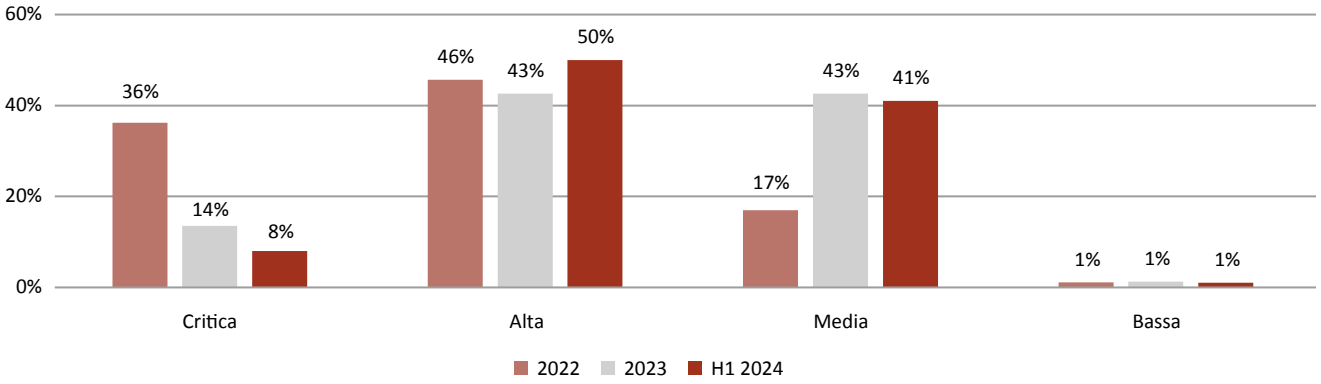


Fig. 1.7: Andamento della *severity* degli attacchi in Italia (2022-H1 2024)

Fonte: Clusit, Rapporto sulla sicurezza ICT in Italia, novembre 2024



le telecomunicazioni – a differenza di quanto visto a livello globale – non figura nelle categorie di vittime in cui è stata registrata una quota di attacchi pari almeno all'1% del totale.

In termini di severity, la situazione italiana assume un andamento particolare (Fig. 1.7). Difatti, **gli incidenti con impatto "critico" sono proporzionalmente più contenuti se comparati coi dati globali (31%), costituendo appena l'8% nella prima parte dell'anno e registrando un sostanziale decremento rispetto ai due anni precedenti, rispettivamente, del 28% e del 6%.** La quota più elevata di attacchi nel H1 2024 è – in linea con il dato globale – ricondotta a una severity "alta" (50%), per la quale si registra un incremento del 7% sul 2023. Diversamente, nel nostro Paese l'impatto "medio" è stato associato al 41% degli attacchi nel periodo considerato (-2%), contro un 19% a livello globale.

In questo scenario, il recente **rapporto di Tinexta Cyber** ("*Risk Report 2024 H1*") fornisce un interessante spaccato sulle principali minacce informatiche a livello globale e nazionale – con un focus particolare sugli attacchi di tipo ransomware – che sono emerse nel primo semestre del 2024 grazie a un'attività di raccolta e analisi dati con tecniche OSINT e CLOSINT, oltre che con strumenti e tecnologie proprietarie di *threat intelligence.*

Ebbene, guardando alla distribuzione della **minaccia cyber in Italia** (Fig. 1.8), si può osservare come **la maggior parte delle aziende colpite nei primi sei mesi dell'anno in corso abbia meno di 50 dipendenti (53%; -5% sul semestre precedente),** che se considerate insieme a quelle con 51-100 dipendenti (20%; +9%), restituiscono una situazione piuttosto allarmante che vede una quota cospicua di attacchi rivolta verso le imprese di piccole e medie dimensioni.

Guardando al fatturato, il dato appare ancora più chiaro. Infatti, **l'86% delle aziende colpite afferisce alla fascia fino a 250 milioni di dollari, registrando un incremento pari al 77% rispetto al semestre precedente**. Seguono – con notevole distacco – le imprese con un fatturato compreso tra i 250-499 milioni di dollari (10%), mentre i soggetti che superano i 500 milioni di dollari mostrano valori residuali (4%), il che conferma un evidente interesse degli attaccanti verso le PMI.

Come accennato, **tra le minacce cibernetiche più insidiose degli ultimi anni va annoverato l'attacco ransomware**, che si sostanzia in un'operazione con cui l'attaccante si introduce nei sistemi di un'organizzazione per cifrarne i dati, al fine di ottenere il pagamento di un riscatto necessario a rendere le informazioni nuovamente disponibili al legittimo proprietario e/o a non diffonderle pubblicamente.

Fig. 1.8: La distribuzione della minaccia cibernetica in Italia (H1 2024)

Fonte: Tinexta Cyber, Risk Report 2024 H1, novembre 2024

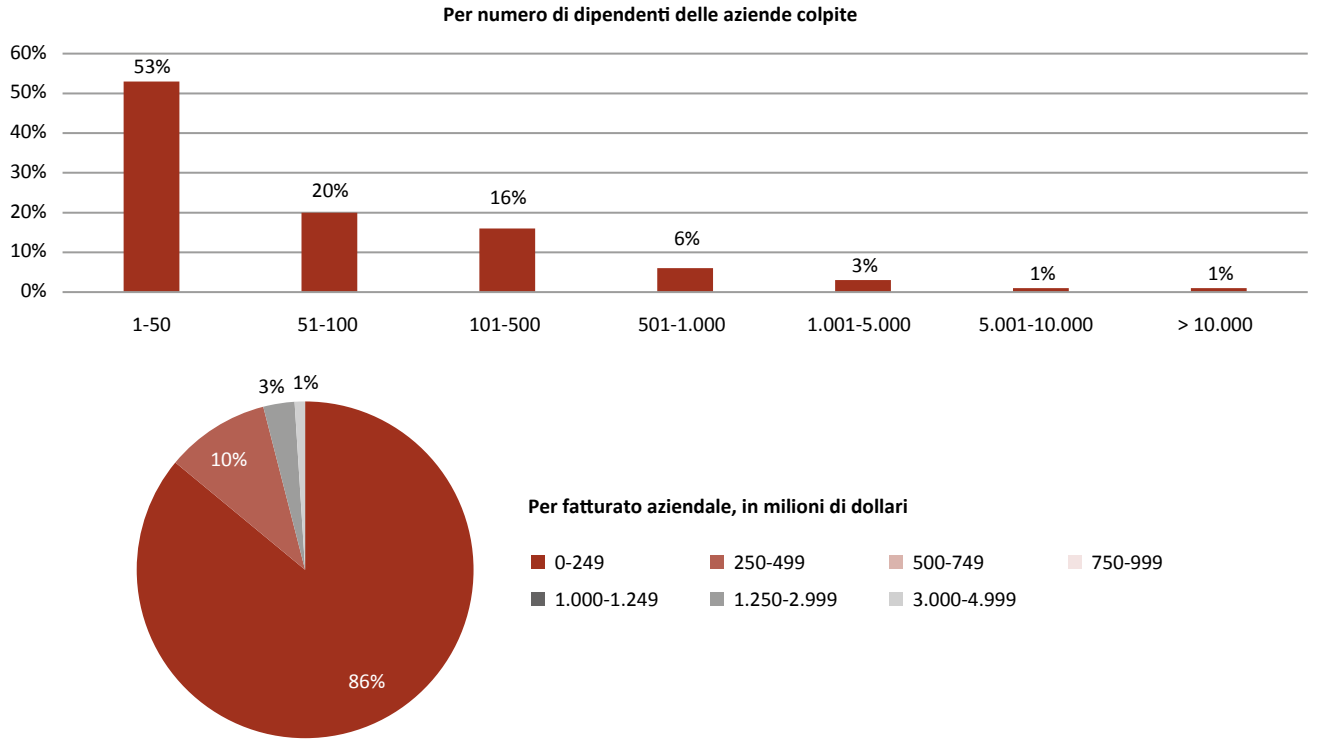
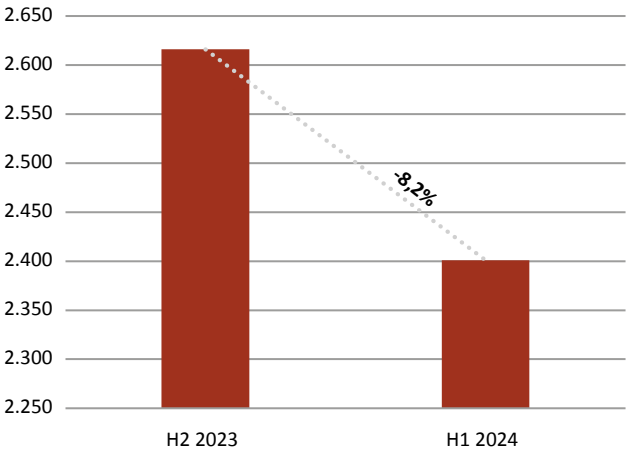


Fig. 1.9: Andamento degli attacchi ransomware a livello globale

Fonte: Tinexta Cyber, Risk Report 2024 H1, novembre 2024

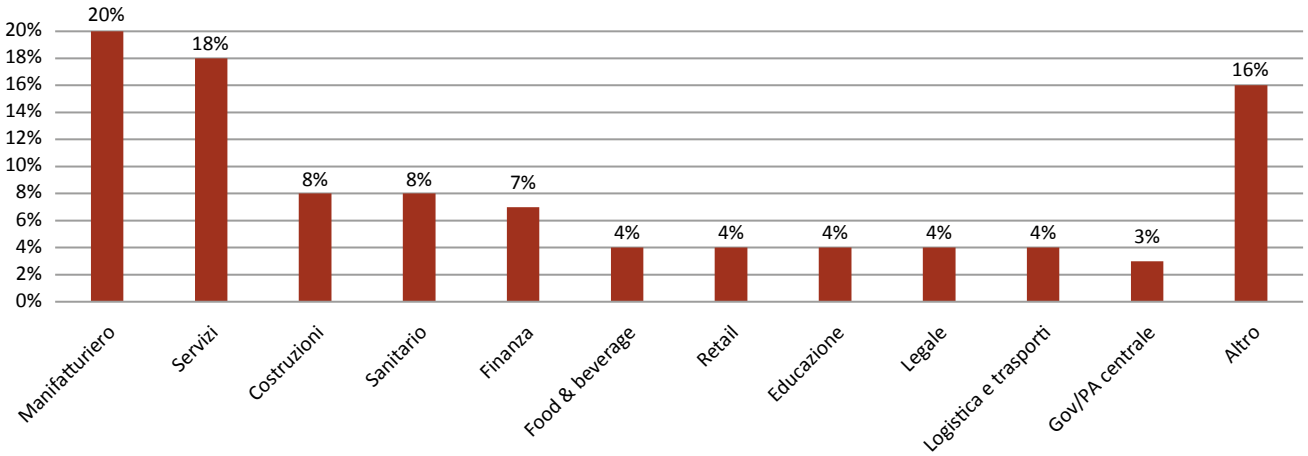


Secondo gli ultimi dati di Tinexta Cyber, **il totale delle vittime di attacchi ransomware a livello globale è diminuito dell'8,2% su base semestrale, essendo passato dalle 2616 dell'H2 2023 alle 2401 dell'H1 2024** (Fig. 1.9).

Rispetto all'analisi settoriale nell'H1 2024 (Fig. 1.10), **il manifatturiero risulta il più bersagliato da questa tipologia di minaccia, attestandosi al 20% su scala globale**, seguito – con un leggero distacco – dal settore dei servizi (18%), delle costruzioni (8%) e dal sanitario (8%). In coda a questa classifica si colloca il comparto governativo e della PA centrale (3%). È opportuno evidenziare come, rispetto al periodo precedente, gli attacchi ransomware riconducibili alla categoria "Altro" sono aumentati vertiginosamente e infatti tale categoria è passata da un mero 5% al 16%.

Fig. 1.10: Attacchi ransomware a livello globale, per settore (H1 2024)

Fonte: Tinexta Cyber, Risk Report 2024 H1, novembre 2024



Se per un verso si riducono gli attacchi ransomware a livello globale, è pur vero che su base semestrale vi è stato un incremento del 5,3% rispetto al numero di Paesi colpiti, che passano da 94 a 99 (Fig. 1.11). Parallelamente, **si registra un aumento piuttosto marcato con riguardo ai gruppi malevoli attivi in questo campo (gang ransomware), che sono passate da 52 a 73 nell'ultimo periodo considerato, segnando un preoccupante +40,4%.**

Fig. 1.11: Paesi colpiti da ransomware e gruppi attivi (H2 2023 – H1 2024)

Fonte: Tinexta Cyber, Risk Report 2024 H1, novembre 2024

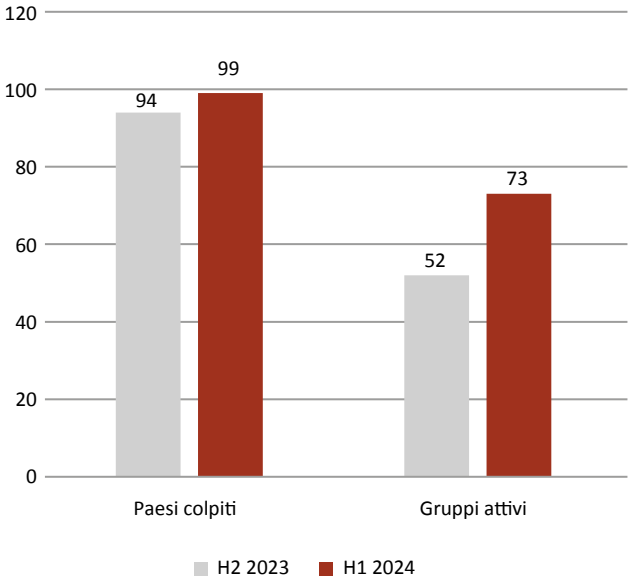


Fig. 1.12: Top 8 Paesi colpiti da attacchi ransomware (H1 2024)

Fonte: Tinexta Cyber, Risk Report 2024 H1, novembre 2024

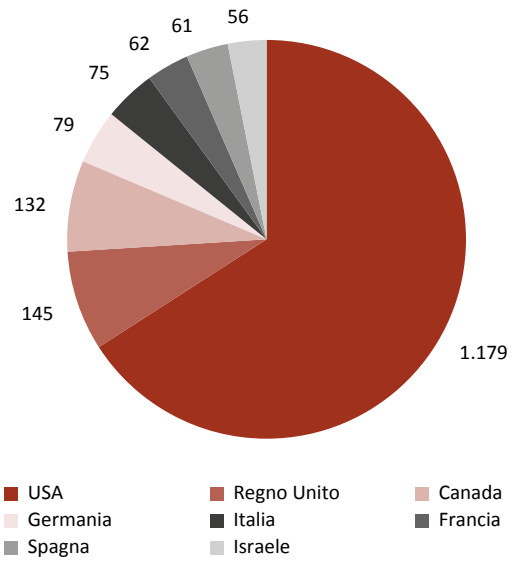
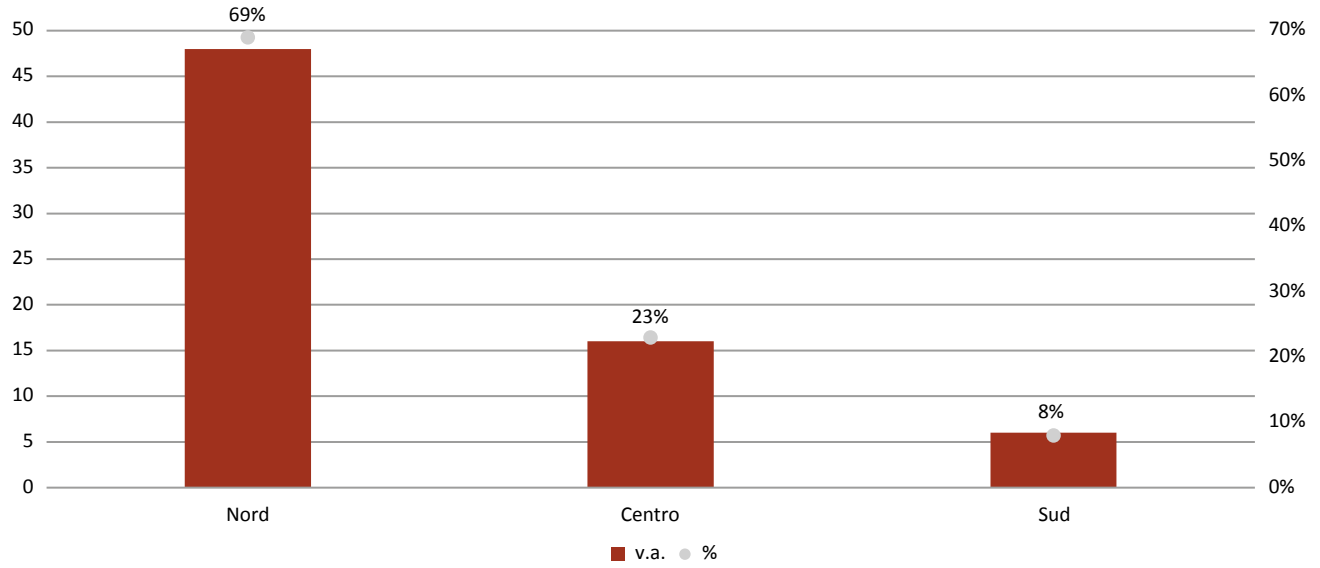


Fig. 1.13: Attacchi ransomware in Italia, per area geografica (H1 2024)

Fonte: Tinexta Cyber, Risk Report 2024 H1, novembre 2024



Tra i **paesi più colpiti nel primo semestre di quest'anno** si può osservare, senza sorprese, il **primato degli Stati Uniti, che si confermano come bersaglio prioritario delle gang ransomware con oltre 1.170 vittime** (Fig. 1.12). Seguono – con differenze quantitative importanti – il Regno Unito (145 vittime) e il Canada (132), mentre l'Italia occupa il quinto posto con 75 vittime, poco distante dalla Germania (79). Simili risultanze rendono evidenti come anche i Paesi europei siano particolarmente attenzionati ed esposti alle minacce di tipo ransomware.

Rispetto alla **distribuzione geografica delle vittime nel nostro Paese** (Fig. 1.13), gli ultimi dati di Tinexta Cyber mostrano **una maggiore concentrazione nelle regioni settentrionali, che raccolgono il 69% del totale, seguite da quelle del Centro (23%) e, infine, dalle regioni del Sud e le isole (8%)**. Si tratta di evidenze che riflettono quanto visto in precedenza rispetto a una più elevata concentrazione di attacchi, non solo di tipo ransomware, verso il settore manifatturiero, che è particolarmente presente nel Nord Italia.

1.2. LO STATO DEGLI INVESTIMENTI IN CYBERSICUREZZA IN UE NEL CONTESTO GLOBALE E IN ITALIA

In un contesto in cui i cyberattacchi sono sempre più gravi e numerosi, **gli investimenti** in cybersicurezza assumono un'importanza significativa in quanto rappresentano la prima risposta, in termini preventivi, alle esigenze che incombono su imprese e pubbliche amministrazioni e che derivano dalle nuove dinamiche del cyberspazio.

Nell'ultima versione del report "NIS Investments", pubblicato dall'ENISA a novembre 2024, vengono analizzate le attività di impiego economico per la sicurezza informatica a livello europeo, intervistando esponenti di 1.350 organizzazioni - pubbliche e private - residenti in tutti e 27 gli Stati Membri (50 per Paese), appartenenti agli 11 "settori ad alta criticità" sottoposti alla direttiva NIS2 (a cui è stato aggiunto il manifatturiero), ossia: 1) Energia; 2) Trasporti; 3) Bancario; 4) Infrastrutture dei mercati finanziari; 5)

Fig. 1.14: Spesa mediana in sicurezza informatica, per Stato Membro (in € milioni)

Fonte: ENISA, NIS Investments Report, novembre 2024

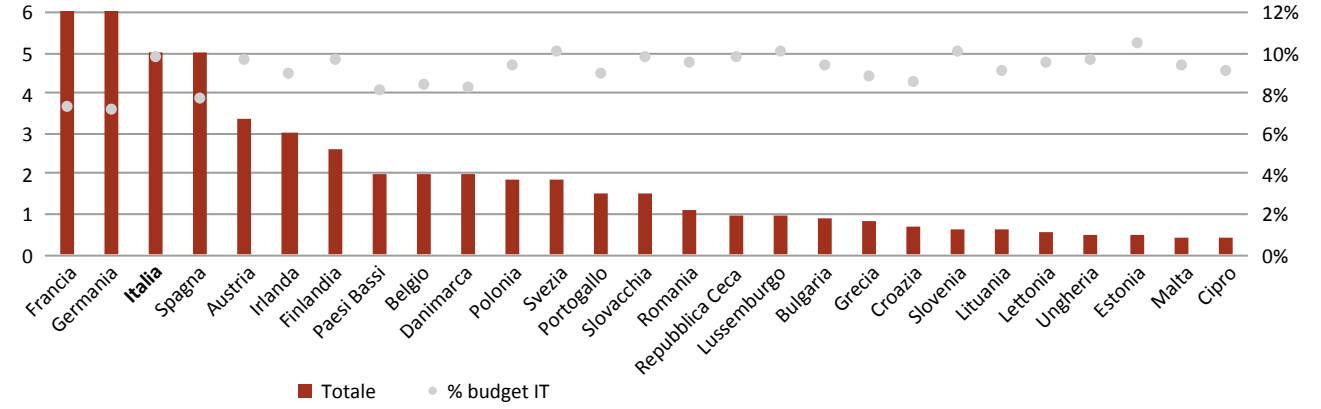
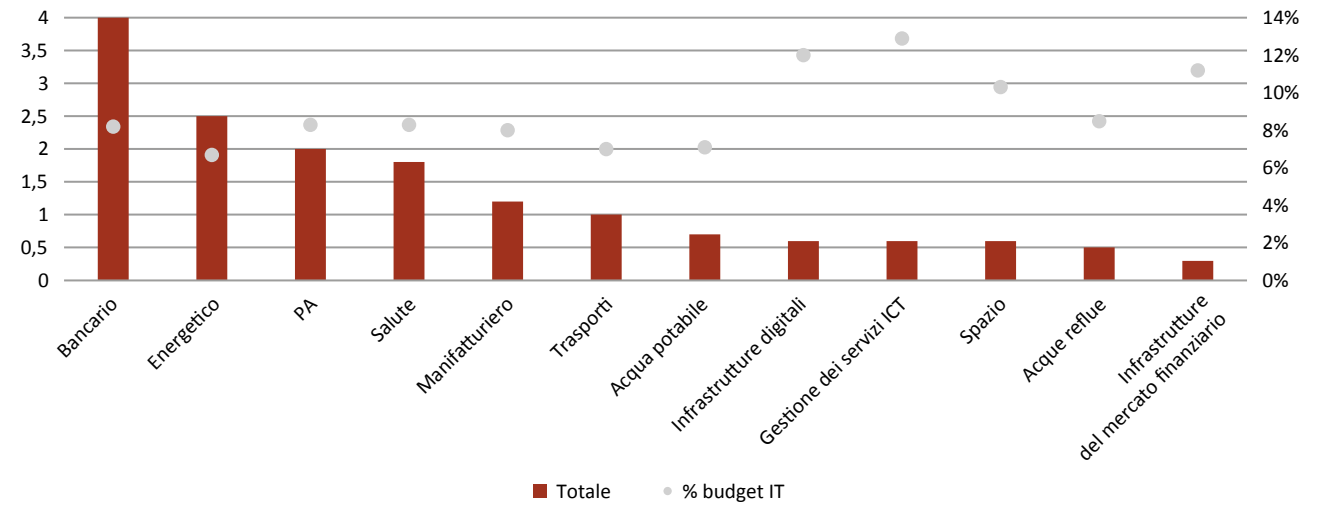


Fig. 1.15: Spesa mediana in sicurezza informatica, per settore NIS2 (in € milioni)

Fonte: ENISA, NIS Investments Report, novembre 2024



Salute; 6) Acqua potabile; 7) Acque reflue; 8) Infrastrutture digitali; 9) Gestione dei servizi ICT; 10) Pubblica Amministrazione; 11) Spazio.

Il rapporto appena menzionato mostra che **le organizzazioni francesi e tedesche sono quelle che spendono di più in valore mediano (€6 milioni), seguite da quelle italiane e spagnole (€5 milioni).** Tali investimenti rappresentano nel caso della Francia e della Spagna rispettivamente il 7,2% e il 7,1% del budget IT, mentre **per l'Italia corrispondono al 9,6%** (Fig. 1.14). L'Estonia è lo Stato Membro in cui le organizzazioni vedono la percentuale più alta del proprio budget IT allocata a favore della cybersicurezza (10,3%).

Volgendo uno sguardo ai singoli settori, si può osservare come **le aziende bancarie sono le più propense a investire in cybersicurezza, avendo riportato un valore**

mediano di €4 milioni, pari al 8,2% del budget IT (Fig. 1.15). Seguono quelle del settore energetico con €2,5 milioni (6,7% del budget IT) e la Pubblica Amministrazione con €2 milioni (8,3% del budget IT). Agli ultimi posti vi sono le imprese che operano nel comparto spaziale (€0,6 milioni – 10,3% del budget IT), le acque reflue (€0,5 milioni – 8,5% del budget IT) e le infrastrutture del mercato finanziario (€0,3 milioni – 11,2% del budget IT). In tema, appare interessante osservare la quota di **Full-Time Equivalent** (FTE – Equivalente a Tempo Pieno) che si occupano di cybersicurezza nei soggetti sottoposti alla disciplina NIS2 (Fig. 1.16). Ebbene, **la**

Fig. 1.16: FTE mediano in sicurezza informatica, per Stato Membro

Fonte: ENISA, NIS Investments Report, novembre 2024

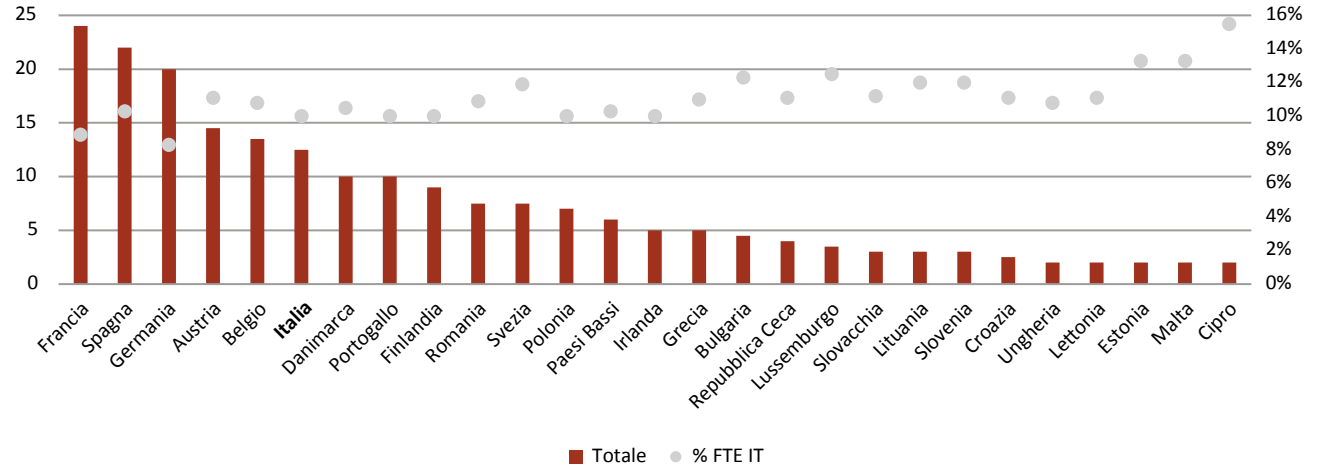
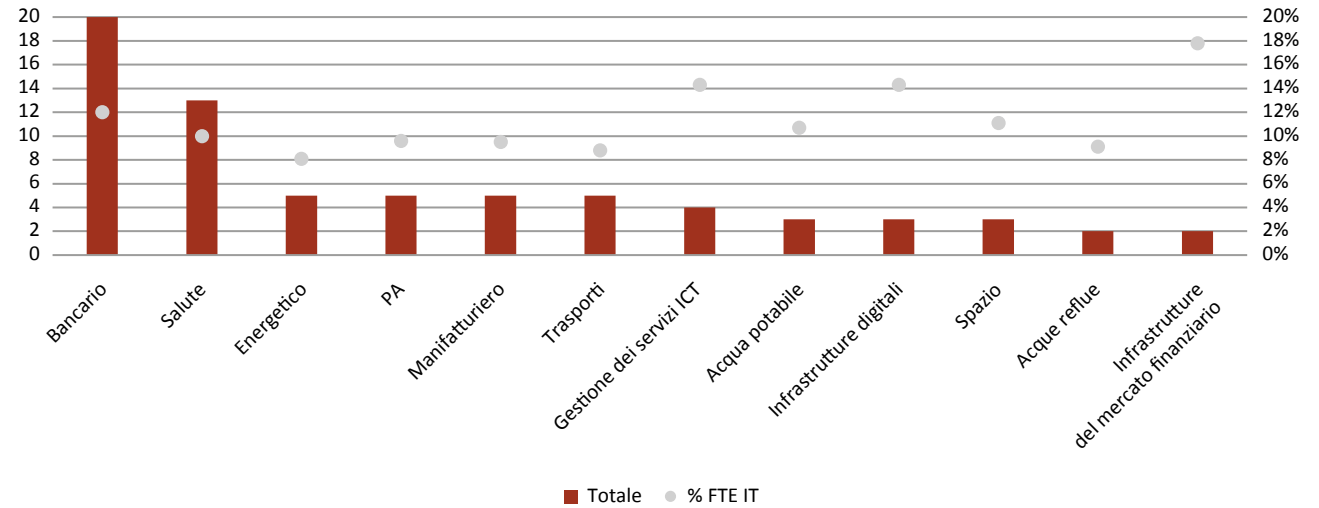


Fig. 1.17: FTE mediano in sicurezza informatica, per settore NIS2

Fonte: ENISA, NIS Investments Report, novembre 2024



Francia primeggia, mostrando un valore mediano di 24 FTE, seguita dalla Spagna (22) e dalla Germania (20). Se si parametra la quota di personale a tempo pieno in cybersicurezza al totale di FTE IT emerge che sono Cipro, a pari merito con Malta, ed Estonia ad avere la percentuale più elevata, ossia rispettivamente il 15,5% e il 13,3%. Irlanda, Francia e Germania si collocano in coda, con una quota di FTE impiegati in cybersicurezza ordinatamente del 10%, del 8,9% e del 8,3% rispetto agli FTE in ambito IT.

Il numero mediano più elevato di FTE in cybersicurezza si registra in capo alle imprese bancarie (20 FTE; 12% di FTE IT) e sanitarie (13 FTE; 10% di FTE IT). Seguono i soggetti del comparto energetico (5 FTE; 8,1% di FTE IT), che presentano valori simili rispetto a PA (5 FTE; 9,6% di FTE IT), manifatturiero (5 FTE; 9,5% di FTE IT) e trasporti (5 FTE; 8,8% di FTE IT). Diversamente, le imprese del settore spaziale (3), delle acque reflue (2) e le infrastrutture del mercato finanziario (2) detengono le quote più basse (Fig. 1.17). Tuttavia, queste ultime si posizionano prime in classifica se si considera il personale a tempo pieno in cybersicurezza con quello IT (17,8%).

1.3. LA PREPARAZIONE ALLA NIS2 NEL CONTESTO EUROPEO E NAZIONALE

L'edizione di quest'anno del report di ENISA contiene anche un utile spaccato **sulla preparazione dei soggetti intervistati rispetto all'implementazione della direttiva NIS2**, che è divenuta applicabile lo scorso 18 ottobre in tutti gli Stati Membri. Tuttavia, al 28 novembre, solo 4 Paesi hanno recepito questo importante atto normativo nei termini previsti (Italia, Belgio, Croazia e Lituania). Per tutti gli altri il ritardo si è tradotto nell'apertura di una procedura di infrazione da parte della Commissione europea.

In questo scenario**, il livello di awareness sulla NIS2 e sui rispettivi adempimenti varia significativamente tra gli Stati Membri e i settori**. Più nel dettaglio, si passa dal 100% di Francia e Finlandia al 82% della Croazia e al 80% di Malta, mentre **l'Italia si colloca in quinta posizione con il 96% di awareness** (Fig. 1.18). Rispetto ai settori la disomogeneità è ancor più marcata (Fig. 1.19), **7 settori su 12 raggiungono un valore pari o prossimo al 100%,** di converso, **lo spazio si col-**

Fig. 1.18: Livello di awareness rispetto alla direttiva NIS2, per Stato Membro

Fonte: ENISA, NIS Investments Report, novembre 2024

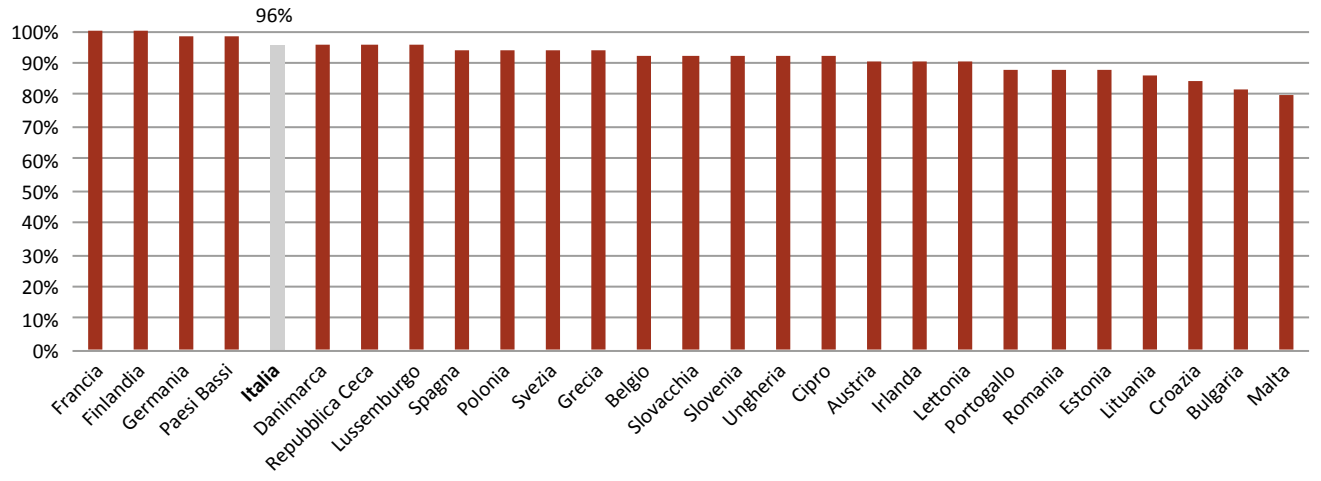
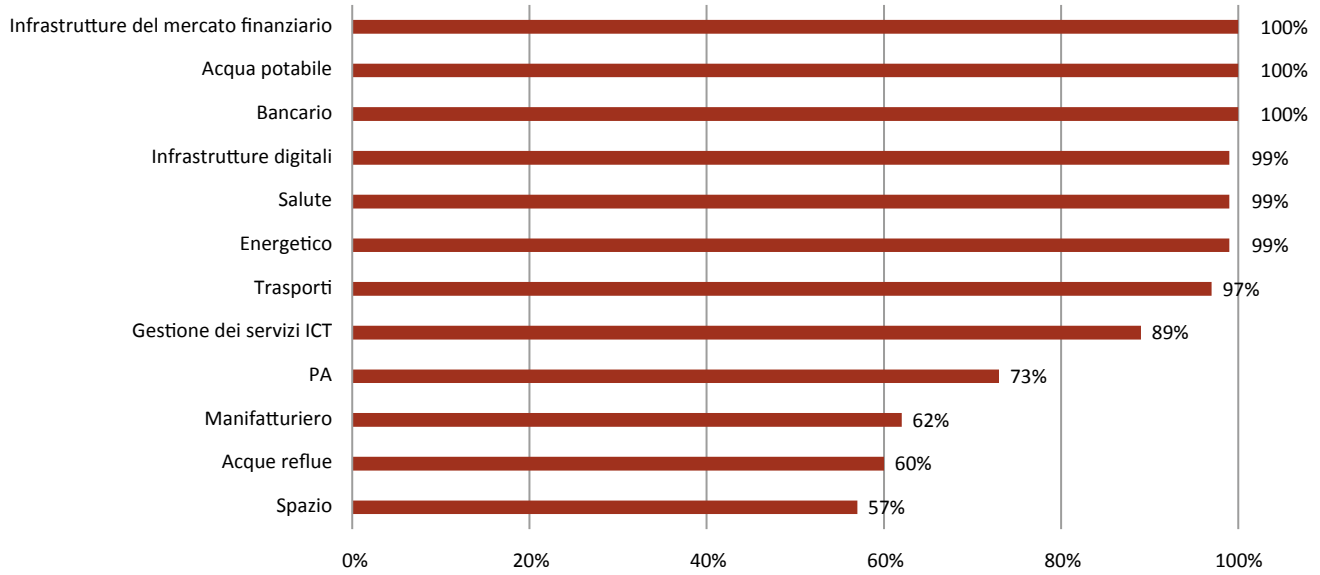


Fig. 1.19: Livello di awareness rispetto alla direttiva NIS2, per settore NIS2

Fonte: ENISA, NIS Investments Report, novembre 2024



loca in ultima posizione col 57%, preceduto da acque reflue (60%), manifatturiero (62%) e PA (73%), evidenziando un urgente bisogno di aumentare la consapevolezza in questi settori.

Quanto detto vale ancor di più se si volge uno sguardo alle **variazioni di budget programmate per far fronte alla compliance richiesta dalla disciplina NIS2**. Infatti, considerando tutte le organizzazioni intervistate, **oltre il 38% ha dichiarato di non aver bisogno di ulteriore budget per implementare le disposizioni della direttiva e un ulteriore 14% non ritiene possibile procedere a un incremento delle risorse** (Fig. 1.20). In particolare, come si può notare dal grafico successivo, i soggetti italiani fanno registrare un preoccupante 58% alla voce "Non c'è bisogno di un incremento" che, se sommato con il 6% per "Non c'è possibilità di incrementarlo" e a una quota complessiva del 33% rispetto a un incremento permanente del budget/investimento una tantum, restituisce una situazione quantomeno preoccupante con riferimento al nostro Paese.

Rispetto ai settori, appare incoraggiante che **il comparto spaziale raggiunga l'80% se si considerano congiuntamente gli incrementi permanenti al budget e gli investimenti una tantum** (Fig. 1.21). **Seguono le infrastrutture del mercato finanziario (63%), le PA (56%) e le infrastrutture digitali (54%).** In coda (40%), si posizionano i settori bancario, energetico e acque reflue. Tuttavia, per i primi due è opportuno evidenziare che – come emerge anche dai dati sopracitati – si tratta di comparti decisamente virtuosi in tema di investimenti in cybersicurezza, per cui tali valori non dovrebbero destare particolare preoccupazione, a differenza del segmento delle acque reflue che si colloca in penultima posizione con riguardo alla spesa mediana in sicurezza informatica.

Altro tema assolutamente centrale è rappresentato dal **coinvolgimento degli organi di gestione dei soggetti NIS2 nell'approvazione delle misure di gestione dei rischi di cybersicurezza**, dovendo altresì supervisionarne la conseguente attuazione e potendo essere destinatari di pesanti sanzioni in caso di violazioni.

Fig. 1.20: Variazioni al budget per l'implementazione della direttiva NIS2, per Stato Membro

Fonte: ENISA, NIS Investments Report, novembre 2024

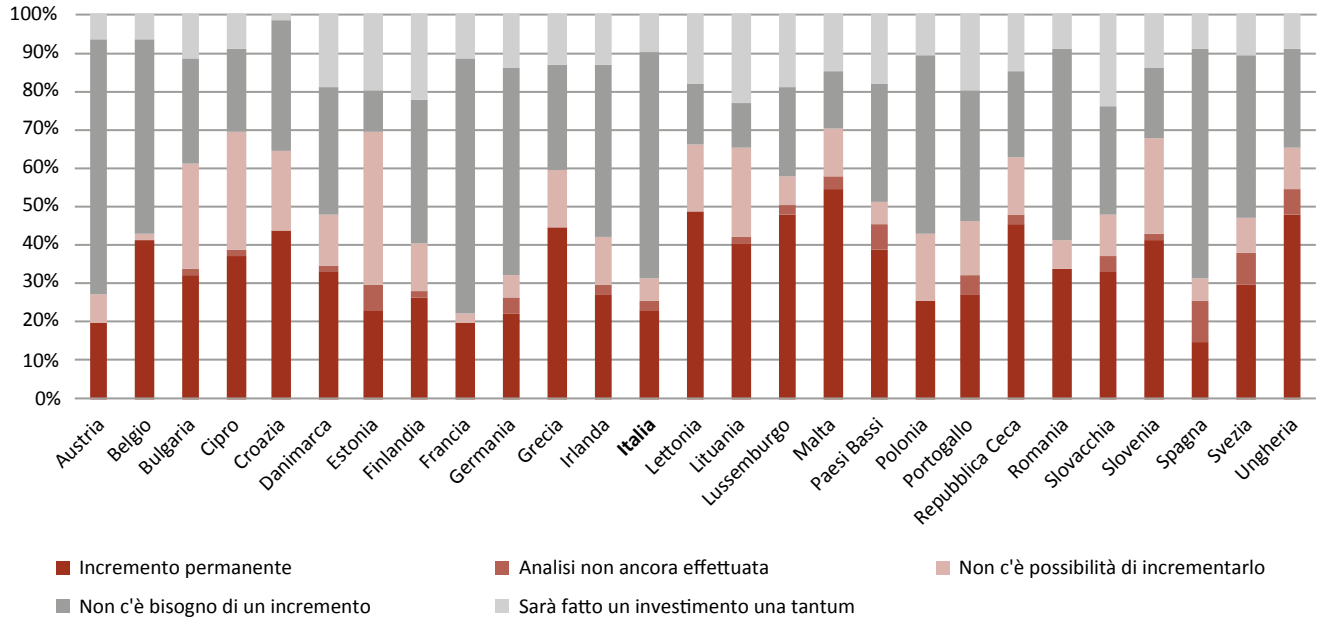


Fig. 1.21: Variazioni del budget per l'implementazione della direttiva NIS2, per settore NIS2

Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024

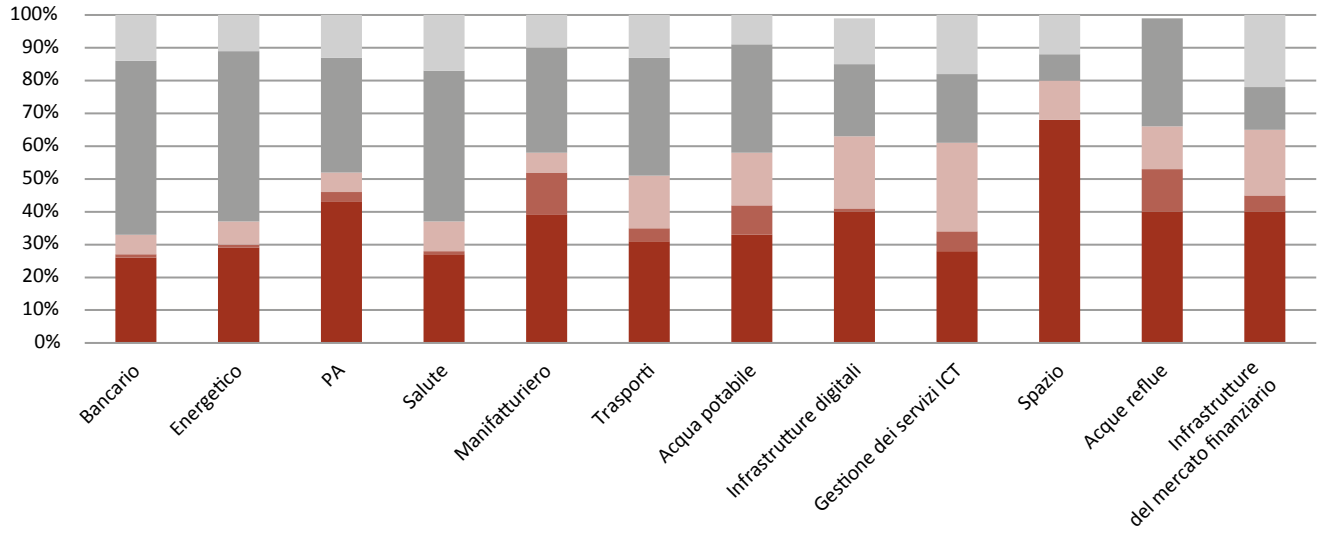


Fig. 1.22: Coinvolgimento dei vertici nella formazione in cybersecurity, per Stato Membro

Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024

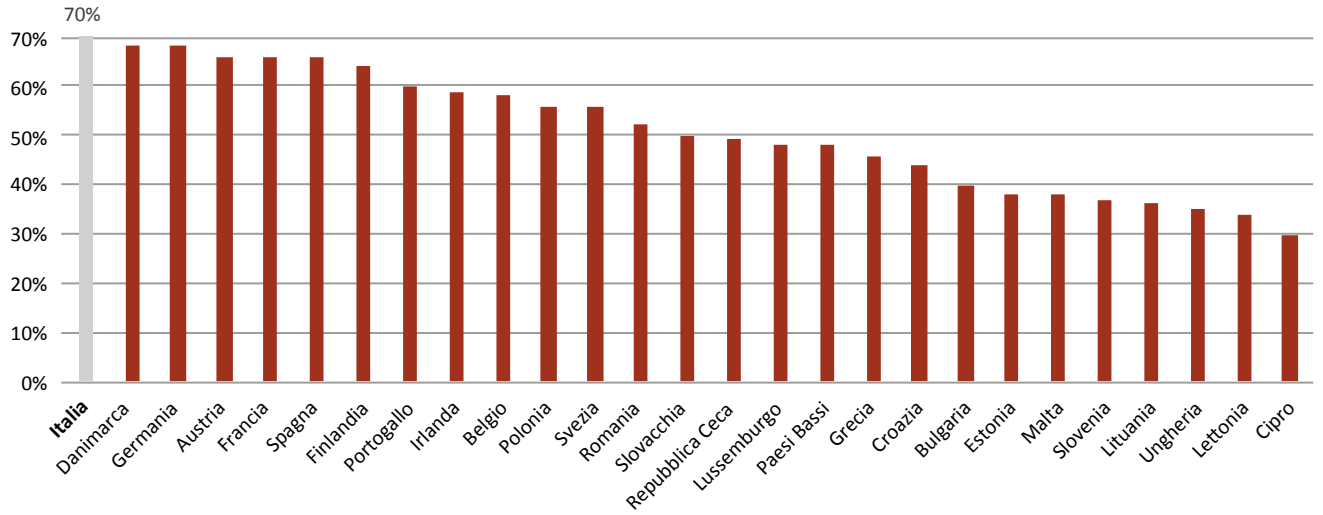
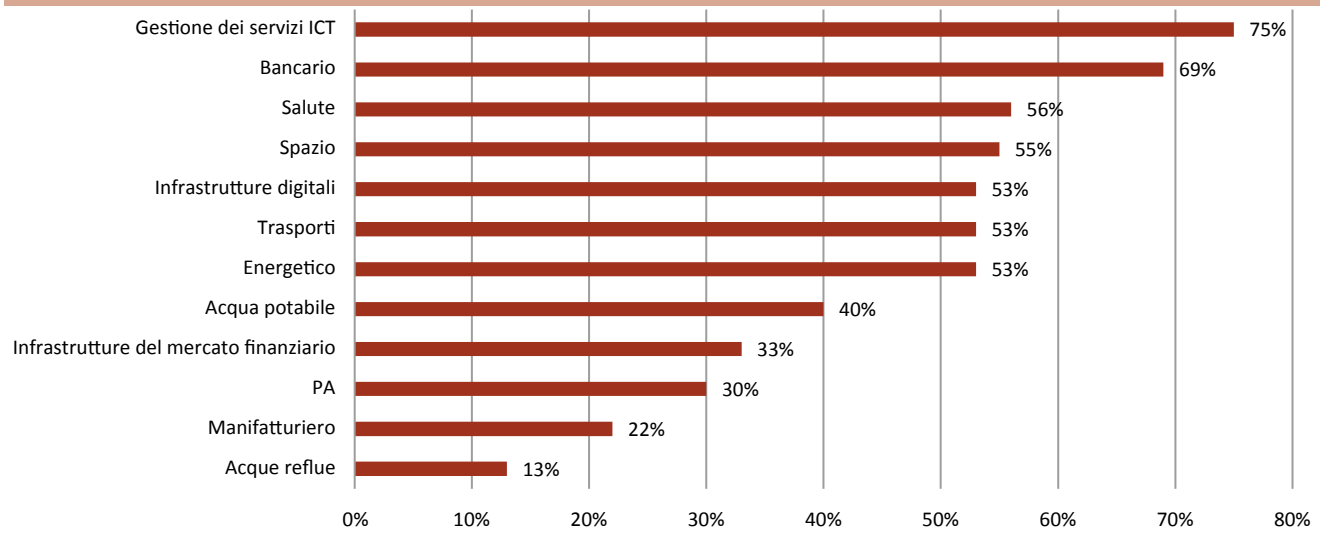


Fig. 1.23: Coinvolgimento dei vertici nella formazione in cybersecurity, per settore NIS2

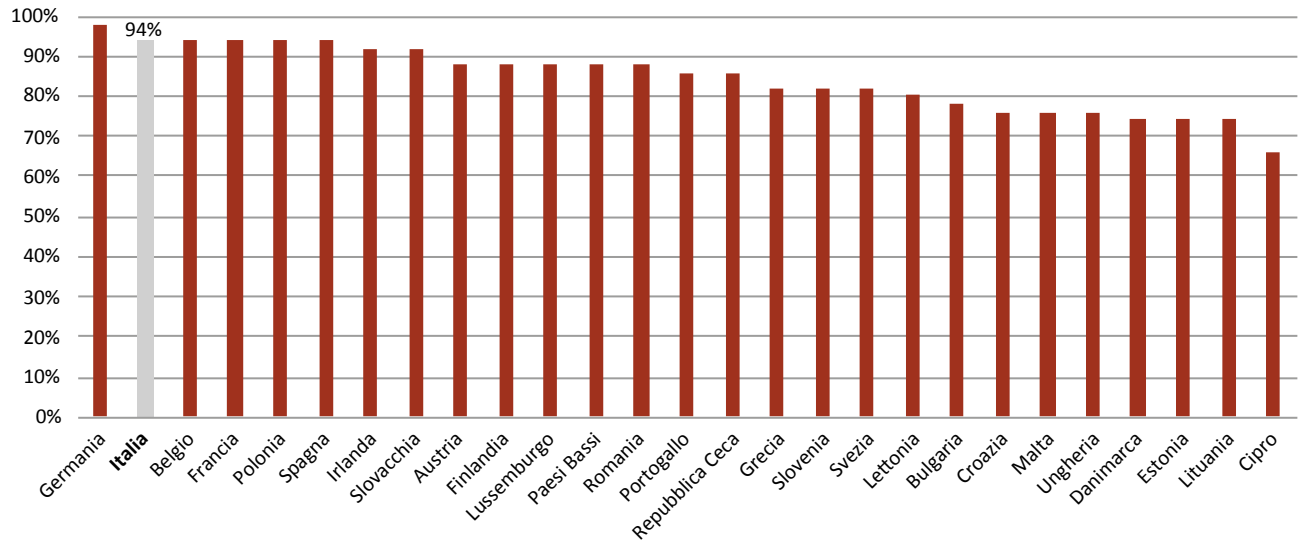
Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024



Per adempiere a queste nuove responsabilità viene previsto che i componenti di tali organi seguano una formazione specifica in materia di sicurezza informatica. Sul punto, **dai dati ENISA emerge che l'Italia è lo Stato Membro più virtuoso, in quanto il 70% delle organizzazioni intervistate a livello nazionale coinvolge i propri vertici nella formazione in cybersicurezza** (Fig. 1.22). Seguono poi Danimarca e Germania col 68%, mentre alle ultime posizioni si trovano Ungheria (35%), Lettonia (34%) e Cipro (30%).

Fig. 1.24: Coinvolgimento dei vertici nell'approvazione delle misure di gestione dei rischi di cybersecurity, per Stato Membro

Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024



Con riguardo ai settori (Fig. 1.23), gestione dei servizi ICT – che ricomprende i segmenti B2B dei fornitori di servizi gestiti e dei servizi di sicurezza gestiti – è quello che performa meglio (75%), seguito da bancario (69%), salute (56%) e spazio (55%). Chiudono la classifica, la PA (30%), il manifatturiero (22%) e – ancora una volta – le acque reflue (13%). Tali dati evidenziano come **sia decisamente prioritario promuovere una maggiore sensibilizzazione sui temi della cybersicurezza, in particolare in settori critici come la PA e il manifatturiero**, poiché dal primo dipendono molti servizi essenziali per i cittadini e il secondo costituisce una fetta rilevante del tessuto imprenditoriale a livello europeo e nazionale.

Rispetto **all'approvazione delle misure di gestione dei rischi cyber**, anche in questo caso **l'Italia si posiziona tra i primi della classe** (Fig. 1.24)**, più nello specifico al secondo posto (94%)** – a pari merito con Belgio, Francia, Polonia e Spagna – e poco dopo la Germania (98%). Invece, in coda troviamo Danimarca, Estonia, Lituania (tutti e tre al 74%) e Cipro (66%).

Volgendo uno sguardo ai settori, **gestione dei servizi ICT si conferma al primo posto (96%)**, seguito dalle infrastrutture del mercato finanziario (95%), le quali - come visto - figurano tra le ultime posizioni per coinvolgimento dei vertici nella formazione in cybersicurezza, e dai segmenti bancario ed energetico (89%). Chiudono questa classifica PA (80%), manifatturiero (74%) e acque reflue (60%), con una quota decisamente più elevata rispetto a quella vista precedentemente sulla formazione dei soggetti apicali (Fig. 1.25). Ne emerge che, soprattutto in questi tre settori, i vertici si occupano di approvare le misure di cybersicurezza senza aver preventivamente avuto una formazione adeguata in materia.

Dato che **la sicurezza della supply chain è un elemento centrale sia per la cybersicurezza in generale, sia nella direttiva NIS2**, specificamente nella parte in cui si prescrive di **valutare le vulnerabilità specifiche per ogni diretto fornitore di servizi**, nonché la **qualità complessiva dei prodotti e delle pratiche di cibersicurezza**, comprese le procedure di sviluppo sicuro,

Fig. 1.25: Coinvolgimento dei vertici nell'approvazione delle misure di gestione dei rischi di cybersecurity, per settore NIS2

Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024

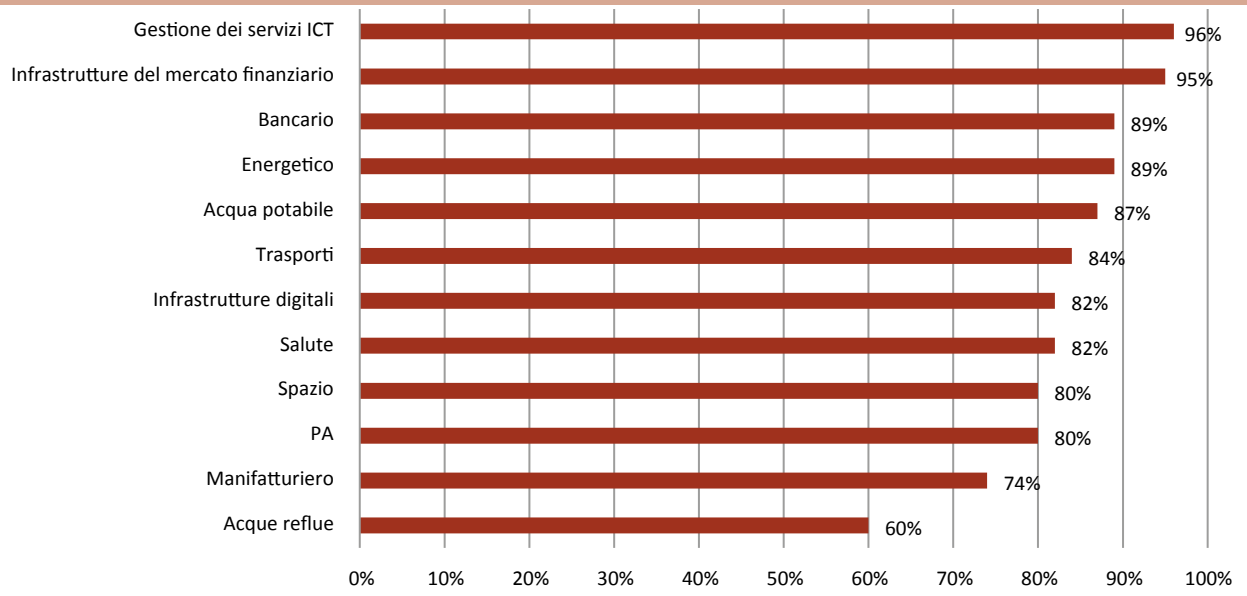


Fig. 1.26: Presenza di policy per la gestione dei rischi di cybersecurity delle terze parti (partner, vendor, fornitori), per Stato Membro

Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024

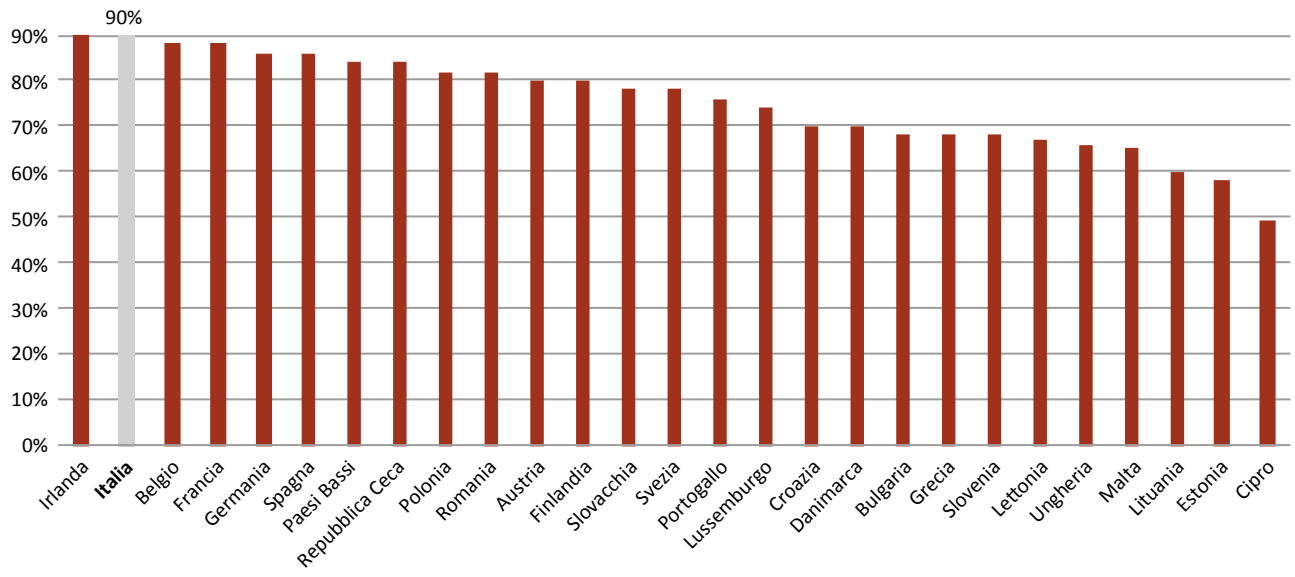
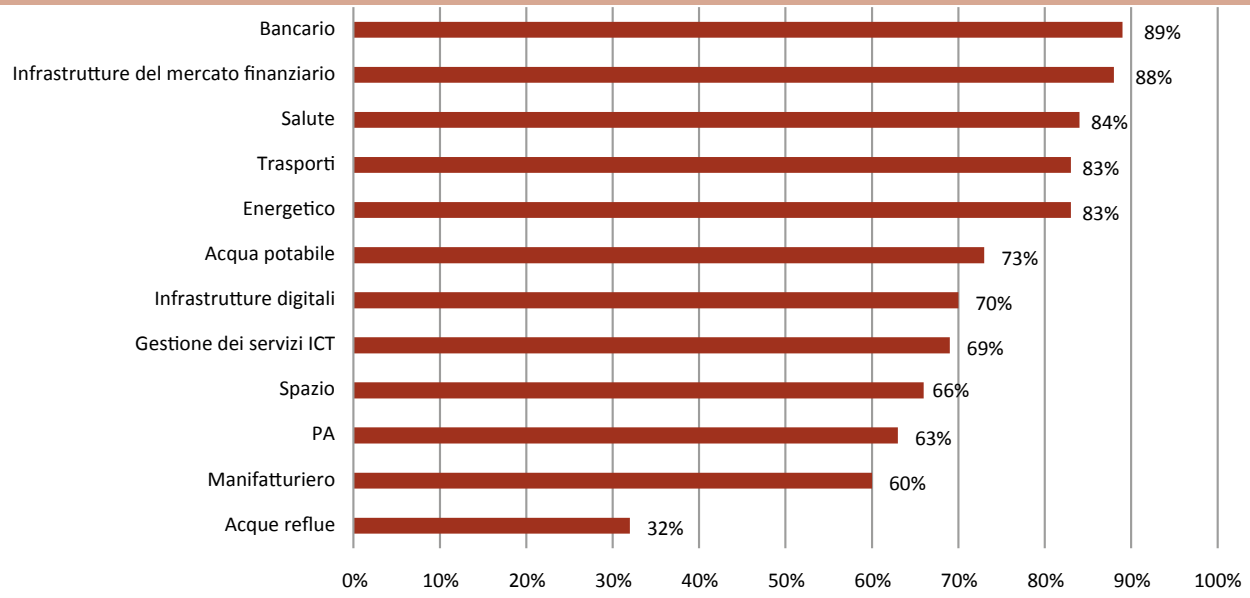


Fig. 1.27: Presenza di policy per la gestione dei rischi di cybersecurity delle terze parti (partner, vendor, fornitori), per settore NIS2

Fonte: Fonte: ENISA, NIS Investments Report, novembre 2024



appare fondamentale per i soggetti pubblici e privati **stabilire policy chiare e adeguate atte a prevenire e gestire i rischi relativi alle terze parti** (come partner, vendor e fornitori). Sul tema, **le organizzazioni italiane fanno collocare il nostro Paese in prima posizione** (Fig. 1.26) insieme all'Irlanda (90%). Seguono Belgio e Francia (88%), mentre chiudono la classifica Lituania (60%), Estonia (58%) e Cipro (49%). Tra i settori (Fig. 1.27), **quello che performa meglio anche in questa occasione è quello bancario (89%)**, seguito dalle infrastrutture del mercato finanziario (88%) e dal comparto sanitario (84%). Viceversa, **in coda rivediamo nuovamente PA (63%), manifatturiero (60%) e, infine, acque reflue (32%).**

icom 2005 25
istituto per la competitività

CAPITOLO 2

L'ECOSISTEMA NORMATIVO SULLA CYBERSECURITY

2.1. L'EVOLUZIONE DEL FRAMEWORK EUROPEO SULLA CYBERSECURITY

2.1.1. Il Cybersecurity Package: la direttiva NIS 2 e il nuovo scenario normativo

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 scaduto il 17 ottobre scorso. 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.

È scaduto lo scorso 17 ottobre il termine ultimo per il recepimento, da parte degli Stati membri, della **Direttiva n. 2555/2022 (NIS2)**, pubblicata il 27 dicembre 2022 ed entrata in vigore il 17 gennaio 2023. Tale direttiva fa seguito all'adozione, nel 2016, della **prima direttiva NIS** (recepita in Italia con il d. lgs. n. 65/2018) – con la quale per la prima volta sono state definite misure organiche rivolte esplicitamente alla sicurezza delle informazioni e alla cybersicurezza – di cui cerca di risolvere una serie di criticità applicative, 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.

Partendo da tale scenario, **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 e soggetti importanti (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, 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 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 CER, anche quest'ultima da recepire entro lo scorso 17 ottobre. 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.
La tabella che segue (Tab. 2.1) riassume e confronta le principali disposizioni contenute nelle due direttive NIS, 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.
Il 14 settembre 2023, la Commissione europea ha pubblicato i primi orientamenti sull'applicazione di alcune norme fondamentali della Direttiva NIS2, ossia l'art. 4 (paragrafi 1 e 2) e l'art. 3, paragrafo 4. 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 n. 2554/2022 – DORA), 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 (art. 23); 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.

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 ri-

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. 21)
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)

schi 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.
Lo scorso 17 ottobre è stato invece pubblicato il **Regolamento di Esecuzione (UE) 2024/2690 che dettaglia le modalità di applicazione della Direttiva NIS2 per un sottoinsieme di soggetti critici**, ma fornisce alcuni primi spunti rispetto al contenuto delle misure di sicurezza e alle definizioni di incidenti significativi per i quali persiste obbligo di notifica.
L'allegato al Regolamento di Esecuzione, in particolare, definisce le modalità di implementazione delle misure di sicurezza, evidenziando l'importanza di adottare i requisiti tecnici e metodologici delle misure in considerazione del grado di esposizione ai rischi, delle proprie dimensioni, della probabilità che si verifichino incidenti e della relativa gravità, ivi compreso l'impatto sociale ed economico.
Lo stesso regolamento fornisce inoltre alcune linee guida generali per la classificazione degli eventi in «incidenti significativi», quali quelli che hanno comportato o possono comportare:

- una perdita finanziaria rilevante per il soggetto (superiore a 500 000 euro o, se tale importo è inferiore, al 5% del suo fatturato totale annuo dell'esercizio precedente);
- l'esfiltrazione di segreti commerciali;
- il decesso o danni considerevoli alla salute di una persona.

A ciò si aggiungono l'ipotesi di un accesso non autorizzato e di carattere malevolo ai sistemi informativi e di rete, con rischio di gravi perturbazioni operative, quella di incidente ricorrente (così come definito all'art. 4) ed i casi in cui sia soddisfatto uno o più criteri di cui agli artt. 5-14 che si occupano delle singole categorie di soggetti colpiti da incidenti significativi (fornitori di servizi DNS, cloud computing, data center, reti di distribuzione dei contenuti, servizi di sicurezza gestiti, mercati online, motori di ricerca online, social network e servizi fiduciari).

2.1.2. Verso la prima revisione del Cybersecurity Act (CSA)

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]; 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,

2 Si v. infra, par. 3.2."

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 ri-

spetto 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.

2.1.3. *La sicurezza dei prodotti con elementi digitali: il Cyber Resilience Act (CRA)*

Sebbene i principali obblighi si applicheranno a partire dall'11 dicembre 2027, lo scorso 10 dicembre è entrato in vigore il Regolamento n. 2024/2847 (Cyber Resilience Act).

Si tratta di un regolamento straordinariamente importante che si inquadra nella cornice definita dalla Strategia lanciata nel 2020 e che mira a rispondere all'esigenza, nella logica di assicurare un ecosistema europeo complessivamente sicuro, di garantire che i dispositivi utilizzati da cittadini, imprese e pubbliche amministrazioni rispondano a standard di sicurezza adeguati.

La normativa dettata dal regolamento, in particolare, persegue il fine di 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.

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 importanti (All. III, Classe I e II) e quelli critici (All. IV), individua i requisiti essenziali di cibersicurezza (All. I), le informazioni ed istruzioni da fornire all'utilizzatore (All. II) prevedendo che alcuni prodotti critici di particolare rilevanza per la sicurezza informatica siano sottoposti a una valutazione di terze parti da parte di un organismo autorizzato prima di essere venduti nel mercato UE. Lo stesso regolamento conseguentemente individua una serie corposa di obblighi a carico di produttori, importatori e distributori. I primi, nello specifico, sono chiamati a svolgere una serie di attività e a compiere numerosi adempimenti tra cui:

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. garantire un periodo di assistenza è di almeno cinque anni;
c. 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;
d. documentare in maniera proporzionata alla natura del prodotto ed ai rischi, gli aspetti concernenti il prodotto, incluse le vulnerabilità di cui venga a conoscenza;
e. dotarsi di appropriate policy e procedure, incluse quelle di identificazione e gestione delle vulnerabilità;
f. fornire informazioni ed istruzioni sul prodotto che siano chiare e comprensibili;
g. 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;
h. 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;
i. inviare ad ENISA (entro 24 ore) una notifica di preallarme di una vulnerabilità attivamente sfruttata, una notifica entro 72 ore ed una relazione finale entro 14 giorni dalla messa a disposizione di una misura correttiva o di attenuazione (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);
j. individuare un punto di contatto unico e garantire che esso sia facilmente identificabile dagli utilizzatori;
k. redigere la dichiarazione di conformità UE (in tutte le lingue dei paesi in cui il prodotto è immesso in commercio) ed attestare il rispetto dei requisiti essenziali di cibersicurezza.

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 del regolamento 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, il regolamento 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 controllo.
Rispetto a questi ultimi, in particolare, il regolamento 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. 27 **"Presunzione di conformità"** con la quale viene attribuito alla Commissione il potere adottare atti di esecuzione che stabiliscano specifiche comuni relative ai requisiti tecnici che forniscono i mezzi per soddisfare i requisiti essenziali di cibersicurezza di cui all'allegato I. A ciò si aggiunge il potere della stessa Commissione di adottare atti delegati per integrare il regolamento specificando i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità dei prodotti con elementi digitali ai requisiti essenziali di cibersicurezza o a parti di essi di cui al medesimo allegato I.
Ampio spazio è dedicato agli organismi di valutazione della conformità, di cui il regolamento indica i requisiti (art. 39), gli obblighi operativi (art. 47), gli obblighi di informazione (art. 49) nonché alle procedure di notifica da seguire.

Rispetto a **sorveglianza ed *enforcement***, il regolamento affida agli Stati membri la designazione di un'autorità deputata alla sorveglianza del mercato e dei prodotti con elementi digitali di cui definisce i relativi requisiti e gli specifici poteri.
Molto rilevanti i poteri attribuiti alla Commissione. Ed infatti, oltre ad incoraggiare ed agevolare lo scambio di esperienze tra le autorità di vigilanza del mercato designate dagli Stati membri ed al potere di adottare atti delegati come sopra evidenziato, la Commissione riveste un ruolo di primaria importanza nell'ambito della procedura di salvaguardia dell'UE (art. 55) nonché nella procedura a livello di Unione relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo (art. 56) e nello svolgimento delle indagini a tappeto che generalmente vengono coordinate dalla Commissione stessa (art. 60).
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. 13 e 14 e dunque degli obblighi a carico dei fabbricanti. 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.
È attualmente è in fase di costituzione il Cyber Resilience Act Expert Group (CRA Expert Group), che assisterà e consiglierà la Commissione su questioni rilevanti per l'implementazione del CRA.

2.1.4. *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, dal 17 gennaio 2025 è pienamente applicabile 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)[3]. 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

3 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.

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 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.
In attuazione del DORA, il 24 ottobre scorso è stato pubblicato il Regolamento delegato della Commissione che integra il regolamento (UE) n. 2022/2554 per quanto riguarda le norme tecniche di regolamentazione sull'armonizzazione delle condizioni per lo svolgimento delle attività di sorveglianza, mentre il 2 dicembre è stato adottato il Regolamento delegato della Commissione relativo alle norme tecniche di regolamentazione per specificare i criteri per determinare la composizione del gruppo di esame congiunto che garantisce una partecipazione equilibrata del personale delle AEV e delle autorità competenti interessate, la loro designazione, i compiti e le modalità di lavoro.

2.1.5. Uno scudo per l'Europa: il Cyber Solidarity Act (CSoA)

È stato pubblicato lo scorso 15 gennaio il **Regolamento UE n. 2025/38 (Cyber Solidarity Act)** che punta a definire misure volte a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi. Tale obiettivo è perseguito, in particolare, mediante l'istituzione di una rete paneuropea di poli informatici, un meccanismo per le emergenze di cibersicurezza ed uno di riesame degli incidenti di cibersicurezza. Si tratta di strumenti importanti, attraverso i quali l'UE intende sviluppare e potenziare capacità coordinate in materia di rilevamento e capacità comuni in materia di conoscenza situazionale, sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala, nella mitigazione del loro impatto e nella ripresa dagli stessi, e per sostenere gli altri utenti nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala.
Nel rispetto delle competenze degli Stati membri e ad integrazione delle attività svolte dalla rete di CSIRT, da EU-CyCLONe e dal gruppo di cooperazione NIS, il regolamento istituisce, come anticipato, il **sistema europeo di allerta per la cibersicurezza** che si caratterizza per essere una rete paneuropea di infrastrutture costituita da poli informatici nazionali e transfrontalieri che aderiscono su base volontaria, con compiti di raccolta e condivisione di informazioni relative a minacce ed incidenti informatici. I poli nazionali, in particolare, sono istituiti dagli Stati membri e mediante specifico accorso scritto, possono portare alla costituzione, qualora siano almeno 3, di un consorzio

ospitante un polo transfrontaliero. Particolare attenzione è dedicata alla **cooperazione e condivisione di informazioni tra poli informatici transfrontalieri e al loro interno** (art. 6) nella logica di promuovere e migliorare il rilevamento delle minacce informatiche e rafforzare le capacità della rete di CSIRT di prevenire e rispondere agli incidenti o di attenuarne l'impatto ed accrescere il livello di cibersicurezza.

Molto interessante **l'istituzione della riserva dell'UE per la cibersicurezza**, di cui la Commissione ha la responsabilità di attuazione e che consiste in servizi di risposta erogati da fornitori di fiducia di servizi di sicurezza gestiti selezionati cui possono accedere soggetti specificatamente individuati mediante la formulazione di specifica richiesta da veicolare secondo la procedura e con i contenuti indicati. Ad ENISA il compito di mappare, ogni due anni, i servizi necessari agli utenti individuati dal regolamento.

Il **meccanismo di riesame degli incidenti di cibersicurezza** consente ad ENISA, su richiesta della Commissione o di EU-CyCLONe, con il sostegno della rete di CSIRT e con l'approvazione degli Stati membri interessati, di riesaminare e valutare le minacce informatiche, le vulnerabilità sfruttabili note e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o incidente di cibersicurezza su vasta scala. Al termine del riesame e della valutazione di un incidente e al fine di trarre gli opportuni insegnamenti per evitare o attenuare futuri incidenti, l'ENISA presenta una relazione di riesame dell'incidente a EU-CyCLONe, alla rete di CSIRT, agli Stati membri interessati e alla Commissione per sostenerli nello svolgimento dei loro compiti.

2.1.6. Il futuro della cybersecurity in UE tra Digital Networks Act e Rapporto Draghi

Partendo dalla constatazione della centralità rivestita dalle reti di tlc per il processo di transizione digitale e per la competitività dell'UE, nel tentativo di comprendere le dinamiche di mercato e gli sviluppi tecnologici in atto, il 21 febbraio scorso è stato pubblicato dalla Commissione europea il Digital connectivity package, comprensivo del **White Paper "*How to master Europe's digital infrastructure needs?*"** e della **Raccomandazione per la sicurezza e resilienza delle infrastrutture via cavo sottomarine**.

Il libro bianco, in particolare, oggetto di una consultazione pubblica conclusasi lo scorso 30 giugno, si presenta come un documento ampio che affronta tematiche strategiche connesse alla convergenza tecnologica tra telecomunicazioni e cloud, al ruolo critico delle infrastrutture digitali nonché alle sfide presenti e future anche relative alla cybersecurity.

Il tema della connettività rappresenta l'assoluto protagonista del libro bianco che, partendo dalla constatazione della correlazione tra deployment di infrastrutture di TLC fisse e mobili e sviluppo economico e della conseguente irrinunciabilità, per la competitività dell'UE nel contesto globale, della disponibilità di reti e tecnologie digitali performanti, descrive i trend generali evidenziando con particolare enfasi l'attuale incapacità delle infrastrutture di connettività europee di fronteggiare le sfide presenti e future poste da una società ed un'economia fondata sui dati sia lato offerta che lato domanda. Nello specifico, partendo dalle evidenze del rapporto sullo stato del Digital Decade del 2023, il documento constata una situazione di arretratezza sia rispetto alla copertura in fibra (soprattutto nelle aree rurali), sia con riguardo allo sviluppo di reti 5G standalone, soprattutto rispetto a USA, Cina e Corea del Sud. Oltre all'arretratezza dello sviluppo infrastrutturale, il documento in esame evidenzia anche come una lenta transizione degli operatori dell'UE verso soluzioni cloud per i servizi di comunicazione elettronica presenterebbe il rischio di ulteriori dipendenze nel settore dei servizi digitali e sottolinea l'importanza della rete satellitare ed il contributo che la stessa può offrire in particolare nelle aree remote e rurali dove non è disponibile connetti-

vità VHCN nonché per la gestione delle crisi. In questo scenario generale, **il macro obiettivo perseguito consiste nell'assicurare ampia disponibilità, anche nelle aree rurali, di infrastrutture di connettività di elevata qualità, affidabili e sicure attraverso la definizione di un quadro regolamentare che incentivi la transizione dalle reti in rame tradizionali alle reti in fibra ottica, lo sviluppo di reti 5G ed altre reti wireless nonché di infrastrutture basate sul cloud**.

Oltre all'avanzamento della copertura, **specifica attenzione è rivolta alle evoluzioni tecnologiche e a nuovi modelli di business** abilitati da App Economy, IoT, Data Analytics, AI o innovative forme di distribuzione dei contenuti come lo streaming video di alta qualità che richiedono, evidentemente, un aumento esponenziale delle prestazioni di elaborazione, archiviazione e trasmissione dei dati. La capacità di elaborare e trasportare grandi quantità di dati su internet ha spinto all'archiviazione e all'elaborazione remota dei dati nel cloud, tra il cloud e l'utente finale attraverso le Content Delivery Network (CDN) e vicino all'utente finale con l'edge computing favorendo, nella ricostruzione della Commissione, la virtualizzazione delle funzioni di rete nel software e la possibilità di spostare queste funzioni nel cloud o nell'edge computing.

Partendo dalle evidenze emerse nell'ambito della consultazione pubblica svoltasi nel 2023, ampia attenzione è dedicata all'attuale **situazione finanziaria del settore** e all'impatto che essa esercita sulla capacità dell'UE di mettere in campo gli investimenti necessari per la trasformazione della connettività indispensabile per beneficiare delle evoluzioni tecnologiche. Nello specifico, viene descritta la contrazione dei ricavi del settore ormai in atto da diversi anni, la cui gravità è accresciuta dal confronto con altre aree geografiche, alla quale si accompagna una crescita dell'indebitamento in un contesto generale che vede l'accesso ai finanziamenti più difficile e costoso e gli investimenti privati piuttosto limitati anche in considerazione della ridotta marginalità attesa.

Viene descritta la contrazione dei ricavi del settore ormai in atto da diversi anni, la cui gravità è accresciuta dal confronto con altre aree geografiche, alla quale si accompagna una crescita dell'indebitamento in un contesto generale che vede l'accesso ai finanziamenti più difficile e costoso e gli investimenti privati piuttosto limitati anche in considerazione della ridotta marginalità attesa.

La profittabilità dell'investimento dipende, infatti, dal take-up delle reti a sua volta condizionato dallo sviluppo e dal take-up di applicazioni e use cases data intensive. All'arretratezza europea in termini di copertura si aggiungono ostacoli connessi all'assenza di un mercato unico per reti e servizi di comunicazione elettronica. Ed infatti, viene descritta la sussistenza di 27 mercati nazionali con diverse dinamiche di offerta e domanda, differenti livelli di copertura di reti VHCN, diverse procedure e tempistiche di assegnazione dei diritti d'uso dello spettro e in generale diversi approcci regolamentari che pongono obblighi diversi (anche in materia di sicurezza ad esempio) che riducono le economie di scala aggravando ulteriormente la tendenza alla contrazione dei ricavi. Dal punto di vista degli assetti dei vari mercati nazionali, il documento enfatizza la presenza di oltre 100 operatori di rete fissa e 50 mobili di cui soltanto un numero esiguo presente in diversi mercati nazionali. Nel segmento mobile, in particolare, 16 MS hanno 3 operatori, 9 ne hanno 4 e 2 ne hanno 5. Sussistono, inoltre, grandi differenze nei prezzi (sia nel fisso che nel mobile) praticati sia tra gli Stati membri che rispetto agli USA.

Rispetto alla **gestione dello spettro**, in particolare, sebbene l'UE abbia tracciato le condizioni tecniche di utilizzo dello spettro e gli Stati membri si siano invece concentrati sul rilascio delle autorizzazioni e la gestione delle stesse e disallineamenti nell'impiego di tecnologie wireless e nuovi servizi, così come dinamiche interferenziali, possano avere ripercussioni a livello europeo (ostacolando anche lo sviluppo del 5G) sollecitando una gestione più coordinata dello

spettro per massimizzarne il valore economico e sociale. L'auspicio verso una maggiore armonizzazione della gestione dello spettro poggia anche nelle prospettive di sviluppo delle reti satellitari che, evidentemente, riducono, se non azzerano, il legame col territorio, imponendo una riflessione del tutto nuova. Con riferimento al quadro regolamentare vigente, il paper sottolinea l'importanza del cloud come driver di innovazione e volano per la virtualizzazione delle reti oltre che per un ripensamento del set di regole vigenti in una logica di armonizzazione degli obblighi e di riduzione degli ostacoli. L'evoluzione tecnologica e i cangianti modelli di business stanno favorendo una graduale convergenza ed il superamento della tradizionale distinzione tra operatori e fornitori di servizi ivi compresi i cloud providers che attualmente non sono destinatari di alcuna regolamentazione (nel CCE mentre diverso è il caso della NIS2) pur gestendo il backbone delle reti così come i cavi sottomarini attraverso cui transita più del 60% del traffico internazionale. Nonostante l'ecosistema stia andando nella direzione della convergenza, **il paper segnala la persistenza di un quadro regolamentare ancora fortemente diversificato e la necessità di supportare lo sviluppo dei servizi della società dell'informazione anche attraverso una semplificazione fondata, tra l'altro, sull'affermazione del principio del paese d'origine** per cui i singoli fornitori dovrebbero essere esonerati dal dover essere compliant con le singole discipline dei singoli Stati Membri nonché sulla previsione di regole uniformi che considerino la convergenza tra i tradizionali fornitori di reti e servizi da un lato e di servizi cloud dall'altro. In questo scenario, gli operatori vedrebbero ridurre gli oneri e i costi della compliance, accedere ad importanti economie di scala ed accrescere così la propria solidità finanziaria attraendo conseguentemente gli investimenti privati. Dal punto di vista della legislazione applicabile e dell'individuazione dell'Autorità competente a regolare l'accesso alle reti e ai servizi offerti ai clienti finali, il paper suggerisce l'individuazione secondo la logica della vicinanza all'utente finale. Ad ostacolare la creazione di un mercato unico, nell'analisi svolta dalla Commissione, sono anche le differenti obbligazioni concernenti la sicurezza e la reportistica degli incidenti. Il documento, a tale riguardo, ribadisce da un lato la sovranità dei singoli stati membri sui temi legati alla cybersecurity ma suggerisce, al contempo, l'opportunità di garantire una maggior cooperazione tra Stati al fine di individuare un set di condizioni ed adempimenti uniforme.

Sul tema sicurezza, il white paper dedica inoltre specifica attenzione al tema dei fornitori (par. 2.4.1. "*Challenge of trusted suppliers"*) sollecitando, in un contesto geopolitico sempre più caratterizzato da tensioni e conflitti, la necessità di affidarsi a fornitori diversificati e fidati, per evitare vulnerabilità e dipendenze, con potenziali effetti a catena sull'intero ecosistema industriale. Non manca nel white paper un richiamo espresso al 5G Toolbox ed alle misure raccomandate per mitigare i rischi per le reti 5G, in particolare la valutazione del profilo di rischio dei fornitori e l'applicazione di restrizioni per i fornitori considerati ad alto rischio, comprese le necessarie esclusioni da asset chiave.

Secondo la visione della Commissione, le lacune lasciate dai venditori ad alto rischio nella catena di fornitura richiedono lo sviluppo di nuove capacità fornite da attori esistenti o nuovi e dunque importanti azioni in termini di ricerca e innovazione (R&I) nelle tecnologie chiave rilevanti per le reti di comunicazione sicure.

Partendo da tali considerazioni e ad integrazione delle stesse, **il paper individua tre pilastri di azione comprensivi di diversi scenari e, nello specifico: 1) creazione di un "Hub di connettività NextGen: Network 3C",** ossia un ecosistema aperto a semiconduttori, capacità di calcolo in tutti i tipi di ambienti edge e cloud, tecnologie radio, infrastrutture di connettività, gestione dei dati e applicazioni attraverso il quale, mediante una serie di progetti pilota su larga scala tesi a realiz-

zare infrastrutture e piattaforme integrate end-to-end si punta a favorire lo sviluppo di capacità attraverso l'innovazione aperta e le competenze tecnologiche; **2) completamento del Mercato Unico Digitale**, attraverso il miglioramento delle norme già introdotte con il Codice europeo delle comunicazioni elettroniche e, nello specifico, un ripensamento dell'attuale quadro normativo al fine di garantire condizioni di parità a livello normativo e diritti e obblighi equivalenti per tutti gli attori e gli utenti finali delle reti digitali. Tra gli scenari delineati dalla Commissione, il 5 in particolare, mira a ridurre gli oneri per le aziende, ad individuare misure per accelerare lo switch-off del rame (anche considerando, nello scenario 7, la possibilità di facilitare "l'ecologizzazione" delle reti digitali, promuovendo lo spegnimento tempestivo delle reti in rame e il passaggio a un ambiente completamente in fibra ottica) e rivedere le politiche di accesso alla rete in fibra attraverso la definizione di un prodotto europeo di accesso all'ingrosso, mentre il sesto, si concentra sull'opportunità di garantire una governance più armonizzata dello spettro e valutare soluzioni per condizioni di autorizzazione e selezione più allineate, o addirittura processi di selezione o autorizzazione unici, per le comunicazioni terrestri e satellitari e altre applicazioni innovative. Per quanto attiene, nello specifico, il tema del copper switch-off, il white paper sottolinea come la migrazione dalle reti in rame tradizionali alle nuove reti in fibra sia un processo chiave per facilitare la transizione verso il nuovo ecosistema di connettività e contribuisca agli obiettivi green dell'UE promuovendo, al contempo, l'adozione dei nuovi servizi e contribuendo così ad aumentare il rendimento degli investimenti in fibra e a sostenere il raggiungimento dell'obiettivo del Decennio Digitale. Lo stesso documento evidenzia altresì la necessità di mettere in campo attività di pianificazione e monitoraggio che siano in grado di tutelare le dinamiche concorrenziali e le esigenze degli utenti finali, in particolare dei gruppi vulnerabili e degli utenti finali con disabilità. In tale logica il libro bianco evidenzia come la definizione di una data per il raggiungimento dello switch-off del rame potrebbe garantire la certezza della pianificazione in tutta l'Unione e l'opportunità per gli utenti finali di beneficiare di connessioni in fibra in tempistiche analoghe. Entrando nel merito delle possibili tempistiche, il white paper ritiene appropriato raggiungere lo switch-off del rame per l'80% degli abbonati nell'UE entro il 2028 e per il restante 20% entro il 2030. Una tabella di marcia così chiara per lo switch-off del rame sosterrebbe, secondo la Commissione, gli obiettivi di connettività del 2030 e invierebbe un segnale forte agli investitori; **3) creazione di infrastrutture digitali sicure e resilienti per l'Europa.**

Soffermando l'attenzione sul tema della sicurezza, il white paper evidenzia la necessità, per garantire la crescita economica ed i benefici per la società connessi alla realizzazione di infrastrutture all'avanguardia, di prestare un'adeguata attenzione alla sicurezza fisica, in particolare in relazione all'infrastruttura dorsale ed alla trasmissione dei dati da un capo all'altro della rete. In particolare, in questa terza sezione, il documento individua 5 scenari che propongono una serie di iniziative tra cui il potenziamento delle attività di R&I a sostegno delle nuove tecnologie in fibra e via cavo, una revisione di strumenti quali sovvenzioni, appalti, operazioni di miscelazione nell'ambito di InvestEU e strutture di miscelazione delle sovvenzioni, l'architettura di un sistema di governance comune dell'UE per le infrastrutture di cavi sottomarini, l'armonizzazione dei requisiti di sicurezza nelle sedi internazionali, che possono essere riconosciuti attraverso un sistema di certificazione UE specifico.

Specifica attenzione è dedicata ai progressi dell'informatica quantistica ed alla necessità di iniziare a **sviluppare strategie di transizione verso un'infrastruttura digitale sicura dal punto di vista quantistico** e, dunque, sicura contro gli attacchi messi in campo da computer quantistici. In questa logica, il white paper individua nella crittografia post-quantistica (PQC) uno strumento promettente per rendere le comunicazioni ed i dati resistenti

agli attacchi quantistici. Per affrontare queste sfide viene proposto uno sforzo coordinato a livello di UE, che coinvolga principalmente le agenzie governative e che consenta di sincronizzare gli sforzi per garantire l'allineamento delle tabelle di marcia a livello dell'Unione, con tempistiche concrete per il raggiungimento degli obiettivi, standard comuni che assicurino interoperabilità.
Nella medesima sede viene anche enfatizzata l'importanza di assicurare la sicurezza delle infrastrutture di cavi sottomarini, cruciali per la sovranità dell'UE.
Sul punto, in particolare, il white paper sottolinea l'importanza di potenziare le attività di ricerca e di rafforzare gli investimenti nella realizzazione di nuove infrastrutture strategiche di cavi sottomarini ed al rafforzamento della sicurezza e della resilienza di quelle esistenti. A questo proposito, viene proposta l'istituzione di un elenco di Strategic Cable Projects of European Interest (CPEI) e di un relativo sistema di etichettatura dei progetti strategici di cavi di interesse europeo che affronterebbero i rischi, le vulnerabilità e le dipendenze identificate, da concepire secondo gli standard tecnologici più avanzati.
Nel declinare azioni concrete, **lo stesso documento suggerisce l'istituzione di un sistema di governance comune dell'UE per le infrastrutture di cavi sottomarini**, che comprenda: 1) elementi aggiuntivi da considerare per mitigare e affrontare i rischi, le vulnerabilità e le dipendenze nell'ambito di una valutazione consolidata a livello di UE e priorità per aumentare la resilienza; 2) criteri rivisti per aggiornare i cavi esistenti o per finanziarne di nuovi; 3) un aggiornamento dell'elenco di priorità co-creato di CPEI, sia intra-UE che internazionali, basato sull'importanza strategica e sul rispetto dei criteri di cui sopra; 4) finanziamenti comuni per tali progetti, anche potenzialmente attraverso fondi azionari a cui l'Unione potrebbe partecipare insieme agli Stati membri per ridurre il rischio di investimenti privati; 5) ulteriori azioni per rendere sicure le catene di approvvigionamento ed evitare la dipendenza da fornitori di Paesi terzi ad alto rischio.

Se questi sono i principali temi affrontati e le proposte avanzate dalla Commissione, **il 6 dicembre scorso Il Consiglio UE ha reso pubbliche le proprie conclusioni sul White Paper**. Si tratta di un testo che enfatizza la centralità delle infrastrutture nel processo di digitalizzazione, l'importanza di accrescere gli investimenti (anche ricorrendo all'intervento pubblico nel rispetto della disciplina sugli aiuti di Stato) ed assicurare modelli di business sostenibili per gli operatori mobili in particolare, la necessità di assicurare ampia disponibilità delle infrastrutture per accompagnare la digitalizzazione di imprese, cittadini e pubbliche amministrazioni, l'opportunità di rafforzare attività di ricerca e di supportare modelli di business innovativi a beneficio di cittadini ed imprese europei. Specifica enfasi è riservata al servizio universale ed alla necessità di assicurare a tutti i cittadini un'adeguata qualità della connettività.
Rispetto al tema del completamento del mercato unico digitale, il Consiglio evidenzia la necessità di favorire lo switch-off del rame assicurando al contempo che esso non si traduca in negativi effetti sulla competizione nei singoli mercati rilevanti e rileva altresì l'opportunità di evidenziare come la posa della fibra non rappresenti l'unico strumento attraverso cui favorire l'allineamento del settore digitale ai target europei sul clima essendo altrettanto rilevante rendere più efficienti le tecniche di utilizzo delle reti digitali. Specifica attenzione è riservata al tema dello spettro, rispetto al quale viene affermata con forza la competenza nazionale sulla gestione ed assegnazione dei diritti d'uso delle frequenze, così come la necessità di agire sulle interferenze dei servizi globali di navigazione satellitare di cui vengono rilevati rischi significativi per la sicurezza e di agire congiuntamente nelle pertinenti sedi internazionali.
Se quelli appena descritti sono i contenuti principali del white paper ed il posizionamento del Consiglio UE sullo stesso, **la *Raccomandazione sulla sicurezza e la resilienza delle infrastrutture dei cavi sottomarini* individua una serie di azioni a livello nazionale ed europeo attraverso le quali si punta a rafforzare**

la sicurezza e la resilienza dei cavi sottomarini attraverso un migliore coordinamento in tutta l'UE, sia in termini di governance che di finanziamento.

In particolare, la raccomandazione punta ad individuare azioni tese a supportare l'installazione o l'ammodernamento significativo di infrastrutture di cavi sottomarini a condizione che coinvolgano almeno due Stati membri, colleghino uno Stato membro con una o più isole, regioni ultraperiferiche o paesi e territori d'oltremare e stabiliscano o migliorino in modo significativo la connettività tra uno o più Stati membri e paesi terzi, compresi i paesi in via di adesione e i paesi vicini, direttamente o indirettamente attraverso altre infrastrutture collegate all'UE. Entrando nel merito dei principali contenuti, la raccomandazione descrive azioni da mettere in capo a livello di Stati membri tese a promuovere la sicurezza e la resilienza dei cavi sottomarini attraverso il rafforzamento degli obblighi dei fornitori e degli operatori nell'attuazione della direttiva NIS 2, supportare le attività di stress test da parte degli operatori di cavi sottomarini e predisporre procedure nazionali di rilascio dei permessi che siano veloci (al riguardo si incoraggia, tra l'altro, il ricorso a procedure online, la nomina di autorità responsabili che agevolino e coordinino le procedure amministrative ed un rafforzamento delle attività di coordinamento tra le autorità nazionali). A livello UE, invece, gi Stati membri sono incoraggiati a: a) assistere la Commissione nella mappatura dei cavi sottomarini esistenti (da aggiornare almeno annualmente); b) valutare rischi, vulnerabilità e dipendenze, con specifica attenzione alla supply chain; c) definire un "Cable Security Toolbox" che definisca misure di mitigazione dei rischi in particolare con riguardo ai fornitori ad alto rischio; d) scambiare regolarmente informazioni su incidenti, *awareness* e pratiche applicate; e) formare esperti con un appropriato livello di esperienza; f) favorire l'impiego di soluzioni innovative per l'individuazione e la deterrenza delle minacce contro le infrastrutture di cavi sottomarini; g) redigere una lista di progetti strategici su cavi di interesse europeo (con relativa urgenza, timeline e criticità in termini di sicurezza) con aggiornamento almeno annuale sulla base dei rischi, delle vulnerabilità e delle dipendenze riscontrate in materia; h) cooperare nella promozione e nello sviluppo di cavi sottomarini; i) mettere in campo investimenti.

Se il White Paper sul Futuro dell'Infrastruttura digitale europea è un documento programmatico che ambisce fornire degli spunti di riflessione per la prossima Commissione sulle politiche da attuare per rafforzare il Mercato Unico europeo in ambito digitale, **lo scorso 9 settembre è stato presentato il rapporto "*The future of European competitiveness*", a firma di Mario Draghi su incarico dalla stessa Commissione europea**.

Si tratta, in questo caso, di un'analisi economica di ampio respiro sul livello di competitività dell'UE, che esamina le sfide affrontate dall'industria e dalle imprese nel mercato unico attraverso la disamina di numerosi settori che vanno dall'energia ai trasporti, dalle materie prime alla decarbonizzazione, fino alla space economy e alla difesa e che individua tre distinte aree di intervento per rilanciare la crescita sostenibile: la riduzione del divario di innovazione con gli Stati Uniti e la Cina, soprattutto nelle tecnologie avanzate, un piano congiunto per la decarbonizzazione e la competitività ed infine l'aumento della sicurezza e la riduzione delle dipendenze.

Rispetto alle tecnologie digitali innovative che stanno guidando e sempre più guideranno la crescita e la competitività delle singole regioni del globo, la staticità della struttura industriale europea ha indotto bassi investimenti e poca innovazione determinando un forte ritardo dell'UE: infatti, circa il 70% dei modelli di base di IA sono stati sviluppati negli Stati Uniti dal 2017 e tre "hyperscaler" statunitensi rappresentano da soli oltre il 65% del mercato cloud globale ed europeo. Il più grande operatore cloud europeo rappresenta solo il 2% del mercato UE mentre l'informatica

quantistica vede cinque delle prime dieci aziende tecnologiche a livello globale in termini di investimenti nel settore quantistico con sede negli Stati Uniti e quattro in Cina mentre nessuna si trova nell'UE. Nello specifico, la tecnologia digitale viene individuata dal rapporto come il fattore chiave dell'aumento del divario di produttività tra l'UE e gli Stati Uniti a partire dalla metà degli anni '90, momento in cui l'UE si è mostrata incapace di capitalizzare la prima rivoluzione digitale guidata da Internet, sia in termini di creazione di nuove imprese tecnologiche che di diffusione della tecnologia digitale nell'economia.

Rispetto al cloud, in particolare, il rapporto parte dalla constatazione di un forte svantaggio competitivo dell'UE che probabilmente si aggraverà in conseguenza del fatto che il mercato è caratterizzato da continui e massicci investimenti, economie di scala e servizi multipli offerti da un unico fornitore per giungere ad evidenziare la necessità, per l'Europa, di non rinunciare a sviluppare il proprio settore tecnologico interno e, per le aziende europee, di mantenere una posizione di rilievo nei settori in cui è richiesta la sovranità tecnologica, come la sicurezza e la crittografia (soluzioni di "sovereign cloud"). Partendo da tale constatazione, il rapporto lancia una serie di proposte, tra cui quella di prevedere un passaporto per i servizi cloud a livello UE nonché di incoraggiare la definizione di accordi contrattuali commerciali per la cessazione del traffico dati e la condivisione dei costi dell'infrastruttura (Interconnection).

Se è grave – e forse incolmabile – il divario nel cloud, rispetto all'IA e in particolare l'IA generativa, il documento ha evidenziato come si tratti di una tecnologia in evoluzione in cui le aziende dell'UE hanno ancora l'opportunità di ritagliarsi una posizione di leadership in segmenti selezionati e come, in particolare, l'Europa rivesta un ruolo di primaria importanza nella robotica autonoma, rappresentando la sede di circa il 22% delle attività mondiali e nei servizi di IA, con circa il 17% delle attività.

Molta attenzione è dedicata al tema della sicurezza. Con riferimento ai settori delle apparecchiature per le telecomunicazioni e dei software, in particolare, il rapporto sottolinea come essi siano fondamentali per la resilienza informatica dell'UE, la sicurezza delle infrastrutture strategiche e la protezione dei dati dei cittadini e delle imprese ed affronta in maniera trasparente il tema della concorrenza proveniente dall'oriente nonché le restrizioni messe in campo nei confronti di fornitori ad alto rischio da un numero certamente minoritario di SM per giungere a proporre il rafforzamento della sicurezza e dell'autonomia strategica aperta delle reti di comunicazione digitale dell'UE attraverso il sostegno ai fornitori di apparecchiature e software per le comunicazioni con sede nell'UE.

Rispetto alla capacità delle imprese digitali innovative di attrarre investimenti, il rapporto evidenzia forti carenze, sottolineando come non ci sia alcuna azienda europea con una capitalizzazione di mercato superiore a 100 miliardi di euro che sia stata creata da zero negli ultimi cinquant'anni, a differenza del contesto statunitense che vede sei società con una valutazione superiore a 1.000 miliardi di euro create in questo periodo.

Un ruolo particolarmente importante, nella ricostruzione delle ragioni all'origine del ritardo europeo nelle tecnologie digitali innovative, è ricoperto dalla cornice normativa esistente. Il rapporto Draghi evidenzia infatti in maniera molto chiara la sussistenza di un atteggiamento normativo dell'UE nei confronti delle aziende tecnologiche che, in generale, ostacola l'innovazione: prova evidente ne è la corposità degli atti normativi, che ammonta a circa 100, con oltre 270 autorità di regolamentazione attive nelle reti digitali in tutti gli Stati membri.

Si tratta di un ecosistema evidentemente molto complesso che, secondo il rapporto, introduce una serie di ostacoli normativi, limitazioni all'uso dei dati, procedure farraginose, costose e frammentate a livello di Stati membri che scoraggiano gli investimenti e certamente limitano la capacità di crescita e la competitività delle

aziende europee agevolando, di fatto, le imprese più grandi che possiedono la capacità finanziaria e l'incentivo a sostenere i costi di conformità anche se elevati.
Al fine di superare l'attuale percezione delle imprese che per oltre il 60% considerano la regolamentazione un ostacolo agli investimenti (per il 55% delle PMI in particolare gli ostacoli normativi e gli oneri amministrativi rappresentano la sfida più grande da affrontare), il rapporto offre una serie di indicazioni di carattere generale, oltre a formulare proposte di interventi specifici. In particolare, **si sollecita, per i settori prioritari, di valorizzare il principio della neutralità competitiva e dunque orientare la regolamentazione in una logica di facilitazione dell'ingresso nel mercato e di adattamento ai cambiamenti dell'economia ed alle tempistiche dettate dall'innovazione tecnologica**. A tal fine è molto interessante l'approccio proposto che sollecita una valutazione delle fusioni che consideri l'impatto della concentrazione sul futuro potenziale di innovazione nelle aree innovative essenziali.
Ispirato dal medesimo intento di valutare attentamente gli impatti delle regole sui mercati e sulle dinamiche competitive, **il documento evidenzia da un lato l'importanza di compiere una valutazione approfondita dell'impatto della regolamentazione digitale e di altro tipo sulle piccole imprese, con l'obiettivo di escludere le PMI dalle normative che solo le grandi imprese sono in grado di rispettare**; **dall'altro, sollecita la riduzione del ricorso alla regolamentazione ex ante a livello nazionale in favore di un'applicazione ex post per la concorrenza nei casi di abuso di posizione dominante**. In una logica di semplificazione si propone poi l'armonizzazione delle norme e dei processi di concessione delle licenze a livello europeo e l'individuazione di caratteristiche di progettazione delle aste a livello europeo per contribuire a creare dimensioni di scala.
Per agevolare gli operatori europei nel restare al passo con i nuovi sviluppi tecnologici, il rapporto raccomanda l'istituzione di un organismo europeo con la partecipazione di soggetti pubblici e privati per sviluppare standard tecnici omogenei per l'implementazione di API di rete ed edge computing.
Con l'obiettivo, poi, di ridurre la complessità, il rapporto suggerisce la nomina di un nuovo vicepresidente della Commissione per la semplificazione, con il compito di snellire l'acquis e di dedicare, all'inizio di ogni mandato della Commissione, un periodo fisso di almeno sei mesi alla valutazione sistematica e alle prove di stress dell'intera regolamentazione esistente per settore di attività economica e, successivamente, una seconda fase focalizzata sulla semplificazione e l'eliminazione di sovrapposizioni e incoerenze, con priorità ai settori economici in cui l'Europa è particolarmente esposta alla concorrenza internazionale ed avvalendosi di un'unica metodologia per le valutazioni d'impatto. In una logica di armonizzazione, il documento raccomanda inoltre di arricchire la disciplina sul recepimento delle direttive con un nuovo requisito standard che imponga agli Stati membri di valutare sistematicamente la nuova normativa, utilizzando la stessa metodologia delle istituzioni comunitarie.
Entrando ora nel merito della terza linea d'azione, ossia il rafforzamento della sicurezza e la riduzione delle dipendenze, il rapporto enfatizza la dipendenza dell'Europa dall'esterno e, dunque, la vulnerabilità potenziale del continente europeo, per un'ampia gamma di soluzioni che vanno dalle materie prime critiche alle tecnologie avanzate e, **con riguardo alle tecnologie digitali, raccomanda, con riferimento alle telecomunicazioni, il rafforzamento delle considerazioni sulla sicurezza nell'approvvigionamento tecnologico, favorendo il ricorso a fornitori di fiducia dell'UE per l'assegnazione dello spettro in tutte le future gare d'appalto e a promuovere i fornitori di apparecchiature di telecomunicazione con sede nell'Unione come strategici nelle trattative commerciali**.

2.2. L'ECOSISTEMA NORMATIVO NAZIONALE SULLA CYBERSECURITY

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

vello 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.

2.2.2. La direttiva NIS2 in Italia e il percorso di implementazione

Il quadro normativo nazionale in materia di cybersicurezza si è notevolmente ampliato negli ultimi anni, anche per impulso del legislatore eurounitario. Difatti, l'Italia rientra tra i primi Paesi dell'Unione ad essersi dotato di un **atto di recepimento della direttiva NIS2, ossia il d. lgs. 4 settembre 2024, n. 138, che è entrato in vigore il 16 ottobre scorso**. Rispetto al dettato normativo, dopo una serie corposa di definizioni (tra cui rileva l'approccio multirischio che permea l'intero framework[4]) viene delineato l'ambito di applicazione della disciplina NIS2 nel contesto nazionale, specificando – in via generale – che vi rientrano tutti quei soggetti pubblici e privati riconducibili ai settori e ai sottosettori indicati negli allegati, a condizione che superino i massimali per le piccole imprese. Tuttavia, sul punto sono previste alcune eccezioni, che sono puntualmente individuate all'art. 3 del decreto in questione[5].
Quanto alla **governance**, come anticipato, l'ACN viene confermata come Autorità nazionale competente e punto di contatto unico NIS. All'ampliarsi dell'ambito di applicazione soggettivo, rispetto alla disciplina NIS1 aumentano le Autorità di settore NIS (i Ministeri), tra cui figura anche la Presidenza del Consiglio dei ministri, competente per i settori gestione dei servizi TIC (in collaborazione con ACN), spazio, PA, società in house, partecipate e a controllo pubblico. Molto rilevante anche l'istituzione, in via permanente, del Tavolo per l'attuazione della disciplina NIS (art. 12), avente compiti quali la formulazione di proposte e pareri per l'adozione di iniziative, linee guida e atti di indirizzo e la previsione della possibilità di coinvolgere, nelle rispettive riunioni, rappresentanti del mondo dell'università, enti e istituti di ricerca, nonché operatori privati interessati. Assoluta centralità viene riconosciuta anche al Ministero della Difesa che, insieme ad ACN, è individuato quale Autorità nazionale di gestione delle crisi informatiche.
Venendo nello specifico agli **adempimenti richiesti**, dal 1° gennaio al 28 febbraio di ogni anno successivo

4 Art.2, dd): "cosiddetto approccio *all-hazards*, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati".

5 In tema, il portale predisposto dall'ACN contiene informazioni utili per guidare imprese e soggetti pubblici a comprendere se ricadono o meno nell'ambito di applicazione della disciplina NIS2 a livello nazionale: https://www.acn.gov.it/portale/nis/ambito-registrazione

alla data di entrata in vigore del decreto NIS2, i soggetti essenziali e importanti devono registrarsi (o aggiornare la propria registrazione) sulla piattaforma digitale resa disponibile dall'ACN[6], la quale costituisce anche lo strumento di contatto predefinito per le successive comunicazioni, a partire da quella sull'inclusione/permanenza o meno nell'elenco dei soggetti NIS2. In un secondo momento (15 aprile-31 maggio), tali soggetti devono fornire o aggiornare diverse informazioni, tra cui lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o altrimenti a loro disposizione.

Con riferimento alle prescrizioni in tema di **misure di sicurezza** (art. 24) e **segnalazione degli incidenti** (art. 25 ss.) non si segnalano particolari differenze rispetto al testo della direttiva NIS2, per cui sarà fondamentale attendere la normativa di dettaglio per valutare l'impatto sui soggetti NIS2, soprattutto con riguardo a quelli di piccole dimensioni e a quei settori non sottoposti ad altre regolamentazioni in ambito cybersecurity[7]. Sul punto, l'ACN, anche tramite raccomandazioni e linee guida vincolanti, si occuperà di stabilire termini, modalità, specifiche e tempi graduali di implementazione degli obblighi previsti da tale disciplina, differenziandoli, fra l'altro, per settore, sottosettore e tipologia di soggetto essenziale o importante (art. 31).

L'art. 27 consente all'ACN di imporre ai soggetti essenziali e ai soggetti importanti di utilizzare categorie di prodotti, servizi e processi ICT certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza di cui all'art. 49 CSA[8]. Qualora un simile sistema non sia ancora stato adottato per il caso di specie, l'ACN può rendere mandatorie categorie di prodotti, servizi e processi ICT che siano certificati nell'ambito di schemi di certificazione riconosciuti a livello nazionale o europeo. Si tratta di un'eventualità certamente condivisibile e che, complice uno scenario in termini di attacchi cibernetici non propriamente ottimale tanto a livello europeo che nazionale, va nella direzione di garantire una più robusta postura di cibersicurezza, oltre a essere un'opportunità per rafforzare la fiducia verso prodotti, servizi e processi ICT certificati, non sono nel territorio nazionale, ma anche in ambito UE.

Ampio spazio (art. 34 ss.) è dedicato alla descrizione delle **attività di vigilanza ed esecuzione, nonché di supporto e assistenza, in capo ad ACN**, i cui criteri, procedure e modalità di svolgimento sono demandati a un successivo DPCM. L'ultima parte del decreto si focalizza sulle disposizioni finali e transitorie, tra cui rilevano particolarmente quelle previste dall'art. 40, il quale contiene i termini e le modalità di adozione dei diversi decreti attuativi, nella forma di DPCM o determinazioni dell'ACN.

Inoltre, sono stabilite **apposite norme di coordinamento con la disciplina del Perimetro di Sicurezza Nazionale Cibernetica – PSNC**, tra cui l'equivalenza degli obblighi di gestione del rischio e di notifica di incidente previsti dalla legge perimetro (n. 133/2019), l'esclusione dall'ambito di applicazione dell'elenco di beni ICT e dell'obbligo di notifica per un incidente avente un impatto su tali beni che sia stato già notificato. Quest'ultima disciplina – che ha origine con il d. l. 105/2019, convertito con la legge n. 133/2019, a cui ha fatto seguito un importante e articolato percorso attuativo, giunto a completamento con il DPCM n. 92/2022 – mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti

6 La piattaforma sarà resa disponibile a partire dal 01/12/2024.

7 In tema, sarà certamente rilevante tenere conto anche degli adempimenti richiesti dal d. lgs. 4 settembre 2024, n. 134 di recepimento in Italia della Direttiva CER (2022/2557) che, a differenza della NIS2, si focalizza maggiormente su aspetti inerenti la protezione fisica delle infrastrutture critiche.

8 Con le opportune differenze, la possibilità di rendere mandatori simili schemi di certificazione si rinviene in altre normative a livello UE (es: art. 8 CRA) e nazionale (art. 6, d. lgs. 3 agosto 2022, n. 123).

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 di più, i soggetti pubblici e privati che in ambito nazionale saranno obbligati al rispetto della NIS2 (e, in alcuni casi, sottoposti anche al PSNC) devono garantire la compliance con gli adempimenti previsti dalla **legge 28 giugno 2024, n. 90 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"** (nota come "legge sulla cybersicurezza"), la quale è entrata in vigore lo scorso 17 luglio e di cui si dirà più approfonditamente in seguito[9]. Tra le principali novità, si introduce l'obbligo di provvedere tempestivamente (senza ritardo e, in ogni caso, entro 15 giorni dalla ricezione dell'apposita comunicazione) all'adozione di interventi risolutivi indicati dall'ACN in merito a specifiche vulnerabilità a cui tali soggetti vengano ritenuti potenzialmente esposti. La misura è richiesta agli enti della PA che ricadono direttamente nell'ambito di applicazione della legge sulla cybersicurezza, come pure a quei soggetti privati che sono tenuti a osservare altre normative in materia di cybersicurezza (NIS1 e NIS2, PSNC, decreto telco). Ad ogni modo, nel caso in cui l'operatore manchi o ritardi l'attuazione di tali interventi, si vedrà comunicare all'Agenzia un avviso circa il fatto che la reiterazione di una simile omissione nell'arco di 5 anni comporterà l'irrogazione di una sanzione tra i 25-125 mila euro, a meno che non espliciti i motivi di natura tecnico-organizzativa che impediscano di adempiere entro il suddetto termine.
Ebbene, se questo è il quadro normativo, **ACN, autorità competente NIS, sta puntualmente seguendo le fasi attuative della disciplina NIS**. In particolare, dal 1° dicembre 2024 al 28 febbraio 2025, le medie e grandi imprese, in alcuni casi anche le piccole e microimprese, e le Pubbliche amministrazioni a cui si applica, sono tenute alla registrazione sul portale servizi ACN.
La prima fase attuativa si svolgerà tra febbraio ed aprile 2025, periodo che vedrà avviare tutti i tavoli settoriali, il censimento e la registrazione dei soggetti, l'adozione dell'elenco dei soggetti NIS, la notifica ai soggetti NIS e l'elaborazione ed adozione obblighi di base.
La seconda fase attuativa, invece, si svolgerà tra la metà di aprile 2025 e la metà di aprile 2026. A gennaio 2026, in particolare, scatterà l'obbligo di notifica di base, mentre entro aprile si procederà all'elaborazione ed adozione del modello di categorizzazione delle attività e dei servizi oltre all'elaborazione e adozione degli obblighi a lungo termine. Entro settembre 2026, invece, sarà realizzata la completa implementazione delle misure di sicurezza di base.
Dalla metà di aprile 2026, infine, prenderà il via la terza fase attuativa che vedrà la categorizzazione delle attività e dei servizi e l'implementazione degli obblighi a lungo termine.

2.2.3. *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 (di seguito: "legge perimetro"), 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 inte-

9 Si v. infra, par. 2.2.4.

ressi 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 sono sostanziate nell'adozione dei seguenti decreti:

1. **DPCM 30 luglio 2020, n. 131**: ha definito le modalità e i criteri procedurali di individuazione dei soggetti (pubblici e privati) inclusi nel PSNC e che, pertanto, sono tenuti al rispetto delle misure e degli obblighi previsti dalla legge perimetro 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;
2. **DPR 5 febbraio 2021 n. 54**: ha definito le procedure, le modalità e i termini da seguire ai fini delle valutazioni da parte del CVCN e dei CV del Ministero dell'interno e del Ministero della difesa, ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati;
3. **DPCM 14 aprile 2021, n. 81**: 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 Italia, 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 PSNC, 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[10];
4. **DPCM 15 giugno 2021**: ha individuato le categorie di beni, sistemi e servizi ICT destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica[11], disponendo altresì l'aggiornamento almeno annuale delle categorie individuate;
5. **DPCM 18 maggio 2022, n. 92**: 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.

Quest'ultimo decreto ha 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

10 Rispetto alle misure di sicurezza, il DPCM n. 81/2021 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, allegato B ; b) entro trenta mesi dalla stessa data, con riferimento all'adozione delle misure previste dalla categoria B, appendice 2, allegato B. 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.

11 Le misure di sicurezza rientrano nelle seguenti categorie: 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.

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.

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.

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, procedurale e tecnica 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.

Pertanto, dal complesso puzzle normativo sul Perimetro di Sicurezza Nazionale Cibernetica emerge quanto segue: i soggetti pubblici e privati che offrono servizi essenziali o svolgono funzioni essenziali e che sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici[12] 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 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, 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'e-**

12 Interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro.

secuzione dei test (art. 6); iii) esecuzione dei test di hardware e software (art. 7).

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 complessità". 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 previste all'art. 6 del DPR n. 54/2021.

Inoltre, i soggetti pubblici e privati inclusi nel PSNC perimetro sono tenuti a adeguare i propri processi interni per garantire la compliance con le altre normative che a livello nazionale si occupano della materia della cybersicurezza, tra cui la NIS2 come visto nel paragrafo precedente.

Le due normative condividono, fra l'altro, un **approccio attento nei confronti della supply chain**. Più nel dettaglio, il decreto legislativo di recepimento della

NIS2 prevede specificamente che il soggetto essenziale o importante, nel valutare l'adeguatezza delle misure di sicurezza da adottare, tenga conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica di tali fornitori, anche con riguardo alle loro pratiche di sviluppo sicuro. Allo stato attuale, **non vi sono altre indicazioni sul piano legislativo rispetto alle modalità con cui tale obbligo vada declinato nella fase di implementazione della disciplina**. Tuttavia, in virtù di una logica sistemica, **è auspicabile che si faccia tesoro dell'esperienza applicativa di questi anni con riguardo al PSNC e ciò anche al fine di evitare sovrapposizioni di adempimenti, in particolar modo per quegli operatori che saranno obbligati al rispetto di entrambe le discipline**. Più nel dettaglio, nella realtà applicativa del PSNC la valutazione dei fornitori – che si concretizza prima di procedere all'inserimento di un "bene ICT" nell'apposito elenco – si tende a effettuare con l'ausilio di appositi questionari somministrati ai singoli fornitori. Ebbene, al fine di coordinare e armonizzare in maniera efficace gli adempimenti in merito ai controlli sulla supply chain, **si potrebbe immaginare di individuare, a cura di ACN, un unico questionario applicabile per una o più famiglie di prodotti, che sia altresì facilmente riutilizzabile. Tale integrazione potrebbe essere resa applicativa con uno dei prossimi decreti attuativi previsti dal decreto legislativo di recepimento della NIS2**.

In secondo luogo, appare necessario fare riferimento agli adempimenti previsti dalla **legge 28 giugno 2024, n. 90 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"** (di seguito, "legge sulla cybersicurezza")[13]. Per i soli soggetti ricompresi nel PSNC, l'art. 3 della legge sulla cybersicurezza opera una serie di modifiche sulle tempistiche degli obblighi di notifica degli incidenti che abbiano un impatto su reti, sistemi informativi e servizi informatici diversi da quelli inseriti nell'elenco di beni ICT[14], nonché sulle rispettive sanzioni in caso di inadempimento. In particolare, la tempistica originariamente prevista ("*entro 72 ore*"), viene sostituita come segue: a) prima segnalazione entro 24 ore dal momento in cui il soggetto sia venuto a conoscenza dell'incidente; b) segnalazione completa entro 72 ore che decorrono dal medesimo termine. Per di più, come accennato, il legislatore ha introdotto *ex novo* una sanzione pecuniaria da 25mila a 125 mila euro in caso di inosservanza di tale obbligo.

Altra novità peculiare introdotta dalla legge sulla cybersicurezza riguarda la disciplina in materia di contratti pubblici di beni e servizi informatici (art. 14), in quanto sono stati introdotti alcuni "*elementi essenziali di cybersicurezza*" che dovranno essere rispettati, fra l'altro, dagli enti della pubblica amministrazione e dai soggetti privati ricompresi nel PSNC. Tali elementi saranno dettagliati in un DPCM da adottarsi entro 120 giorni dalla data di entrata in vigore della presente legge (che, si ricorda, è il 17 luglio 2024). Per di più, lo stesso decreto – che non è stato ancora emanato – indicherà le ipotesi in cui debbano applicarsi determinati criteri di premialità per le proposte o le offerte che contemplino l'uso di tecnologie cyber italiane o UE, come pure di Paesi NATO o Paesi terzi che abbiano in essere accordi di collaborazione con l'UE o la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Quindi, pare potersi affermare che **il quadro sin qui delineato può assumere un ruolo di primaria importanza per l'efficienza e l'efficacia delle attività di *procurement* del soggetto incluso PSNC (con impatti non secondari nei confronti del fornitore interessato), il quale deve comunque osservare le regole europee e nazionali sugli appalti pubblici**, con particolari criticità che si palesano soprattutto

13 Si v. infra, par. 2.2.4.

14 *Art.1, co.3-bis, d. l. n. 105/2019, così come convertito con modificazione dalla legge n. 133/2019*

nell'ipotesi in cui, dopo l'esecuzione e il superamento dei test, venga richiesto allo stesso soggetto e/o al fornitore di implementare determinate prescrizioni di sicurezza prima di procedere all'affidamento (es: integrare funzionalità o cambiare parametri per rendere più cyber-sicuro quell'asset nello specifico ambiente operativo), che possono giungere a modificare sostanzialmente il "bene ICT" che si intende acquistare e, dunque, a generare forti criticità nell'ambito della singola procedura di selezione del fornitore.

È chiaro, infatti, che tutte le volte in cui si renda necessario, a seguito di singoli test, operare interventi correttivi di una certa importanza ad opera del soggetto selezionato, si palesa il rischio niente affatto astratto, che il secondo classificato nell'ambito della procedura di gara, attivi un contenzioso rilevando la diversità della natura del bene pre e post test. Ebbene, sul punto la legge tace, non fornendo alcuna linea guida per i soggetti acquirenti.

2.2.4. *La legge nazionale sulla cybersicurezza*

I soggetti pubblici e privati che in ambito nazionale saranno obbligati al rispetto della direttiva NIS2 e del relativo decreto di recepimento interno (e, in alcuni casi, sottoposti anche alla disciplina PSNC) dovranno adeguare i propri processi interni per garantire la compliance con nuovi e più stringenti adempimenti previsti dalla legge 28 giugno 2024, n. 90 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" (di seguito, "**legge sulla cybersicurezza**"), la quale è entra in vigore lo scorso 17 luglio. Pertanto, in tale sede si porrà il focus sulle principali prescrizioni rivolte a PA e imprese, tralasciando la seconda parte della legge in questione che introduce nuovi reati informatici[15].

Innanzitutto, **appare opportuno evidenziare che i soggetti pubblici che ricadono nell'ambito di applicazione della nuova legge sulla cybersicurezza sono sostanzialmente i medesimi di quelli ricomprese nel decreto NIS2**. In primo luogo (art.8), questi ultimi sono tenuti a dotarsi – qualora non sia già presente – di una **struttura per la cybersicurezza** nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, il che potrebbe costituire un punto di criticità verso il rafforzamento sostanziale della sicurezza cibernetica dell'ecosistema pubblico. Tuttavia, in un'ottica di semplificazione, la norma precisa che tale struttura possa essere individuata anche nell'ufficio del responsabile per la transizione digitale. In ogni caso, essa è tenuta quantomeno a: i) sviluppare politiche e procedure di sicurezza delle informazioni; ii) produrre e aggiornare un documento in cui si definiscono i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'ente; iii) pianificare e attuare interventi di potenziamento delle capacità per la gestione dei rischi cyber; iv) pianificare e attuare l'adozione delle misure previste dalle linee guida dell'ACN; v) monitorare e valutare in maniera continuativa le minacce alla sicurezza e alla vulnerabilità dei sistemi, al fine di procedere prontamente con gli aggiornamenti di sicurezza.

In secondo luogo (art.8), tali soggetti sono tenuti a istituire un **referente per la cybersicurezza** in possesso di specifiche professionalità e competenze in cybersicurezza, che però non sono esplicitamente e chiaramente definite. Egli funge essenzialmente da punto di contatto unico con l'ACN anche per le altre normative settoriali in materia. Pertanto, il suo nominativo va comunicato in via obbligatoria all'Agenzia. Anche in questo caso sono previste alcune semplificazioni, in quanto il referente può essere alternativamente individuato nel responsabile per la transizione

15 Appare opportuno segnalare sul punto l'introduzione del reato di estorsione informatica, in quanto si tratta di un ulteriore e fondamentale tassello per contrastare gli attacchi cibernetici di tipo ransomware che ormai dilagano a livello internazionale, europeo e, in particolar modo, nazionale.

digitale, così come nel dipendente di un'altra PA, previa autorizzazione da parte dell'ente di appartenenza e nell'ambito delle risorse disponibili a legislazione vigente senza determinare nuovi o maggiori oneri per la finanza pubblica.

In terzo luogo (art.1), viene sancito **l'obbligo di notifica per quegli incidenti richiamati nella Determina del DG di ACN del 3 gennaio 2023** – applicabile, inizialmente, solo per i soggetti nel PSNC – prevedendo una prima segnalazione entro un massimo di 24 ore dal momento in cui l'ente pubblico è venuto a conoscenza dell'incidente e una seconda, completa, entro le 72 dallo stesso termine. In tema, il legislatore ha operato una differenza in termini soggettivi, in quanto per le PA centrali, le Regioni e Province autonome di Trento e Bolzano, nonché le Città metropolitane, tali obblighi si applicheranno dalla data di entrata in vigore del provvedimento (17 luglio 2024), mentre per gli altri soggetti pubblici dal 180° giorno successivo. Ad ogni modo, in caso di violazioni, l'ACN comunicherà al soggetto che, se l'inadempimento si ripeterà nell'arco di 5 anni, si procederà all'applicazione di un sanzione tra i 25 mila e i 125 mila euro, che può determinare anche responsabilità disciplinare e amministrativo-contabile in capo ai funzionari e ai dirigenti responsabili.

Tutti gli obblighi sin qui menzionati ricalcano quanto già richiesto ai soggetti PSNC e, a breve, a quelli NIS2, mostrando il chiaro intento del legislatore di allineare e armonizzare il quadro normativo nazionale, evitando il più possibile incertezze interpretative e sovrapposizioni in termini di compliance.

In quarto luogo (art.2), tra i principali adempimenti richiesti agli enti della PA, come pure ai soggetti privati che ricadono nell'ambito di applicazioni di altre normative in materia di cybersicurezza (NIS1 e NIS2, PSNC, decreto telco), figura anche quello di **provvedere tempestivamente (senza ritardo e, in ogni caso, entro 15 giorni dalla ricezione dell'apposita comunicazione) all'adozione di interventi risolutivi indicati dall'ACN in merito a specifiche vulnerabilità a cui tali soggetti vengano ritenuti potenzialmente esposti**. Nel caso in cui l'operatore manchi o ritardi l'attuazione di tali interventi, si vedrà comunicare dall'Agenzia un avviso circa il fatto che la reiterazione di una simile omissione nell'arco di 5 anni comporterà l'irrogazione di una sanzione tra i 25-125 mila euro, a meno che non espliciti i motivi di natura tecnico-organizzativa che impediscano di adempiere entro il suddetto termine. **In questa, così come in altre disposizioni analizzate con riguardo al decreto NIS2, si coglie un approccio proteso *in primis* al supporto verso la PA e le imprese private**.

Quanto ai soggetti privati sopra richiamati, la legge sulla cybersicurezza non identifica nello specifico la struttura interna su cui ricade l'onere di adempiere agli interventi risolutivi dell'ACN, a differenza di quanto stabilito per la PA. In tema, se da un lato per i soggetti PSNC una simile responsabilità potrebbe ricadere sulla figura dell'incaricato per l'implementazione del perimetro e sulla relativa articolazione[16], dall'altro sorgono alcuni dubbi con riguardo ai soggetti NIS e, soprattutto, agli operatori tlc. Difatti, questi ultimi non hanno a disposizione un riferimento normativo specifico che si occupi di definire in maniera chiara e univoca la figura e/o la struttura che potrebbe farsi carico di un simile adempimento[17].

Altra novità peculiare introdotta dalla legge sulla cybersicurezza riguarda la disciplina in materia di contratti pubblici di beni e servizi informatici (art. 14), in quanto sono stati **introdotti alcuni "*elementi essenziali di cybersicurezza*" che dovranno essere rispettati, fra l'altro, dagli enti della pubblica amministrazione e dai soggetti privati ricompresi nel PSNC**, come accennato nel paragrafo precedente.

16 Allegato B, Misura ID.AM-6, DPCM 81/2021.

17 Nel caso dei soggetti NIS vengono in aiuto le "Linee guida per l'adozione delle misure di sicurezza da parte degli OSE e per la notifica degli incidenti" che, ad oggi, non sono disponibili pubblicamente.

In definitiva, il dettato normativo sin qui analizzato contiene prescrizioni certamente condivisibili, soprattutto per quanto riguarda il rafforzamento della cybersicurezza per i soggetti pubblici, anche perché per certi aspetti anticipa e completa il quadro che emerge dal decreto NIS2, il quale si rivolge, si ricorda, anche alla PA. Tuttavia, permangono alcune criticità in merito alla clausola di **invarianza finanziaria**, che potrebbe condurre a una sostanziale inattuazione del provvedimento nelle pubbliche amministrazioni. Non solo, **la previsione di un termine così ristretto per adottare gli interventi risolutivi dell'ACN (15 giorni)**, nel caso in cui quest'ultima segnali la sussistenza di specifiche vulnerabilità in capo al soggetto interessato, potrebbe mettere in seria difficoltà tutti gli operatori – pubblici e privati – ricompresi nell'ambito di applicazione della legge sulla cybersicurezza, qualora essi debbano risolvere vulnerabilità di tipo *0-day* o, in ogni caso, che richiedano un ingente sforzo sul codice da parte degli sviluppatori/fornitori.

2.2.5. *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. 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. 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.

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 PSNC, 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). 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.

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. 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. 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.
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, il DPCM n. 179/2020 ha distinto cinque macrocategorie di beni e rapporti rilevanti ai fini dell'esercizio del controllo sugli investimenti esteri diretti: a) le infrastrutture critiche; b) le tecnologie critiche; c) i fattori produttivi critici; d) le informazioni critiche; e) le attività economiche di rilevanza strategica.
Il DPCM n. 180/2020, invece, ha sostituito il precedente DPR n. 85/2014. In particolare, rispetto al settore delle comunicazione 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. Inoltre, una novità rilevante è stata introdotta con il **d. l. n. 104/2023** (c.d. Decreto Asset) 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 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, come si approfondirà meglio infra. Entrando nel merito delle innovazioni introdotte, certamente la più rilevante, per l'impatto deflattivo che ad essa si accompagna, è l'introduzione dell'istituto della prenotifica previsto dall'art. 7 del regolamento. All'impresa interessata alla definizione di acquisizioni, delibere, costituzioni, o altri atti o operazioni in progetto,

in particolare, è consentito trasmettere un'informativa alla Presidenza del Consiglio dei Ministri in merito a tale progetto, al fine di ricevere entro 30 giorni una pronuncia che dichiari, rispettivamente, l'applicabilità/inapplicabilità della normativa Golden Power con conseguente sussistenza/insussistenza dell'obbligo di notifica, oppure l'applicabilità della normativa Golden Power ma l'insussistenza dell'obbligo di notifica, in quanto manifestamente assenti gli estremi per l'esercizio dei poteri speciali (nel caso di applicabilità della disciplina è prevista la possibilità di adottare raccomandazioni). Dalla mancata adozione di alcuna decisione da parte del Gruppo di Coordinamento entro i 30 giorni previsti, discende per i soggetti prenotificanti l'obbligo di presentare una formale notifica. Molto importante anche l'intervento di semplificazione contenuto nell'art. 6 che consente al Gruppo di Coordinamento, su proposta dal Ministero responsabile dell'istruttoria e della proposta per l'esercizio dei poteri speciali, di adottare decisioni di non esercizio dei poteri speciali autonomamente, in caso di unanimità tra le amministrazioni rappresentate nello stesso Gruppo di Coordinamento e, dunque, senza la necessaria convocazione e delibera del Consiglio dei ministri.

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.

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.

2.2.5.1. Esercizio dei poteri speciali e andamento delle notifiche

I dati pubblicati nella relazione sull'attività del Governo svolta sulla base dei poteri speciali confermano la tendenza incrementale delle notifiche e prenotifiche ai sensi del decreto-legge 21/2012[18]. Infatti, nel 2023 il numero totale di informative presentate

18 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 2023, Camera dei Deputati, presentata dal Sottosegretario di Stato alla Presidenza del Consiglio dei ministri Mantovano e trasmessa alla Presidenza il 1 luglio 2024.

è pari a 727 (di cui 577 notifiche e 150 prenotifiche), in aumento di circa l'11,7% rispetto all'anno precedente, in cui se ne erano registrate 651 (608 notifiche e 43 prenotifiche). È opportuno evidenziare che **l'utilizzo a regime dello strumento della prenotifica ha prodotto una lieve flessione su base annua del numero di notifiche. Infatti, considerando esclusivamente queste ultime, il trend risulta essere in miglioramento per tutti i settori considerati**.

Per quanto riguarda il comparto **difesa e sicurezza nazionale** (art. 1, d. l. n. 21/2012), nel 2023 le notifiche pervenute sono 55, in diminuzione del 23% 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 2023, il loro numero è pari a 14, in discesa di quattro unità rispetto all'anno precedente e inferiore di quasi un terzo rispetto a quanto rilevato nel 2021, anno in cui è stato introdotto l'obbligo di notificare il piano annuale 5G (Fig.2.2).

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 (2023)

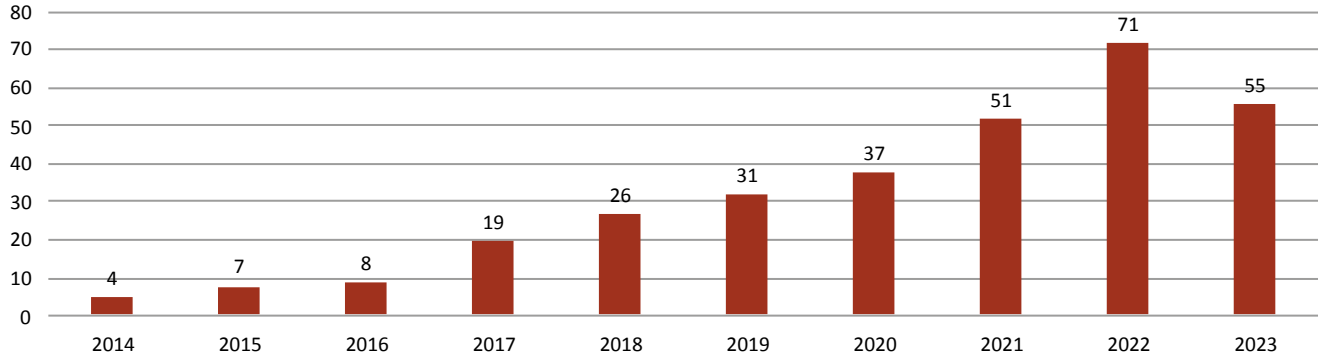
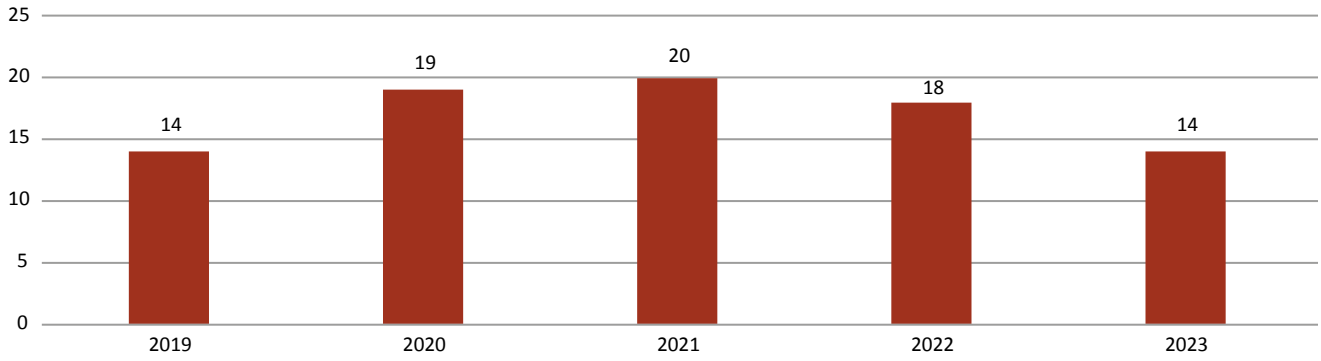


Fig. 2.2: Tecnologie 5G: il trend delle notifiche

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 (2023)



Infine, rispetto alle **altre macrocategorie ricomprese nell'art.2** (energia, trasporti, comunicazioni e settori indicati nel Reg. UE 2019/542), si evidenzia un decremento poco superiore al 2% rispetto al 2022 (Fig.2.3), rimanendo comunque il comparto in cui si concentra larga parte delle notifiche (88% per il 2023; +3% sull'anno precedente).

Nel 2023, 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 121 e 98 operazioni di istruttoria curate (Fig.2.4).

Fig. 2.3: Energia, Trasporti, Comunicazioni e altri 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 (2023)

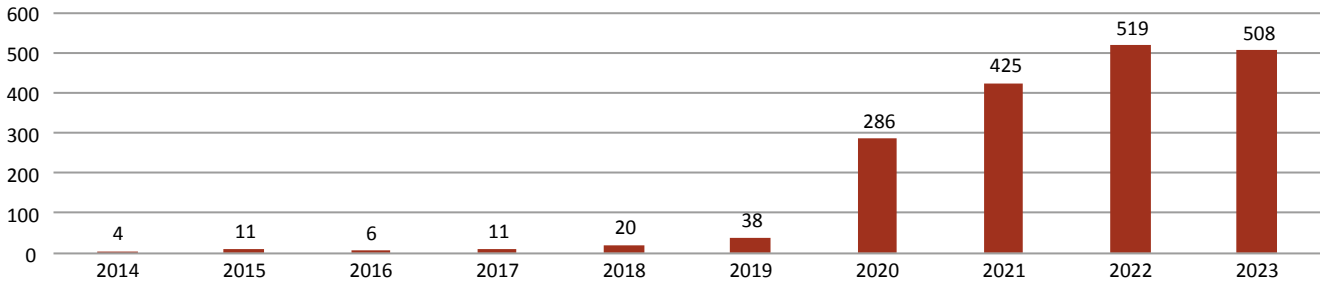
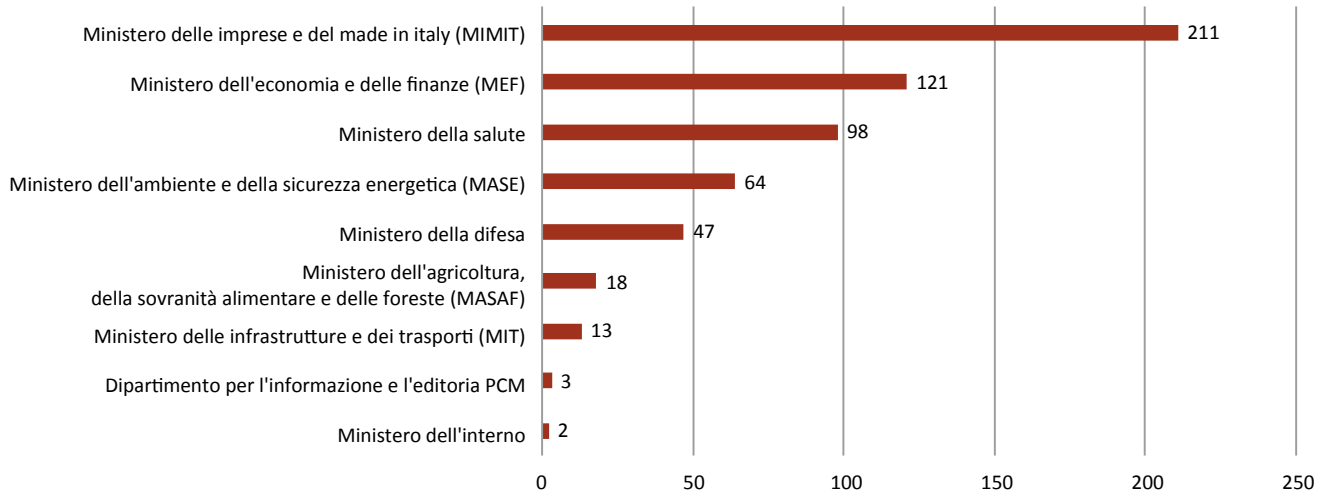


Fig. 2.4: La responsabilità istruttoria delle notifiche (2023)

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 (2023)



All'esito dell'istruttoria, delle 577 notifiche pervenute nel corso del 2023, per 30 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 (2023)

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 (2023)

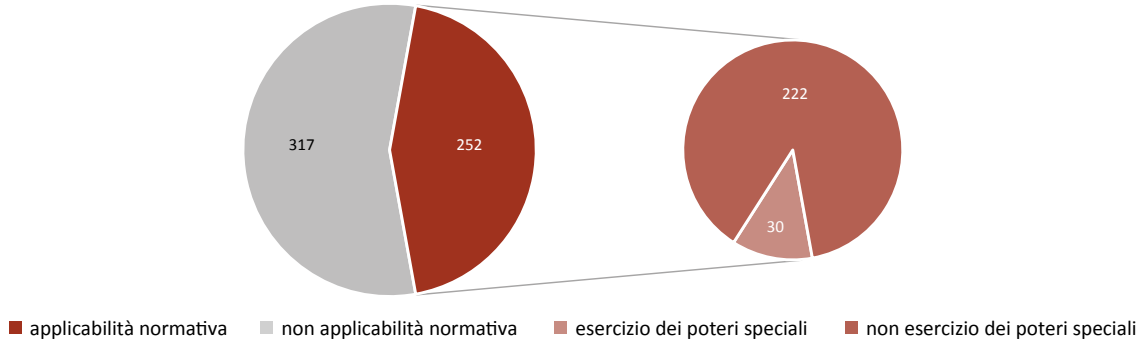
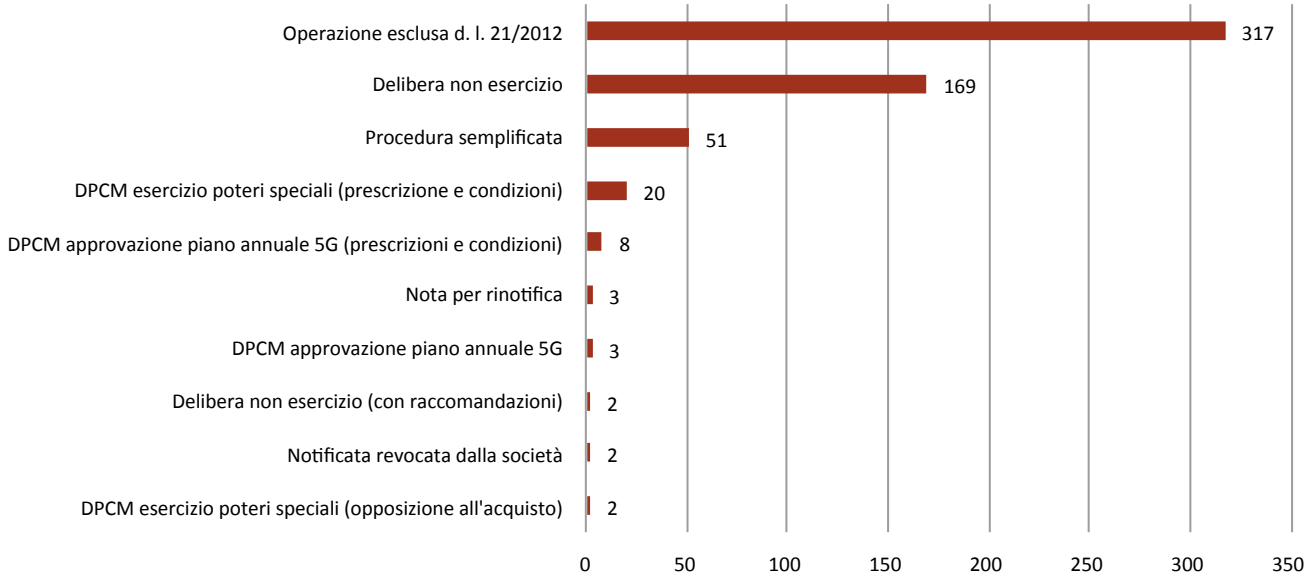


Fig. 2.6: Esito dettagliato della trattazione delle notifiche (2023)

Note: Il dato relativo ai DPCM di approvazione del piano annuale 5G con prescrizioni/condizioni include anche i DPCM relativi agli aggiornamenti dei piani

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 (2023)



- 20 notifiche sono state oggetto di esercizio dei poteri speciali mediante imposizione di specifiche condizioni e prescrizioni;
- In 8 casi si è proceduto ad approvare i piani annuali 5G, o relativi aggiornamenti, con prescrizioni/condizioni;
- Per 2 notifiche è stato esercitato il potere di opposizione all'acquisto di partecipazioni.

Al contrario, per 222 notifiche non sono stati esercitati i poteri speciali:

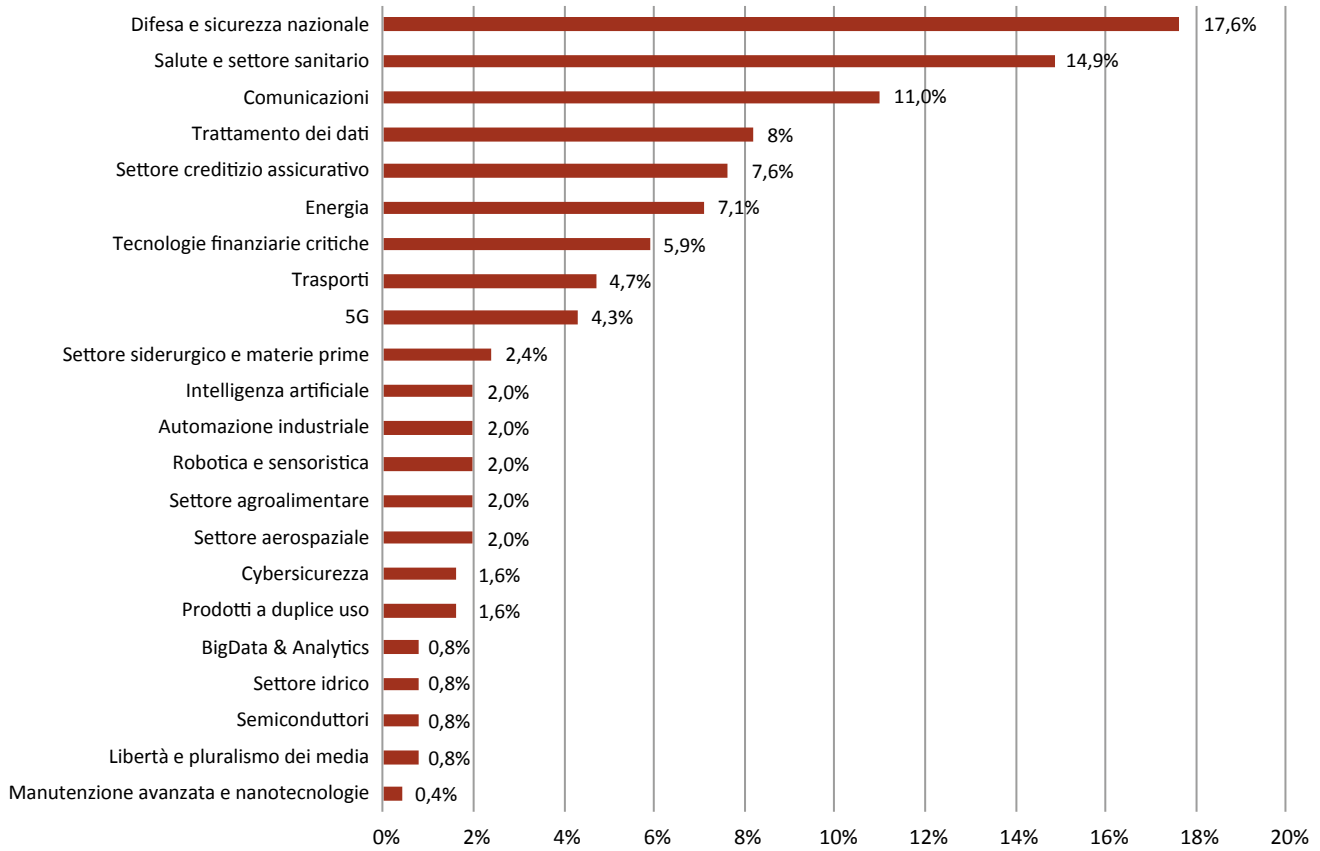
- Per 169 è stata adottata una delibera di non esercizio dei poteri speciali;
- Per 51 è stato disposto il non esercizio dei poteri speciali con procedura semplificata per le operazioni infragruppo;
- Per 2 notifiche, la delibera di non esercizio dei poteri speciali ha previsto delle raccomandazioni rivolte al soggetto notificante.

Inoltre, **317 notifiche sono state ritenute non rientranti nella disciplina Golden Power, pari al 54% del totale e in linea con quanto riscontrato nel 2022, evidenziandosi un utilizzo spesso cautelativo dello strumento della notifica**.

Considerando le sole operazioni rientranti nell'am-

Fig. 2.7: Notifiche per settore strategico (2023)

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 (2023)



bito di applicazione del Golden Power (Fig.2.7), spiccano quelle relative al comparto difesa e sicurezza nazionale per oltre il 17%, seguite dal settore salute e sanità (18,6%) e comunicazioni (14,9%) e comunicazioni (11%). **Quanto ai settori strategici correlati alle nuove tecnologie rilevanti ai sensi dell'art. 9, DPCM n. 179/2020 richiamato *supra*, le notifiche raggiungono il 9,6% del totale (contro un 13% del 2022)**, suddivise così come segue: intelligenza artificiale (2%), automazione industriale (2%), robotica e sensoristica (2%), cybersicurezza (1,6%), *Big Data* & *analytics* (0,8%), semiconduttori (0,8%), manutenzione avanzata e nanotecnologie (0,4%).

È opportuno sottolineare che l'istituto della prenotifica – divenuto operativo dal 24 settembre 2022 – nel 2023 ha fatto registrare ben 150 prenotifiche, quasi totalmente riconducibili ai settori di cui all'art. 2 (140), mentre le restanti 10 unità afferiscono al comparto difesa e sicurezza nazionale[19]. Nel 85% dei casi non è stata richiesta alcuna notifica formale dell'operazione, potendosi affermare che tale istituto stia assolvendo la ratio di semplificare l'intero procedimento.

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

icom 2005 25
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*

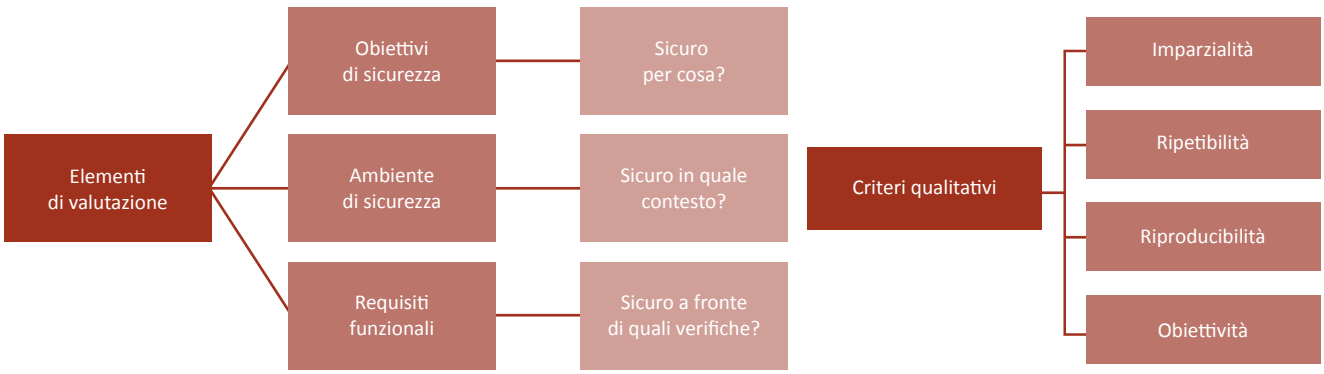
È ormai opinione diffusa, in particolare nel contesto europeo, che la spinta verso una sempre maggiore interoperabilità e standardizzazione rappresenti una delle principali chiavi anche per garantire ulteriore affidabilità e sicurezza all'ecosistema digitale e ai prodotti e servizi che in esso vengono 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 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

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

Fonte: elaborazioni I-Com su varie



sotto esame: il primo consiste negli obiettivi di sicurezza, che definiscono l'intenzione per cui si vuole 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[20], tra cui i requisiti di sicurezza (SFR) e di garanzia (SAR), che risultano determinanti per misurare quantitativamente il grado di sicurezza del TOE stesso[21]. 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**, i dati forniti da Jtsec[22], aggiornati al **2023**, ne hanno registrate **470** (Fig. 3.3). Si tratta di un valore particolarmente positivo rispetto agli ultimi cinque anni, che ha superato anche le più rosee aspettative, le quali prospettavano il raggiungimento di 413 certificazioni a livello globale.

20 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.

21 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.

22 Il report è disponibile al seguente link: https://www.jtsec.es/blog-entry/135/common-criteria-statistics-2023

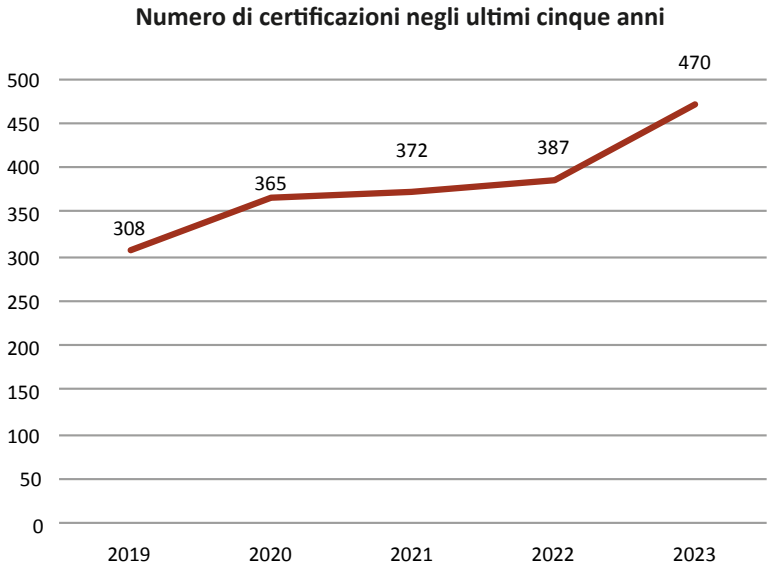
Fig. 3.2: I 7 livelli di sicurezza EAL

Fonte: elaborazioni I-Com su varie

- **EAL1** – **Testato Funzionalmente:** si applica quando è richiesta una certa sicurezza nel funzionamento corretto del TOE, ma le minacce alla sicurezza non sono considerate serie
- **EAL2** – **Testato Strutturalmente:** si applica quando sviluppatori o utenti richiedono un livello di sicurezza di livello da basso a moderato. Richiede la cooperazione dello sviluppatore per la consegna di informazioni e risultati di test
- **EAL3** – **Testato e controllato:** si applica quando gli sviluppatori o utenti richiedono un livello moderato di sicurezza e un'indagine approfondita del TOE senza una sostanziale riprogettazione
- **EAL4** – **Progettato, testato ed esaminato secondo metodologie:** la maggiore garanzia di qualità che si possa ottenere senza ricorrere a strumenti specialistici. Di norma il massimo livello di sicurezza del software raggiungibile sviluppando un prodotto software già esistente
- **EAL5** – **Progetto semiformale e testato:** pensato per garantire alti livelli di sicurezza. I prodotti EAL5 vengono in genere progettati e sviluppati fin dall'inizio con lo scopo di soddisfare questi requisiti specifici
- **EAL6** – **Progetto semiformale, verificato e testato:** usato per ottenere un'alta affidabilità in termini di sicurezza, sviluppata in un ambiente ingegneristico di sviluppo rigoroso. Si applica per settori ad alto rischio potenziale, dove il valore dei beni in gioco giustifica i maggiori costi
- **EAL7** – **Progetto formale, verificato e testato:** applicato raramente, e solo a sistemi con funzioni limitate a un ambito molto specifico e suscettibili di una estesa analisi formale

Fig. 3.3: Tendenze dei certificati *Common Criteria*

Fonte: Jtsec beyond IT security, "CC Statistics 2023", giugno 2024



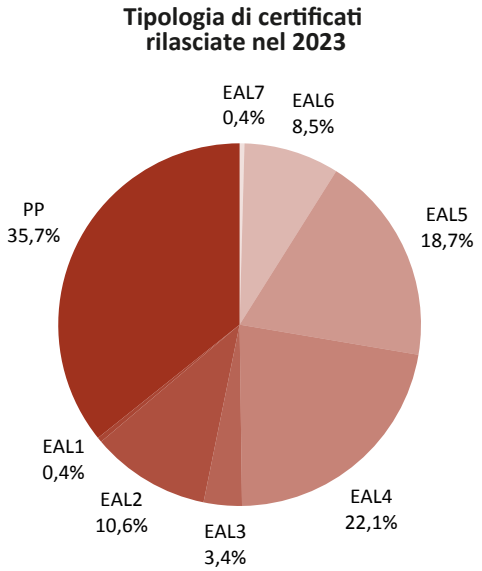
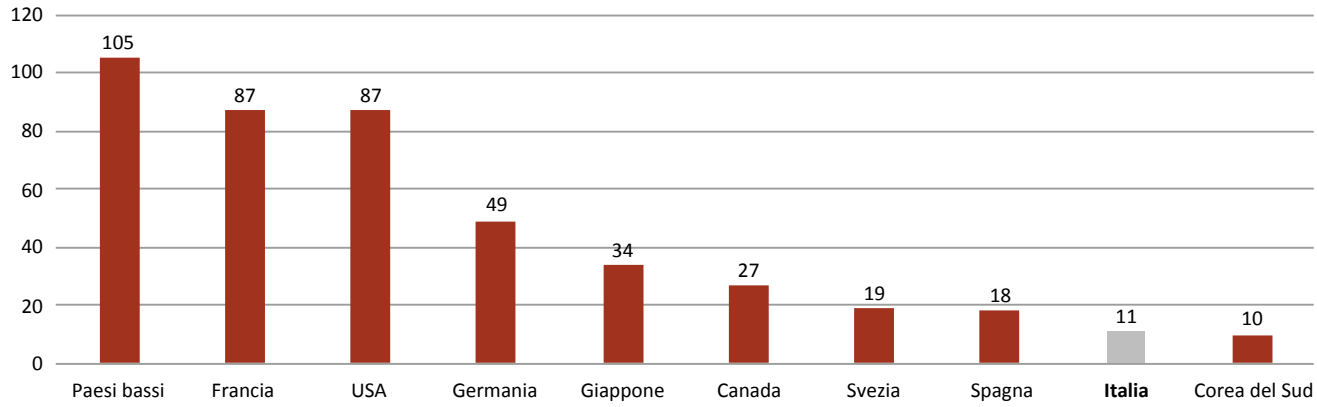


Fig. 3.4: Top 10 Paesi per certificazione prodotti con *Common Criteria* (2022)

Fonte: Jtsec beyond IT security, "CC Statistics 2023", giugno 2024



Per concludere, è opportuno fare riferimento ai dati Jtsec circa **i primi 10 Paesi nel mondo che hanno certificato prodotti con i *Common Criteria* nel 2023** (Fig. 3.4). Si può osservare come **l'Italia** rientri in questa classifica, mantenendo il **nono posto a livello globale** con 11 certificazioni (nel 2022 erano state 15). Inoltre, si può notare come nel **2023 la Francia e gli USA siano stati superati dai Paesi Bassi al primo posto, con uno scarto di ben 18 prodotti certificati**, e che la Corea del Sud abbia sorpassato Singapore (rispetto all'anno precedente), ritagliandosi un posto in questa classifica. In termini percentuali, **la top 3** (Paesi Bassi, Francia e USA) **rappresenta il 60% delle certificazioni totali**, mentre i successivi 3 paesi (Germania, Giappone e Canada) costituiscono il 23%. Inoltre, sempre a livello UE, anche la Svezia (19) e la Spagna (18) si posizionano nella Top 10 globale.

3.2. GLI EUROPEAN COMMON CRITERIA (EUCC)

A seguito di un lungo processo iniziato nel 2019 dall'ENISA, che ha visto la creazione del gruppo di lavoro "EUCC *Ad Hoc Working Group*" (EUCC-AHWG) e la consultazione di tutti gli stakeholder interessati, il 31 gennaio 2024 la Commissione europea ha adottato il **Regolamento di esecuzione (UE) 2024/482** *(Implementing Act)*[23] **con cui i Common Criteria Europei** (*Common Criteria based European candidate cybersecurity certification scheme* – **EUCC**) **sono diventati ufficialmente parte della legislazione europea** e possono supportare la certificazione volontaria di un numero maggiore di prodotti e sistemi ICT[24]. Parallelamente, l'ENISA ha pubblicato una serie di documenti tecnici a supporto (*state-of-the-art documents*)[25], i quali specificano metodi di valutazione, tecniche e strumenti applicabili alla certificazione di prodotti ICT o a requisiti di sicurezza riferiti a una categoria gene-

23 Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

24 Il presente regolamento si applicherà a partire dal 27 febbraio 2025, salvo il capo IV e l'allegato V, che sono applicabili dal 27 febbraio 2024.

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

rica di prodotti ICT, al fine di armonizzare i criteri di valutazione o i profili di sicurezza.
La versione attualmente disponibile di tali meccanismi di certificazione si fonda su un modello ispirato agli schemi ISO/IEC 15408 e ISO/IEC 18045 e consente di stabilire una certificazione uniforme in grado di **raggiungere i due livelli di garanzia di sicurezza più alti previsti dall'art. 52 del Cybersecurity Act**, ovverosia quello "sostanziale" e quello "elevato", coinvolgendo autorità nazionali e prendendo in considerazione valutazioni di terze parti indipendenti. **È escluso dagli EUCC il livello "base" – nonché l'autovalutazione della conformità – 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 "elevato". Inoltre, gli EUCC includono la possibilità di certificare i *Protection Profiles*, consentendo una definizione armonizzata di requisiti di sicurezza associati a categorie specifiche di prodotti.
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.
Per quanto concerne il **rilascio delle certificazioni**, questo avverrà da parte di **organismi accreditati e riconosciuti (ISO/IEC 17065), previa autorizzazione dell'Autorità nazionale di certificazione della cibersicurezza (in Italia, l'ACN)**, mentre **chi richiede la certificazione dovrà fornire all'ITSEF[26] e all'organismo di certificazione tutte le informazioni necessarie a tal fine**, ivi compresi i dettagli sul prodotto ICT, il relativo codice sorgente, il link al sito web del richiedente che renda evidenti le informazioni supplementari sulla cibersicurezza previste dall'art. 55 CSA (es: raccomandazioni per l'uso sicuro dei prodotti, periodo di assistenza garantita, metodi per ricevere informazioni sulle vulnerabilità, ecc.), la descrizione delle procedure di gestione e segnalazione delle vulnerabilità, oltre che eventuali altre certificazioni – basate su altri schemi europei e/o nazionali – già ottenute dal richiedente per il prodotto ICT oggetto della valutazione.
Inoltre, **si prevede che il titolare di un certificato EUCC possa apporre un marchio e un'etichetta sul prodotto ICT che ha completato con successo il processo di certificazione**, al fine di dimostrare la conformità al succitato regolamento e ciò costituirà certamente un ulteriore elemento di garanzia e fiducia nei confronti di partner, clienti e consumatori finali.
Quanto al **periodo di validità** di un certificato EUCC, è previsto che questo sia stabilito da chi rilascia la certificazione, fermo restando il limite temporale di **cinque anni**, che **può essere esteso solo dall'autorità nazionale di certificazione della cibersicurezza**.
L'*Implementing Act*, in particolare ai Capi IV e V (artt. 21-31), prevede un **articolato sistema di monitoraggio della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza, degli organismi di certificazione e dei titolari di certificazioni EUCC**. In particolare, questi ultimi sono tenuti a monitorare

26 ITSEF – Information Technology Security Evaluation Facility; l'art. 2(7) del Regolamento di esecuzione lo definisce come: "una struttura di valutazione della sicurezza delle tecnologie dell'informazione, che è un organismo di valutazione della conformità quale definito nell'articolo 2, punto 13), del regolamento (CE) n. 765/2008, che svolge attività di valutazione".

autonomamente i prodotti certificati con EUCC, con riguardo al livello di affidabilità indicato nella certificazione e alle rispettive vulnerabilità, tenendo in debita considerazione qualsiasi fonte, anche esterna (es: utenti o ricercatori nel settore della sicurezza), da cui si possa evincere la sussistenza di una vulnerabilità.

Altro aspetto di rilievo concerne la **gestione e la divulgazione delle vulnerabilità dei prodotti che abbiano ottenuto un certificato EUCC** (Capo VI). Più nel dettaglio, viene prescritto al titolare del certificato di istituire e mantenere una serie di procedure per la gestione delle vulnerabilità, nonché metodi per ricevere informazioni sulle stesse da fonti esterne (compresi gli utenti), organismi di certificazione e ricercatori nel settore della cybersicurezza. In aggiunta, nel caso in cui si rilevi una potenziale vulnerabilità, essa deve essere appositamente registrata e, contestualmente, va effettuata un'analisi di impatto ad hoc, da far confluire in una relazione da trasmettere senza indebito ritardo all'organismo di certificazione o all'autorità nazionale di certificazione della cibersicurezza. Per di più, qualora da tale relazione emerga che la vulnerabilità riscontrata non è residua e non può essere risolta, il certificato EUCC viene revocato dall'organismo che lo ha rilasciato.

Ad ogni modo, una piena attuazione del sistema EUCC richiederà probabilmente nuove discussioni in sede comunitaria e la stesura di linee guida per facilitare il periodo di transizione, che corrisponde a 12 mesi, che aumentano a 24 se il processo di certificazione prende inizio entro i 12 mesi dall'entrata in vigore dell'*Implementing Act* (27 febbraio 2024), al termine del quale le certificazioni che si basano su un sistema nazionale di certificazione della cibersicurezza dovrebbero cessare di operare (oppure essere sottoposte a riesame) per lasciare definitivamente spazio agli EUCC.

In base a quanto esposto, è evidente che gli EUCC potranno comportare 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. A conferma dell'interesse verso gli EUCC, **un'indagine condotta da I-Com** con il sostegno di alcune delle principali associazioni di categoria e che ha coinvolto 150 imprese appartenenti a vari settori (tra cui utilities, trasporti e tlc/digitale)[27], **ha consentito di registrare che, indipendentemente dal fatto che l'impresa avesse adottato o intendesse adottare una certificazione di cybersicurezza, il 74,5% dei rispondenti si è mostrato parzialmente o totalmente d'accordo in merito al fatto che standard comunitari (come, appunto, gli EUCC) possano incentivare il ricorso a tali strumenti (+4,5% su base annua)**.

3.2.1. Il ruolo delle certificazioni nel quadro normativo europeo e nazionale

Come visto nei capitoli precedenti, le sfide legate alla cybersicurezza sono sempre più complesse da affrontare sia per la natura degli attacchi cibernetici, sempre più complessi e dinamici, sia per il crescente numero di adempimenti derivanti dal quadro regolatorio europeo e nazionale in materia, che impone alle imprese la necessità di mettere in campo risorse crescenti per supportare i maggiori investimenti richiesti in risorse umane, processi e tecnologie. **In questo contesto, è evidente la necessità di garantire una risposta quanto più armonizzata possibile a livello eurounitario e dunque il contributo al raggiungimento di tale obiettivo che il ricorso a standard comuni di certificazione in tutti gli Stati Membri potrebbe of-**

27 Si v. infra. Cap. 4.

frire non solo per la creazione di un ecosistema digitale più sicuro e cyber-resiliente, ma anche per il rafforzamento della fiducia verso prodotti, servizi e processi ICT. Naturalmente, ciò presuppone che tali strumenti siano strutturati per essere adeguatamente flessibili, così da stare al passo con l'evoluzione della minaccia cibernetica[28].

Se è evidente l'opportunità offerta dalla certificazione di cybersicurezza non può non considerarsi l'eventualità che, a livello unionale o nazionale, si opti per rendere mandatoria tale certificazione per alcuni prodotti, servizi e processi ICT e/o per determinate categorie di soggetti, a partire dalle infrastrutture critiche[29]. Una simile possibilità d'altronde è prevista anche dalla **direttiva NI2**, in particolare all'**art. 24**, che consente agli Stati Membri, al fine di dimostrare la conformità a determinati adempimenti di cui all'art. 21 (misure di sicurezza), di imporre ai soggetti essenziali e importanti di utilizzare prodotti, servizi e processi ICT che siano stati certificati sulla base di uno dei sistemi europei di certificazione della cibersicurezza a norma dell'art. 49 CSA. Tra questi, come anticipato, rientrano gli EUCC. Parallelamente, il secondo paragrafo conferisce alla Commissione europea il potere di adottare atti delegati per integrare la NIS2 per il medesimo scopo, qualora si ravvisi un insufficiente livello di cibersicurezza. In tal caso, la procedura comporta una preliminare valutazione di impatto e diverse consultazioni con gli stakeholder pertinenti, secondo quanto stabilito dall'art. 56 CSA. Quest'ultima disposizione risulta centrale poiché, nel prevedere in prima istanza che la certificazione della cibersicurezza è volontaria, sottolinea che può essere specificato diversamente dal diritto dell'UE o degli SM e, nel primo caso, affida alla Commissione la valutazione circa l'efficacia e l'efficienza dell'utilizzo di sistemi europei di certificazione della cibersicurezza e, se opportuno, la decisione sul rendere obbligatorio uno specifico sistema di questo tipo. Nel fare ciò, in primo luogo, la Commissione dovrebbe dare priorità agli OSE (operatori di servizi essenziali) – secondo la definizione contenuta nella prima direttiva NIS – che, con la NIS2, sono pressoché identificabili con i soggetti ricompresi nei settori ad alta criticità di cui all'allegato I[30]. In secondo luogo, essa tiene in considerazione una serie di elementi, tra cui: i) l'impatto sui fabbricanti e sui fornitori di tali prodotti, servizi o processi ICT, nonché sui relativi utenti, in termini di costi, benefici sociali ed economici derivanti dal previsto aumento di sicurezza; ii) lo stato dell'arte, con riferimento al diritto degli SM e dei paesi terzi in materia; iii) le risultanze del processo di consultazione (da svolgersi in maniera aperta, trasparente e inclusiva) con tutti gli stakeholder pertinenti e gli Stati Membri. Ciò posto, **assoluta rilevanza rivestono i costi legati alle certificazioni e dunque la necessità che gli stakeholder possano contribuire alla realizzazione di un'analisi costi-benefici e all'individuazione di apposite metriche e criteri per valutare l'efficacia e l'efficienza nel tempo degli schemi europei di certificazione della cibersicurezza, a partire dagli EUCC**. In particolare, tali parametri dovrebbero essere funzionali a comprendere l'effettivo miglioramento quantitativo o qualitativo della cybersicurezza dei prodotti, servizi e processi ICT sottoposti a certificazione.

A livello nazionale, il CSA – pur avendo la forma del regolamento e quindi in larga parte direttamente applicabile – ha necessitato di un intervento di adegua-

28 Tali aspetti, come si evince dal primo URWP (Union Rolling Work Programme for European cybersecurity certification) pubblicato dalla Commissione europea, saranno presi in considerazione – parimenti all'esperienza maturata nel corso degli anni dai soggetti certificati/certificatori – nella revisione del Cybersecurity Act (CSA).

29 Il white paper di EY, Direttiva NIS 2 (marzo 2024) evidenzia i vantaggi della mandatorietà degli EUCC. È consultabile al seguente link: https://www.ey.com/it_it/forms-it_it/direttiva-nis2-ita.html

30 Tale valutazione deve essere effettuata al più tardi due anni dopo l'adozione del primo sistema europeo di certificazione della cibersicurezza, per cui entro il 27 febbraio 2026.

mento interno. Ebbene, l'**art. 6 del d. lgs. 3 agosto 2022, n. 123**[31] prescrive che in mancanza di un diritto dell'UE armonizzato, l'ACN possa adottare, previa consultazione con gli stakeholder, norme tecniche in cui si preveda la certificazione obbligatoria basata su un sistema europeo come gli EUCC. Per di più, qualora si dia seguito a questo approccio, il soggetto obbligato a ottenere la certificazione non è tenuto al versamento degli oneri per il rilascio del certificato, che invece sono previsti in un regime su base volontaria. Per di più, l'**art. 27 del d. lgs. n. 138/2024 di recepimento della NIS2 in Italia** prescrive che l'Autorità nazionale competente NIS (l'ACN) può imporre ai soggetti essenziali e importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC che siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza ex art. 49 CSA.

Nel framework normativo eurounitario di recente adozione non mancano altrettanti riferimenti che potrebbero far propendere, se non verso un'obbligatorietà, certamente verso una maggiore centralità di certificazioni basate sullo schema EUCC, viste anche come possibili strumenti di semplificazione della compliance. Ad esempio, l'**art. 17 del Cyber Solidarity Act (CSoA)** che impone al soggetto che intenda essere riconosciuto come fornitore di fiducia nell'ambito della riserva UE per la cibersicurezza di essere certificato in conformità a un sistema di certificazione UE per il servizio di sicurezza gestito, entro due anni dalla data di applicazione di tale sistema.

Considerato l'impatto rilevante sull'intera catena del valore dei prodotti con elementi digitali, appare opportuno fare riferimento anche al **Cyber Resilience Act (CRA)**, con particolare riguardo a quelle disposizioni che richiamano un sistema europeo di certificazione della cibersicurezza. Come evidenziato dal **Considerando n. 46** del presente regolamento, i prodotti con elementi digitali critici utilizzano già ampiamente varie forme di certificazione e sono altresì ricompresi nel sistema EUCC. Per di più, come stabilito dall'**art. 8**, viene conferito il potere alla Commissione di assoggettare obbligatoriamente i prodotti digitali "critici" a una certificazione europea in materia di cibersicurezza, previa valutazione del potenziale impatto sul mercato e a seguito di consultazioni con gli stakeholder pertinenti, prestando particolare attenzione al caso in cui tali prodotti siano destinati a essere utilizzati nell'ambito dei soggetti essenziali, così come definiti dalla direttiva NIS2. Inoltre, l'**art. 27(8)** prescrive che i prodotti e i processi ICT certificati nell'ambito di un sistema europeo di certificazione della cibersicurezza si presumono di per sé conformi ai requisiti essenziali di cybersicurezza di cui all'allegato I, potendo in tal modo vedersi scomputare gli adempimenti richiesti dal successivo **art. 32** (Procedure di valutazione della conformità per prodotti con elementi digitali).

Pertanto, è possibile affermare che i sistemi europei di certificazione della cibersicurezza, a partire dagli EUCC, costituiranno un tassello cruciale nel facilitare la compliance anche rispetto ai numerosi adempimenti previsti dal CRA. In merito, seppur sia passato relativamente in sordina, il **Regolamento delegato (UE) 2022/30 ha integrato la Direttiva (UE) 2014/53 (Radio Equipment Directive – RED)** inerente l'immissione sul mercato interno dell'Unione di apparecchiature radio, richiedendo ai rispettivi fabbricanti, importatori e distributori di osservare e successivamente dimostrare il rispetto dei requisiti essenziali, inclusi quelli in termini di cybersicurezza, prescritti per le diverse tipologie di tali apparecchiature. Pertanto, va tenuto conto che il Regolamento delegato

31 Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

summenzionato costituisce una *lex specialis* rispetto al CRA e sarà applicabile a breve (dal 1° agosto 2025), anche se in via temporanea, ossia fino alla piena operatività del CRA (prevista per il 2027) per i prodotti ricompresi in entrambe le normative in questione, al fine di evitare sovrapposizioni in tema di requisiti essenziali di cibersicurezza.

Ciò premesso, **è indispensabile**, infatti, **che le imprese possano avere certezze e tempi definiti per l'implementazione di normative che puntano – o quantomeno dovrebbero puntare – a semplificare e migliorare la cibersicurezza**. 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 imprese che gestiscono sistemi ICT e reti. In quest'ottica, **la disponibilità di standard di sicurezza condivisi a livello eurounitario, come gli EUCC, diventa cruciale per garantire la resilienza di apparati, reti e sistemi complessi**.

Pertanto, nell'immaginare il futuro ecosistema normativo nazionale che sarà delineato con la piena applicabilità e l'adeguamento, rispettivamente, di direttive – a partire dalla NIS2 – e regolamenti in materia di cybersicurezza, sarà certamente importante l'adozione di una metodologia unica che possa raccogliere gli input relativi a un efficientamento della metodologia di test come prevista in ambito UE. Ciò dovrà avvenire mantenendo saldi **alcuni importanti requisiti**, ossia che sia **applicabile agli asset strategici** e che possa traguardare una **corretta e tempestiva gestione della variabilità delle versioni SW**, la **riusabilità** delle certificazioni, un **tempo definito di esecuzione dei test,** oltre a un **appropriato management delle vulnerabilità**. Infine, va evidenziato che, nonostante le importanti semplificazioni e innovazioni apportate dallo schema EUCC rispetto ai *Common Criteria*, **le procedure e le risorse necessarie per affrontare il processo di certificazione appaiono di primaria importanza per le organizzazioni interessate**. In questo senso, potrebbe risultare utile **discutere proattivamente con gli stakeholder sulla possibilità di prevedere l'obbligatorietà circa l'adozione di certificazioni della cybersicurezza riconducibili alla metodologia EUCC** (come previsto, tra l'altro, dall'art. 24 NIS2 e dall'art. 27 del relativo atto di recepimento interno).

icom 2005 25
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**, l'Istituto per la Competitività (I-Com) ha riproposto e aggiornato un'indagine avviata a partire dall'anno scorso, avvalendosi anche del sostegno di alcune delle principali associazioni di categoria, che in questa edizione ha coinvolto 150 imprese appartenenti a vari settori: utilities (acqua, rifiuti ed energia), trasporti, TLC/digitale, ecc. La survey si è svolta in modalità completamente online tra il 20 maggio e il 2 luglio 2024 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 21 domande.

Osservando la distribuzione dei rispondenti per settore (Fig. 4.1) è possibile notare come **la maggior quota di imprese rientri tra le utilities in entrambi gli anni considerati** (38,67% nel 2024 e 58,62% nel 2023). Le aziende del comparto ICT occupano stabilmente il secondo posto, risultando più che raddoppiate rispetto alla precedente indagine, corrispondendo al 32% del campione, seguite da Tlc (8,67%) e trasporti (4%). Per di più, oltre il 16% dei rispondenti appartiene ad altri settori (+5% su base annua), di cui ben 6 afferiscono a quello finanziario e 5 al manifatturiero.

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 59,33%, seguite dalle piccole (meno di 50 dipendenti con fatturato non superiore ai €10 milioni) con il 22,67% (+8% rispetto al 2023) e, infine, dalle medie imprese (meno di 250 dipendenti con fatturato non superiore ai €43 milioni), le quali occupano il 18% del totale (-6%).

Fig. 4.1: Distribuzione dei rispondenti per settore

Totale rispondenti 2024: 150 su 150
Totale rispondenti 2023: 145 su 145
Fonte: Elaborazioni I-Com

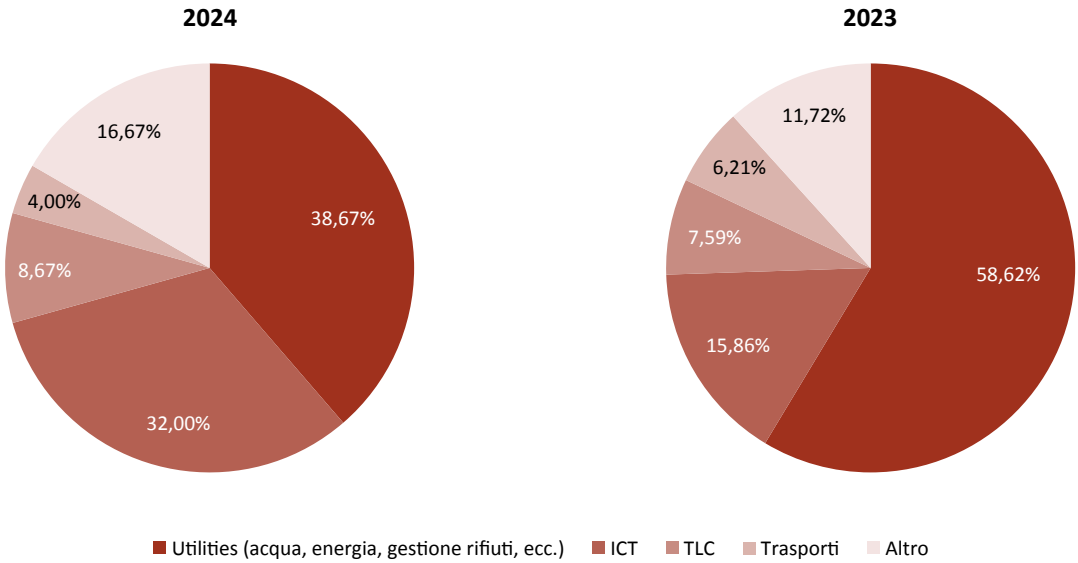
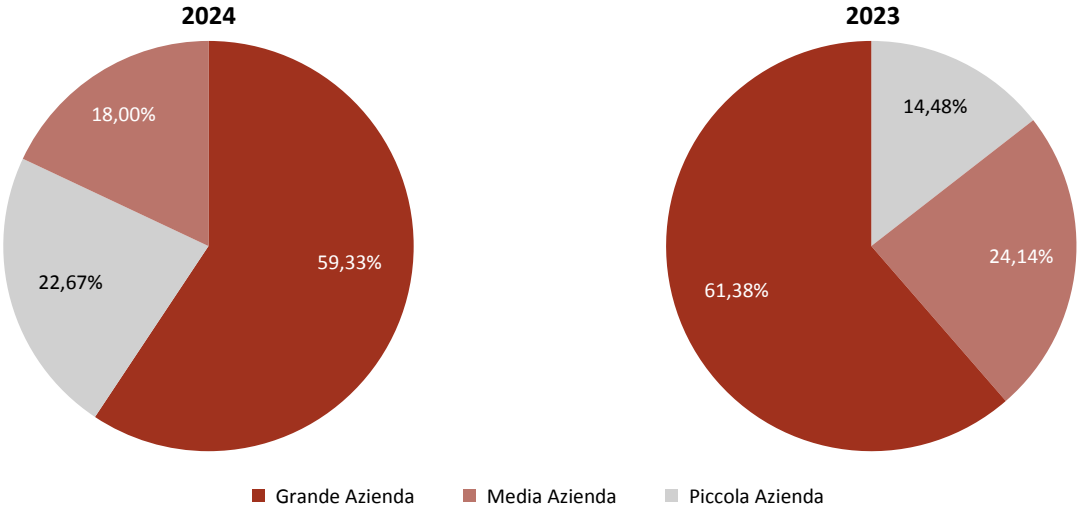


Fig. 4.2: Distribuzione dei rispondenti per dimensione aziendale

Totale rispondenti 2024: 150 su 150
Totale rispondenti 2023: 145 su 145
Fonte: Elaborazioni I-Com



4.2. ANALISI DEI RISULTATI

La seconda sezione dell'indagine **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.

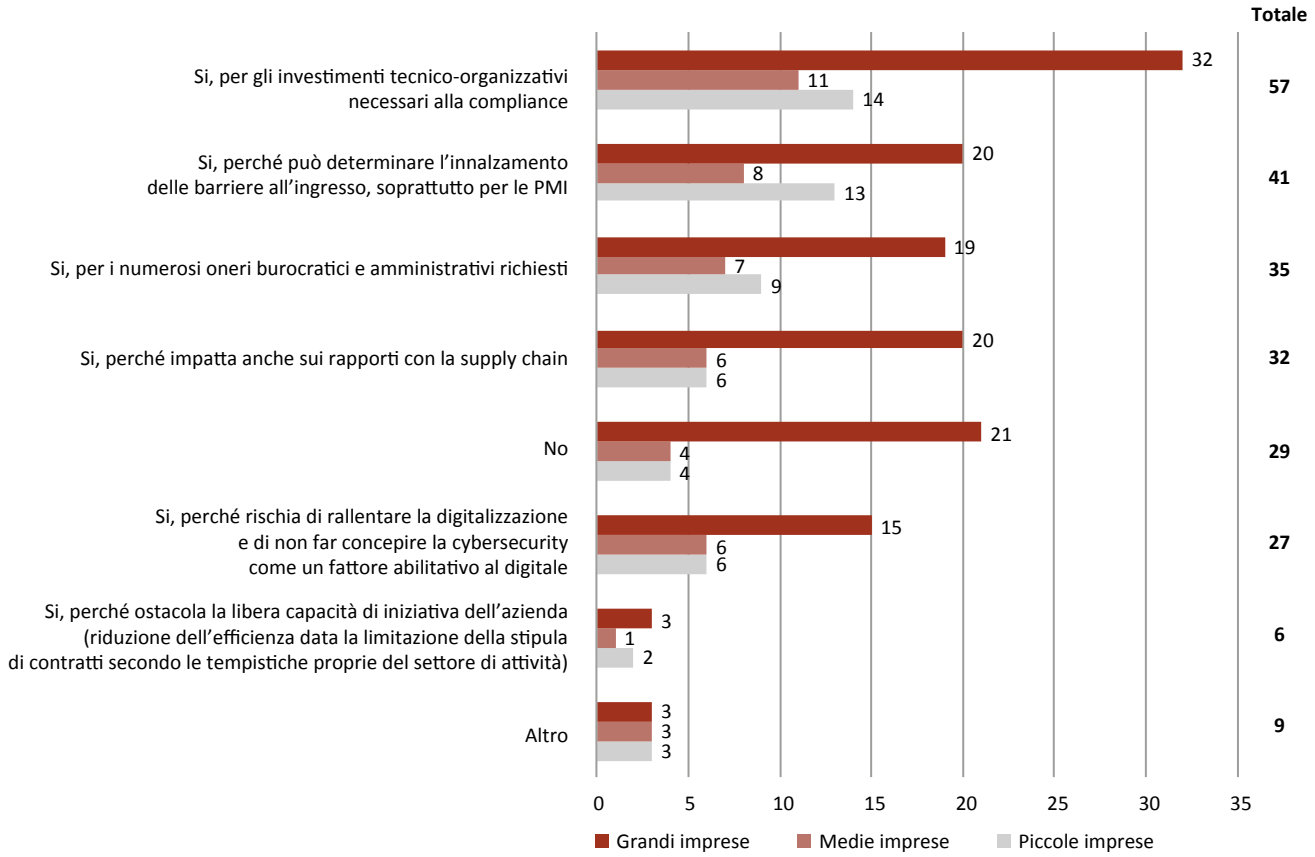
Innanzitutto, ai soggetti partecipanti è stato chiesto di fornire una valutazione circa l'impatto degli adempimenti prescritti dalle normative in cybersicurezza sulla competitività aziendale (Fig. 4.3). **Per le grandi imprese rilevano maggiormente gli investimenti tecnico-organizzativi necessari alla compliance (32 risposte), così come per le aziende di medie dimensioni (11) e per le piccole imprese (14).**

Considerando unitamente tutte le classi dimensionali, altri due motivi ricorrenti tra i rispondenti si rivedono nella **preoccupazione circa l'innalzamento delle barriere all'ingresso, soprattutto per le PMI (41 risposte in totale)** e la numerosità degli oneri burocratici e amministrativi richiesti (35 risposte in totale). Viceversa, gli adempimenti previsti da normative in ambito cibersicurezza vengono più limitatamente ritenuti come ostacoli rispetto alla libera capacità di iniziativa dell'azienda (6 risposte in totale) e alla considerazione della cybersecurity come un fattore abilitante al digitale (27 risposte in totale).

Inoltre, alla voce "Altro" 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.

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

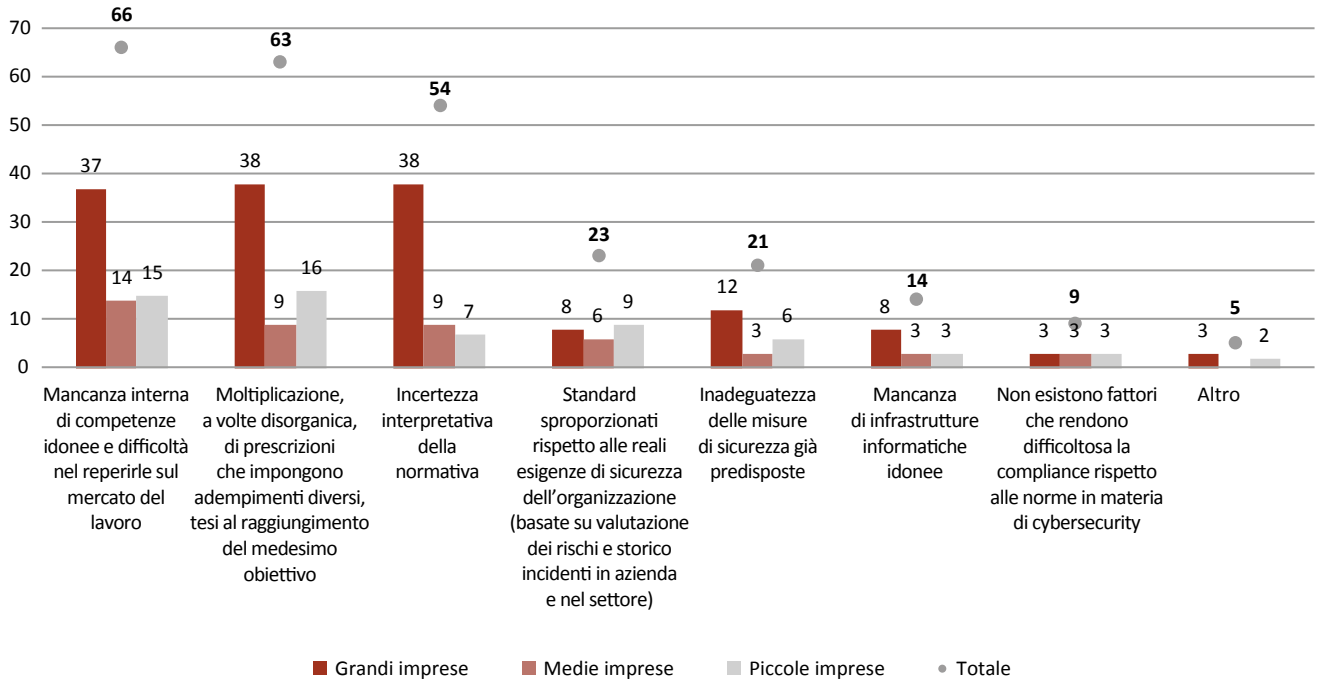
Note: Possibilità di più risposte
Totale dei rispondenti: 118 su 150
Fonte: Elaborazioni I-Com



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 sia internamente, sia sul mercato del lavoro (66 risposte in totale), seguito dalla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (63 risposte) e dall'incertezza interpretativa della normativa (54 risposte).** Invece, tra le opzioni meno selezionate rileva, con 9 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 e conoscenza interna alle organizzazioni rispetto alle normative in ambito cybersecurity, per cui sarebbe opportuno rifarsi a consulenti esperti, sia la presenza di standard che richiedono modelli di *assessment* differenti con conseguente complessità nella gestione di relativi piani di *improvement*.

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: 118 su 150
Fonte: Elaborazioni I-Com



Come si evince dal grafico successivo (Fig. 4.5), **il maggior numero di imprese rispondenti assegna meno del 3% del budget IT alla cybersecurity.** Non sorprende che figurino in quota superiore le grandi imprese (27) 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 (10 in totale, di cui 4 grandi imprese) – di un'allocazione superiore al 15% del budget IT a disposizione.

Peraltro, agli operatori economici intervistati è stato chiesto di dichiarare la vita media dei rispettivi strumenti di sicurezza hardware e software (Fig. 4.6). **Il 59,48% dei rispondenti ha affermato di dismettere tali strumenti mediamente dopo 5 anni, mentre il 34,48% (che comprende 27 grandi imprese) lo fa a seguito di 3 anni di utilizzo.** Solamente il 4,31% delle aziende esegue l'aggiornamento delle proprie tecnologie dopo 12 anni, ben 2 di esse appartengono alla categoria di piccole dimensioni. 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, i feedback pervenuti sono piuttosto diversificati (Fig. 4.7). Appare interessante evidenziare che tra le piccole imprese prevalgono le risposte che, da un lato, denotano l'assegnazione di lavoratori appo-

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: 115 su 150
Fonte: Elaborazioni I-Com

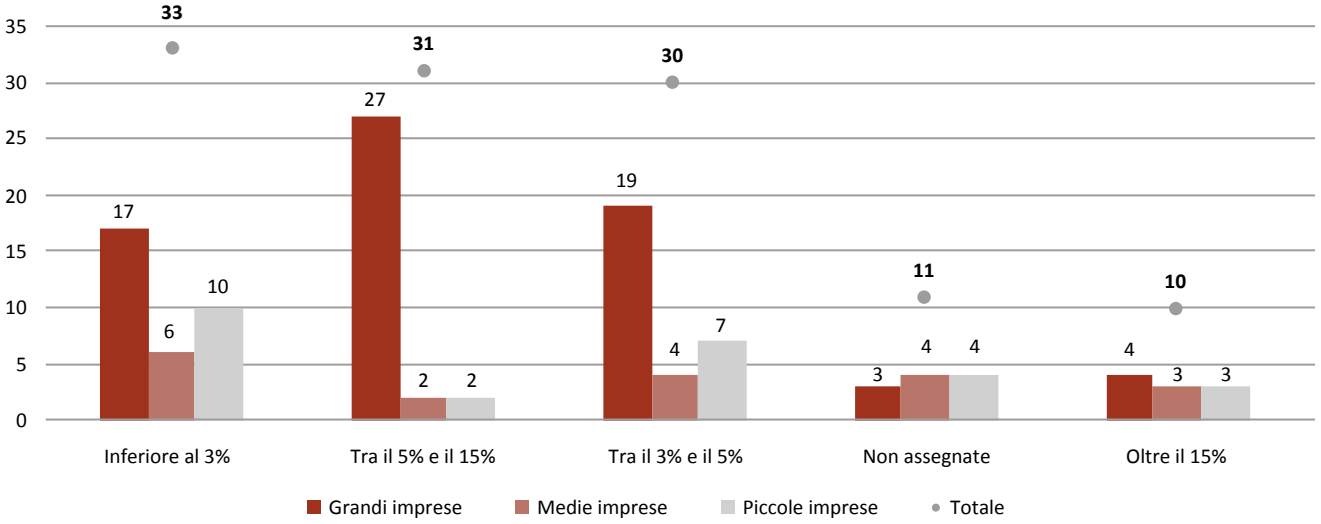
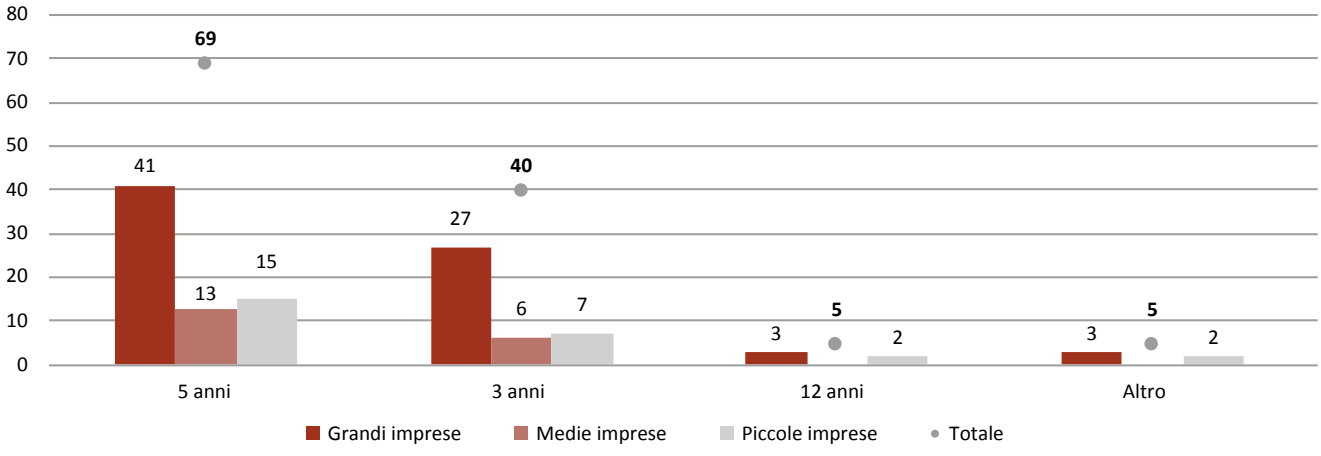


Fig. 4.6: Qual è la vita media dei vostri strumenti di sicurezza (hardware e software)?

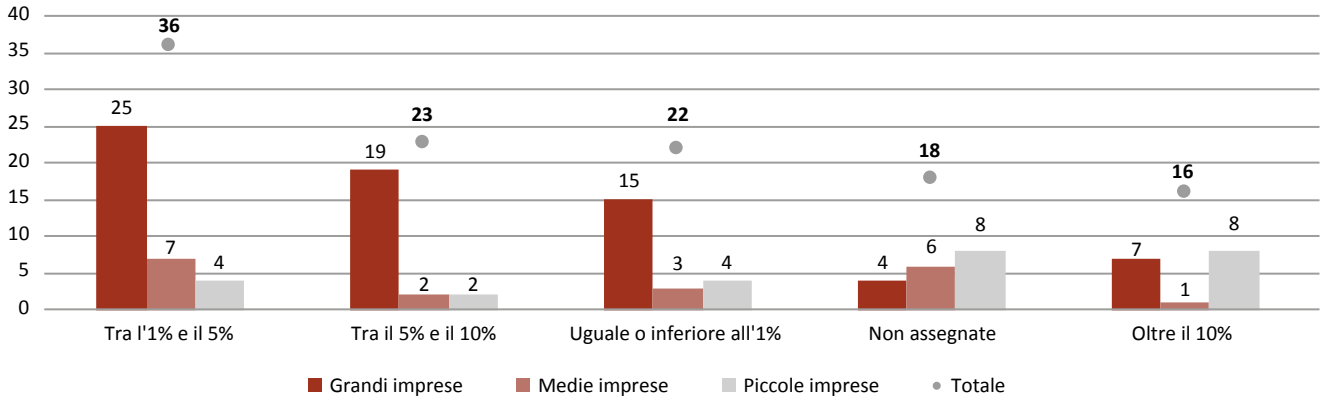
Note: Possibilità di un'unica risposta
Totale dei rispondenti: 116 su 150
Fonte: Elaborazioni I-Com



sitamente dedicati alla cibersicurezza come assente e, dall'altro, superiore al 10% rispetto alla quota di personale IT a tempo pieno. Fra le medie imprese rispondenti si riscontra una preponderanza per l'assegnazione di personale ad hoc tra l'1 e il 5%, così come nel caso delle grandi imprese.

Fig. 4.7: A quanto ammontano le risorse umane assegnate alla cybersecurity rispetto agli FTE impiegati in ambito IT nella sua impresa?

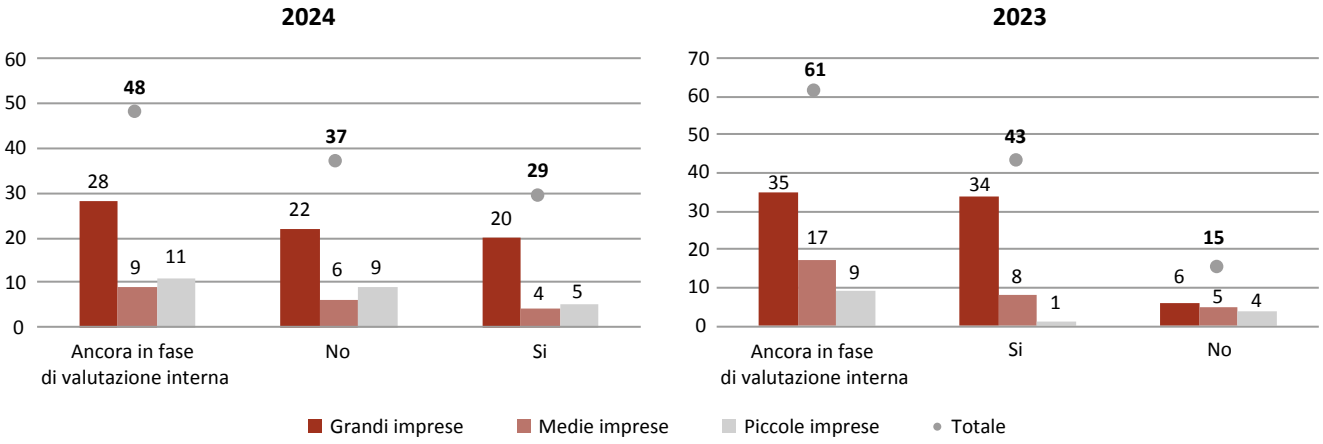
Note: Possibilità di un'unica risposta
Totale rispondenti: 115 su 150
Fonte: Elaborazioni I-Com



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, anche quest'anno è

Fig. 4.8: 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 dal prossimo 17 ottobre, è previsto un incremento delle risorse destinate alla cybersecurity?

Note: Possibilità di un'unica risposta
Totale rispondenti 2024: 114 su 150
Totale rispondenti 2023: 119 su 145
Fonte: Elaborazioni I-Com



stato chiesto alle aziende partecipanti di fornire indicazioni su **un eventuale incremento delle risorse destinate alla cybersecurity** (Fig. 4.8).

Sul punto, si può osservare **come il 42,11% dei rispondenti stia ancora valutando tale eventualità, il 9% in meno rispetto al 2023, mentre solo il 25,44% ha già deciso di aumentare gli investimenti in cybersicurezza, facendo registrare un sostanziale peggioramento su base annua (-11%).** Pertanto, appaiono più marcati i risultati afferenti alla mancata volontà di incrementare le risorse in questione. Difatti, mentre nel 2023 solo 15 aziende avevano fornito parere negativo (includenti 6 grandi imprese), nella presente edizione della survey a scegliere tale opzione se ne contano 22 in più, con numeri preoccupanti per le imprese di grandi dimensioni (22).

Il grafico successivo (Fig. 4.9) 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 effettuati dal 58,77% dei rispondenti, seguiti dalla pianificazione di audit interni (42,11%) e dall'utilizzo di strumenti per la simulazione di attacchi**, tra cui si possono annoverare le campagne di phishing (36,84%). Risulta interessante anche il dato relativo all'utilizzo di tutte le modalità di valutazione sin qui richiamate, che interessa il 28,95% delle imprese. In ultimo, è importante notare come 11 rispondenti (1 grande impresa, 2 medie imprese e 8 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. 4.10), è emerso che **il 65,79% dei rispondenti è dotato di firewall e il 59,65% di antivirus.** A seguire, circa il 54% utilizza sistemi di autenticazione, mentre oltre il 50% ha investito in *training* e *awareness* e filtri antispam. Viceversa, fra gli ambiti di investimento meno selezionati spiccano le sonde anti-intrusione (25,44%), le esercitazioni di cybersicurezza (18,42%) e i *pki services* (circa il 3%).

Fig. 4.9: Come viene valutato in concreto il livello di sicurezza informatica interno all'organizzazione?

Note: Possibilità di più risposte
Totale rispondenti: 114 su 150
Fonte: Elaborazioni I-Com

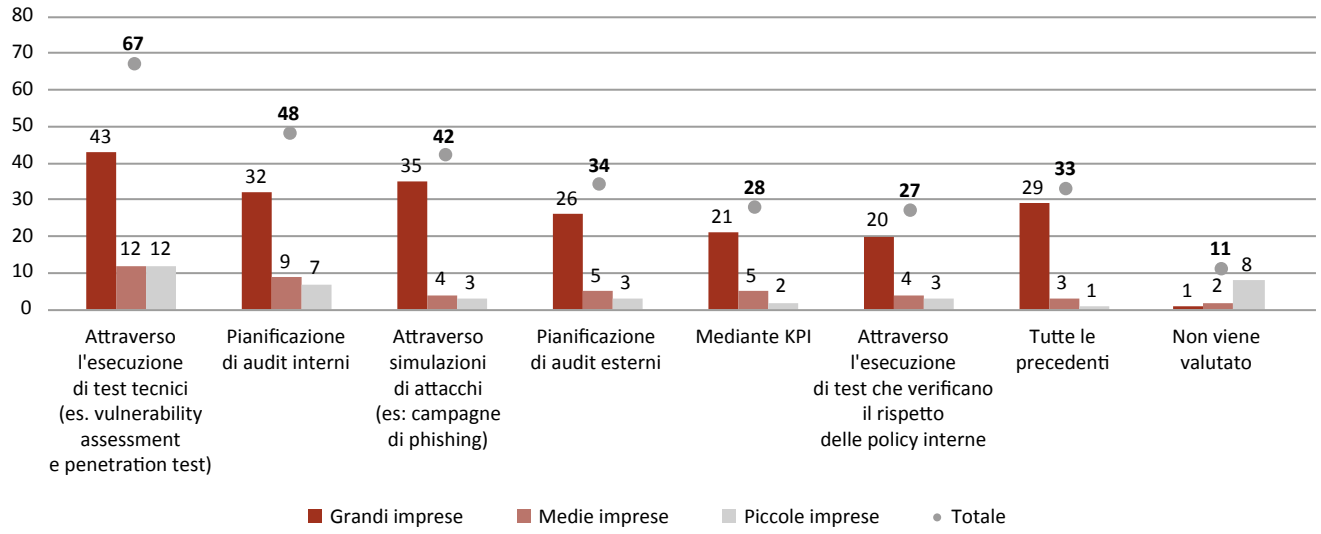
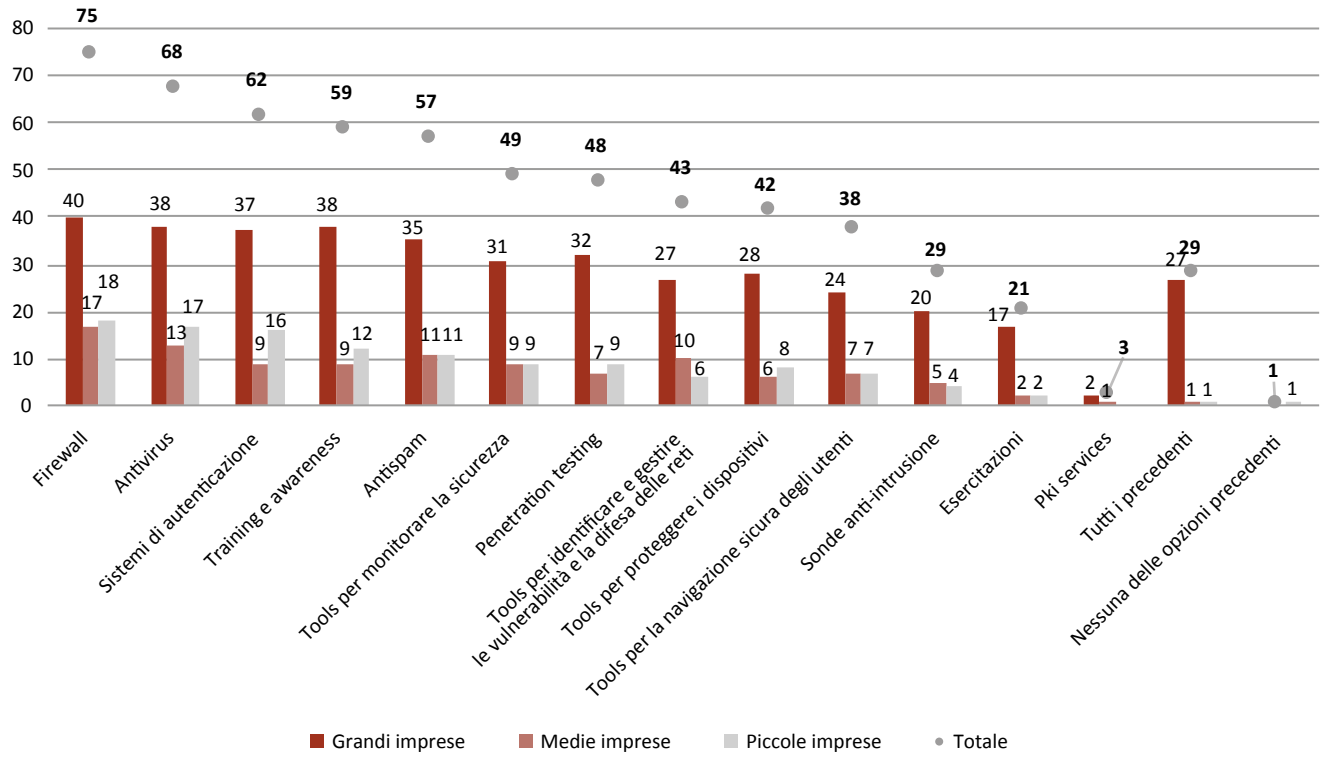


Fig. 4.10: Su quali investimenti si è concentrata la sua impresa in termini di cybersecurity?

Note: Possibilità di più risposte
Totale rispondenti: 114 su 150
Fonte: Elaborazioni I-Com



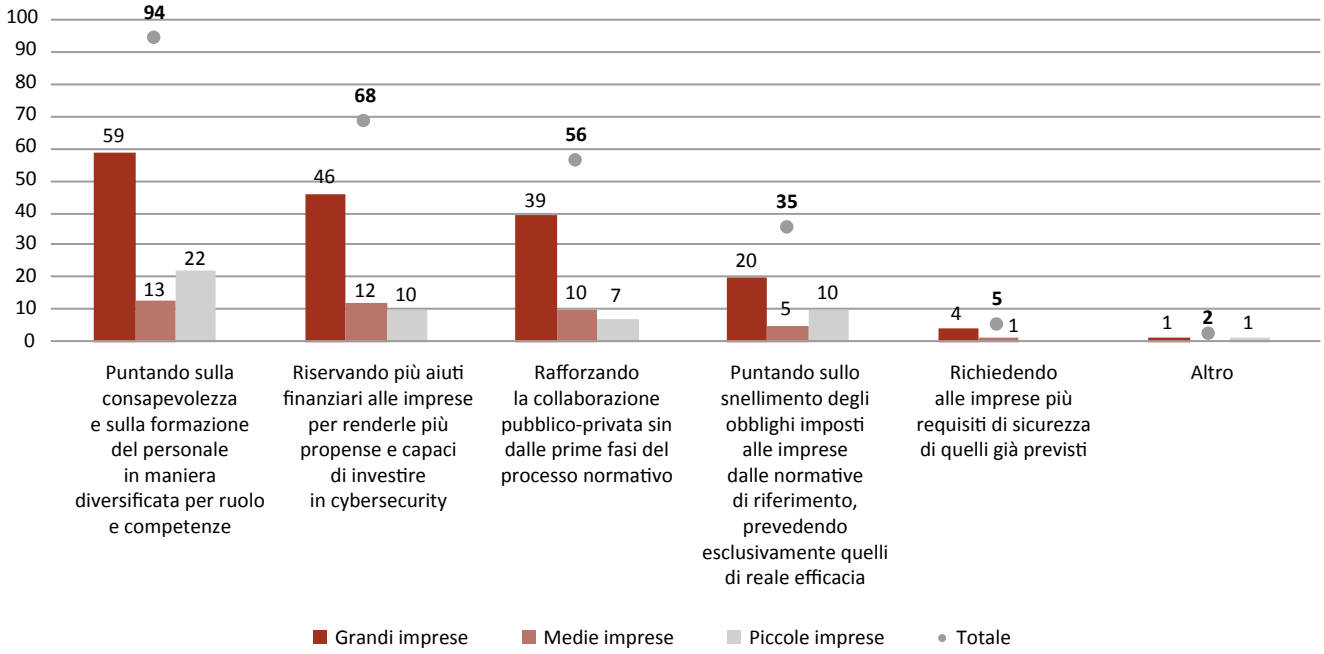
Scrutando più nel dettaglio i feedback pervenuti, si può osservare come gli ultimi strumenti citati siano pressoché inutilizzati dalle piccole e dalle medie imprese.

Analizzando le risposte pervenute con riguardo alle modalità con cui poter **migliorare i livelli di sicurezza informatica** (Fig. 4.11), **l'81,74% 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 è ricaduta sul riservare più aiuti finanziari alle imprese, in quanto ciò è ritenuto necessario per stimolare gli investimenti in cybersecurity (59,13%), mentre il 48,70% dei rispondenti sostiene che si debba rafforzare la collaborazione pubblico-privata sin dalle prime fasi del processo normativo. La risposta meno gettonata (4,35%) – e che riguarda unicamente 4 grandi imprese e 1 di medie dimensioni – è stata richiedere più requisiti di sicurezza di quelli già previsti.

In merito all'adozione di una o più **certificazioni volontarie di cybersicurezza** (Fig. 4.12), si può osservare che **la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione**. Tuttavia, emergono segnali moderatamente positivi se si confrontano i dati su base annua (Fig. 4.13). Difatti,

Fig. 4.11: In che modo ritiene possibile migliorare i livelli di sicurezza informatica?

Note: Possibilità di max. 3 risposte
Totale rispondenti: 115 su 150
Fonte: Elaborazioni I-Com



mentre nell'edizione 2023 i rispondenti che dichiaravano ciò corrispondevano a oltre il 63%, nell'ultima rilevazione sono scesi al 48%. Tra questi, le piccole imprese sono quelle che hanno performato meglio rispetto all'anno scorso (-23,2%), seguite dalle grandi (-15,5%) e, infine, dalle medie (-13%).

Considerando solo le grandi imprese rispondenti, il 47% delle stesse ha già adottato una o più certificazioni di cybersecurity (+11%), mentre un ulteriore 12,8% sta lavorando per ottenere la prima entro un anno. Di converso, tra le medie imprese i risultati sono ben diversi, seppur in miglioramento rispetto all'anno precedente, in quanto un mero 27,7% ha acquisito almeno una certificazione (+16,7%), mentre l'11% intende ottenere la prima certificazione entro un anno. Quanto alle piccole imprese, solo in 2 casi è stata già adottata una certificazione (nel 2023 se ne registrava solo una) e altre 7 puntano a perseguire la prima entro un anno (+22%).

Analizzando anche lo spaccato settoriale (2024), **le ICT spiccano per numero tra le grandi imprese che hanno adottato una o più certificazioni (8);** viceversa, le aziende dei trasporti chiudono la classifica con 2 soggetti, i quali hanno adottato un'unica certificazione. Con riferimento alle medie e piccole imprese, quelle del settore ICT sono le più numerose con una certificazione.

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 ISO 23301. Altre tipologie indicate sono Common Criteria, TIA-942, Uptime Institute e SOC 2.

Fig. 4.12: Qual è la posizione della sua impresa circa le certificazioni volontarie di cybersicurezza? (2024)

Note: Possibilità di un'unica risposta
Totale rispondenti 2024: 112 su 150
Fonte: Elaborazioni I-Com

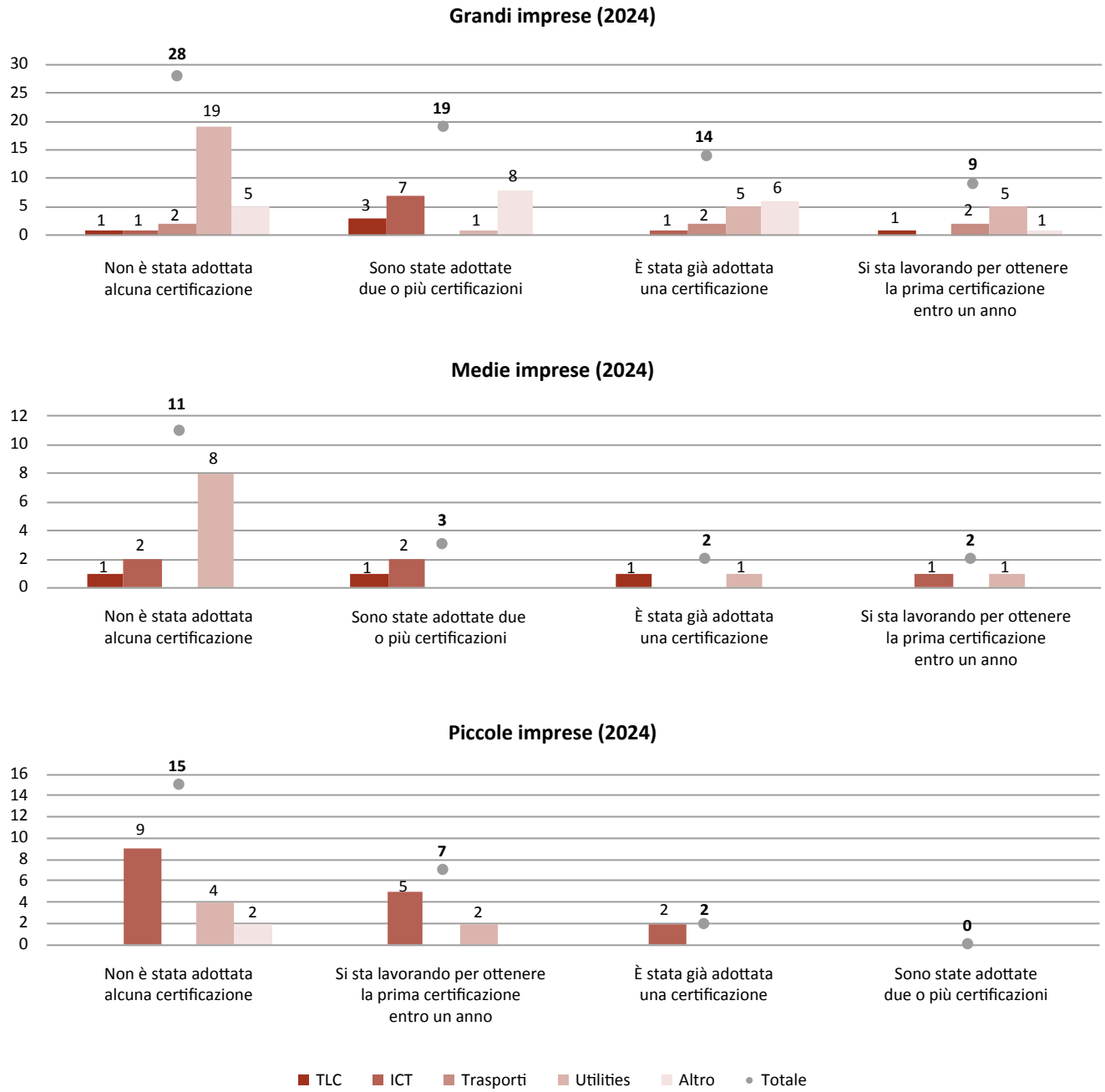
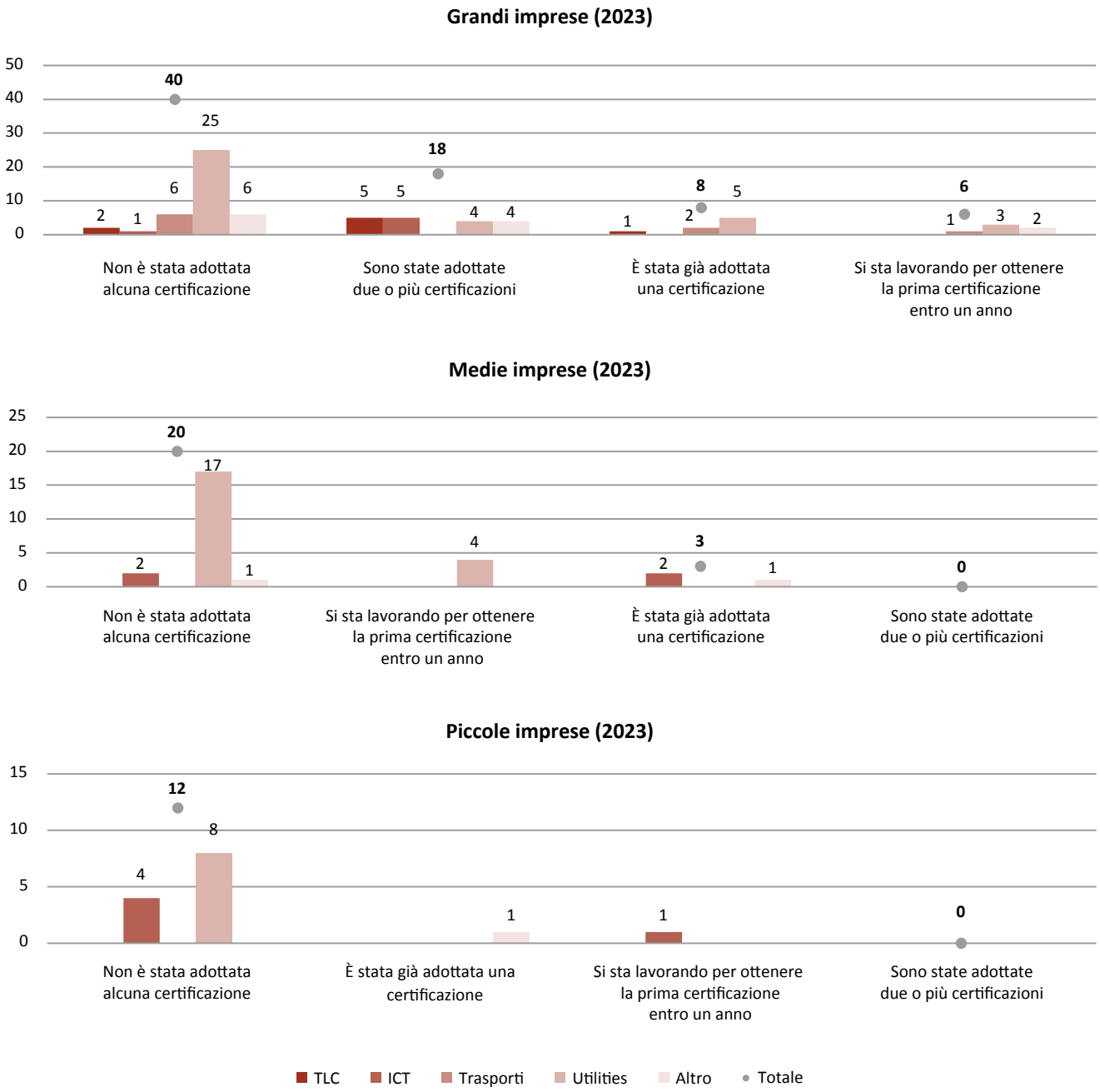


Fig. 4.13: Qual è la posizione della sua impresa circa le certificazioni volontarie di cybersicurezza? (2023)

Note: Possibilità di un'unica risposta
Totale rispondenti 2023: 113 su 145
Fonte: Elaborazioni I-Com



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). Similmente a quanto osservato per il 2023, il principale intralcio risiede nei **costi elevati** del processo di certificazione, che non sono percepiti come proporzionati ai benefici che ne possono conseguire (34,8% dei rispondenti). In secondo luogo, quasi il 19% sostiene che i **tempi per l'esecuzione** della valutazione e il rilascio della certificazione sono troppo lunghi. In terzo luogo, il 14,5% 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.
Diversamente, il 30% delle imprese non rinviene difficoltà particolari nell'ottenimento di una certificazione, segnando un incremento dell'8% rispetto alla precedente indagine. Nell'ambito della voce "Altro" è stata più volte richiamata la scarsità di risorse – umane e finanziarie – da dedicare al processo di certificazione.
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 (46,3% dei rispondenti), una maggiore consapevolezza dei dipendenti e dei collaboratori esterni (39%) e più possibilità di partecipare a bandi di gara pubblici o privati (28%).** Peraltro, è interessante evidenziare come quasi il 22% dei rispondenti non abbia valutato effetti direttamente riconducibili all'ottenimento della certificazione (+7% sul 2023).
Inoltre, si può osservare come solo il 12% dei rispondenti (quasi tutte grandi imprese) non abbiano registrato alcun effetto utile successivamente all'adozio-

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: 111 su 150
Fonte: Elaborazioni I-Com

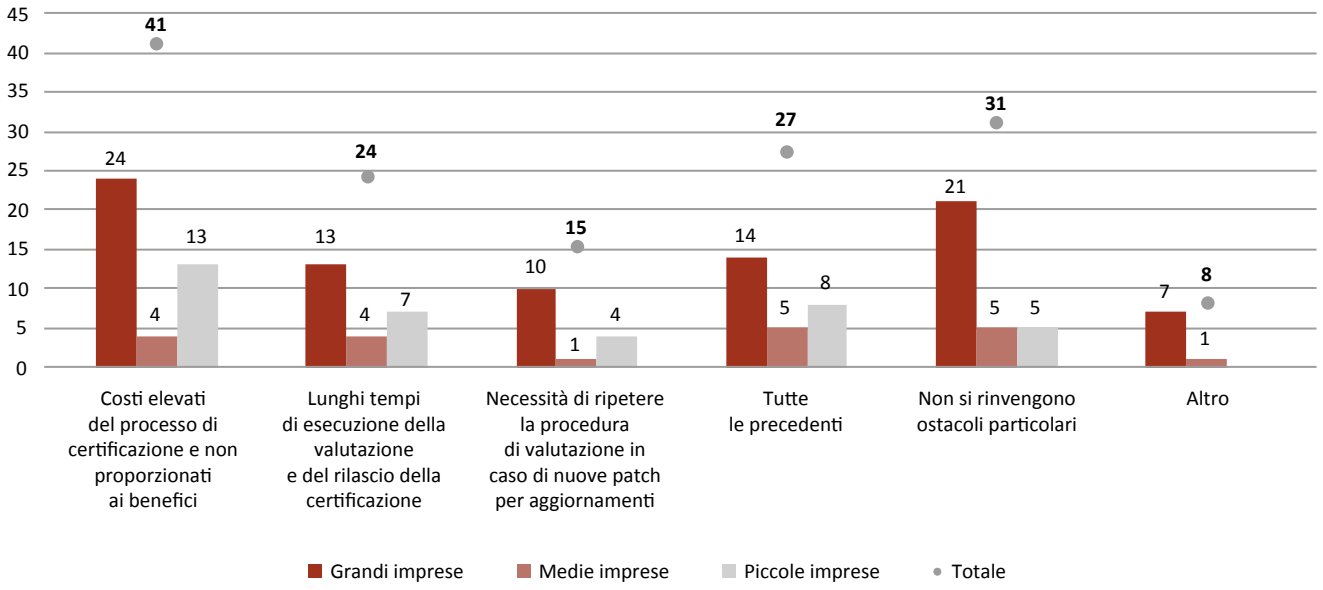
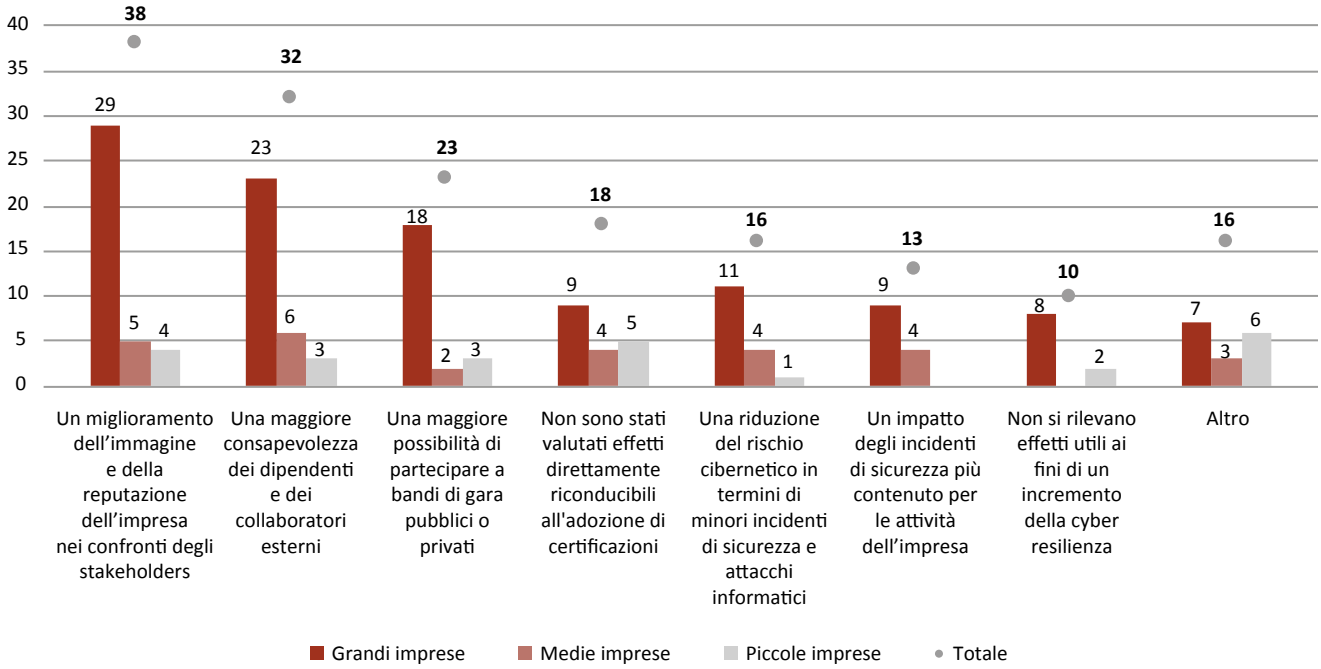


Fig. 4.15: Qualora la sua organizzazione abbia adottato almeno una certificazione di cybersecurity, quali sono stati i principali effetti direttamente riconducibili ad essa?

Note: Possibilità di max. 4 risposte
Totale rispondenti: 82 su 150
Fonte: Elaborazioni I-Com



ne di una certificazione di cybersecurity. Alla voce "Altro" si segnala, fra l'altro, l'aumento della consapevolezza in seno al board aziendale e una maggiore facilità a interfacciarsi con le terze parti.

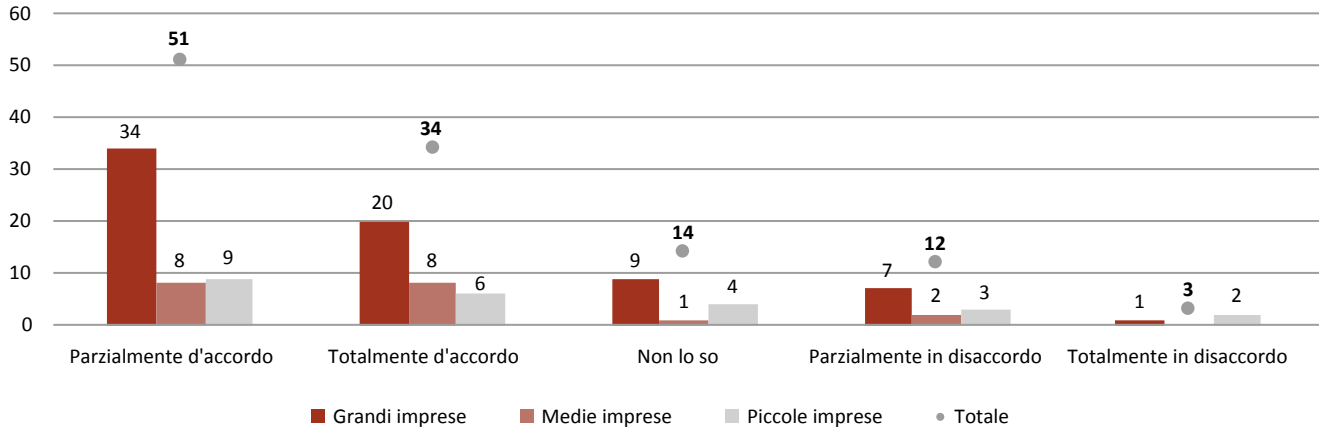
Dalla domanda successiva (Fig. 4.16) emerge che, indipendentemente dal fatto che l'impresa abbia adottato o intenda adottare una certificazione di cybersicurezza**, il 74,5% dei rispondenti è parzialmente o totalmente d'accordo in merito al fatto che standard comunitari – come gli *European Common Criteria-based cybersecurity certification scheme* (EUCC) – possono incentivare il ricorso a tali strumenti (+4,5% rispetto al 2023).** Appare incoraggiante che le imprese silenti sul tema siano diminuite dell'11% su base annua.

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 – possono comportare una serie di vantaggi, tra cui la semplificazione del processo di certificazione e una maggiore appetibilità sul mercato, connessa all'accrescimento delle competenze interne e della propria reputazione. Inoltre, si è evidenziato che **uno standard comunitario potrebbe agevolare il ricorso a simili strumenti, in particolar modo nel caso in cui si riesca a uniformare i requisiti imposti dai diversi atti normativi europei in materia di cybersicurezza, oltre a semplificarne il processo interpretativo.**

Di converso, è stata richiamato a più riprese il rischio che l'introduzione di standard comunitari non faccia altro che aumentare la confusione sul tema, traducendosi in una mera semplificazione (per le grandi

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 150
Fonte: Elaborazioni I-Com



imprese) o un aggravamento (per le PMI) degli obblighi. Allo stesso modo, si è espressa qualche preoccupazione sull'adozione di tali standard – quantomeno in prima battuta – data la complessità percepita e la mancanza di competenze sul mercato del lavoro.

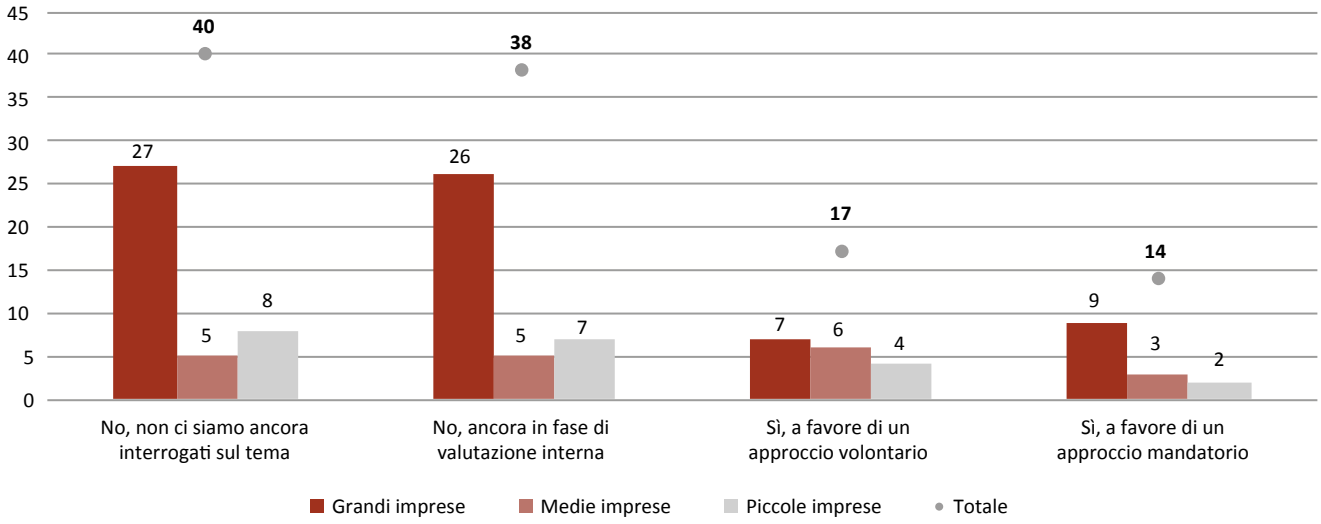
Posto che lo scorso 31 gennaio la Commissione europea ha adottato il Regolamento di esecuzione 2024/482 *(Implementing Act)*[32] con cui gli EUCC sono diventati ufficialmente parte della legislazione europea, nell'ultima edizione della presente indagine è stato chiesto ai partecipanti di rendere noto il punto di vista della propria organizzazione circa l'eventualità di un **approccio mandatorio o meno sull'adozione di schemi di certificazioni europei** come, appunto, gli EUCC (Fig. 4.17). Ebbene**, oltre il 70% dei rispondenti ha dichiarato che non si è ancora assunta una posizione sul tema. Pertanto, la restante quota di imprese si divide tra chi ha optato per un approccio volontario (15,6%) e chi per quello mandatorio (12,8%).**

Con riguardo ai vantaggi riportati dai rispondenti circa un approccio mandatorio, rileva l'aumento dei livelli di sicurezza dell'intero ecosistema, soprattutto per i settori critici e per quelle infrastrutture con rilevanti impatti per la sicurezza, mentre un approccio volontario potrebbe portare a una riduzione complessiva degli investimenti in cybersicurezza e, di conseguenza, del livello di quest'ultima. Parallelamente, non andrebbero sottostimati i maggiori oneri richiesti in tal caso, in particolar modo per le PMI, per cui – come evidenziato da alcune imprese intervistate – è importante che si accompagnino e supportino gli operatori nel processo di certificazione, affinché si agevoli il più possibile la loro adozione. Per di più, si suggerisce di legare la previsione di schemi di certificazione di prodotto mandatori con la semplificazione della procedura di valutazione del Centro di Valutazione e Certificazione Nazionale (CVCN) in favore dell'operatore che acquisti un prodotto già certificato.

32 Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

Fig. 4.17: In virtù del rilievo che le normative eurounitarie e nazionali sembrano conferire agli schemi europei di certificazione della cybersicurezza, come gli EUCC (es: art. 24 NIS 2; artt. 8 e 27 CRA; art. 6 d.lgs n. 123 del 2022), la sua organizzazione ha già maturato un punto di vista circa i vantaggi/svantaggi di un approccio volontario o mandatorio a tali schemi?

Note: Possibilità di un'unica risposta
Totale rispondenti: 109 su 150
Fonte: Elaborazioni I-Com



Invece, chi ha optato per un approccio volontario, sostiene che uno dei principali vantaggi sta nella flessibilità di scelta in capo alle singole organizzazioni nel definire tipologie e tempistiche circa l'adozione di uno schema di certificazione della cybersicurezza in base alle proprie necessità, risorse e capacità. Inoltre, si segnala anche che non tutte le aziende potrebbero far fronte a un regime mandatorio, in quanto non sussisterebbero le opportune skills per essere compliant.

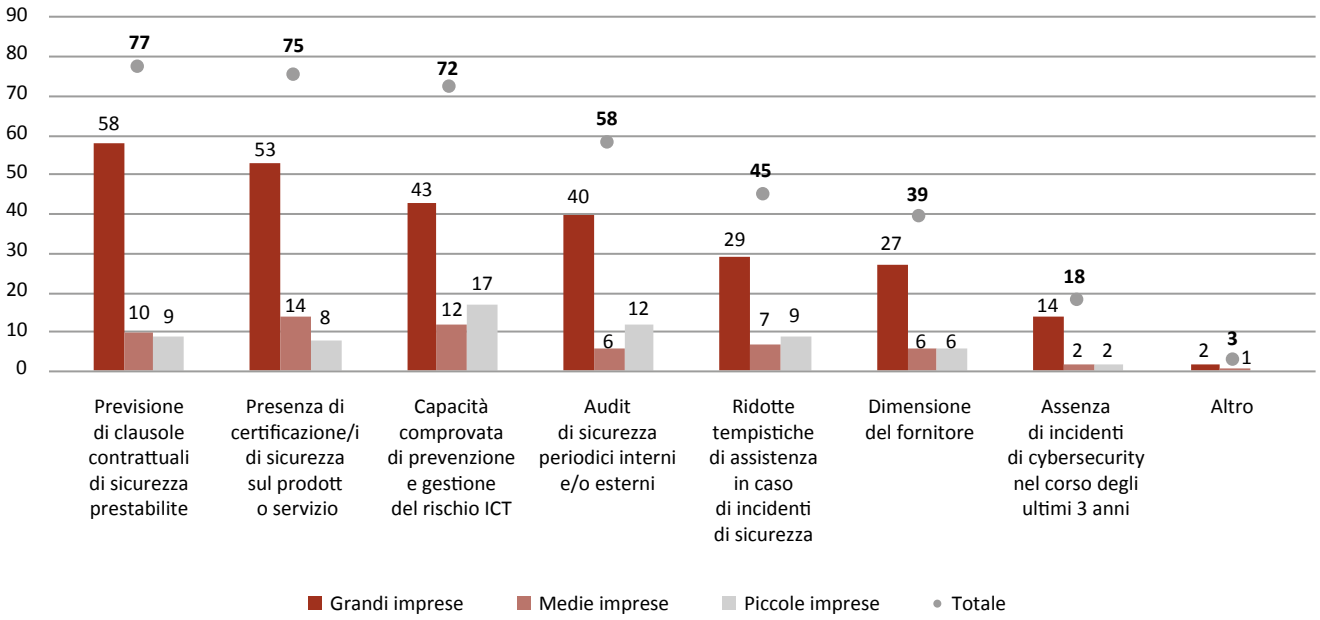
Agli intervistati è stato chiesto altresì di indicare i **principali parametri che prendono in considerazione nella scelta di un fornitore che eroghi servizi o fornisca prodotti Ict** (Fig. 4.18). A riprova dell'importanza della standardizzazione in tale ambito, circa **il 67% dei rispondenti valuta la presenza di certificazioni di sicurezza sul prodotto o servizio (tra grandi e medie imprese si supera il 73%), accanto alla previsione di clausole contrattuali di sicurezza prestabilite (68,7%) e alla capacità comprovata di prevenire e gestire il rischio Ict (64,2%).**

Quest'ultimo aspetto è stato il più selezionato tra le piccole imprese (77,2%). **Il parametro meno considerato in assoluto per la scelta di un fornitore Ict concerne l'assenza di incidenti di cybersecurity nel corso degli ultimi 3 anni (16%).**

L'ultima sezione della presente indagine riguarda più nello specifico alcuni aspetti connessi al PSNC e alle attività del CVCN. Più nel dettaglio (Fig. 4.19), 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 27% dei rispondenti non si rilevano particolari criticità in tal senso, registrando un decremento del 3% rispetto a quanto osservato per il 2023, mentre il 20,7% non ha espresso un'opinione in merito (-2%).**

Fig. 4.18: 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: 112 su 150
Fonte: Elaborazione I-Com



La restante quota di feedback pervenuti evidenzia, invece, alcune problematiche: **43 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 (+9,7% su base annua);** 26 aziende convengono che la necessità di esaminare tali beni Ict nel relativo ambiente operativo determini la ripetizione di test sugli stessi beni (+2,5%); 23 imprese si preoccupano che la parziale incertezza sulle attività di valutazione possa rappresentare un disincentivo dato il rischio reputazionale conseguente a un eventuale ko (+6,2%).

Il grafico successivo (Fig. 4.20) riassume le diverse posizioni dei rispondenti con riferimento a una valutazione complessiva della disciplina sul PSNC. Più nel dettaglio, è possibile osservare come il **21,9% (soprattutto grandi imprese) si ritenga assolutamente soddisfatto dalle regole e dagli adempimenti previsti nell'ambito del Perimetro, percentuale leggermente aumentata rispetto al 2023 (+1,2%)**. Parallelamente, poco più dell'8% nel 2024 e del 10% nell'anno precedente, considera tale normativa come eccessivamente gravosa, recando solo un minimo beneficio per la sicurezza nazionale. Invece, il restante 69,52% (68,8% nel 2023) si colloca nel mezzo. Il maggior numero, 48 imprese (52 nel 2023), 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, **25 rispondenti (21 nel 2023) hanno denunciato che l'approccio adottato impone adempimenti sproporzionati ai soggetti inclusi nel Perimetro.**

Fig. 4.19: Ai sensi della disciplina sul Perimetro di Sicurezza Nazionale Cibernetica il CVCN può prescrivere dei test obbligatori per valutare la sicurezza di beni, sistemi e servizi ICT dei soggetti inseriti nell'ambito del perimetro stesso e vincolarne all'esito l'effettiva possibilità di procedere con gli acquisti. Quale è la vostra attuale percezione?

Note: Possibilità di max. 3 risposte
Totale rispondenti 2024: 111 su 150
Totale rispondenti 2023: 110 su 145
Fonte: Elaborazione I-Com

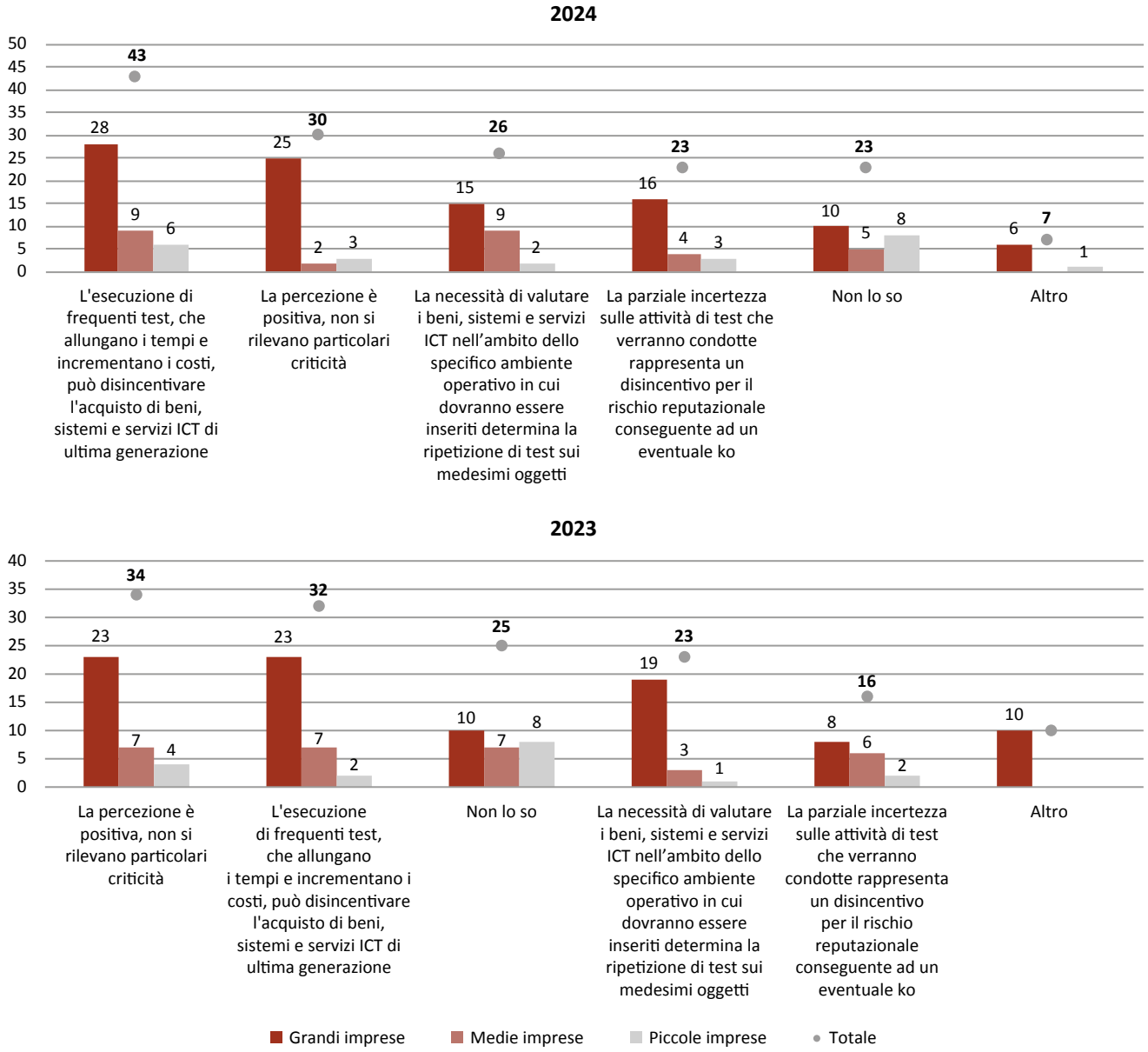
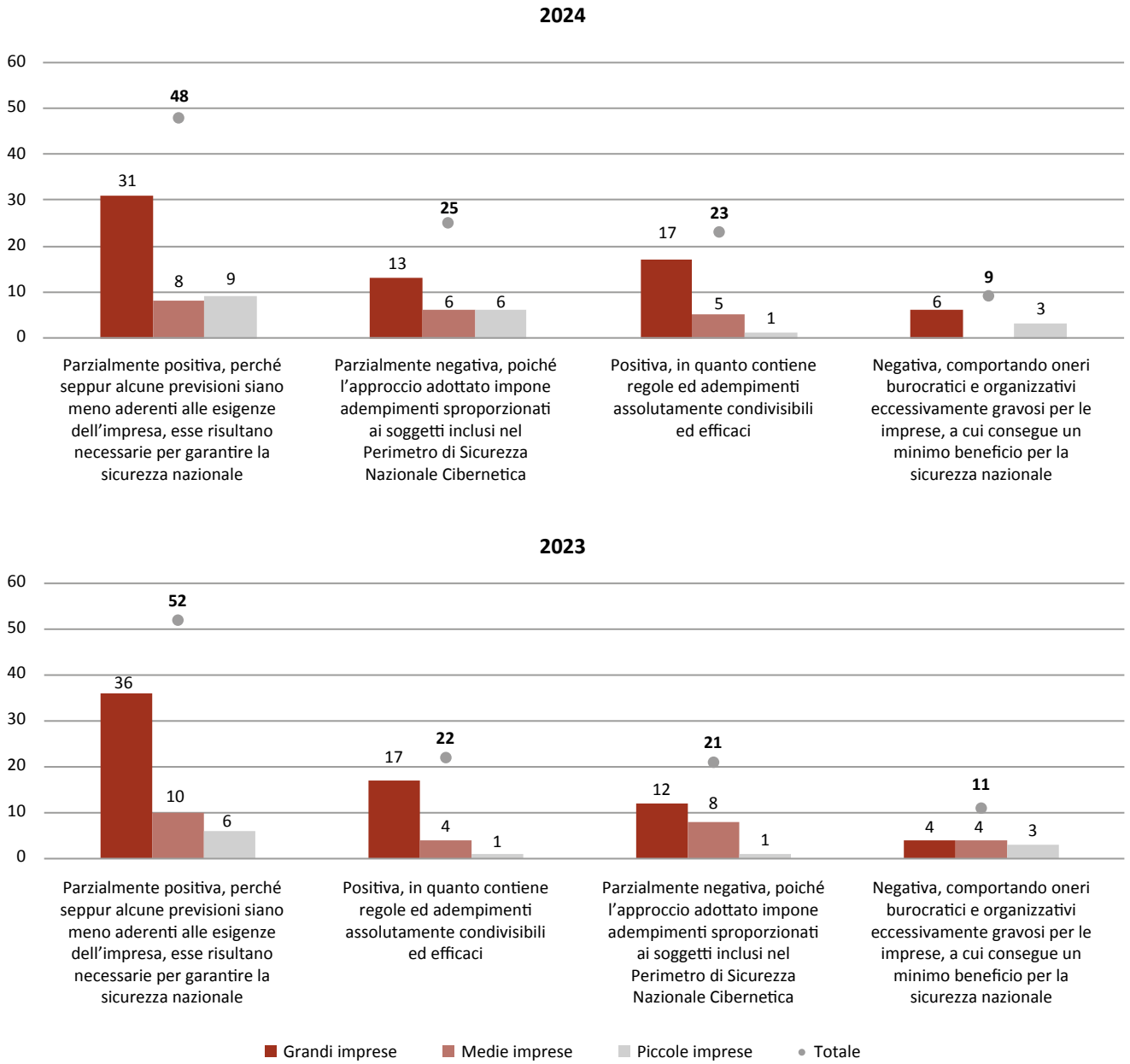


Fig. 4.20: La disciplina sul perimetro di sicurezza nazionale cibernetica è ormai giunta a completamento e sono partite le attività del CVCN, in attesa dell'accreditamento dei LAP. Qual è la vostra percezione attuale?

Note: Possibilità di un'unica risposta
Totale rispondenti 2024: 105 su 150
Totale rispondenti 2023: 106 su 145
Fonte: Elaborazione I-Com

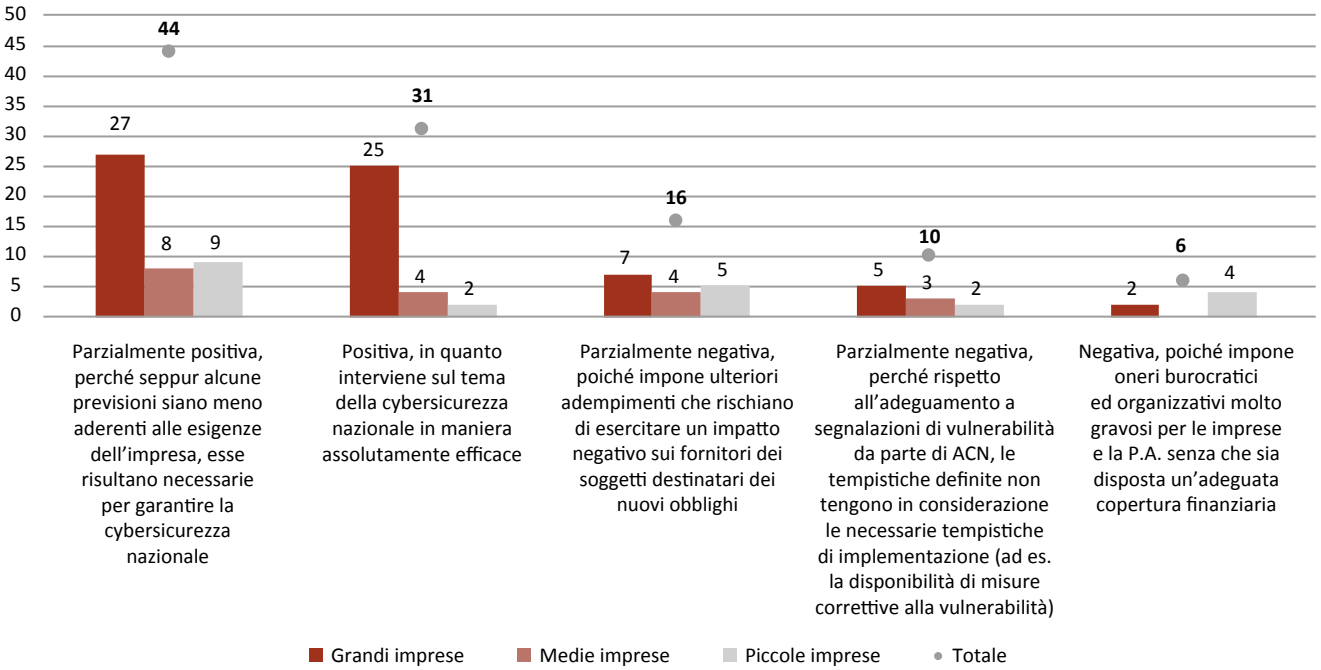


Un ulteriore quesito ha posto luce sul punto di vista delle imprese circa la l. n. 90/2024 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" che si rivolge anche a un'ampia platea di soggetti privati, tra cui quelli già sottoposti ad altre discipline[33] (Fig. 4.21). In particolare, si rileva **che quasi il 29% delle aziende ha dichiarato parere positivo, in quanto la normativa interviene sul tema della cybersicurezza nazionale in maniera assolutamente efficace.**

Diversamente**, il 5,61% dei rispondenti mostra una valutazione negativa, in virtù della previsione di oneri burocratici ed organizzativi molto gravosi, aggravati dalla clausola di invarianza finanziaria**. **Circa il 65% degli intervistati ha fornito risposte intermedie.** Più nel dettaglio, una prevalenza significativa (44 organizzazioni) sostiene che l'effetto della disciplina in questione sia parzialmente positivo, perché seppur alcune previsioni siano meno aderenti alle esigenze dell'impresa, esse risultano necessarie per garantire la cybersicurezza nazionale, mentre 26 imprese hanno dato parere parzialmente negativo, considerando che la normativa impone ulteriori adempimenti che rischiano di essere sfavorevoli per i fornitori dei

Fig. 4.21: La normativa recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" si rivolge anche a un'ampia platea di soggetti privati, tra cui quelli già sottoposti ad altre discipline (es: Perimetro di Sicurezza Nazionale Cibernetica, direttiva NIS2, Codice delle Comunicazioni Elettroniche). Qual è la vostra percezione sull'impianto normativo in questione?

Note: Possibilità di un'unica risposta
Totale rispondenti: 107 su 150
Fonte: Elaborazione I-Com



33 Si v. supra, par. 2.2.1.

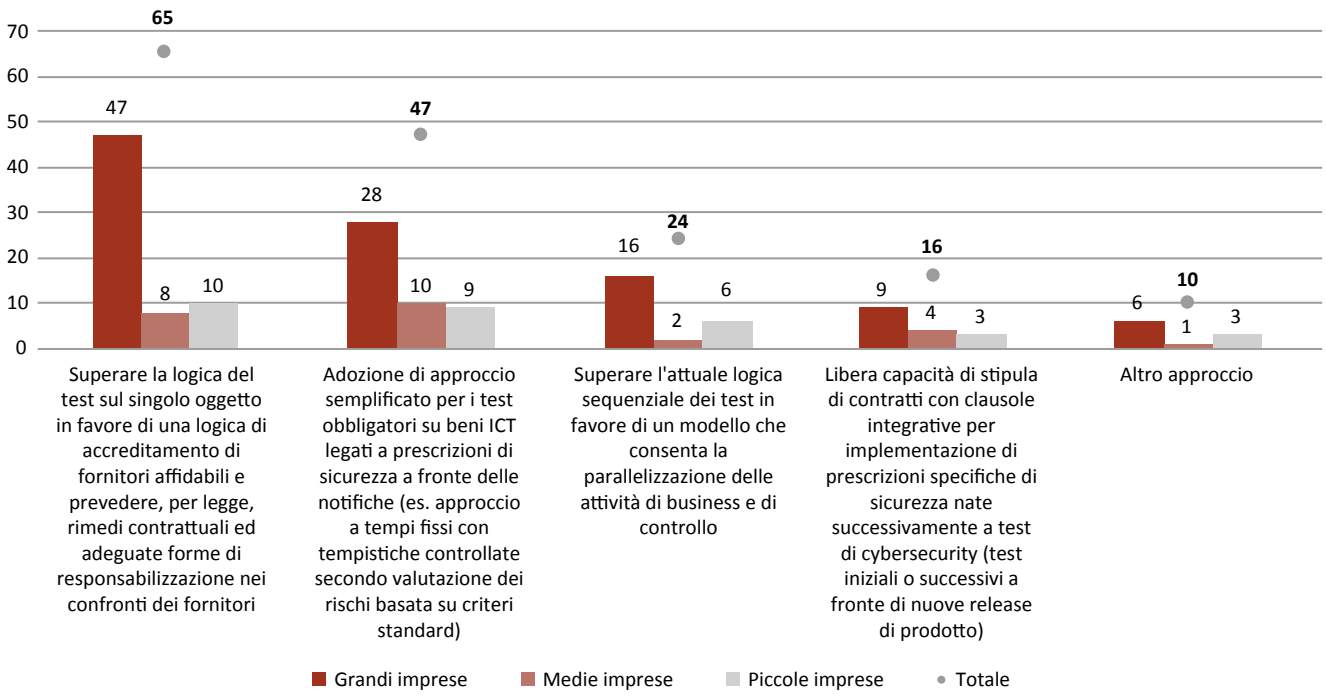
soggetti destinatari dei nuovi obblighi (16) e perché rispetto all'adeguamento a segnalazioni di vulnerabilità da parte di ACN, le tempistiche definite non tengono in adeguata considerazione le necessarie tempistiche di implementazione (10).

L'ultima domanda del questionario richiede agli intervistati di proporre alcuni aspetti su cui insistere per migliorare l'ecosistema della cibersicurezza in Italia (Fig. 4.22). Sul punto**, il 60,75% dei rispondenti ritiene 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 (+4,5% su base annua). 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 il 44%, di cui ben 19 PMI.**

Con riguardo agli altri approcci proposti dalle imprese intervistate, pare opportuno fare riferimento all'armonizzazione dei requisiti delle normative in materia di cybersicurezza, a un più ampio utilizzo delle certificazioni a norma del Cybersecurity Act, prevedendo, fra l'altro, la semplificazione della procedura di valutazione dinanzi al CVCN, oltre che a una maggiore standardizzazione in ogni ambito legato alla cibersicurezza, attribuendo specifici punteggi per una valutazione più agevole. Inoltre, è stata proposta da diversi rispondenti l'introduzione nelle scuole dell'educazione "*cybernetica*", vista come evoluzione di quella civica.

Fig. 4.22: Quali ulteriori aspetti andrebbero considerati per migliorare lo stato della cybersecurity in Italia?

Note: Possibilità di più risposte
Totale rispondenti: 107 su 150
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 – giunta alla seconda edizione – 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 investimenti tecnico-organizzativi necessari alla compliance**, nonché per la numerosità degli oneri burocratici e amministrativi richiesti, oltre che per l'innalzamento delle barriere all'ingresso, soprattutto per le PMI, il che può avere ripercussioni anche sui rapporti con la supply chain (+5,2% sul 2023), con l'ulteriore conseguenza – evidenziata dal 22,9% dei rispondenti (+7,7%) – 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** (66 risposte in totale), seguita dalla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (63 risposte) e dall'incertezza interpretativa della normativa (54 risposte). Peraltro, alcune imprese hanno posto l'attenzione sugli standard che richiedono modelli di *assessment* differenti con inevitabili ripercussioni sulla gestione dei relativi piani di *improvement*.
Altro dato di fondamentale rilievo riguarda le risorse economiche dedicate specificamente alla cybersicurezza, per cui è emerso che **il maggior numero dei rispondenti assegna meno del 3% del budget IT alla cybersecurity, mentre solo 10 soggetti (di cui 4 grandi imprese) vi allocano più del 15% del budget IT a disposizione**. Inoltre, appare rilevante evidenziare che, mentre nella precedente rilevazione circa il 57% delle piccole imprese riconosceva una quota di personale appositamente dedicato alla cyber uguale o inferiore all'1% rispetto agli FTE impiegati in ambito IT, nella presente edizione della survey questo valore si è notevolmente abbassato al 15%.
Per di più, nonostante lo scenario non sia propriamente ottimistico e considerando che le direttive NIS2 e CER saranno applicabili a breve (dal 18 ottobre 2024), **il 42% delle imprese rispondenti sta ancora valutando se incrementare le risorse destinate alla cibersicurezza e solo un mero 25,4% ha già deciso di aumentare gli investimenti in cybersicurezza**, un valore dell'11% più basso su base annua.
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, parimenti a quanto registrato nel 2023**. Ad ogni modo, tra le imprese che hanno adottato almeno uno standard di questo tipo quasi tutte hanno optato per la famiglia delle ISO27000. Simili risultanze sarebbero giustificate – secondo il 35% 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 (19%).
Piuttosto rilevante sul punto è il segnale lanciato da alcuni soggetti intervistati, per cui **un ridotto ricorso**

a tali strumenti sarebbe influenzato dalla scarsità di risorse – umane e finanziarie – da dedicare al processo di certificazione. Appare incoraggiante, invece, che **il 74,5% dei rispondenti sia d'accordo in merito al fatto che standard comunitari (es. EUCC) possono incentivare le imprese a certificarsi, segnando un incremento del 4,5% sul 2023**, e che siano diminuiti dell'11% i soggetti silenti sul tema. Peraltro, nella scelta di un fornitore che eroghi servizi o fornisca prodotti ICT circa il 67% dei rispondenti valuta la presenza di certificazioni di sicurezza sul prodotto o servizio e tra grandi e imprese si supera addirittura il 73%.

Nonostante lo scorso 31 gennaio sia stato adottato il Regolamento di esecuzione con cui gli EUCC sono diventati ufficialmente parte della legislazione europea e che diverse normative, europee e nazionali (da ultimo, il decreto NIS2), contemplano la possibilità di rendere mandatoria la certificazione di cibersicurezza per determinati prodotti, servizi e processi ICT, **oltre il 70% dei rispondenti non ha ancora avviato (o, in alcuni casi, portato a termine) la valutazione sui vantaggi/svantaggi circa la volontarietà o l'obbligatorietà di tali strumenti.**

Ad ogni modo, 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 PSNC 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 anche nel 2023, a conferma del fatto che si tratti di un aspetto particolarmente sentito nel Paese.

Con riguardo alla seconda domanda in tema, partendo dal presupposto che poco meno del 22% 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 60,7% 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 (+4,5% su base annua), 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 la necessità di **armonizzare il più possibile i requisiti delle diverse normative UE e nazionali in materia di cybersicurezza.** Meritevole di attenzione anche il riferimento a incentivare l'utilizzo di certificazioni ai sensi del Cybersecurity Act, prevedendo, fra l'altro, la semplificazione della procedura di valutazione dinanzi al CVCN. Inoltre, è stata proposta da diversi rispondenti l'introduzione dell'educazione "cybernetica" nelle scuole, vista come naturale evoluzione di quella civica.

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 2005 25
istituto per la competitività

CAPITOLO 5

L'IMPORTANZA DELLA CONSAPEVOLEZZA E DELLA FORMAZIONE IN CIBERSICUREZZA NEL CONTESTO NAZIONALE

5.1. LA CYBERSICUREZZA PER I CITTADINI E LE IMPRESE: LO STATO DELL'ARTE

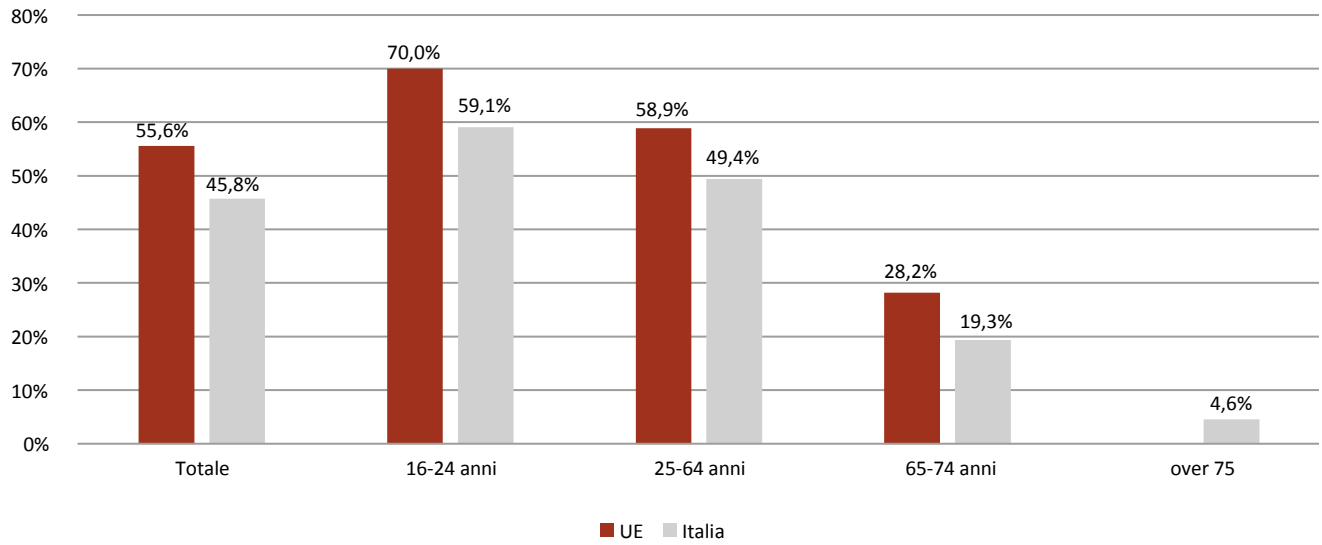
Uno degli elementi strategici da cui passa la lotta al cybercrimine è certamente il livello di competenze in campo digitale dei cittadini. L'ultima rilevazione Eurostat (risalente al 2023) ci dà modo di ragionare sulla situazione in essere nel campo in questione, restituendoci **un quadro certamente non confortante né per l'Europa, né tantomeno per l'Italia** (Fig. 5.1). **Nel nostro continente è infatti ancora esigua la fetta di popolazione provvista delle capacità digitali anche solamente ad un livello considerato basico (55,6%).** Analizzando la popolazione per categorie anagrafiche vediamo, come prevedibile, una notevole differenza tra le varie classi d'età. Mentre i giovani (età compresa tra i 16 e i 24) appaiono essere al passo con la transizione digitale (dato pari al 70%), lo stesso non si può concludere a proposito delle fasce più adulte della popolazione. **Solamente il 28,2% delle persone con età tra i 65 e 74 anni in UE possiede competenze digitali almeno di base**, lasciando spazi ad ovvie considerazioni in tema di elevata esposizione ai pericoli del cybercrime.

Le statistiche sulle competenze digitali appaiono ancor più negative se guardiamo alla situazione italiana. Il dato relativo alla popolazione complessiva con competenze almeno di base si attesta al **45,8%**, ed anche quelli suddivisi per classe d'età risultano tutti al di sotto delle medie europee.

Gli stessi dati Eurostat suggeriscono **un grave problema di fiducia della popolazione europea verso l'*Internet of things*** (Fig. 5.2). **Uno dei principali timori dei cittadini del vecchio continente nell'utilizzo delle tecnologie IoT è proprio legato ai problemi di sicurezza**. In particolare, **in Europa quasi il 7% dei cittadini è restio all'utilizzo di dispositivi IoT per paura**, dato perlopiù determinato dalla popolazione in età adulta. Infatti, se da un lato solamente 5% dei giovani ha sollevato questa perplessità, il dato sale a poco più del 7% per i cittadini compresi nella fascia 25-64 anni e 65-74.

Fig. 5.1: Quota di individui con competenze digitali almeno di base (2023)

Fonte: Eurostat
Note: Dato europeo mancante per gli over 75



L'Italia, oltre ad apparire indietro rispetto alla media UE nel campo delle competenze digitali, mostra anche **meno contezza dei possibili rischi che la navigazione in rete può provocare**. Il dato italiano è pari solamente all'1,1% aggregando la totalità della popolazione, mentre scende addirittura allo 0,6% per i giovani, per poi riaumentare, seppur in maniera impercettibile, per le fasce più adulte. Quanto detto denota un'evidente **carenza strutturale della percezione verso i pericoli della rete anche tra i più giovani**, che ci sembra ragionevole attribuire in particolar modo ad uno **scarso livello di sensibilizzazione verso tematiche simili**, che dovrebbe partire sin da dentro le scuole già dai primi anni di istruzione dei giovani.

Fig. 5.2: Quota di individui che non utilizza l'*Internet of things* per timori legati alla sicurezza (2024)

Fonte: Eurostat
Note: Dato europeo mancante per gli over 75

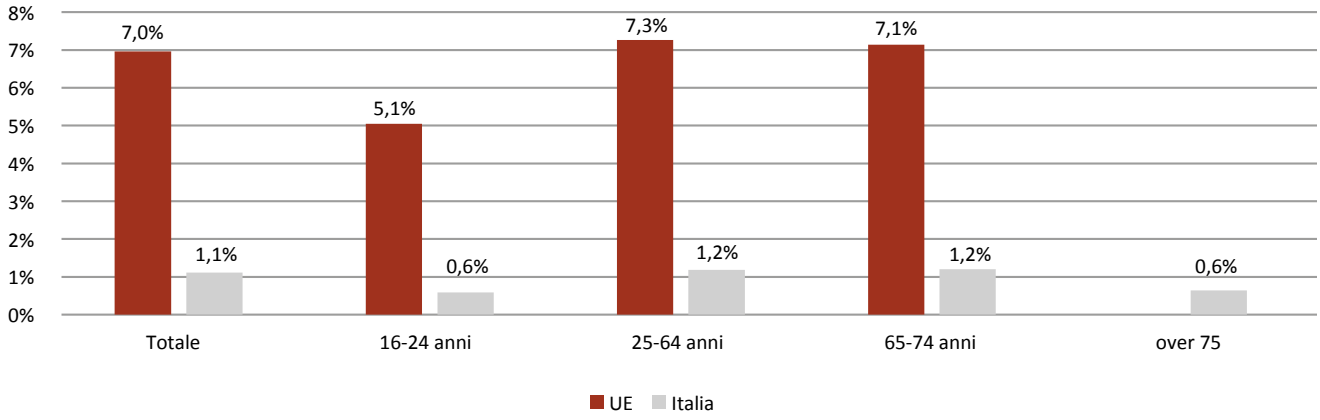
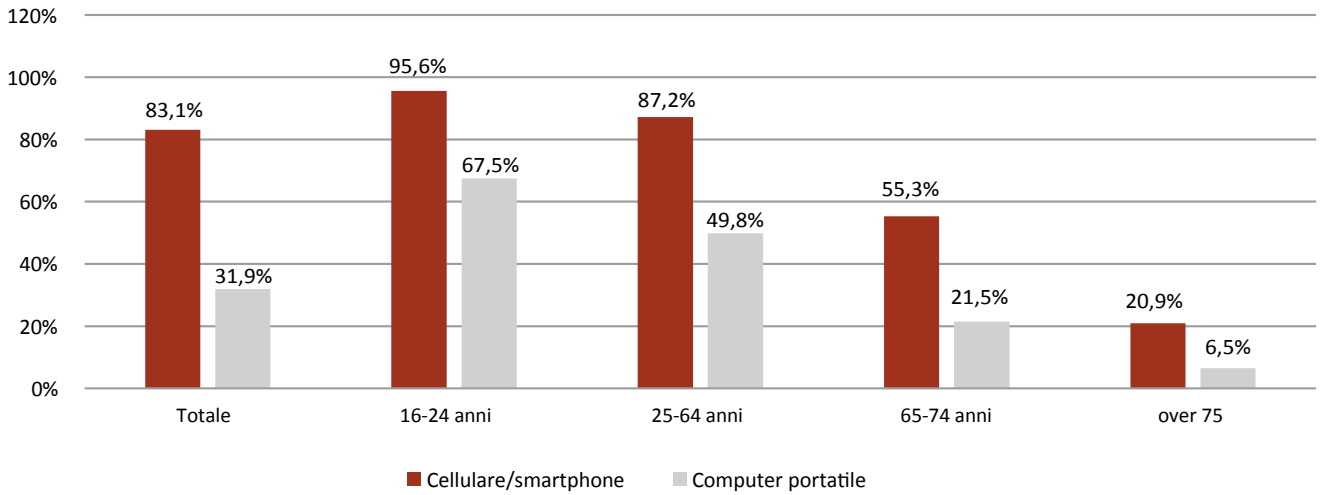


Fig. 5.3: Quota di individui per tipo di dispositivo utilizzato per l'accesso ad Internet in Italia (2023)

Fonte: Eurostat



Un'ulteriore fonte di preoccupazione deriva dal fatto che, a differenza del PC, sia in Italia che in Europa **la quota di individui che utilizza lo smartphone per accedere al web è ben più elevata rispetto alla popolazione con competenze digitali almeno di base. Scarse competenze si traducono inevitabilmente in una maggior vulnerabilità alle minacce informatiche.** A tal proposito, i dati derivanti dall'ultimo resoconto sulle attività effettuate dalla polizia Postale forniscono ulteriore concretezza a quest'ipotesi (Fig. 5.4). **Nel 2024 è stato registrato un aumento delle attività fraudolente perpetrate in rete. Ciò è vero tanto in merito al numero di casi trattati (+2389 rispetto al 2023), quanto in relazione all'ammontare delle somme sottratte, che è passato dai circa 137 milioni di euro del 2023 ai 181 milioni del 2024**. Tali dati sottolineano l'urgenza di un deciso cambio di rotta in merito al binomio competenze/consapevolezza dei cittadini italiani in campo digitale.

Destinatari dei possibili rischi derivanti dall'intenso utilizzo degli strumenti digitali non sono solamente i cittadini, bensì anche **le imprese**. Per tale ragione, queste ultime stanno da tempo investendo ingenti risorse per dotare i propri addetti delle adeguate competenze per un idoneo utilizzo degli strumenti ICT.

Tuttavia, effettuando un confronto dal 2016 in poi (Fig. 5.5), anche in questo caso l'Italia, nonostante i miglioramenti registrati su base annua, soffre il confronto con l'Europa. Basti pensare che **nel 2024 solamente il 17.85% delle imprese con più di 10 addetti hanno erogato formazione in ambito digitale, a fronte di un dato europeo di circa il 22.27%**.

Peraltro, la situazione non cambia se si considerano gli investimenti destinati alla formazione del personale specializzato in ICT/IT (dato europeo del 11.40% contro uno nazionale del circa 7% nel 2024).

Nonostante ciò, secondo gli ultimi aggiornamenti Eurostat (Fig. 5.6), anche nel 2024 le imprese italiane sono state **meno soggette ad incidenti di sicurezza che hanno causato l'interruzione dei servizi (dato europeo del 20,1% contro uno italiano del 14,4%**) rispetto alla media UE.

Questo lascia ben sperare circa la preparazione del personale e dei sistemi di sicurezza delle imprese ICT italiane nel fronteggiare importanti problemi di cyberiscurezza, facendo allo stesso tempo auspicare nuovi sforzi futuri per aumentare detta resilienza.

Fig. 5.4: Numero di casi trattati e somme sottratte (in milioni di euro) in relazione alle truffe online in Italia (2023-2024)

Fonte: Resoconto attività 2024 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica

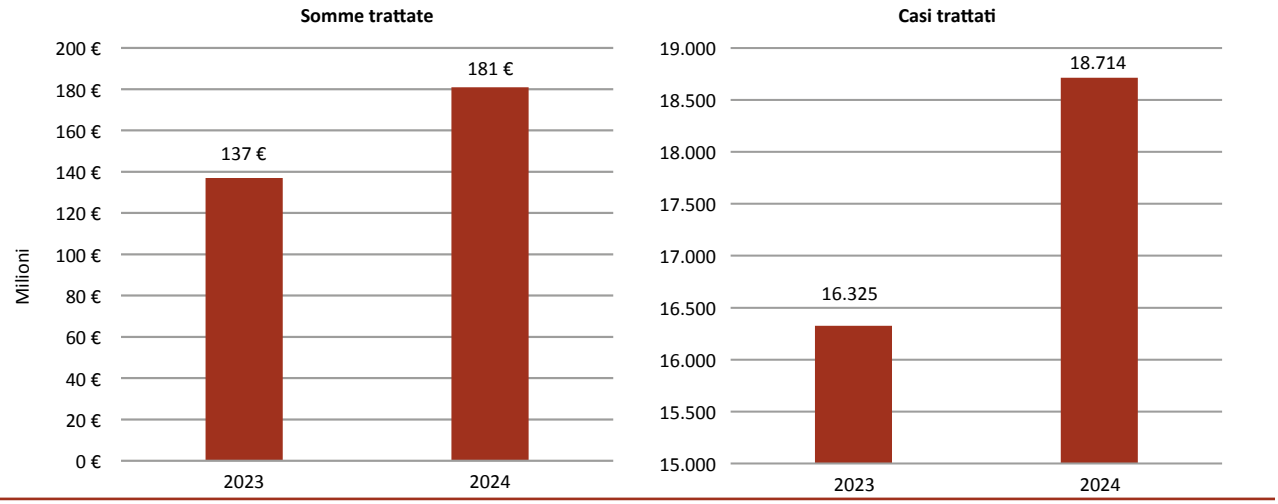


Fig. 5.5: Formazione erogata in materia ICT da imprese con più di 10 addetti (2016-2024)

Fonte: Eurostat
Note: I dati riferiti all'anno 2021 e 2023 non sono stati pubblicati nel database di Eurostat

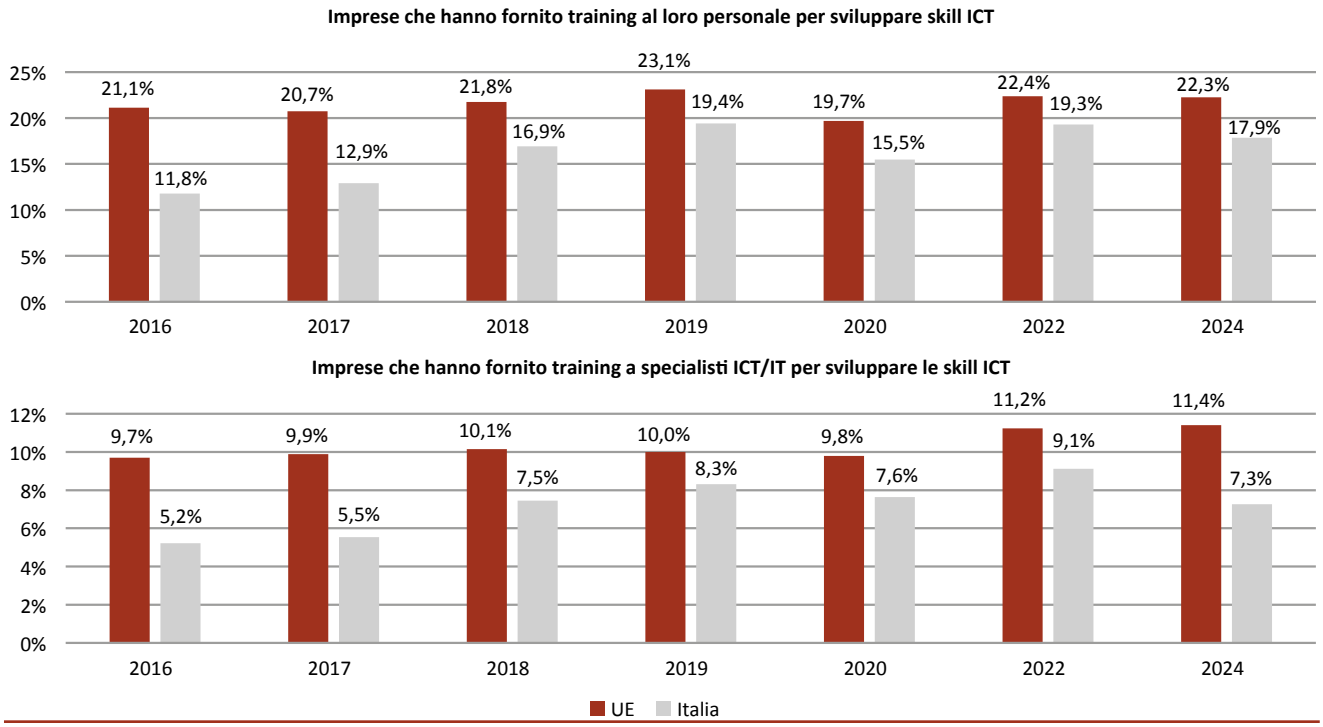


Fig. 5.6: Quota di imprese con più di 10 addetti che hanno subito un incidente di sicurezza che ha causato l'interruzione dei servizi ICT (2024)

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

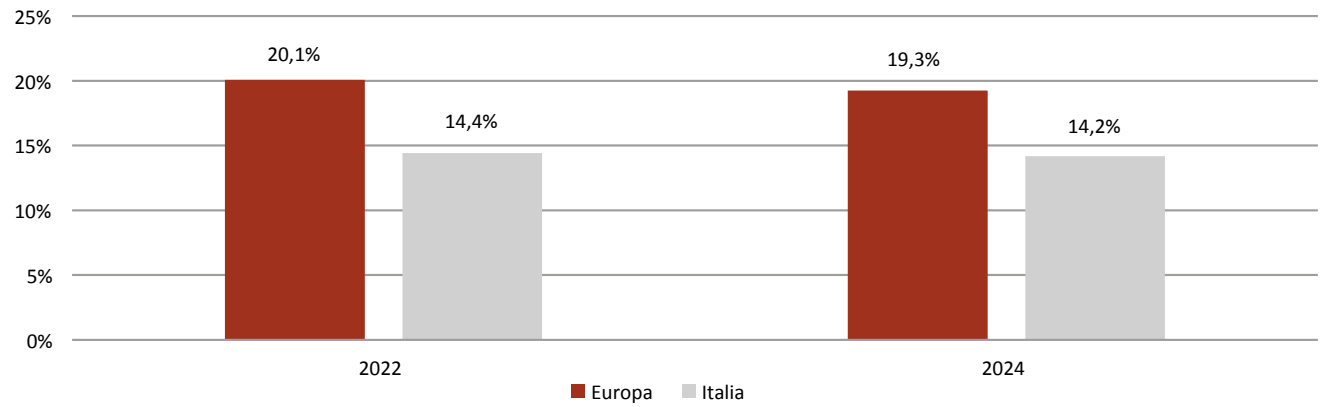
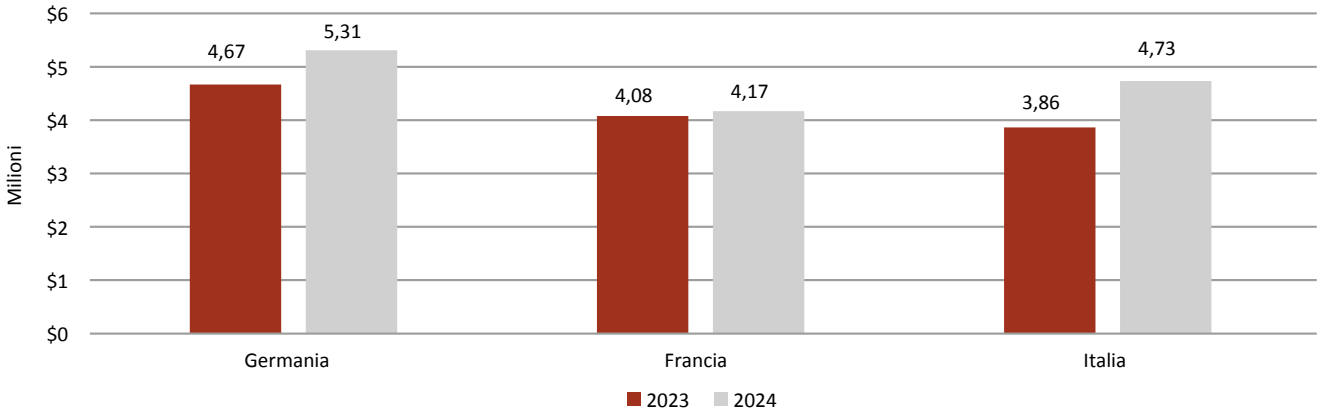


Fig. 5.7: Costo medio di una violazione di dati per Paese (in $ milioni)

Fonte: IBM Security, Cost of a Data Breach Report 2024



Un ultimo aspetto rilevante da considerare è il **costo medio derivante da una violazione dei dati**, dal momento che proprio questi ultimi, vista la crescente importanza che stanno acquisendo, sono ormai tra i bersagli prediletti dagli attacchi di cybersicurezza (Fig. 5.7). L'ultimo rapporto "IBM security, cost of a data brech report" contiene statistiche aggiornate al 2024 proprio su questo argomento. In particolare, **l'Italia è quinta tra i Paesi considerati dallo studio, con un costo medio per singolo data breach di circa cinque milioni di dollari**. Sono invece gli Stati Uniti a capeggiare la classifica, con un dato pari 9,4 milioni di dollari, il che certamente non stupisce data l'immenso bacino di dati presente negli USA. A livello europeo, gli altri due Paesi presenti nello studio, ovvero Germania e Francia, presentano una dinamica tra il 2023 ed il 2024 sostanzialmente rassomigliante quella italiana. In particolare, tutti questi Paesi hanno visto aumentare il costo medio derivante da una violazione di dati. Andando più nel dettaglio, **tra i tre è stato proprio il nostro Paese a far registrare l'incremento più marcato**, anche se il dato tedesco in valore assoluto rimane ancora superiore, essendosi attestato nel 2024 ad un valore pari a 5,3 milioni di dollari.

5.2. L'OFFERTA FORMATIVA NAZIONALE IN MATERIA DI CIBERSICUREZZA

5.2.1. 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 2024/2025, si registra la presenza di **774 corsi di formazione universitaria**, **in notevole crescita rispetto ai 520 individuati a inizio 2024, il che fa segnare un incremento di circa il 48% su base annua**. I corsi analizzati includono sia insegnamenti singoli all'interno di corsi di laurea più generici[34] ("**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. 5.8), 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 2024/2025 un totale di 774 unità tra insegnamenti e corsi di studio sulla

34 Esempio: un insegnamento in Cybersecurity all'interno della LM in Informatica.

cybersecurity. Tra questi, sono stati osservati 323 insegnamenti singoli all'interno di corsi di laurea magistrale, 158 insegnamenti singoli all'interno delle lauree triennali, **86 progetti di ricerca in dottorati**, 69 corsi singoli in master di II livello e 54 in master di I livello, a fronte di **31 lauree magistrali**, **30 master**, 16 corsi all'interno di dottorati di ricerca, 11 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 lauree 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 abbiano raggiunto le 38 unità**. Tuttavia, queste appaiono ancora **relativamente poche e quasi tutte collocate, salvo rare eccezioni (7), 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 a 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 116 corsi "specializzati" tra master e progetti di ricerca in dottorati** a fronte delle 38 tra lauree triennali e biennali dedicate. Pertanto, è importante notare come **la formazione specializzata in materia di cibersicurezza in Italia abbia raggiunto quota 154 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. 5.9), con una forte concentrazione nel **Lazio** (180 corsi), in **Lombardia** (119) e in

Fig. 5.8: Offerta formativa specializzata e non specializzata in materia di cybersecurity per tipo (a.a. 2024-25 vs a.a. 2023-2024)

Fonte: I-Com, gennaio 2025

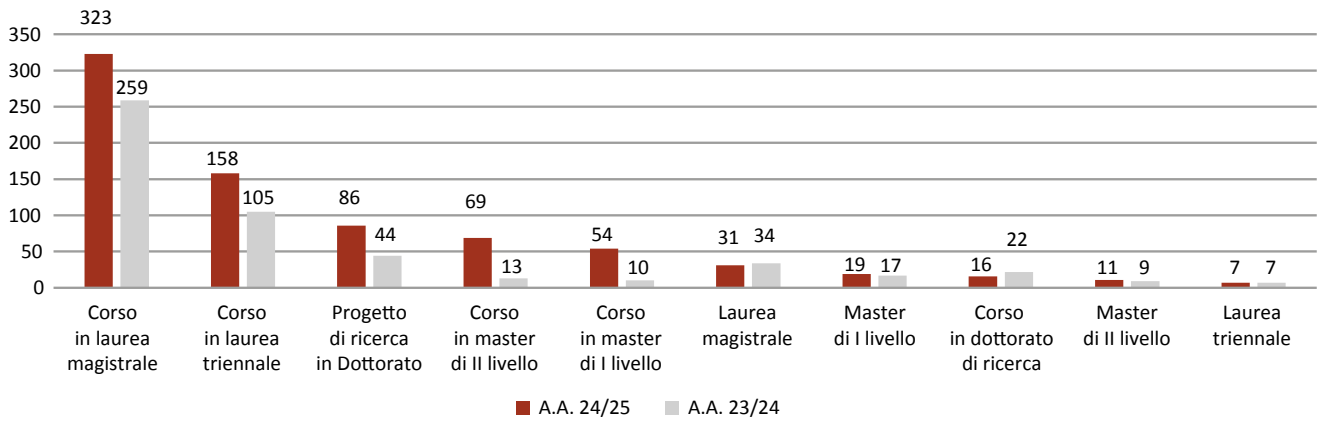
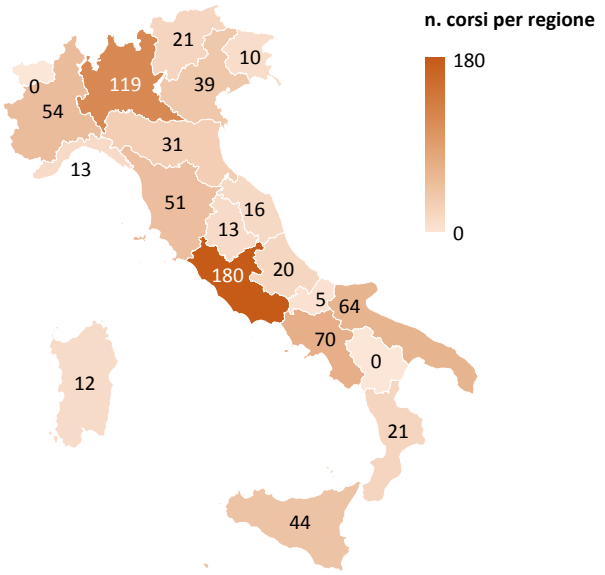


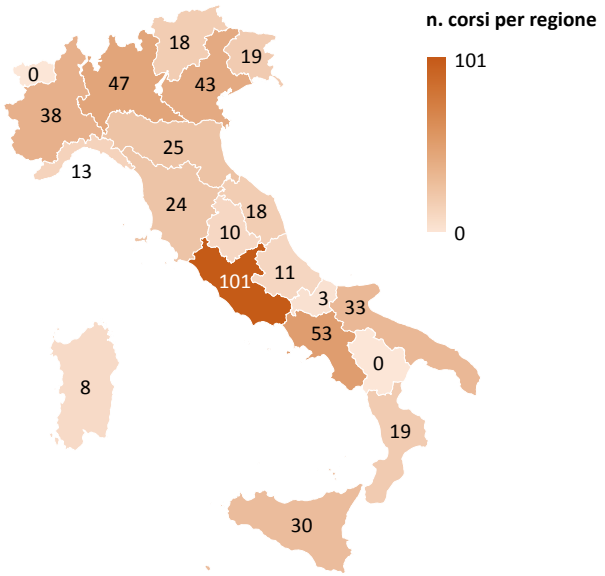
Fig. 5.9: Offerta formativa sulla cybersecurity per regione (a.a. 2024-25 vs a.a. 2023-2024)

Fonte: I-Com, gennaio 2025

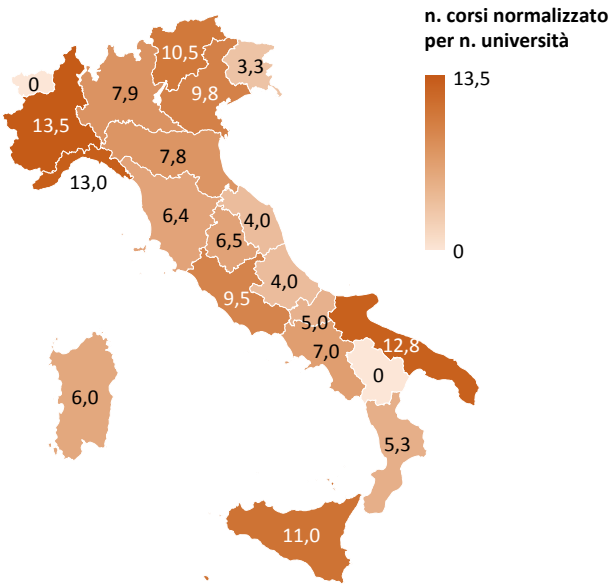
N. corsi e insegnamenti per regione (A.A. 24/25)



N. corsi e insegnamenti per regione (A.A. 23/24)



N. corsi e insegn. normalizzati per n. di università per regione (A.A. 24/25)



N. corsi e insegn. normalizzati per n. di università per regione (A.A. 23/24)

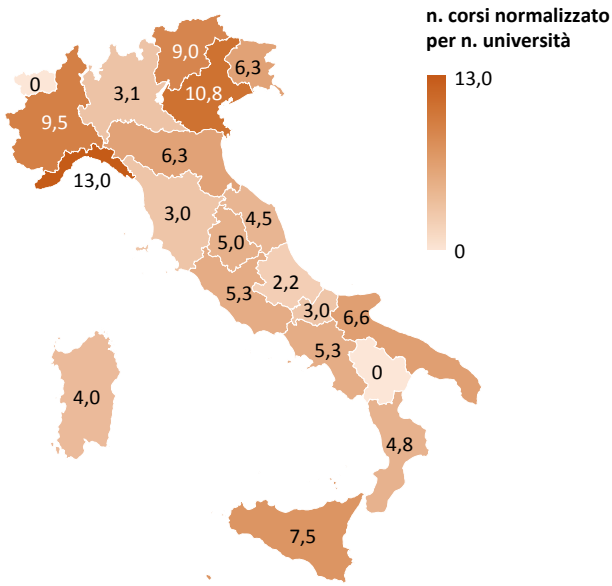
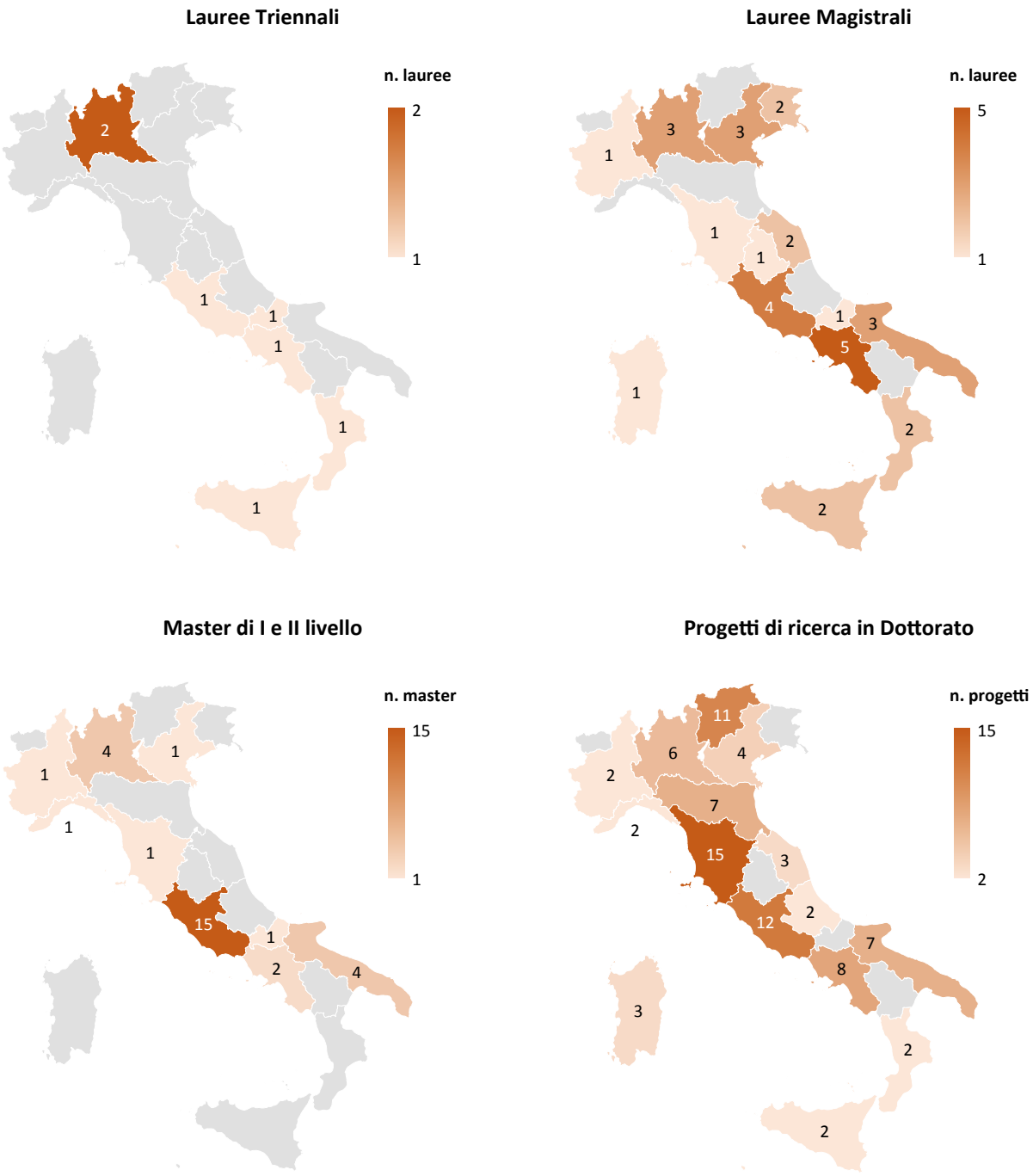


Fig. 5.10: Offerta formativa specializzata sulla cybersecurity per regione (a.a. 2024-25)

Fonte: I-Com, gennaio 2025



Campania (70), seguite da Puglia (64) e Toscana (51). Il Piemonte, in particolare, risulta nettamente primo in termini di corsi in cybersecurity normalizzati per il numero di università presenti sul territorio regionale (con un rapporto di 13,5:1), seguita da Liguria (13:1) e Puglia (12,8:1). **A livello regionale, a gennaio 2025 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere**.

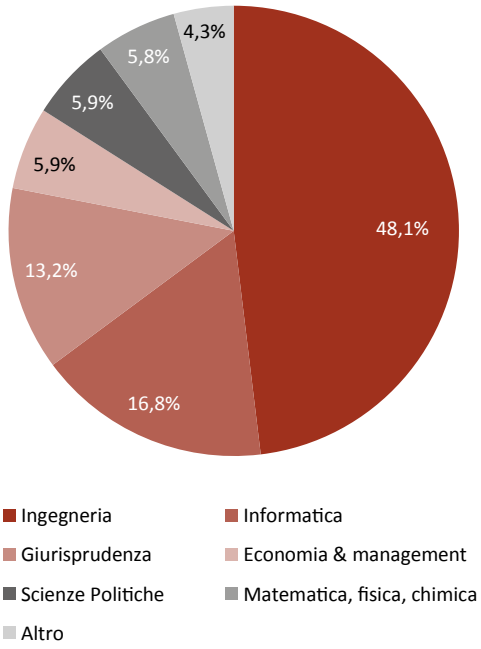
Analizzando **la distribuzione geografica e universitaria dell'offerta formativa specializzata** (Fig. 5.10), **ossia quella che comprende corsi di studi interamente dedicati alla cybersecurity, il Lazio si conferma la regione più interessata con 32 percorsi complessivi**, catalizzando ben 5 tra lauree magistrali e triennali dedicate. Per quanto concerne la specializzazione post-laurea, invece, nel Lazio si registrano 12 progetti di ricerca in dottorato e 15 master, seguito da Toscana (15 progetti di ricerca in dottorato e 1 master) e Puglia (7 progetti di ricerca in dottorato e 4 master) a pari merito col Trentino Alto-Adige (11 progetti di ricerca in dottorato), mentre chiudono la classifica Abruzzo, Calabria, Sicilia (ciascuno con 2 progetti di ricerca) e Molise con 1 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 30 - **19 di I Livello e ulteriori 11 di II Livello** - di cui **15 con sede nel Lazio**. Complessivamente, l'alto numero di Master sembrerebbe suggerire **un'elevata domanda di approfondimento post-laurea su questi temi**, probabilmente dovuta a un mismatch - sebbene in progressiva riduzione - tra domanda e offerta di tali competenze sul mercato del lavoro e alla diffusione della consapevolezza che tali conoscenze possano costituire un valore aggiunto nel mondo del lavoro.

Analizzando **il numero di insegnamenti o corsi di studio sulla cybersicurezza divisi per dipartimento** (Fig. 5.11), si osserva come quasi la metà di essi faccia capo a **dipartimenti di ingegneria (48,1%)**, ovverosia il triplo di quelli offerti dal **dipartimento di informatica (16,8%)**. **Poco più del 13% del totale fa capo al dipartimento di giurisprudenza** (o scienze giuridiche), seguito dai dipartimenti di **economia & management e scienze politiche, entrambi al 5,9%**, e dai dipartimenti di **matematica, fisica e chimica (5,8%)**.

Fig. 5.11: Offerta formativa sulla cybersecurity per dipartimento (a.a. 2024-25)

Note: non è stato possibile individuare o recuperare il dipartimento di afferenza per tutti i corsi o insegnamenti.
Fonte: I-Com, gennaio 2025



5.2.2. La sicurezza informatica nei corsi ITS

Il Ministero dell'Istruzione definisce gli **Istituti Tecnici Superiori (ITS)** 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 - Turismo**, **Tecnologie della informazione e della comunicazione**. Il portale online curato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE) evidenzia che sul territorio nazionale risultano presenti **147 ITS** (Fig. 5.12)[35]. **La regione che ospita il numero maggiore di istituti è la Lombardia (25)**, 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, il Molise e l'Umbria si limitano a un solo istituto.

La costante diffusione degli ITS registratasi negli ultimi anni 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

Fig. 5.12: Distribuzione degli ITS per regione

Fonte: INDIRE (ultima consultazione: 17/01/2025)

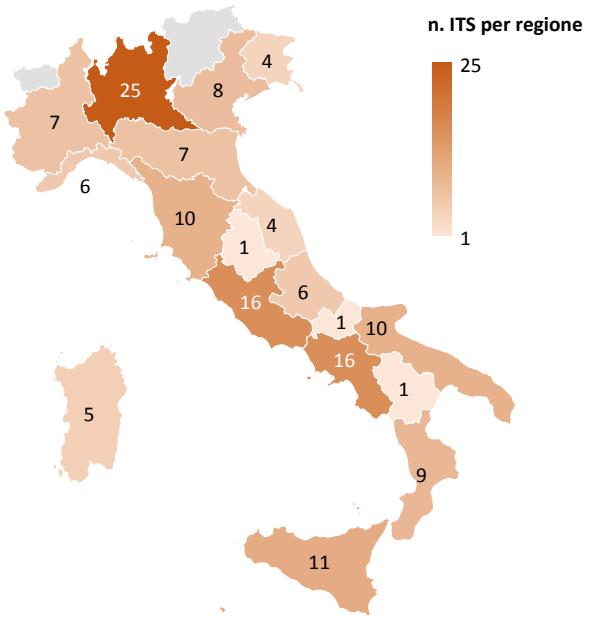
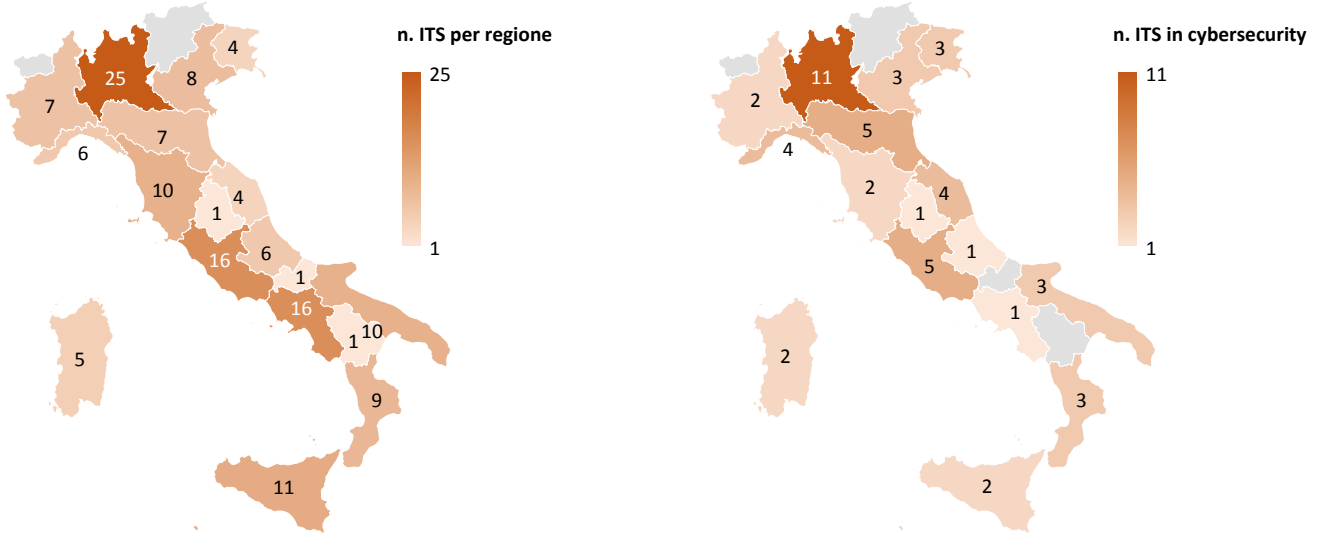


Fig. 5.13: Comparazione tra il numero di ITS per regione e ITS che si occupano di Cybersecurity

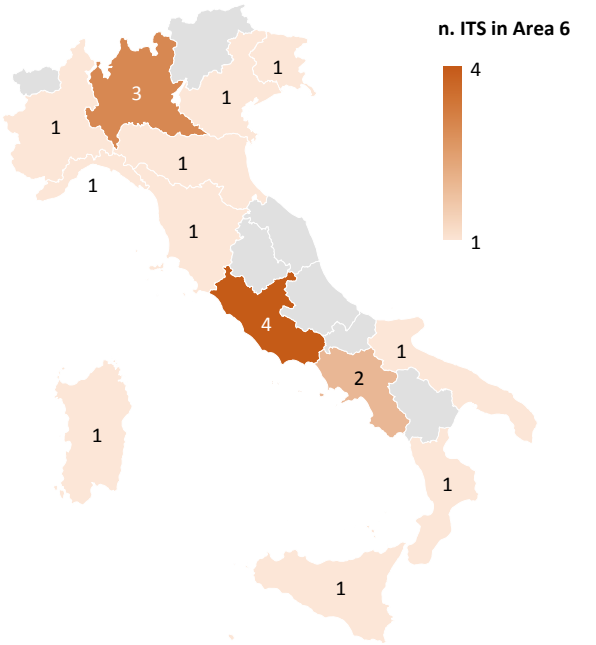
Fonte: INDIRE (ultima consultazione: 17/01/2025); I-Com (gennaio 2025)



35 Il portale di INDIRE è disponibile al seguente indirizzo: https://www.indire.it/progetto/its-istituti-tecnologici-superiori/dove-sono-gli-its/ (ultima consultazione 17/01/2025).

Fig. 5.14: Numero degli ITS collocati nell'area 6 (Tecnologie dell'informazione e della comunicazione)

Fonte: INDIRE (ultima consultazione: 17/01/2025)



di offrire curricula in cybersecurity al fine di formare i nuovi esperti del settore. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-Com (Fig. 5.13), **gli ITS che si occupano di cybersicurezza sono il 35,4% rispetto al numero complessivo di quelli attivi, una quota più che raddoppiata rispetto alla rilevazione precedente effettuata a inizio 2024**. La **Lombardia** primeggia con 11 istituti su 25 totali, seguita dall'**Emilia-Romagna** (5 su 7) e dal **Lazio** (5 su 16). Viceversa, l'Abruzzo e la Campania registrano un solo istituto ciascuno che si occupa di cybersicurezza, rispettivamente, su un numero di 6 e 16 totali per regione.

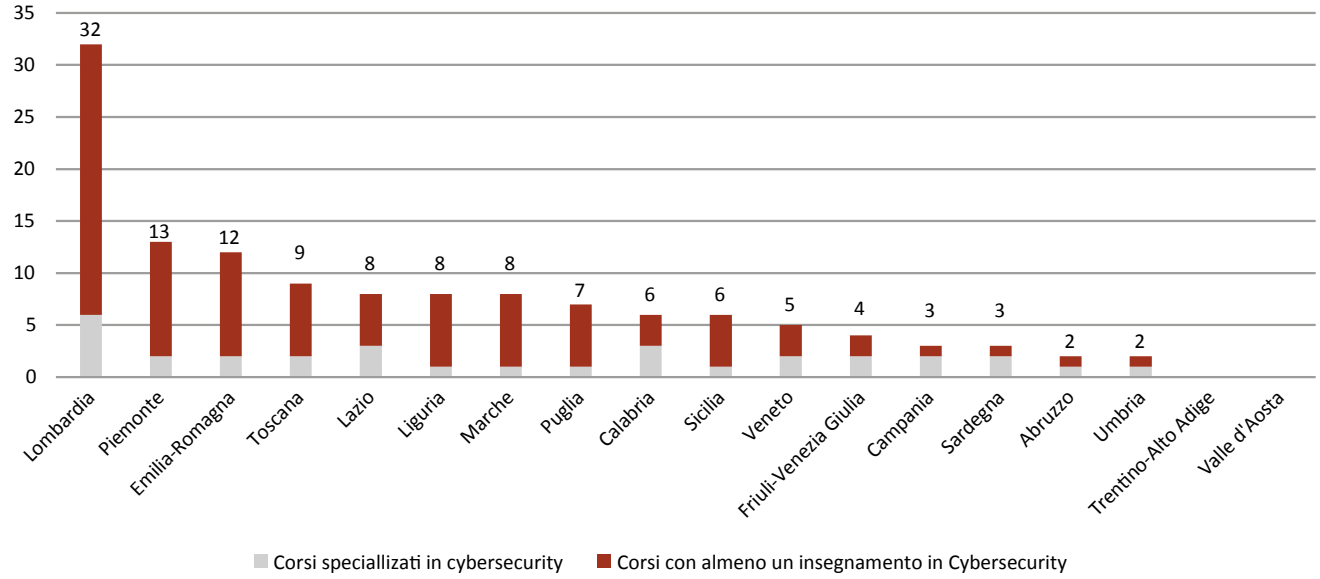
Oltre il 70% di questi corsi fa capo agli ITS appartenenti all'**area delle Tecnologie dell'Informazione e della Comunicazione (area 6)** che generalmente offre percorsi su metodi e tecnologie per lo sviluppo di sistemi software, organizzazione e fruizione dell'informazione e della conoscenza, architetture 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. 5.14) si osserva che il Lazio ha il numero maggiore di ITS appartenenti all'area ICT, immediatamente seguito dalla Lombardia e dalla Campania, anche se contestualmente sono lasciate scoperte sette regioni: Valle d'Aosta, Trentino-Alto Adige, Marche, Umbria, Molise, Abruzzo e Basilicata.

L'area 6 non è l'unica coinvolta, in quanto la cibersicurezza risulta un tema altamente trasversale, come visto altresì nel paragrafo precedente con riguardo alla formazione universitaria. Pertanto, anche nelle altre aree strategiche si rinvengono sia corsi specifici, tra cui **"Tecnico superiore nei processi di governance e compliance in ambito di sicurezza delle informazioni"**[36], "**Cybersecurity dei sistemi e delle reti"**[37], oppure "**Sistemi e sicurezza informatica**"[38], sia insegnamenti singoli/moduli all'interno di percorsi incentrati su materie differenti, tra cui **"Digital transformation specialist"**[39], **"Informatico biomedicale"**[40] e **"Artificial Intelligence specialist"**[41]. È possibile distinguere i **corsi specializzati sulla sicurezza informatica** dai **corsi con almeno un insegnamento incentrato sul tema** (Fig. 5.15). La Lombardia presenta una relazione di 6 corsi specifici rispetto a

36 Il corso è erogato dall'ITS "Fondazione M.A.S.K." (Calabria), che rientra nell'Area "Nuove tecnologie per il Made in Italy".
37 Il corso è erogato dall'ITS "Accademia Nautica dell'Adriatico", che rientra nell'Area "Mobilità Sostenibile".
38 Il corso è erogato dall'ITS "Fabriano", che rientra nell'Area "Efficienza Energetica".
39 Si fa riferimento all'ITS "Logistica – LAST", che rientra nell'Area "Mobilità Sostenibile".
40 Si fa riferimento all'ITS "Alessandro Volta", che rientra nell'Area "Nuove tecnologie della vita".
41 Si fa riferimento all'ITS "Turismo e Nuove tecnologie Marche", che rientra nell'Area "Tecnologie innovative per i beni e le attività culturali – Turismo".

Fig. 5.15: Distribuzione per regione corsi specializzati in Cybersecurity e corsi con almeno un insegnamento in Cybersecurity

Fonte: I-Com, gennaio 2025



26 insegnamenti appartenenti alla seconda categoria. A sua volta, il Piemonte è connotato da un rapporto di 2 a 11, seguito dall'Emilia-Romagna (2 a 10) e dalla Toscana (2 a 7). Campania e Sardegna presentano 2 corsi specializzati e un unico corso non specifico ciascuno, mentre l'Abruzzo e l'Umbria si fermano a un'unità per tipologia. Infine, Trentino-Alto Adige e Valle d'Aosta sono le due regioni che non presentano alcun corso afferente alle due categorie summenzionate, non avendo alcun ITS attivo sul territorio.

CONCLUSIONI

La sicurezza informatica rappresenta oggi una priorità strategica nazionale e internazionale, accentuata dalle recenti tensioni geopolitiche. Come emerge chiaramente dai dati contenuti in questo studio**, gli attacchi informatici sono diventati più sofisticati e frequenti**, spingendo governi e organizzazioni internazionali a sviluppare normative e strategie per proteggere cittadini, aziende e istituzioni.

Nonostante un peggioramento del quadro generale, è interessante segnalare come l'ICT faccia registrare una lieve flessione (-3%) degli eventi malevoli. Se tale trend sarà confermato dai dati completi sul 2024, si potrà evidenziare che i segmenti di mercato più maturi in termini di cybersicurezza – anche per impulso della regolamentazione applicabile – sono proprio quelli che riescono a gestire e a reagire meglio agli attacchi in uno scenario che vede la minaccia cibernetica avanzare costantemente.

A livello italiano, gli eventi relativi al H1 2024 sono leggermente diminuiti rispetto al medesimo periodo del 2023. Tuttavia, per comprendere se c'è stato un effettivo miglioramento dello scenario di cibersicurezza italiano appare opportuno verificare il trend su base annuale. Dal punto di vista settoriale, **la categoria merceologica per cui si rileva un maggior numero di attacchi in Italia è – per la prima volta – il manifatturiero**, che fa registrare un importante incremento rispetto al 2023 raggiungendo una quota pari al 19% (+6%). Tali dati trovano conferma anche in un analisi di **Tinexta Cyber** che sottoscrive come tale comparto sia uno dei più bersagliati a livello globale. Considerata l'importanza che ha questo settore nel tessuto economico nazionale e la prevalenza di PMI, che appaiono meno attrezzate dal punto di vista dei sistemi di cybersicurezza, questo dato è certamente molto allarmante e deve spingere ad un'opportuna riflessione.

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. **La NIS2 è divenuta applicabile lo scorso 18 ottobre in tutti gli Stati Membri**. Tuttavia, al 28 novembre, solo 4 Paesi hanno recepito questo importante atto normativo nei termini previsti (**Italia**, Belgio, Croazia e Lituania). Per tutti gli altri il ritardo si è tradotto nell'apertura di una procedura di infrazione da parte della Commissione europea.

L'ultimo rapporto "NIS Investments" vede le organizzazioni italiane ben posizionate – al 2° posto dopo quelle francesi – sul versante degli investimenti. Ottimo è anche il dato sulla **preparazione dei soggetti intervistati rispetto all'implementazione della direttiva**. Il livello di awareness in Italia è pari al 96%, dato che colloca il nostro Paese in quinta posizione a livello comunitario. **L'Italia è addirittura lo Stato Membro più virtuoso nel coinvolgimento degli organi di gestione nella formazione in cybersicurezza (70% delle organizzazioni intervistate).** Rispetto **all'approvazione delle misure di gestione dei rischi cyber**, anche in questo caso l'Italia si posiziona tra i primi della classe, più nello specifico al secondo posto (94%).

Dato che **la sicurezza della supply chain è un elemento centrale sia per la cybersicurezza in generale, sia nella direttiva NIS2**, specificamente nella parte in

cui si prescrive di **valutare le vulnerabilità specifiche per ogni diretto fornitore di servizi**, nonché la **qualità complessiva dei prodotti e delle pratiche di cibersicurezza**, comprese le procedure di sviluppo sicuro, appare fondamentale per i soggetti pubblici e privati **stabilire policy chiare e adeguate atte a prevenire e gestire i rischi relativi alle terze parti** (come partner, vendor e fornitori). Sul tema, **le organizzazioni italiane fanno collocare il nostro Paese in prima posizione** insieme all'Irlanda (90%).

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 ed evitare duplicazioni di adempimenti per il raggiungimento dei medesimi obiettivi, nel tentativo, difficile, ma non impossibile, di trovare un efficace bilanciamento tra l'esigenza di rafforzare la sicurezza da un lato e di favorire l'innovazione dall'altro.

In questo contesto ad elevata complessità si incardina, da un lato, il White Paper e, dall'altro, il rapporto Draghi che nell'analizzare i trend del settore delle comunicazioni elettroniche, il primo, e le ragioni alla base del deficit di competitività dell'UE nel contesto globale, il secondo, hanno focalizzato la propria attenzione anche sul tema della cybersecurity. Il White Paper, nello specifico, dedica specifica attenzione al tema dei fornitori attraverso un richiamo al concetto di ***"trusted suppliers"*** che, tuttavia, rimane abbastanza generico e di difficile declinazione, imponendo un supplemento di riflessione nella logica di garantire qualità dei servizi, sicurezza e fair pricing senza cadere nella tentazione di fondarsi soltanto su considerazioni di carattere geopolitico. Si tratta infatti di un tema molto importante e delicato che senza dubbio può trovare ragionevole e giustificato fondamento nel rispetto, da parte dei fornitori, di tutti gli obblighi e le prescrizioni provenienti dal diritto europeo e nazionale.

Se l'UE è impegnata a disegnare il proprio quadro normativo sulla sicurezza, l'Italia ha completato l'*iter* di **recepimento della direttiva NIS2** con l'adozione del D.Lgs. 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre scorso, che vede in ACN, designata Autorità nazionale competente e punto di contatto unico NIS, il principale soggetto attuatore. Quest'ultima, invero, sta puntualmente seguendo le fasi attuative della disciplina NIS, favorendo quella gradualità e quella certezza che certamente appaiono indispensabili, soprattutto per quelle PMI che per la prima volta si approcciano ad una normativa cyber a così elevata complessità in termini di organizzazione ed investimenti. Certamente il tema dell'allargamento del numero dei soggetti NIS2 è cruciale, così come ineludibile è la fissazione di criteri chiari per il *risk assessment*, ad esempio prendendo come riferimento alcuni standard già utilizzati nel PSNC. In tal senso, il contributo delle certificazioni, siano esse mandatorie o no, potrà essere dirimente così come il contributo

da parte dei fornitori il cui supporto sarà indispensabile per i soggetti NIS2.
Sarà allo stesso tempo cruciale garantire l'effettivo coordinamento con le altre le disposizioni relative alla direttiva CER, al regolamento DORA e alla direttiva n. 2556/2022 in materia di servizi finanziari, nonché trarre i possibili insegnamenti dall'esperienza pratica derivante dall'applicazione della disciplina del PSNC. Ed infatti, 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 chiaro che l'esperienza maturata in questi anni sarà preziosa 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**.
Pertanto, nell'immaginare il futuro ecosistema normativo nazionale che sarà delineato con la piena applicabilità e l'adeguamento, rispettivamente, di direttive – a partire dalla NIS2 – e regolamenti in materia di cybersicurezza, **sarà certamente importante l'adozione di una metodologia unica che possa raccogliere gli input relativi a un efficientamento della metodologia di test come prevista in ambito UE**. Ciò dovrà avvenire mantenendo saldi **alcuni importanti requisiti**, ossia che sia **applicabile agli asset strategici** e che possa traguardare una **corretta e tempestiva gestione della variabilità delle versioni SW**, la **riusabilità** delle certificazioni, un **tempo definito di esecuzione dei test**, oltre a un appropriato **management delle vulnerabilità**. Va altresì evidenziato che, **nonostante le importanti semplificazioni e innovazioni apportate dallo schema EUCC rispetto ai *Common Criteria*, le procedure e le risorse necessarie per affrontare il processo di certificazione appaiono di primaria importanza per le organizzazioni interessate**.
L'analisi fin qui condotta ha mostrato come la complessità del quadro normativo e degli adempimenti richiesti sia elevata. A tale riguardo, l'indagine condotta dall'Istituto per la Competitività – giunta alla seconda edizione – 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 investimenti tecnico-organizzativi necessari alla compliance, nonché per la numerosità degli oneri burocratici e amministrativi richiesti, oltre che per l'innalzamento delle barriere all'ingresso, soprattutto per le PMI, il che può avere **ripercussioni anche sui rapporti con la supply chain.**
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**, seguita dalla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo e dall'incertezza interpretativa della normativa.

Altro dato di fondamentale rilievo riguarda le **risorse economiche dedicate specificamente alla cybersicurezza**, per cui è emerso che **il maggior numero dei rispondenti assegna meno del 3% del budget IT alla cybersecurity**, mentre solo 10 soggetti (di cui 4 grandi imprese) vi allocano più del 15% del budget IT a disposizione. Per di più, nonostante lo scenario non sia propriamente ottimistico e l'entrata in vigore delle direttive NIS2 e CER**, il 42% delle imprese rispondenti sta ancora valutando se incrementare le risorse destinate alla cibersicurezza e solo un mero 25,4% ha già deciso di aumentare gli investimenti in cybersicurezza**.

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 un ridotto ricorso a tali strumenti sarebbe influenzato dalla scarsità di risorse – umane e finanziarie – da dedicare al processo di certificazione. Appare incoraggiante, invece, **che il 74,5% dei rispondenti sia d'accordo in merito al fatto che standard comunitari (es. EUCC) possono incentivare le imprese a certificarsi, segnando un incremento del 4,5% sul 2023**, e che siano diminuiti dell'11% i soggetti silenti sul tema. Peraltro, **nella scelta di un fornitore che eroghi servizi o fornisca prodotti ICT circa il 67% dei rispondenti valuta la presenza di certificazioni di sicurezza** sul prodotto o servizio e tra grandi e medie imprese si supera addirittura il 73%.

Nonostante il 31 gennaio 2024 sia stato adottato il Regolamento di esecuzione con cui gli EUCC sono diventati ufficialmente parte della legislazione europea e che diverse normative, europee e nazionali (da ultimo, il decreto NIS2), contemplano la possibilità di rendere mandatoria la certificazione di cibersicurezza per determinati prodotti, servizi e processi ICT, **oltre il 70% dei rispondenti non ha ancora avviato (o, in alcuni casi, portato a termine) la valutazione sui vantaggi/svantaggi circa la volontarietà o l'obbligatorietà di tali strumenti.**

Ad ogni modo, 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 PSNC 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 anche nella precedente edizione, a conferma del fatto che si tratti di un aspetto particolarmente sentito nel Paese. Con riguardo alla seconda domanda in tema, partendo dal presupposto che poco meno del 22% 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 60,7% 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 (+4,5% su base annua), 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 **la necessità di armonizzare il più possibile i requisiti delle diverse normative UE e nazionali in materia di cybersicurezza**. Meritevole di attenzione anche il riferimento a incentivare l'utilizzo di certificazioni ai sensi del Cybersecurity Act, prevedendo, fra l'altro, la semplificazione della procedura di valutazione dinanzi al CVCN. Inoltre, è stata proposta da diversi rispondenti l'introduzione dell'educazione "cybernetica" nelle scuole, vista come naturale evoluzione di quella civica.

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.

Il tema delle competenze e della consapevolezza appare quanto mai complesso con riferimento al contesto nazionale. Ed infatti, i dati citati rivelano 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** e in particolar modo rispetto alle competenze digitali almeno di base. Allo stesso tempo, tra le imprese italiane sembra esserci uno scarso livello di consapevolezza sulla crucialità della formazione dei dipendenti in termini di skills ICT, in quanto **soltanto il 17,9% delle aziende italiane con più di 10 addetti svolge questo tipo di formazione (contro il 22,3% della media UE)**. Peraltro, se si guarda al training di specialisti ICT/IT, il dato è ancora più preoccupante (7,3%). Definisce un ulteriore quadro allarmante l'ultimo rapporto della Polizia Postale sul 2024, il quale rileva un aumento degli illeciti, passati da 16.325 a 18.714 su base annua, e un aumento dell'ammontare sottratto, da 137 milioni di euro a 181. Quest'ultimo dato viene anche affiancato da un costo medio delle violazioni dei dati che in Italia è aumentato in maniera più marcata rispetto a Paesi come Germania e, in particolar modo, Francia.

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**. Inoltre, non andrebbe sottovalutato il valore della **formazione continua, digitale e specializzata in cybersecurity per le imprese, soprattutto se di micro e piccole dimensioni, anche in virtù del fatto che a breve saranno pienamente applicabili importanti normative dell'UE connesse a tale materia**, il che comporterà nuove sfide per i soggetti che ricadono nel rispettivo campo di applicazione.

In questo contesto, **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 **774 tra corsi e insegnamenti offerti a gennaio 2025 rispetto ai 520 individuati a gennaio**

2024, il che fa segnare un incremento di circa il 48% su base annua. In particolare, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 154 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 (180 tra corsi e singoli insegnamenti), in Lombardia (119) e in Campania (70). Di conseguenza, 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. Peraltro, se si considera che oltre il 64% dell'offerta formativa universitaria conteggiata fa capo a dipartimenti prettamente tecnici, come ingegneria e informatica, potrebbe essere opportuno **puntare maggiormente su un dialogo multidisciplinare** in ambito cybersicurezza 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**. In aggiunta, ove possibile, sarebbe certamente utile **certificare maggiormente le conoscenze e le competenze acquisite lungo il percorso universitario**.

Anche nell'ottica di estendere il più possibile la formazione specialistica nell'ambito della cibersicurezza, assumono particolare rilevanza gli Istituti Tecnici Superiori (ITS), i quali possono fungere da ulteriore e fondamentale anello di congiunzione tra la realtà scolastica e quella lavorativa. Attualmente, la formazione garantita dai 147 ITS attivi sul territorio, seppur in aumento, non pare sufficiente a colmare il gap di personale specializzato in questo campo. Di conseguenza, un aumento più consistente di questo tipo di Istituti e, in particolare, **l'incremento degli ITS in ambito ICT (Area 6), nonché di quelli che si occupano di tematiche connesse alla cibersicurezza** (a gennaio 2024, corrispondenti al 35,4% 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.

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 – lucadp/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