IL RUOLO DELLA *CYBER*-RESILIENZA A SUPPORTO DELLA CAPACITÀ DI INNOVAZIONE DELLE IMPRESE

Position Paper

Luglio 2023

Documento realizzato da The European House – Ambrosetti per Huawei Technologies Italia.

Indice

Executive Summary

I cambiamenti abilitati dalle tecnologie digitali hanno trasformato e continuano a trasformare l'economia e la società, includendo in tale trasformazione tutti i settori di attività nonché le vite dei singoli cittadini. Ad oggi, infatti, la digitalizzazione ricopre un ruolo sempre più rilevante all'interno del sistema socio-economico, come dimostrato dai principali numeri sulla digitalizzazione in Italia:

- Guardando all'impatto della digitalizzazione sugli utenti e i cittadini, è possibile notare che il **72,8%** gli utenti utilizzano regolarmente *internet*, gli acquisti online nel 2022 valgono **48,1 miliardi di Euro** (+20% vs. 2021); vi sono **oltre 27 milioni** di SPID* e **26 milioni** di CIE** nel 2021 (+55% vs. 2020); in media **un utente passa 6 ore al giorno su internet e 2 ore sui *social network***.
- Guardando all'impatto della digitalizzazione sulle imprese, invece, il **60%** utilizza servizi di *cloud computing*; **32%** utilizza dispositivi *Internet of Things* (IOT); l'*E-commerce* rappresenta il **17,5%** del fatturato; il **70%** delle persone è preoccupato per l'**uso improprio dei dati**.

Questi dati evidenziano una crescente necessità di **garantire la sicurezza di dati e processi di persone, imprese e istituzioni**.

Relativamente all'economia digitale, il suo ruolo crescente è testimoniato dagli importanti tassi di crescita attesi. In Italia, il suo valore era pari a 68,7 miliardi di Euro nel 2017 (pari al 4,0% del PIL), mentre entro il 2025 si stima che raggiungerà i **91,2 miliardi di Euro** (5,1% del PIL), crescendo a un tasso medio annuo del **+3,6%** e vedendo l'incidenza sul PIL aumentare di 1,5 punti percentuali[1]. Tuttavia, occorre sottolineare come l'incidenza dell'economia digitale è ancora ridotta in Italia nel confronto, per esempio, con la media dell'Unione Europea (6,4% del PIL) e con i Paesi *benchmark*, quali la Francia (6,1%) e la Germania (7,6%). Anche comparando la *performance* dell'UE rispetto agli USA, emergono dei *gap* rilevanti, pari a una differenza di 2,3 punti percentuali (negli USA l'economia digitale vale l'8,7% del PIL).

[1] Dal punto di vista del calcolo, per economia digitale si intende quella rete di attività economiche, transazioni commerciali e interazioni professionali rese possibili dalle tecnologie dell'informazione e della comunicazione (ICT). In particolare, sono inclusi: contenuti e pubblicità digitale, servizi di rete, servizi ICT, *software* e soluzioni ICT, dispositivi e sistemi.

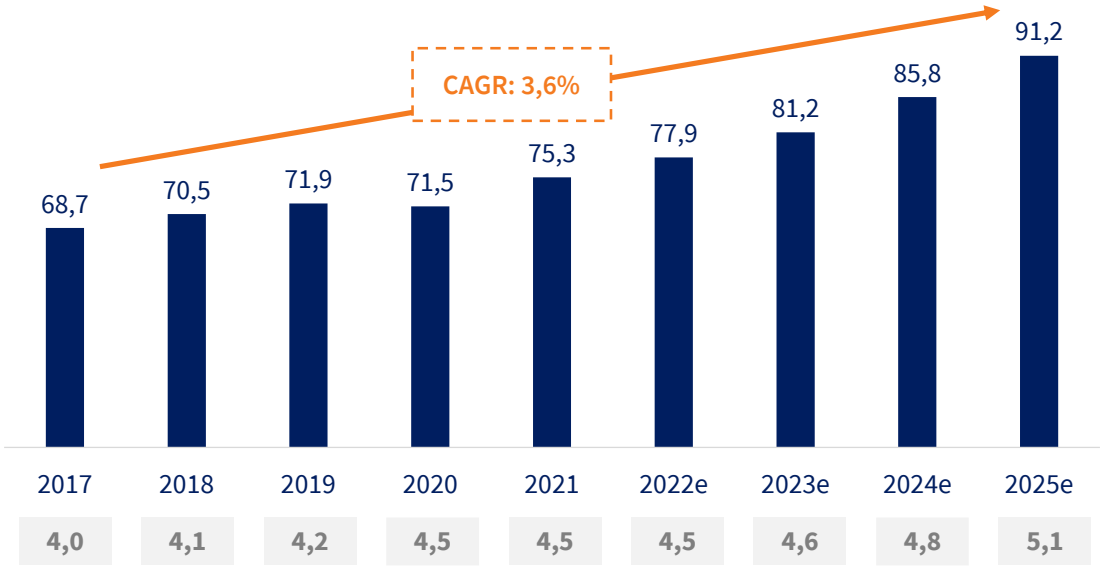

Figura I. Valore dell'economia digitale in Italia (miliardi di Euro e incidenza sul PIL), 2019-2025E. *Fonte: elaborazione The European House – Ambrosetti su dati Anitec-Assinform, Commissione Europea e Banca d'Italia, 2023.*

Parallelamente alla crescita della digitalizzazione, come misurata dall'andamento del valore dell'economia digitale, ma anche dai progressi negli indicatori di digitalizzazione (come il Digital Economy and Society Index della Commissione Europea), si rileva anche un **numero crescente di attacchi informatici**. Nel periodo 2018-2021, infatti, il numero di *cyberattack* in Italia è cresciuto a un tasso medio annuo del +9,4%, passando **da 1.554 a 2.049** in un quadriennio. Osservando la finalità degli attacchi, emerge una preponderanza del *cybercrime* (86% del totale), a cui seguono l'*espionage-sabotage* (10,6%), l'*information warfare* (2,4%) e l'*hacktivism* (1,0%).

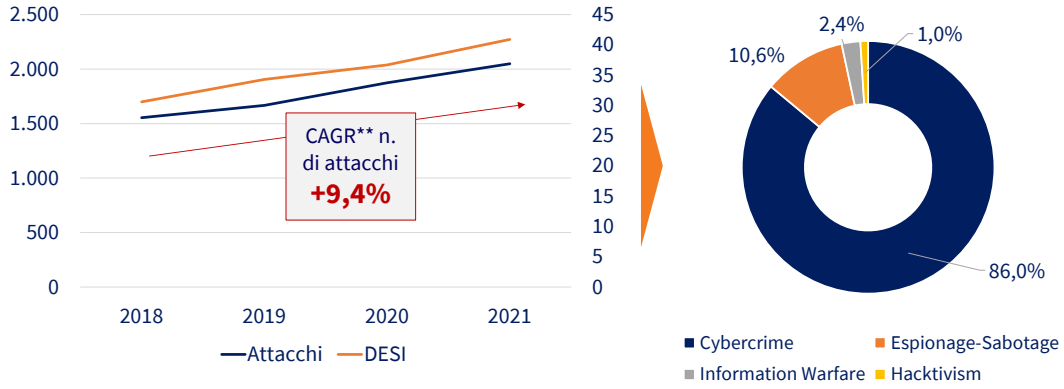

Figura II. Grafico di sinistra: numero di attacchi informatici in Italia (valori assoluti – asse sinistra) e punteggio nel Digital Economy and Society Index (valore da 0 a 100 – asse destra), 2018-2021. Grafico di destra: distribuzione degli attacchi informatici in Italia per finalità (percentuale), 2021. (*) Tasso di crescita annuo composto. *Fonte: elaborazione The European House – Ambrosetti su dati Clusit e Commissione Europea, 2023.*

Nel complesso, provando a sintetizzare il processo di digitalizzazione come quella serie di attività – svolte da imprese e Pubbliche Amministrazioni – finalizzate alla creazione e al miglioramento di servizi, prodotti e modelli di *business*, essa trova i propri fattori abilitanti nei dati, nelle tecnologie e nelle infrastrutture digitali. Su questi si innesta la ***cybersecurity***,

ovvero quelle soluzioni e quei metodi in grado di valorizzare i fattori abilitanti, garantendone la sicurezza e l'operatività. Infine, i fattori abilitanti della digitalizzazione e la *cybersecurity* risultano influenzati da due ulteriori dinamiche esogene, ovvero i fattori organizzativi (riconducibili ai modelli di *governance*, alle competenze, ecc.) e i fattori di contesto (vale a dire il quadro regolatorio e normativo di riferimento).

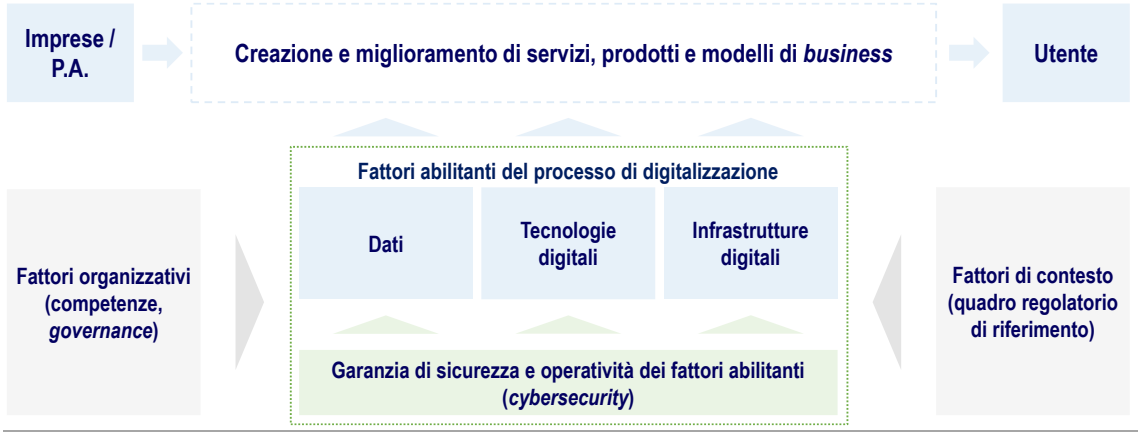

Figura III. L'impatto della digitalizzazione e della *cybersecurity* sull'offerta di servizi agli utenti. *Fonte: elaborazione The European House – Ambrosetti, 2023.*

In un contesto di **crescente pervasività della digitalizzazione** e crescente esposizione a **rischi di sicurezza** diventa dunque cruciale sfruttare le tecnologie di *cybersecurity* per **abilitare approcci di *cyber*-resilienza**. Considerando la *cybersecurity* come quell'insieme dei mezzi, delle tecnologie e delle procedure tesi alla **protezione dei sistemi informatici** in termini di disponibilità, confidenzialità e integrità dei beni o *asset* informatici, risulta fondamentale intendere la *cybersecurity* come un fattore abilitante per la crescita e la continuità delle attività economiche e sociali. In questo quadro, la *cyber*-resilienza si sostanzia dunque nella capacità di **anticipare, resistere, riprendersi e adattarsi** a condizioni avverse, stress, attacchi o compromissioni su sistemi che utilizzano risorse informatiche.

La crescente rilevanza dell'economia digitale e il ruolo strategico giocato dalla *cybersecurity* nel garantirne i processi e le funzioni hanno posto l'accento sulla necessità da parte dei Governi di adottare un **quadro normativo** che tenga conto di questi cambiamenti, cercando di **governare e regolamentare questo fenomeno**.

Il quadro normativo europeo sulla *cybersecurity* riflette la crescente attenzione dell'Unione Europea verso i temi di sicurezza informatica e digitalizzazione, presentando ancora oggi alcuni punti di attenzione legati soprattutto alla capacità delle imprese di implementare le misure richieste, con ricadute importanti sulla loro competitività. I **fattori di costi**, i **tempi** e lo **scopo di azione** delle misure messe in campo dall'Unione Europea rappresentano i principali ostacoli per favorire l'applicazione della normativa senza gravare eccessivamente sulle funzioni e sui processi delle imprese.

La Direttiva di riferimento – ancora oggi, in attesa della piena attuazione della NIS 2 – in materia di sicurezza informatica a livello comunitario è la **Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione** (**NIS**). La finalità della NIS è quella di raggiungere un

elevato livello comune in materia di sicurezza delle reti e dei sistemi di informazione in tutta l'UE, tramite:

- l'identificazione degli operatori di servizi essenziali e digitali;
- l'obbligo di adozione di strategie nazionali di sicurezza della rete e dei sistemi informativi;
- l'istituzione di un gruppo di cooperazione e di una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT);
- l'identificazione di obblighi in materia di sicurezza e notifica degli incidenti;
- l'obbligo di designazione di autorità nazionali competenti, punti di contatto unici e CSIRT.

La nuova Direttiva NIS2, entrata in vigore a gennaio 2023, cerca di affrontare criticità riscontrate nella Direttiva originaria. Il principale elemento di novità è rappresentato dall'ampliamento dei soggetti destinatari della normativa e un'uniformazione dei soggetti inclusi: da "Operatori di Servizi Essenziali" e "Fornitori di Servizi Essenziali", identificati nella precedente Direttiva, a "**Soggetti Essenziali**" e "**Soggetti Importanti**". In questo modo, la nuova Direttiva crea una "gerarchia" di settori strategici sui quali la normativa deve intervenire, differenziandoli per livelli di criticità

La nuova normativa impone **maggiori costi**, soprattutto in termini di ***compliance***, tra cui l'implementazione dei requisiti di sicurezza e degli obblighi di *reporting* e l'applicazione delle misure di supervisione. Secondo le stime della Commissione Europea, i **costi della nuova normativa** per le medie e grandi imprese ammonteranno a circa **35 miliardi di Euro** a livello europeo e a **840 mila Euro in media per azienda**.

All'interno del contesto europeo, l'Italia è stato uno dei primi Paesi a muoversi verso la definizione di norme e strutture per garantire la sicurezza informatica.

Tra le principali azioni messe in campo dal Governo italiano sui temi di sicurezza informatica è importante menzionare l'istituzione del **Perimetro di Sicurezza Nazionale Cibernetica** (**PSNC**), emanato con il Decreto legge n.105, 2019, con l'obiettivo di elevare la sicurezza dei sistemi ICT per le Pubbliche Amministrazioni e alcune imprese private selezionate. Nello specifico, il Perimetro di sicurezza cibernetica nazionale è finalizzato ad assicurare un **livello elevato di sicurezza** delle reti, dei sistemi informativi e dei servizi informatici delle pubbliche amministrazioni, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali, o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Inoltre, a maggio 2022 è stata approvata la nuova **Strategia nazionale di cybersicurezza** (2022-2026) e l'annesso Piano di implementazione. La Strategia intende perseguire **3 obiettivi** fondamentali, collegati a **82 misure** e supportati da **fattori abilitanti** (formazione, promozione della cultura della sicurezza cibernetica e cooperazione), con un ruolo chiave giocato dalle ***partnership*** **pubblico private**

L'esigenza di una riorganizzazione del quadro normativo e, più in generale, di uno sviluppo armonioso della *cybersecurity* in Italia risulta essere particolarmente pressante alla luce di **livelli di sicurezza informatica fortemente eterogenei** nei diversi settori.

A tal proposito, a fronte di investimenti complessivi in ambito ICT pari a 6,2 miliardi di Euro, il **valore tutelato** da tali settori risulta ben più elevato (195 miliardi di Euro), a ulteriore testimonianza del ruolo ricoperto dalle infrastrutture critiche nell'economia del sistema-Paese. La mancata tutela di questi *asset*, tramite il potenziamento di sistemi di sicurezza informatica e ICT, può risultare dunque in **grosse perdite da parte delle imprese e di tutto il Paese**, a seguito del **blocco delle attività** causati da eventuali attacchi *hacker*.

Per indagare la **consapevolezza** e il **ruolo delle *cybersecurity*** all'interno delle imprese italiane – e in particolare quelle appartenenti ai settori strategici – e identificare le **esigenze** prospettiche, è stata realizzata una *survey* strutturata.

In termini di **spesa complessiva**, il **67,1%** delle aziende del campione ha dichiarato di **investire in *cybersecurity,* in media, meno del 10% del proprio *budget* IT**. Un particolare scostamento è rinvenibile nelle **grandi imprese**, dove il **52%** delle realtà investe in *cybersecurity*, in media, **oltre il 10% del proprio *budget* IT**, e in particolare **oltre il 20% per il 28% delle imprese**.

Nell'ambito degli attacchi informatici subiti dall'azienda, è interessante rilevare come per il 42,4% delle imprese la **fonte principale** sia rappresentata dall'**errore umano**, contrapposto al 22,7% delle imprese secondo cui esso sia imputabile principalmente ad un attacco forzato dei sistemi. In ambito di **competenze digitali**, infatti, l'Italia è al **quartultimo posto nell'Unione Europea** per persone con competenze digitali almeno di base, con una quota pari al **45,6%**, inferiore di 8,3 punti percentuali rispetto alla media europea (53,9%).

In questo quadro, quasi 1 impresa del campione su 2 (45,1%) ritiene che l'attuale quadro regolatorio in materia di *cybersecurity* impatti sulla **capacità di innovare e generare crescita** per l'azienda. Approfondendo le motivazioni sottostanti, si rileva che per oltre la metà delle imprese (**55%**), la capacità innovativa è **impattata dai fattori di costo**, ovvero in quanto causa un aumento della burocrazia e dei costi amministrativi per adempiere agli *standard* (30%) e perché comporta costi significativi sia in termini di tecnologie sia in termini di personale da dedicare alle attività di *cybersecurity* (29%).

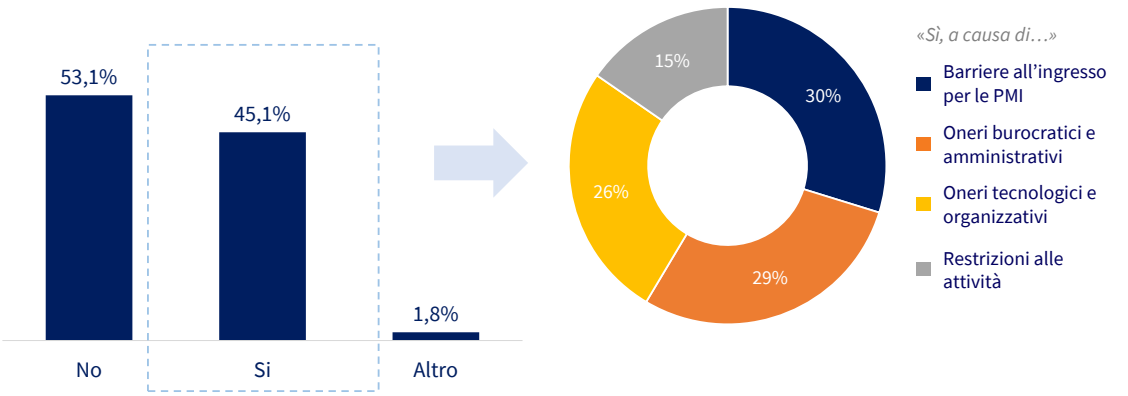

Figura IV. Risposte alla domanda «Reputa che il quadro regolatorio in materia di *cybersecurity* impatti sulla capacità di innovare e generare crescita per l'azienda?» (risposta multipla, massimo 2 risposte). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

In ottica di ottimizzare il *framework* della *cybersecurity* in Italia, promuovendone allo stesso tempo uno sviluppo in chiave competitiva nelle imprese, sono state individuate alcune linee di azione afferenti a tre aree di interventi: supporto alle imprese e alla capacità innovativa, competenze e *awareness* e *governance* e modelli collaborativi.

Con riferimento all'area di supporto alle imprese e alla capacità innovativa sono state identificate le seguenti linee di azione:

- Promozione di un maggiore **allineamento della normativa italiana di *cybersecurity* a *standard* comunitari** e **semplificazione del quadro corrente**, evitando la duplicazione di obblighi in capo agli attori, con riferimento sia all'implementazione della Direttiva NIS 2 sia allo sviluppo di sistemi di certificazione;
- Sviluppo dell'attività di **accompagnamento alle imprese**, per esempio tramite **incentivi per l'acquisto di soluzioni di *cybersecurity***, *in primis* per le imprese coinvolte nella NIS 2, e modelli di **collaborazione di filiera**;
- Definizione di schemi di **mantenimento delle certificazioni** e di **certificazione dei processi**, secondo paradigmi di *security-by-design* e *certification-by-design*;
- Creazione di uno *standard* unificato per la **certificazione tecnica** (come ad esempio EUCC/GSMA 5G NESAS, ecc.), semplificando il processo di certificazione;
- Introduzione di un nuovo modello di servizio per la *cybersecurity* "**CISO as a Service**" (*Chief Information Security Officer* come servizio), prevedendo l'*outsourcing* del ruolo di CISO a un fornitore di servizi specializzato in sicurezza informatica, permettendo soprattutto alle PMI di avere accesso a competenze e risorse esperte in *cybersecurity* senza la necessità di assumere un CISO a tempo pieno.

Con riferimento all'area della capacità innovativa sono state identificate le seguenti linee di azione:

- Promozione delle **competenze tecniche** di *cybersecurity* e delle **competenze digitali diffuse** nella popolazione, anche tramite appositi **quadri di certificazione** e la **collaborazione** tra sistema formativo e delle imprese.
- Introduzione di requisiti di ***disclosure* sulle capacità di *cybersecurity* dei vertici aziendali**, sul modello della «Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure» statunitense.
- Supporto allo **scambio di competenze** nel campo della sicurezza informatica, promuovendo la collaborazione tra professionisti e istituzioni e rafforzando le capacità nel settore di affrontare le nuove sfide.

Con riferimento all'area della *governance* e modelli collaborativi sono state identificate le seguenti linee di azione:

- Attivazione di **meccanismi di consultazione degli *stakeholder*** nell'ambito dell'attività normativa della *cybersecurity*, sul modello delle consultazioni a livello di Unione Europea.
- Supporto alle ***partnership* con Paesi terzi**, sia sotto il profilo industriale sia economico, volto all'aumento dell'offerta di tecnologie europee.
- Definizione **meccanismi trasparenti** per le attività di valutazione dei rischi di sicurezza *end-to-end*, ovvero basati su criteri e *standard* scientificamente applicabili).

Introduzione

Premessa

In un'epoca in cui la digitalizzazione è sempre più diffusa e le minacce cibernetiche sono in costante aumento, la ***cybersecurity*** è diventata una **priorità strategica** per i Paesi di tutto il mondo. La protezione dei sistemi informatici, delle reti e dei dati è diventata, infatti, un elemento fondamentale per la **sicurezza nazionale**, la **competitività** delle imprese e il **benessere** dei cittadini.

In particolare, la **crescente interconnessione delle economie** trova un proprio fondamento nelle c.d. **infrastrutture critiche**, come le reti energetiche, i sistemi di trasporto, le reti di comunicazione, le infrastrutture finanziarie e governative. In un quadro di crescente esposizione di tali infrastrutture ad attacchi informatici, la *cybersecurity* svolge un ruolo strategico nel **proteggere queste infrastrutture critiche**, garantendone la **resilienza** e l'**operatività**, e dunque assicurando il **funzionamento dei sistemi economici e la difesa nazionale**.

La *cybersecurity* rappresenta un prerequisito essenziale anche per la **protezione dei dati** – personali, finanziari, militari, governativi – dagli attacchi cibernetici (si pensi, per esempio, al furto d'identità, alle frodi finanziarie, allo spionaggio o all'*hacking* governativo). Da questo punto di vista, i sistemi di *cybersecurity*, garantendo la protezione di queste informazioni, svolgono un ruolo di importanza strategica nel garantire la ***privacy***, la **sovranità** e la **sicurezza** nazionale.

La *cybersecurity* offre, inoltre, un contributo fondamentale anche nella **promozione della competitività delle imprese**. Tali soluzioni, infatti, sono fattori determinanti per la capacità innovativa dei sistemi economici, *in primis* per lo **sviluppo** e la **sostenibilità** dell'**economia digitale** (si pensi, per esempio, alle attività di *e-commerce*, *e-banking* o *smart manufacturing*). Allo stesso tempo, la *cybersecurity* costituisce un fattore determinante anche per **promuovere l'innovazione** tecnologica e digitale di un Paese. La ricerca e lo sviluppo di tecnologie avanzate, come l'Intelligenza Artificiale, l'*Internet of Things*, la *blockchain* o il 5G, offrono nuove opportunità di crescita dei sistemi economici; al tempo stesso, tali ambiti sono chiamati ad affrontare **nuove sfide** in termini di sicurezza – come violazioni dei dati, intromissioni nei sistemi, furto delle proprietà intellettuali – potendo trovare nella *cybersecurity* la **risposta tecnologica**.

Sulla base di queste considerazioni, l'obiettivo Position Paper "Il ruolo della *cyber*-resilienza a supporto della capacità di innovazione delle imprese" è quello di analizzare lo **stato dell'arte della *cyber*-resilienza** in Italia e nel quadro europeo, qualificandone la funzione strategica per le imprese e indicando le aree di debolezza e ottimizzazione. Lo Studio intende quindi qualificare il **contributo della *cyber*-resilienza per lo sviluppo dell'economia digitale**, sviluppando una **visione strategica di *cyber*-resilienza** per l'Italia basata su un quadro regolatorio in grado di bilanciare innovazione, elevati livelli di sicurezza e crescita.

Dal punto di vista metodologico, le evidenze del *Position Paper* sono state sviluppate anche grazie a un percorso di ascolto di *stakeholder* ed esperti, conclusosi con una Tavola Rotonda di discussione (Roma, 30 maggio 2023).

Un elemento distintivo del progetto è stata l'interazione con i rappresentanti delle istituzioni, del sistema delle imprese e dell'accademia sui temi legati alla sicurezza informatica e al digitale. Si ringraziano per i contributi e i suggerimenti offerti: **Vincenzo Calabrò** (Professore, Università di Reggio Calabria; Funzionario informatico, Ministero dell'Interno), **Vittorio Calaprice** (Analista politico – Affari politici e relazioni istituzionali, Rappresentanza in Italia della Commissione europea), **Mirko Calvaresi** (*Chief Information Officer*, pagoPA), **Anna Cataleta** (*Senior Partner*, P4I-Partners4Innovation), **Andrea Chittaro** (*Senior Vice President Global Security & Cyber Defence*, Snam), **Giovanni Ciminari** (*Head of Cyber Defence*, Sogei), **Nicola Ciulli** (Presidente Nazionale, CNA Digitale), **Fabrizio D'Amore** (Professore, Università La Sapienza; Direttore del Master in Sicurezza delle informazioni e informazione strategica), **Massimiliano D'Angelo** (Direttore centrale Tecnologia Informatica e Innovazione, INPS), **Gennaro Faella** (SVP *Strategic Innovation & Development*, Leonardo Cyber & Security Solutions, Leonardo), **Alessandro Manfredini** (*Direttore Group Security & Cyber Defence*, A2A; Presidente, AIPSA - Associazione Italiana Professionisti Security Aziendale), **Valeria Mazzoni** (Funzionario, Reparto innovazione tecnologica, Ministero della Difesa), **Greta Nasi** (Professore, Università Bocconi; Direttore della Laurea Magistrale in *Cyber Risk Stategy and Governance*, Università Bocconi e Politecnico di Milano), **Luca Nicoletti** (Responsabile del Servizio Programmi Industriali, di sviluppo, ricerca e formazione, Agenzia per la Cybersicurezza Nazionale), **Giulia Pastorella** (Membro, IX Commissione permanente della Camera dei Deputati "Trasporti, poste e telecomunicazioni"; Vice-Presidente, Azione), **Giuseppe Pietrafesa** (Gabinetto del Ministero delle Imprese e del Made in Italy), **Guido Ponte** (*Chief Economist*, TIM), **Domenico Raguseo** (*Head of Cybersecurity*, Exprivia), **Yuri Rassega** (*Chief Information Security Officer*, Enel), **Paolo Salza** (*Chief Risk*, *ESG & Compliance Officer*, RINA; Presidente, CONFORMA - Associazione Organismi Certificazione Ispezione Prova e Taratura), **Guido Scorza** (Componente del Collegio, Garante per la protezione dei dati personali), **Antonio Veraldi** (Responsabile *Business Development*, Experience), **Stefano Zanero** (Professore, Politecnico di Milano; Presidente, Secure Network), **Elisabetta Zuanelli** (Professore, Università di Roma Tor Vergata; Coordinatrice, Partenariato per il Piano di formazione in *Cybersecurity, Cyberthreat e Privacy*).

Il progetto è stato supervisionato e curato operativamente dal Gruppo di Lavoro di The European House – Ambrosetti, composto da:

- Lorenzo Tavazzi (*Partner* e Responsabile Area Scenari e *Intelligence*)
- Francesco Galletti (*Consultant*, Area Scenari e *Intelligence*)
- Luca Celotto (*Consultant*, Area Scenari e *Intelligence*)
- Giuseppe Tiralosi (*Consultant*, Area Scenari e *Intelligence*)
- Luca Trovato (*Area Manager* Lombardia)
- Paola Gandolfo (*Assistant* di progetto)

La struttura del *Position Paper*

Il documento è suddiviso in quattro capitoli:

- **Dalla *cybersecurity* alla *cyber*-resilienza e il ruolo di supporto nella trasformazione digitale**. In questo capitolo viene analizzato il ruolo della *cybersecurity* nel processo di trasformazione digitale del sistema-Paese, illustrano i numeri chiave della *cybersecurity* in Italia e in Europa.
- **Il quadro normativo a livello europeo e italiano e gli elementi evolutivi**. In questo capitolo vengono sistematizzate e analizzate le principali normative in ambito europeo e italiano connesse alla *cybersecurity*, evidenziando i temi aperti del *framework* regolatorio della *cybersecurity* in Europa e in Italia.
- **Le esigenze delle imprese connesse alla *cybersecurity***. In questo capitolo vengono riportati i risultati della *survey*, realizzata da The European House – Ambrosetti alle aziende operanti nei settori che rientrano nel perimetro strategico della *cybersecurity*, mettendo in luce la consapevolezza e il ruolo della *cybersecurity* all'interno delle aziende appartenenti ai settori strategici e il ruolo della *cybersecurity* come leva di sviluppo e innovazione aziendale.
- **Le proposte di ottimizzazione del *framework* della *cybersecurity***. In questo capitolo è riportata la visione strategica di *cyber*-resilienza – individuata sulla base delle analisi, della *survey* alle imprese e dei colloqui con i principali *stakeholder* del settore – in grado di bilanciare innovazione, livelli di sicurezza e crescita.

1. Dalla *cybersecurity* alla *cyber*-resilienza e il ruolo di supporto nella trasformazione digitale

I cambiamenti abilitati dalle tecnologie digitali hanno trasformato e continuano a trasformare l'economia e la società, includendo in tale trasformazione tutti i settori di attività nonché le vite dei singoli cittadini. Ad oggi, infatti, la digitalizzazione ricopre un ruolo sempre più rilevante all'interno del sistema socio-economico, come dimostrato dai principali numeri sulla digitalizzazione in Italia:

- Guardando all'impatto della digitalizzazione sugli utenti e i cittadini, è possibile notare che il **72,8%** gli utenti utilizzano regolarmente *internet*, gli acquisti online nel 2022 valgono **48,1 miliardi di Euro** (+20% vs. 2021); vi sono **oltre 27 milioni** di SPID* e **26 milioni** di CIE** nel 2021 (+55% vs. 2020); in media **un utente passa 6 ore al giorno su internet e 2 ore sui *social network***. Al tempo stesso, il **70%** delle persone è preoccupato per l'**uso improprio dei dati**.
- Guardando all'impatto della digitalizzazione sulle imprese, invece, il **60%** utilizza servizi di *cloud computing*; **32%** utilizza dispositivi *Internet of Things* (IOT); l'*E-commerce* rappresenta il **17,5%** del fatturato.

Questi dati evidenziano una crescente necessità di **garantire la sicurezza di dati e processi di persone, imprese e istituzioni**.

In particolare, la digitalizzazione è sempre più pervasiva, sia in termini di servizi che nascono digitali, sia di attività che fanno leva sulle tecnologie digitali, come *Big Data*, *Artificial Intelligence* e *Internet of Things*.

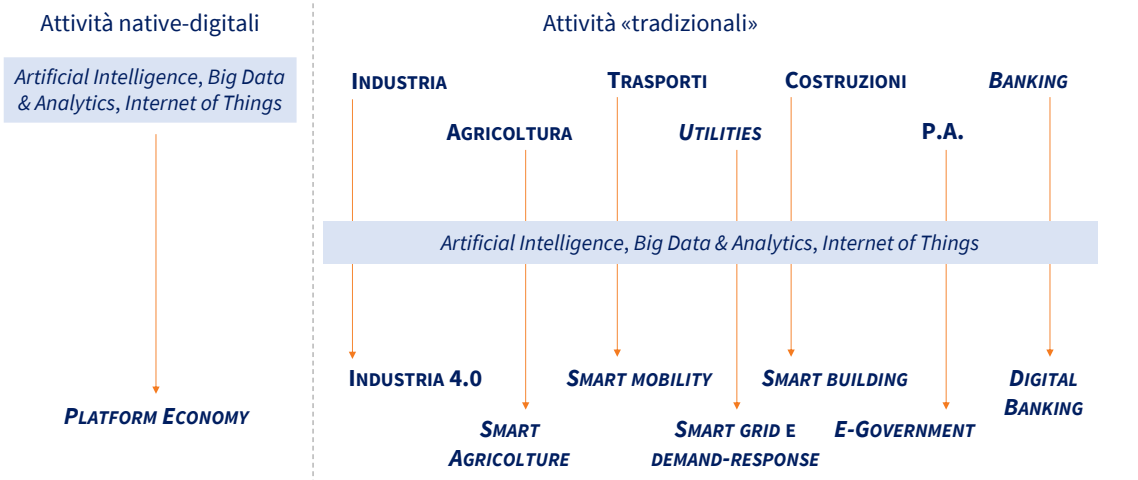

Figura 1.1. Rappresentazione esemplificativa del ruolo della digitalizzazione nelle attività native-digitali e nelle attività "tradizionali". *Fonte: elaborazione The European House – Ambrosetti, 2023.*

Con riferimento a tali tecnologie digitali, i dati rappresentano la base di molti nuovi prodotti e servizi, con impatti positivi sia in termini di produttività sia di efficienza delle risorse in tutti i settori economici, abilitando la personalizzazione e il miglioramento del processo di elaborazione delle politiche e il potenziamento dei servizi pubblici. Non ultimo,

rappresentano una risorsa essenziale per le *start-up* e le piccole e medie imprese (PMI), permettendo di sviluppare e ampliare le loro *value-proposition*. La disponibilità di dati è essenziale, infine, per favorire lo sviluppo dei sistemi di Intelligenza Artificiale, dal riconoscimento morfologico e *insight generation* a tecniche di previsione più sofisticate e, di conseguenza, decisioni migliori.

La centralità del dato nei processi di cambiamento economici e sociali si riflette anche nella quantità crescente che ne viene prodotta e ai cambiamenti nelle modalità di raccolta, elaborazione e utilizzo. La mole di dati che viene prodotta da tutti i dispositivi nel mondo è infatti in continuo aumento ed è previsto che raggiunga circa **181 zettabytes** nel 2025, quadruplicando il valore del 2019 e crescendo ad un tasso annuo del 35%.

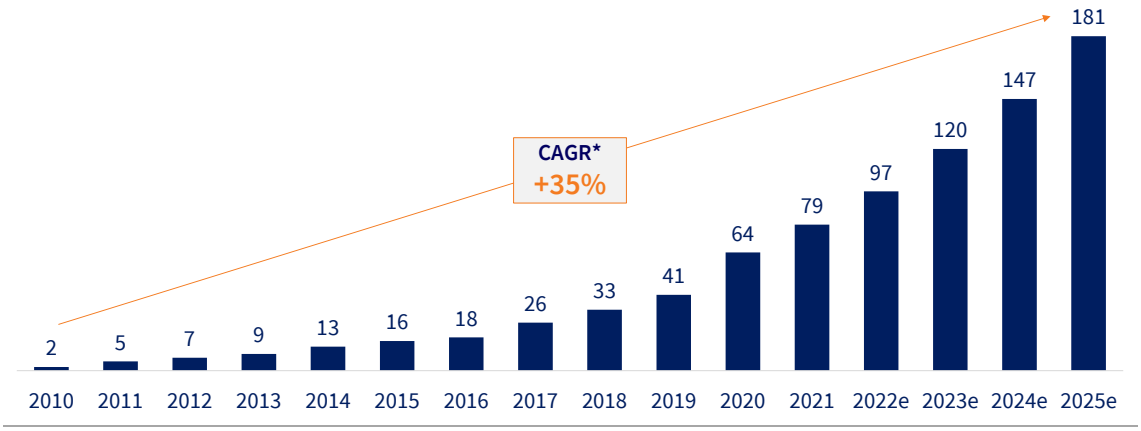

Figura 1.2. Volume di dati creati, elaborati, copiati e consumati a livello globale (Zettabytes), 2010-2025E. (*) Tasso di crescita annuo composto. *Fonte: elaborazione The European House – Ambrosetti su dati IDC, 2023.*

La crescita esponenziale della quantità di dati prodotti determina la necessità, per chi intende estrarre valore dai dati (in primis Istituzioni e aziende), di sviluppare nuove modalità di raccolta, trattamento ed elaborazione. In questo senso, si può osservare la tendenza a un cambio di paradigma, passando da una gestione centralizzata a una decentralizzata. Secondo le stime della Commissione Europea contenute nella sua "Strategia europea per i dati" rilasciata a febbraio 2020, tale cambiamento porterà nei prossimi anni ad avere, per l'80% dei dati, non più un unico centro di raccolta ed elaborazione, ma una **realtà policentrica e decentrata** in cui a più fonti di raccolta dati corrispondono più centri di accumulo ed elaborazione.

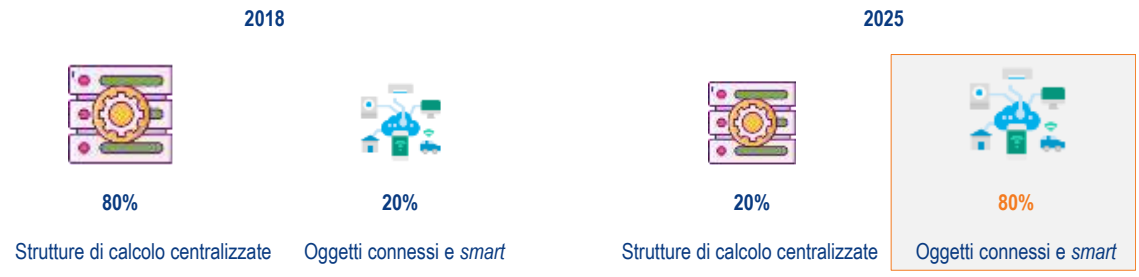

Figura 1.3. Modalità di raccolta ed elaborazione dei dati, 2018 e 2025. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2023.*

Tale trasformazione procede, di pari passo, con la progressiva crescita dell'*Internet of Things*. L'*Internet of Things* ("Internet delle cose") consiste nel rendere gli oggetti (le "cose") riconoscibili e intelligenti tramite la possibilità di trasmettere dati e accedere a informazioni aggregate da parte di altri oggetti. La tecnologia IoT si può applicare a diversi oggetti: dispositivi, apparecchiature, beni, impianti, e così via. Una volta installati, questi dispositivi si definiscono *smart objects*.

Nel 2020, il numero di dispositivi connessi IoT (dispositivi industriali e B2B) ha superato quello dei non-IoT (ovvero dispositivi ad uso personale come pc, *smartphone*, e *tablet*). Il volume di dati generati dai dispositivi IoT, inoltre, dai 14 zettabytes generati nel 2019, raggiungerà i 79 ZB (484x). L'*Internet of Things* permette di generare e valorizzare i dati attraverso la connessione tra i diversi dispositivi (*device-to-device*) e le persone (*device-to-human*). In questa prospettiva, dall'unione delle tecnologie *Cloud* e IoT è possibile dare vita a diverse applicazioni, come per esempio l'***Industrial IoT***, alla base dell'*Intelligent Manufacturing*, e il ***Consumer IoT***.

L'*Industrial IoT* è l'applicazione di strumenti, sensori connessi e altri dispositivi a macchinari e processi in ambito industriale. In questo campo, uno degli ambiti di maggiore applicazione dell'IoT è la **manutenzione predittiva**, che nelle modalità più avanzate diventa **manutenzione prescrittiva**, dove, oltre a segnalare in anticipo il malfunzionamento dei dispositivi IoT, indicano anche come affrontare l'eventuale malfunzionamento. Il *Consumer IoT* concerne invece, tra le altre cose, quei dispositivi tecnologici (*smart TV*, *wearables*, cellulari, ecc.) che si basano su un'elevata customizzazione dell'offerta e sono diretti alla fidelizzazione del cliente. Entrambe queste finalità sono raggiungibili grazie proprio alla grande mole di dati a cui oggi riescono ad accedere le aziende e che permette loro di ottenere un vantaggio competitivo rispetto ai *competitor* sulla base delle capacità di analisi e valorizzazione di tali dati.

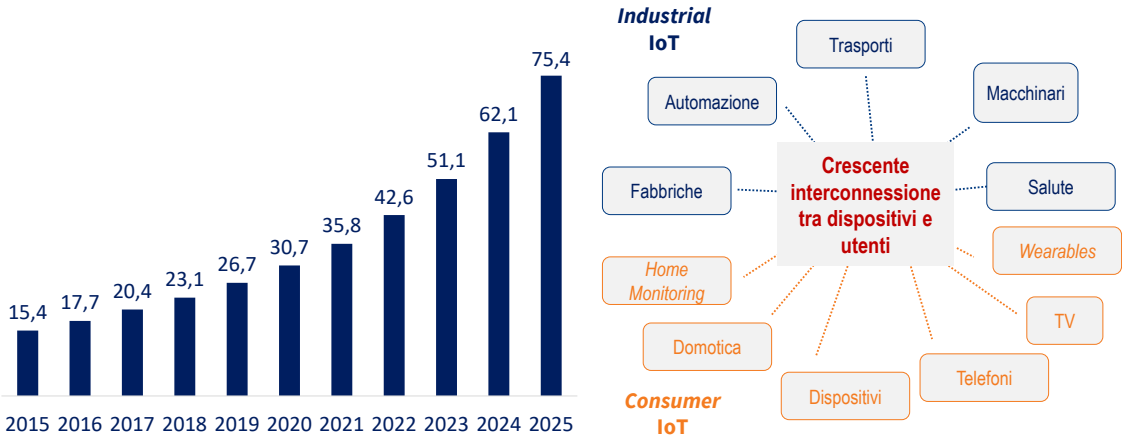

Figura 1.4. Dispositivi IoT connessi a livello globale (miliardi), 2025-2025E. *Fonte: elaborazione The European House – Ambrosetti su dati IDC, 2023.*

Dal numero crescente di dati e dalla pervasività delle tecnologie digitali – *in primis* l'*Internet of Things* – discende quindi una crescente interconnessione tra dispositivi, attori economici e persone. Proprio in questa interconnessione risiedono le maggiori opportunità di

valorizzazione, nel quadro dell'economia digitale. In particolare, il valore dell'economia digitale risulta fortemente connesso a quella estesa catena di attività – la **catena di valore del dato** – che valorizza i dati attraverso differenti ma integrati processi di generazione, raccolta, elaborazione, analisi, automazione e sfruttamento dei dati resi possibili dalle tecnologie digitali abilitanti (es. *Cloud*, IoT, *Big Data Analytics*, Intelligenza Artificiale, ecc.).

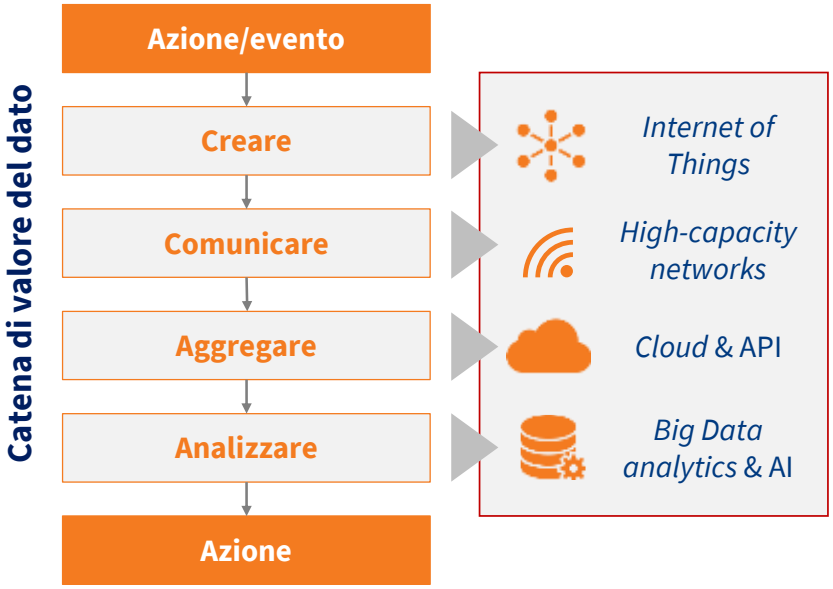

Figura 1.5. Il *Data value loop* generato dall'integrazione delle tecnologie abilitanti della digitalizzazione. *Fonte: elaborazione The European House – Ambrosetti, 2023.*

Nel complesso, provando a sintetizzare il processo di digitalizzazione come quella serie di attività – svolte da imprese e Pubbliche Amministrazioni – finalizzate alla creazione e al miglioramento di servizi, prodotti e modelli di *business*, essa trova i propri fattori abilitanti nei dati, nelle tecnologie e nelle infrastrutture digitali. Su questi si innesta la ***cybersecurity***, ovvero quelle soluzioni e quei metodi in grado di valorizzare i fattori abilitanti, garantendone la sicurezza e l'operatività. Infine, i fattori abilitanti della digitalizzazione e la *cybersecurity* risultano influenzati da due ulteriori dinamiche esogene, ovvero i fattori organizzativi (riconducibili ai modelli di *governance*, alle competenze, ecc.) e i fattori di contesto (vale a dire il quadro regolatorio e normativo di riferimento).

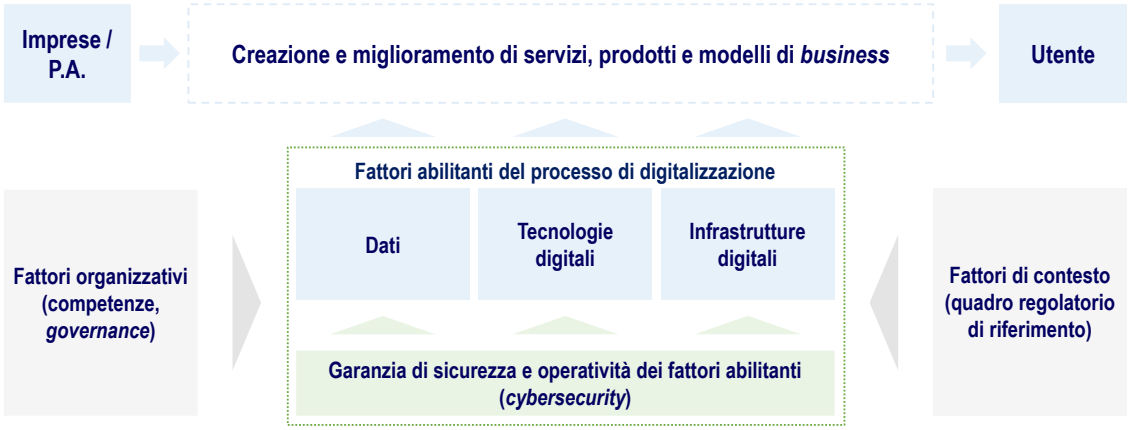

Figura 1.6. L'impatto della digitalizzazione e della *cybersecurity* sull'offerta di servizi agli utenti. *Fonte: elaborazione The European House – Ambrosetti, 2023.*

Relativamente all'economia digitale, il suo ruolo crescente è testimoniato dagli importanti tassi di crescita attesi. In Italia, il suo valore era pari a 68,7 miliardi di Euro nel 2017 (pari al 4,0% del PIL), mentre entro il 2025 si stima che raggiungerà i **91,2 miliardi di Euro** (5,1% del PIL), crescendo a un tasso medio annuo del **+3,6%** e vedendo l'incidenza sul PIL aumentare di 1,5 punti percentuali[2]. Tuttavia, occorre sottolineare come l'incidenza dell'economia digitale è ancora ridotta in Italia nel confronto, per esempio, con la media dell'Unione Europea (6,4% del PIL) e con i Paesi *benchmark*, quali la Francia (6,1%) e la Germania (7,6%). Anche comparando la *performance* dell'UE rispetto agli USA, emergono dei *gap* rilevanti, pari a una differenza di 2,3 punti percentuali (negli USA l'economia digitale vale l'8,7% del PIL).

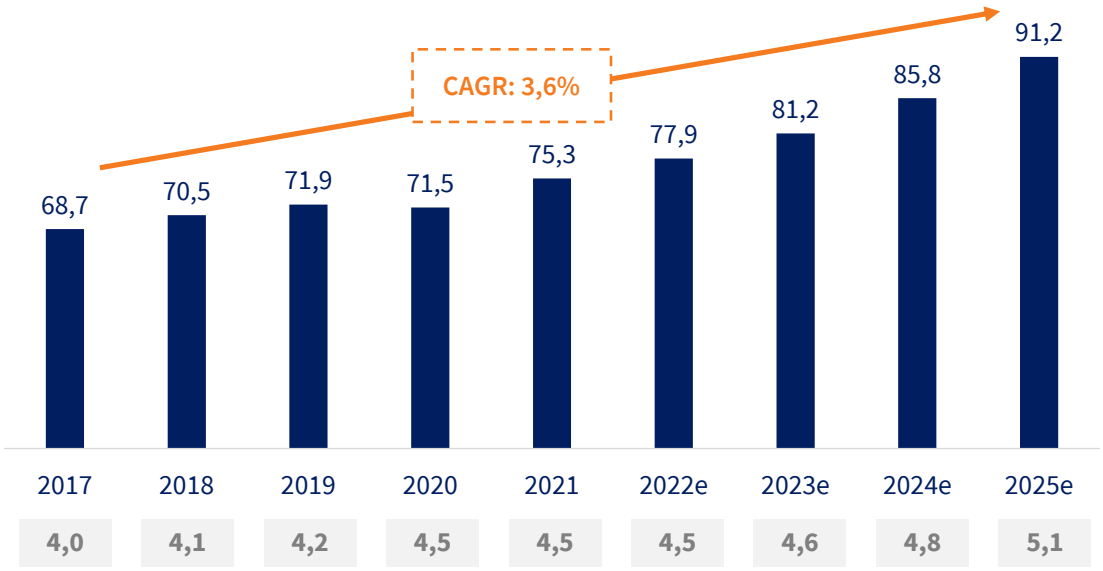

Figura 1.7. Valore dell'economia digitale in Italia (miliardi di Euro e incidenza sul PIL), 2019-2025E. *Fonte: elaborazione The European House – Ambrosetti su dati Anitec-Assinform, Commissione Europea e Banca d'Italia, 2023.*

Parallelamente alla crescita della digitalizzazione, come misurata dall'andamento del valore dell'economia digitale, ma anche dai progressi negli indicatori di digitalizzazione (come il Digital Economy and Society Index della Commissione Europea), si rileva anche un **numero crescente di attacchi informatici**. Nel periodo 2018-2021, infatti, il numero di *cyberattack* in Italia è cresciuto a un tasso medio annuo del +9,4%, passando **da 1.554 a 2.049** in un quadriennio. Osservando la finalità degli attacchi, emerge una preponderanza del *cybercrime* (86% del totale), a cui seguono l'*espionage-sabotage* (10,6%), l'*information warfare* (2,4%) e l'*hacktivism* (1,0%).

[2] Dal punto di vista del calcolo, per economia digitale si intende quella rete di attività economiche, transazioni commerciali e interazioni professionali rese possibili dalle tecnologie dell'informazione e della comunicazione (ICT). In particolare, sono inclusi: contenuti e pubblicità digitale, servizi di rete, servizi ICT, *software* e soluzioni ICT, dispositivi e sistemi.

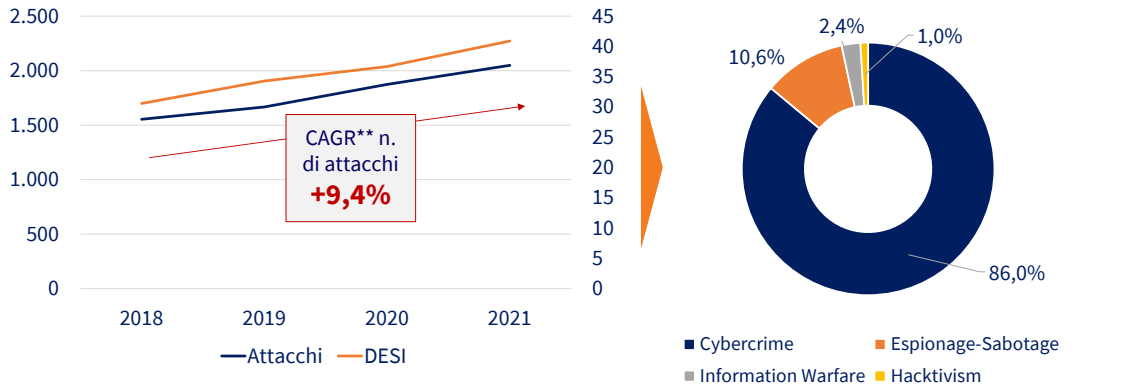

Figura 1.8. Grafico di sinistra: numero di attacchi informatici in Italia (valori assoluti – asse sinistra) e punteggio nel Digital Economy and Society Index (valore da 0 a 100 – asse destra), 2018-2021. Grafico di destra: distribuzione degli attacchi informatici in Italia per finalità (percentuale), 2021. (*) Tasso di crescita annuo composto. *Fonte: elaborazione The European House – Ambrosetti su dati Clusit e Commissione Europea, 2023.*

In termini di tecniche di attacco, emerge un ruolo preponderante dei ***malware*** ("*malicious software*", ovvero *software* dannosi progettati per compromettere o sfruttare qualsiasi tipo di dispositivo, servizio o rete programmabile), riconducibili a **850 attacchi nel 2021**, in aumento del 41% rispetto ai valori del 2018. Nello stesso periodo di riferimento, sono più che raddoppiate le vulnerabilità, passate da 143 a 320 (+124%), e sono aumentate anche le tecniche multiple, cresciute da 64 a 103 (+61%).

Relativamente ai soggetti coinvolti, tutti i settori risultano colpiti dal *cybercrime*, con punte particolarmente elevate – tra i settori critici – nel **comparto governativo** (15,0% degli attacchi), nel **settore ICT** (13,6%) e nella **sanità** (12,8%). Inoltre, è interessante rilevare come il 13,4% degli attacchi siano finalizzati a *target* multipli, evidenziando dunque la capacità degli attori del *cybercrime* di impattare su una pluralità di soggetti.

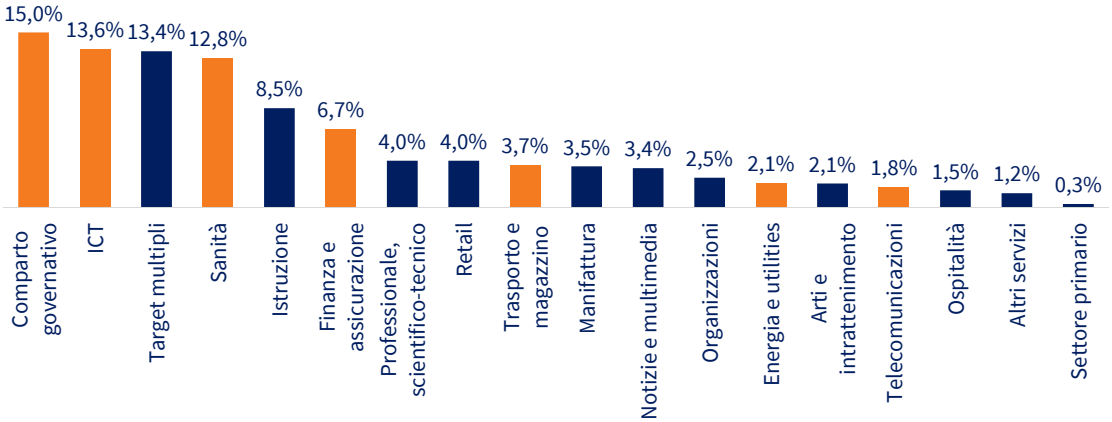

Figura 1.9. Ripartizione degli attacchi informatici in Italia per settore delle vittime (percentuale), 2021. *Fonte: elaborazione The European House – Ambrosetti su dati Clusit, 2023.*

Relativamente all'impatto economico degli attacchi, è stato rilevato come nei settori ad alta regolamentazione in termini di protezione del dato – come per esempio il settore sanitario, finanziario, energetico, farmaceutico, dell'istruzione – i costi tendano ad **accumularsi negli anni successivi alla violazione**. Se, in media, gli attacchi vendono una distribuzione

tendenzialmente maggiore nel primo (52%) e nel secondo anno dall'attacco (29%), e una quota minore nei periodi successivi (19%), tale tendenza si modifica osservando settori a più o meno alta regolamentazione. Per esempio, nei settori a bassa regolamentazione i costi si distribuiscono soprattutto nel primo (66%) e nel secondo anno (26%) e in misura decisamente minore nel periodo successivo (8%); al contrario, nei settori più regolamentati si rileva ancora una quota rilevante dei costi anche dopo il secondo anno dall'attacco (24% del costo dell'attacco). Tale dinamica è connessa al fatto che in tali settori i **costi di regolamentazione e legali** possono contribuire a elevare i costi nel corso degli anni successivi a una violazione.

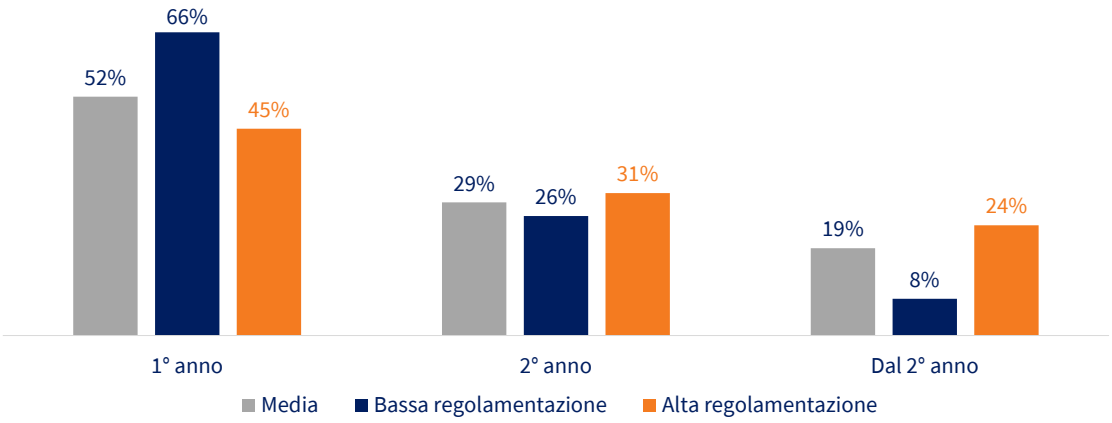

Figura 1.10. Distribuzione temporale dei costi di un attacco informatico, per grado di regolamentazione del settore in termini di protezione del dato (percentuale). *Fonte: elaborazione The European House – Ambrosetti su fonti varie, 2023.*

Dalle evidenze illustrate all'interno di questo capitolo, emerge come – in un contesto di **crescente pervasività della digitalizzazione** e crescente esposizione a **rischi di sicurezza** – diventi cruciale sfruttare le tecnologie di *cybersecurity* per **abilitare approcci di *cyber*-resilienza**. Considerando la *cybersecurity* come quell'insieme dei mezzi, delle tecnologie e delle procedure tesi alla **protezione dei sistemi informatici** in termini di disponibilità, confidenzialità e integrità dei beni o *asset* informatici, risulta fondamentale intendere la *cybersecurity* come un fattore abilitante per la crescita e la continuità delle attività economiche e sociali. In questo quadro, la *cyber*-resilienza si sostanzia dunque nella capacità di **anticipare, resistere, riprendersi e adattarsi** a condizioni avverse, stress, attacchi o compromissioni su sistemi che utilizzano risorse informatiche.

Un esempio emblematico che mette in luce la necessità di adottare un approccio efficace e, allo stesso tempo, resiliente alla sicurezza informatica è rappresentato dal caso dell'attacco *hacker* alla **Colonial Pipeline** in cui, vista l'elevata strategicità degli *asset* detenuti dalla società, un attacco informatico ha provocato un blocco nelle funzioni di approvvigionamento di carburante in tutta la costa orientale degli Stati Uniti.

Case study: l'attacco *hacker* alla Colonial Pipeline che ha rischiato di paralizzare le forniture energetiche nella East Coast

A maggio 2021, la Colonial Pipeline, una delle principali società di trasporto di carburante degli Stati Uniti che gestisce circa il **45% degli approvvigionamenti** lungo la costa orientale, ha subìto un attacco informatico da un gruppo di *hacker* (DarkSide) che ha utilizzato un *ransomware* per bloccare l'accesso ai sistemi informatici della società.

Nonostante la compromissione di Colonial Pipeline riguardasse solo la rete *corporate* dell'azienda, per evitare una **diffusione del virus** nel resto della filiera di distribuzione e fornitura, i dirigenti hanno deciso di **chiudere l'intero oleodotto**, causando la **riduzione della disponibilità** di carburante (2,5 milioni di barili al giorno) e **incrementando il prezzo** del petrolio e l'incertezza dei clienti che hanno gareggiato per impadronirsi delle scorte. Per questa ragione, l'aeroporto di Charlotte ha dovuto modificare gli orari dei voli e quello di Atlanta ha dovuto ricercare altri fornitori di greggio, mentre circa il 70-90% delle stazioni di rifornimento sono rimaste a secco per "crisi di panico" tra i consumatori.

La Colonial Pipeline ha dovuto pagare un riscatto di **4,4 milioni di Dollari** agli *hacker* per ripristinare l'accesso ai propri sistemi, visti gli importanti danni sistemici impartiti all'economia statunitense.

A seguito di questa vicenda, il Presidente degli Stati Uniti ha dovuto dichiarare lo **stato di emergenza** per poter scongiurare una crisi provocata dalla carenza di petrolio e diramare un ordine esecutivo al fine di rafforzare la cyber difesa del Paese.

Il caso di Colonial Pipeline rappresenta un caso emblematico del ruolo strategico giocato dalla *cybersecurity* per garantire la continuità delle operazioni delle infrastrutture critiche che impattano sull'intero sistema-Paese. Il **blocco di un'infrastruttura critica** può infatti provocare **ripercussioni e danni sistemici su tutto il Paese**, a causa della **crescente integrazione** delle tecnologie dell'informazione con gli enti strategici che genera forti interdipendenze nei settori chiave.

Fonte: elaborazione The European House – Ambrosetti fonti varie, 2023.

2. Il quadro normativo a livello europeo e italiano in termini di *cybersecurity*: elementi evolutivi e criticità aperte

Il quadro normativo sulla *cybersecurity* a livello europeo e italiano

La crescente rilevanza dell'economia digitale e il ruolo strategico giocato dalla *cybersecurity* nel garantirne i processi e le funzioni hanno posto l'accento sulla necessità da parte dei Governi di adottare un **quadro normativo** che tenga conto di questi cambiamenti, cercando di **governare e regolamentare questo fenomeno**.

In particolare, nell'ultimo decennio è stata riposta una **crescente attenzione nei confronti della *cybersecurity*** a livello europeo, tramutata nella realizzazione di **strategie comunitarie e direttive** – di cui è di seguito presentata una rassegna – volte alla regolamentazione negli *standard* di sicurezza informatica.

Già nel 2013, infatti, l'Unione Europea si dota dell'**EU Cybersecurity Strategy**, la prima strategia comunitaria sulla *cybersecurity*, finalizzata a raggiungere la *cyber-resilience*, ridurre il *cybercrime*, sviluppare politiche e competenze nell'ambito della Politica di Sicurezza e Difesa Comune, sviluppare risorse industriali e tecnologiche e stabilire uno spazio di *policy* coerente nel contesto europeo. Per dar seguito a queste ambizioni e tramutarle in azioni, nel 2014 è stata emanata la **Direttiva eiDAS**, che fornisce un metodo comune per il riconoscimento dei mezzi di identificazione elettronica tra Paesi membri, delinea un primo quadro normativo relativo ai servizi fiduciari – in particolare alle transazioni monetarie – e stabilisce un quadro giuridico per firme, documenti e servizi elettronici.

Vista la rapida evoluzione del mercato digitale, con particolare riferimento al forte sviluppo dei servizi *online* (*e-commerce*, scambi elettronici, ecc.), l'Unione Europea ha sentito l'esigenza di realizzare una strategia più ampia, che coprisse non solo l'ambito della sicurezza informatica, ma che provasse a indirizzare i nuovi *trend* digitali per favorire la creazione di un mercato unico digitale a livello comunitario. A tal proposito, nel 2015 è stata pubblicata la **Digital Single Market Strategy**, che presenta 3 principali direttive di sviluppo:

- migliorare l'accesso *online* per consumatori e imprese (*e-commerce* e transfrontaliero, geo-*blocking*, diritto d'autore);
- creare un mercato digitale equo e competitivo (norme per settore TLC, media, piattaforme; sicurezza e dati);
- massimizzare il potenziale di crescita (economia dei dati, interoperabilità e *standard*, competenze e P.A.).

L'implementazione di questa strategia ha portato, nel 2016, all'emanazione della **Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione** (**NIS**)[3], la Direttiva di

[3] La Direttiva è stata recepita da tutti gli Stati Membri entro il 2018. L'Italia ha recepito la Direttiva con il Decreto legislativo n.65 del 18 maggio 2018 entrato in vigore il 26 giugno 2018.

riferimento – ancora oggi, in attesa della piena attuazione della NIS 2 – in materia di sicurezza informatica a livello comunitario. La finalità della NIS è quella di raggiungere un elevato livello comune in materia di sicurezza delle reti e dei sistemi di informazione in tutta l'UE, tramite:

- l'identificazione degli operatori di servizi essenziali e digitali;
- l'obbligo di adozione di strategie nazionali di sicurezza della rete e dei sistemi informativi;
- l'istituzione di un gruppo di cooperazione e di una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT);
- l'identificazione di obblighi in materia di sicurezza e notifica degli incidenti;
- l'obbligo di designazione di autorità nazionali competenti, punti di contatto unici e CSIRT.

La NIS, dunque, si rivolge a due tipologie di aziende operanti in Europa: **Operatori dei servizi essenziali** (OES) e **Fornitori di servizi digitali** (FSD).

Gli **OES** sono i soggetti pubblici o privati che soddisfano tre criteri:

- il soggetto fornisce un **servizio essenziale** per il mantenimento di attività sociali e/o economiche fondamentali;
- la fornitura di tale servizio è dipendente dalla **rete e** dai **sistemi informativi**;
- un incidente ha **effetti negativi rilevanti** sulla fornitura di tale servizio.

I **settori** che rientrano nel perimetro dalla Direttiva NIS sono: Acqua potabile; Energia; Infrastrutture digitali; Infrastrutture del mercato bancario e finanziario; Salute; Trasporti.

Dato il ruolo strategico giocato dagli OES per garantire la sicurezza informatica europea, questi sono tenuti ad adottare **misure** finalizzate a tutelarne i relativi *asset*, ovvero:

- **misure tecniche e organizzative** adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni;
- misure adeguate a prevenire e **minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurarne la continuità.

Inoltre, gli OSE sono tenuti a comunicare al CSIRT italiano (gruppo di intervento per la sicurezza informatica in caso di incidente) e all'Autorità competente NIS, senza ingiustificato ritardo, gli **incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti**. A tal proposito, gli Stati membri sono tenuti a stabilire sanzioni pecuniarie[4] e ad adottare le misure necessarie per garantirne l'attuazione.

I **FSD** sono definiti come le aziende che forniscono il loro servizio dietro compenso, a distanza, per via elettronica e su richiesta individuale di un destinatario di servizi. I FSD possono essere classificati in motori di ricerca, servizi di *cloud computing* e piattaforme di commercio elettronico. Diversamente dagli OES, gli FSD sono liberi di adottare le misure che considerano adeguate e proporzionate alla gestione dei rischi, a condizione che forniscano un adeguato

[4] L'Italia con il decreto legislativo 65/2018 ha previsto sanzioni amministrative fino a €150.000.

livello di sicurezza, considerando cinque principali elementi: a) i sistemi e le infrastrutture di sicurezza; b) la gestione dell'incidente; c) la gestione della continuità aziendale; d) monitorare, controllare e testare; e) la conformità con gli *standard* internazionali. Inoltre, la Direttiva NIS non si applica a FSD che sono considerati piccoli e alle micro aziende, ovvero aziende che hanno meno di 50 dipendenti e il cui fatturato totale di bilancio annuo sia inferiore a 10 milioni di Euro.

Nello stesso anno della pubblicazione della Direttiva NIS, l'Unione Europea pubblica il **Regolamento generale sulla protezione dei dati** (**GDPR**), agendo questa volta sulla tutela dei dati personali dei cittadini, armonizzando i sistemi di protezione dei dati personali nell'UE, prescrivendo l'applicazione anche al trasferimento di dati personali al di fuori dell'UE e verso tutte le imprese che processano i dati personali dei cittadini europei.

Fino al 2019 la sicurezza dei sistemi IT utilizzati nei Paesi europei era garantita dai Governi, che si orientavano sulla base di ***Common Criteria***[5], ovvero degli *standard* internazionali per il rilascio di una certificazione di sicurezza informatica per gli apparati ICT.

[5] Nati nel 1996 per fornire livelli di valutazione definiti in modo simile e che riprendono sia il concetto di Target che la centralità del documento Security Target, si sono trasformati nel 1999 in *standard* internazionale ISO/IEC 15408, grazie alla certificazione dell'ISO (International Organization for Standardization), imponendosi come punto di riferimento globale per la valutazione della sicurezza informatica.

Focus: il funzionamento dei *Common Criteria* e il loro ruolo in Europa

I *Common Criteria* dettano la disciplina, a livello internazionale, per la valutazione della sicurezza informatica. Si tratta di criteri che rendono oggettivamente **misurabili**, e quindi **comparabili**, le proprietà di un prodotto o di un sistema informatico in termini di sicurezza.

L'obiettivo principale dell'utilizzo dei *Common Criteria* è quello di **garantire un elevato grado di fiducia, efficacia e correttezza** della documentazione prodotta. L'ente preposto alla verifica di tale documentazione ha, quindi, il compito di costruire l'oggetto della valutazione, o Target of Evaluation (TOE), attenendosi ai criteri qualitativi di imparzialità, ripetibilità, riproducibilità e obiettività.

Il processo di certificazione dei *Common Criteria* prevede la valutazione del TOE in esame e, in particolare, l'identificazione di **tre elementi di valutazione fondamentali**:

- il primo consiste negli **obiettivi di sicurezza**, ossia l'intenzione per cui si procede alla valutazione;
- il secondo si riferisce all'**ambiente di sicurezza**, che corrisponde sia al contesto di utilizzo che all'uso del prodotto/sistema in esame;
- il terzo elemento riguarda i **requisiti funzionali**, vale a dire le verifiche di sicurezza e il livello di *assurance* che ne deriva.

L'ottenimento della certificazione comporta una serie di vantaggi in capo al fornitore del prodotto ICT, tra cui l'**aumento della competitività** sul mercato e, quindi, della domanda. I consumatori, infatti, nel comparare i prodotti/servizi disponibili sul mercato, tendono a preferire quelli corredati da una certificazione di sicurezza.

Data la continua espansione del mondo digitale e il conseguente aumento del rischio cibernetico, negli ultimi anni si è assistito a **crescenti richieste**, e rilasci, di certificazioni di sicurezza nel contesto europeo. I *Common Criteria* hanno, quindi, contribuito significativamente ad accrescere il livello di sicurezza di servizi e prodotti digitali, trascurando tuttavia la necessità di **creare schemi di certificazioni comuni e omogenei** tra i Paesi membri, che hanno dovuto trasporre questi criteri a livello nazionale, tenendo conto delle diverse esigenze dei territori di riferimento.

Fonte: elaborazione The European House – Ambrosetti su I-Com ("Rapporto osservatorio sulla Cibersicurezza"), 2023.

L'applicazione dei *Common Criteria* ha indotto una **proliferazione di schemi di certificazioni** eterogenei tra i diversi Paesi. Nello specifico, il numero di prodotti certificati in Europa è cresciuto negli anni del **60%** rispetto al 2013, raggiungendo il suo apice nel 2021 con un totale di **411**.

L'utilizzo dei *Common Criteria* risulta essere ampiamente diffuso anche al di fuori dell'Unione Europea. Il primo Paese al mondo per certificazioni prodotte sono infatti gli Stati Uniti, con un totale di 90 certificazioni, seguite da Germania (64) e Francia (609). Nella *top*-10 mondiale è anche possibile trovare il Giappone (in quinta posizione con 36 certificazioni), il Canada (in settima posizione con 20 certificazioni) e la Corea del Sud (in decima posizione con 9 certificazioni). In questo contesto, l'**Italia** si posiziona nona con un totale di **11 certificazioni**.

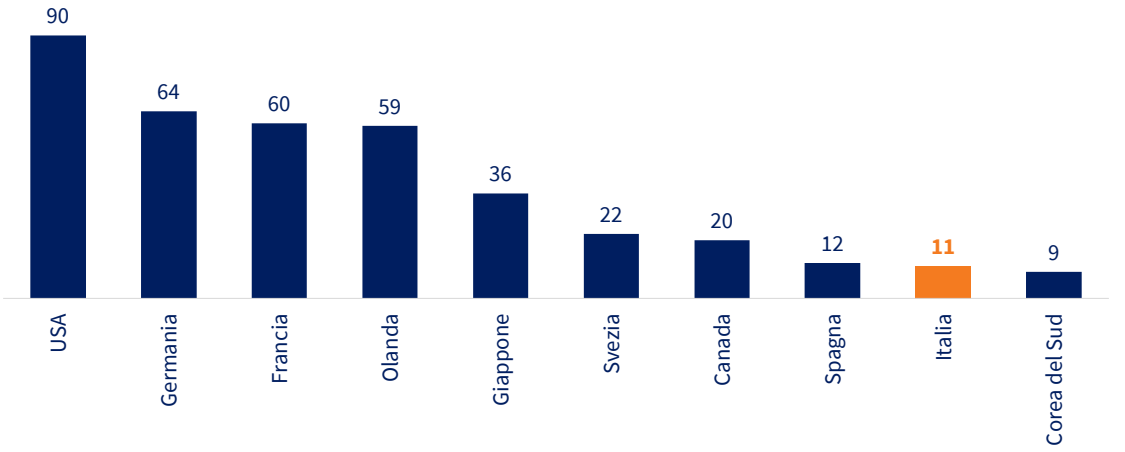

Figura 2.1. *Top*-10 Paesi per certificazioni prodotte con Common Criteria (valore assoluto), 2021. *Fonte: elaborazione The European House – Ambrosetti su dati I-Com, 2023.*

Ad oggi, tuttavia, i *Common Criteria* presentano alcuni elementi di attenzione. In primo luogo, l'**elevata frammentazione** e **complessità** dello scenario di certificazione produce numerosi ostacoli non solo al raggiungimento degli *standard* prefissati, ma anche in termini più generali alla ricerca innovativa di soluzioni e allo sviluppo di livelli minimi di fiducia condivisi tra produttori e consumatori. In particolare, uno dei principali elementi di complessità nel raggiungere gli *standard* auspicati è rappresentato dall'aumento dei costi – a carico dei fornitori – da sostenere per produrre la documentazione richiesta dai sistemi nazionali, costituendo una barriera per lo sviluppo efficiente di tali controlli.

A questo si aggiunge un'**elevata lunghezza dei tempi** di esecuzione della valutazione da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dai laboratori indipendenti per rendere effettive le relative procedure e rilasciare le certificazioni, non conformi al dinamismo evolutivo del settore digitale. I principali operatori del settore sottolineano, infatti, l'insostenibilità di tale processo di certificazione, con un numero di *test* annui che i laboratori sono in grado di eseguire che si aggira sui 10-15, a fronte di un crescente numero di prodotti da certificare, proporzionale al numero di aziende coinvolte all'interno del Perimetro di sicurezza cibernetico[6] (circa 300).

Infine, l'**elevata rigidità** non permette di mantenere la certificazione per prodotti/sistemi su cui vengono installati nuovi aggiornamenti. In questo caso, infatti, il prodotto deve essere sottoposto nuovamente all'intero processo di valutazione, il che comporta ulteriori costi e un disincentivo a investire nello sviluppo di migliorie e innovazioni.

Per sopperire alle esigenze di modifica e uniformità della normativa in tema di certificazione, nel 2019 è stato introdotto l'**EU Cybersecurity Act**[7], con l'obiettivo di creare un nuovo sistema di certificazioni uniforme in tutta Europa. Nello specifico, esso mira a rafforzare il ruolo di

[6] Il tema del Perimetro di sicurezza cibernetico verrà approfondito più avanti nel presente capitolo.

[7] Attualmente l'EU Cybersecurity Act si trova ancora nella fase iniziale di sviluppo.

ENISA[8] nel supportare gli Stati membri nel fronteggiare attacchi e minacce informatiche e nel costituire un *framework* di certificazione di cybersicurezza comune tra i Paesi Membri dell'Unione Europea.

Con riferimento al processo di certificazione, gli **elementi di discontinuità** dell'EU Cybersecurity Act rispetto ai *Common Criteria* applicati nei sistemi nazionali non risiedono tanto nella struttura del meccanismo, quanto nella volontà da parte delle istituzioni europee di affrontare alcune delle principali criticità che tali sistemi presentavano nel rapporto con le dinamiche di mercato (in particolare lunghezza dei tempi ed elevati costi). I principali elementi di discontinuità identificati sono:

- l'adozione di **nuove procedure armonizzate** per la gestione della criticità non previste al momento del rilascio e una procedura di valutazione rapida per le correzioni e le modifiche successive dei prodotti;
- l'introduzione di **nuovi criteri armonizzati** volti a rafforzare il mantenimento dei certificati nel tempo, così da limitare i tempi e i costi per i produttori;
- la realizzazione di un **sito dedicato** alle certificazioni di cybersicurezza contenente le linee guida del sistema adottato e gli *status* delle certificazioni emesse, oltre a un'etichetta specifica per i prodotti certificati che mostri il livello di sicurezza assicurato.

In applicazione del Cybersecurity Act, l'ENISA ha istituito un **gruppo di lavoro** per sostenere la stesura dei *Common Criteria* Europei (EUCC[9]), sulla base di quelli esistenti.

Nonostante gli sforzi europei per uniformare la normativa con riguardo alle certificazioni, permangono ancora diversi **punti di attenzione** non risolti o non chiari sull'implementazione del nuovo schema comune, per esempio:

- la normativa non specifica cosa si intende per «***screening* tecnologico**» e quanto questo dovrà essere intrusivo. Condividere il codice con enti terzi significa mettere a rischio la proprietà intellettuale, con potenziali ricadute sulla competitività;
- la normativa non chiarisce **a quale soggetto imputare i costi** dello *screening* tecnologico, senza risolvere dunque il nodo degli oneri già presente nei *Common Criteria* che ledeva la competitività delle imprese;
- detenere la certificazione, pur non essendo obbligatoria, può avere un effetto discriminante sulla scelta dei fornitori, implicando **distorsioni di mercato** a danno degli operatori più piccoli;
- non è stabilito se gli ***asset* già presenti** all'interno delle PA o delle aziende private soggette a perimetro dovranno essere certificati/aggiornati per soddisfare i nuovi criteri.

L'anno successivo all'EU Cybersecurity Act, nel 2020, l'Unione Europea ha presentato due nuove strategie (EU Security Union Strategy e EU Cybersecurity Strategy) a supporto della sicurezza informatica europea, introducendo per la prima volta il concetto di resilienza

[8] Agenzia dell'Unione europea per la cibersicurezza.

[9] Common Criteria based European candidate cybersecurity certification scheme.

informatica, ovvero la capacità di reagire in modo flessibile ed efficace agli attacchi informatici, minimizzando i danni sui sistemi e i processi aziendali strategici. In particolare, l'**EU Security Union Strategy** punta a:

- creare un **ambiente della sicurezza** adeguato al futuro (protezione e resilienza delle infrastrutture critiche, degli spazi pubblici e digitali);
- affrontare le **minacce in evoluzione** (con particolare riferimento alle minacce informatiche);
- mettere a punto azioni volte alla protezione dei sistemi nazionali e aziendali da **terrorismo e criminalità organizzata**;
- realizzare un forte **ecosistema della sicurezza**, basato su cooperazione, frontiere esterne, ricerca, innovazione, competenze.

Dall'altro lato, l'**EU Cybersecurity Strategy** identifica tre principali linee di azioni su cui agire per garantire livelli di sicurezza adeguati alle sfide attuali future:

- **resilienza, sovranità tecnologica e leadership** (NIS 2, centri operativi per la sicurezza, sostegno a PMI e competenze);
- sviluppo della capacità operativa di **prevenzione, deterrenza e risposta** (Joint Cyber Unit, Cyber Diplomacy Toolbox, fondi);
- promozione di un **ciberspazio globale e aperto** (cooperazione e diplomazia internazionale; investimenti nel quadro del RRF).

In applicazione di queste strategie sulla sicurezza informatica, nel 2021 è stato presentato il **Cyber Resilience Act** (bozza ad oggi ancora in discussione), in cui sono identificate le norme per l'immissione sul mercato dei prodotti; i requisiti e gli obblighi per gli operatori per la progettazione, lo sviluppo e la produzione di prodotti, nonché per la gestione delle vulnerabilità nell'intero ciclo di vita; e infine le norme sulla vigilanza del mercato e sull'applicazione delle stesse.

Inoltre, tra il 2021 e il 2022 sono state presentate due leggi europee, riguardanti la gestione dei dati e i servizi digitali. Il **Data Governance Act** prevede di aumentare la disponibilità di dati da utilizzare, incrementando la fiducia negli intermediari che gestiscono questi dati e rafforzando i meccanismi di condivisione degli stessi all'interno dell'Unione Europea. Dall'altro lato, il **Digital Services Act Package** mira a classificare le piattaforme *gatekeeper*[10] e definirne gli obblighi; impedire ai grandi operatori di abusare del potere di mercato e facilitare l'ingresso nel mercato a operatori nuovi e più piccoli; fornire una nuova legislazione riguardante i contenuti illegali, la pubblicità trasparente e la disinformazione; introdurre nuovi obblighi di trasparenza sui meccanismi di funzionamento degli algoritmi.

A queste leggi, nel 2022 si aggiungono due Direttive. La prima, la **Direttiva CER**, sostituisce la direttiva europea sulle infrastrutture critiche del 2008, identificando misure finalizzate a garantire la fornitura nel mercato interno di servizi essenziali per il mantenimento di funzioni

[10] I fornitori di servizi di piattaforma di base, ovvero i "*core platform services*".

vitali della società o di attività economiche; obblighi per i soggetti critici in termini di rafforzamento della resilienza e di miglioramento della capacità di fornire tali servizi nel mercato interno; e norme sulla vigilanza sui soggetti critici e l'esecuzione delle norme.

La seconda Direttiva è la **NIS 2**, che aggiorna e amplia il perimetro e gli scopi della precedente Direttiva (NIS), a seguito di diverse criticità riscontrate dalla Commissione Europea. Nello specifico, la Commissione ha identificato **sei principali criticità** connesse alla prima Direttiva NIS:

- la **crescente interconnessione e interdipendenza** tra settori non è affrontata;
- il **perimetro** non è chiaramente definito e le **competenze** nazionali connesse ai *provider* digitali non sono chiare;
- i requisiti di **sicurezza e *reporting*** sono divergenti;
- la **supervisione** e l'**attuazione** sono inefficaci;
- le **risorse stanziate** dai Paesi membri per le autorità competenti sono eterogenee;
- la **condivisione di informazioni** tra Paesi è limitata.

A testimonianza di un'implementazione eterogenea, l'Italia ha identificato **0,9 Operatori di Servizi Essenziali (OSE) ogni 100mila abitanti**, mentre la Francia solo 0,4, con una differenza di oltre OSE 400 in termini assoluti tra i due Paesi.

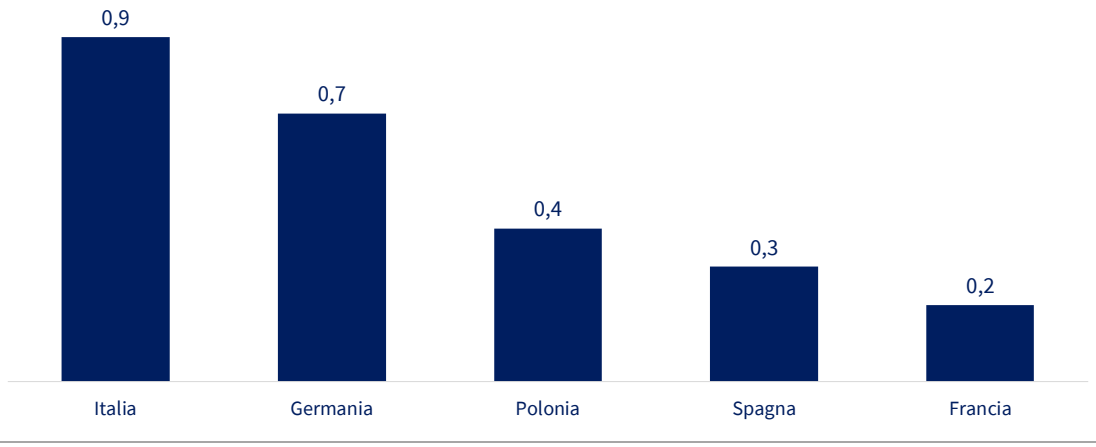

Figura 2.2. Numero di Operatori di Servizi Essenziali (OSE) identificati nell'ambito della NIS (ogni 100 mila abitanti), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2023.*

La nuova Direttiva NIS2, entrata in vigore a gennaio 2023, cerca dunque di affrontare queste criticità. Il principale elemento di novità è rappresentato dall'ampliamento dei soggetti destinatari della normativa e un'uniformazione dei soggetti inclusi: da "Operatori di Servizi Essenziali" e "Fornitori di Servizi Essenziali", identificati nella precedente Direttiva, a "**Soggetti Essenziali**" e "**Soggetti Importanti**". In questo modo, la nuova Direttiva crea una "gerarchia" di settori strategici sui quali la normativa deve intervenire, differenziandoli per livelli di criticità, ovvero:

- settori essenziali: energia, trasporti, banche, infrastrutture finanziarie, acqua potabile, sanità, TLC e servizi digitali;

– settori ad alta criticità: acque reflue, servizi ICT B2B, Pubblica Amministrazione, spazio;
– altri settori critici: servizi postali, rifiuti, industria chimica, alimentare, medicale, informatica ed elettronica, automotive, enti di ricerca.

In aggiunta al criterio della criticità, la NIS2 introduce anche un criterio dimensionale (*size cap*), secondo cui tutte le medie e grandi imprese che operano nei settori o forniscono il tipo di servizi coperti dalla direttiva, rientrano nel suo campo di applicazione.

La normativa ha inoltre previsto **normative più stringenti e specifiche** in termini di *cyber risk management*, di segnalazione e condivisione delle informazioni relative agli incidenti di sicurezza, introducendo un approccio basato sul concetto del c.d. "multirischio".

La nuova normativa impone dunque **maggiori costi**, soprattutto in termini di ***compliance***, tra cui l'implementazione dei requisiti di sicurezza e degli obblighi di *reporting* e l'applicazione delle misure di supervisione. Secondo le stime della Commissione Europea, i **costi della nuova normativa** per le medie e grandi imprese ammonteranno a circa **35 miliardi di Euro** a livello europeo e a **840 mila Euro in media per azienda**. In particolare, per i settori già precedentemente inclusi nel perimetro della normativa NIS, i costi ICT registreranno un incremento del **12%** in 3-4 anni, mentre per i settori non coperti originariamente dalla NIS (che rientrano grazie all'allargamento del perimetro strategico) lo stesso incremento è stimato essere del **22%**.

A livello settoriale, il comparto su cui gravano maggiormente i costi di adeguamento alla nuova normativa è quello dell'***automotive***, che complessivamente richiederà un investimento aggiuntivo di 6,9 milioni di Euro a livello europeo, seguito dal settore energetico (6,0 milioni di Euro), dall'industria meccanica (4,0 milioni di Euro), quella alimentare (3,7 milioni di Euro) e il *retail* alimentare (3,3 milioni di Euro).

Considerando invece il **costo per impresa**, l'*automotive* rimane il settore con maggiore incidenza di costi, seguito da energia, ma risultano anche fortemente colpite le imprese operanti nella farmaceutica e negli altri mezzi di trasporto.

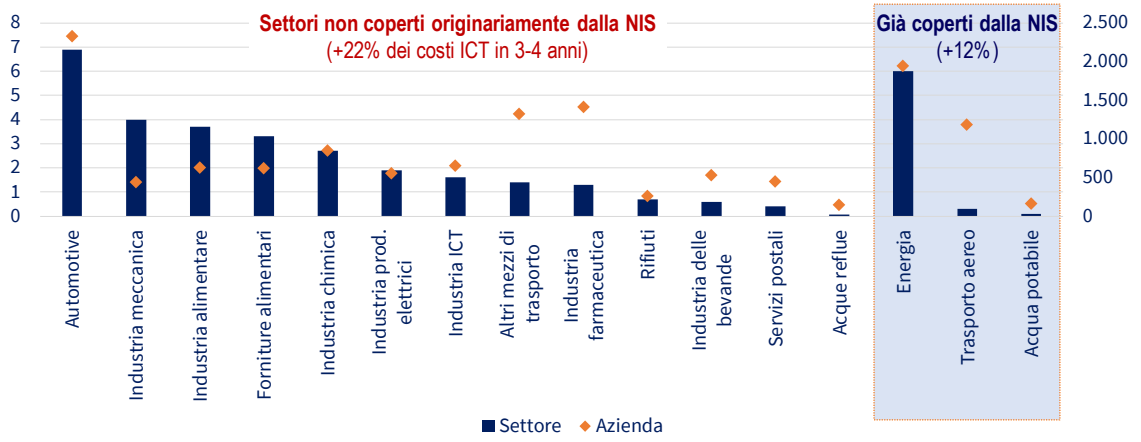

Figura 2.3. Costi ICT aggiuntivi della normativa NIS per le medie e grandi imprese e a livello europeo, a livello settoriale (milioni di Euro, asse sinistro) e a livello aziendale (migliaia di Euro, asse destro), 2020. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2023.*

Lo stesso scenario cambia analizzando esclusivamente le **imprese di media dimensione**, depurando dalle grandi realtà europee. In particolare, il settore maggiormente colpito dai costi di adeguamento risulta essere l'industria alimentare, che raggiunge **1,4 miliardi di Euro** di costi complessivi di *compliance*, pari a due volte il secondo settore, l'industria chimica, che registra circa 700 milioni di Euro di costi. A livello di singola **impresa**, i costi si aggirano su circa 300mila Euro per l'alimentare, seguita dall'industria chimica (280mila Euro) e dalla farmaceutica (circa 170mila Euro).

Complessivamente, per le imprese di media dimensione si stimano circa **3,1 miliardi di Euro** di costi a livello europeo e circa **150 mila Euro** in media per azienda.

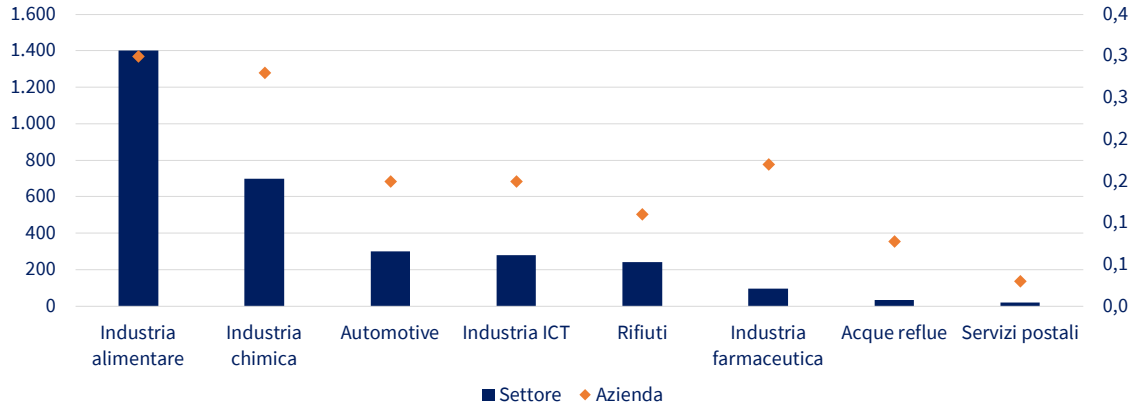

Figura 2.4. Costi ICT aggiuntivi della normativa NIS per le medie imprese a livello europeo e a livello settoriale (milioni di Euro, asse sinistro) e a livello aziendale (milioni di Euro, asse destro), 2020. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2023.*

A seguito alla NIS2, infine, nel 2023 è stato emanato il **Digital Operational Resilience Act** (**DORA**), che identifica: obblighi per le entità finanziarie in materia di gestione dei rischi, segnalazione alle autorità, test di resilienza e condivisione dei dati; obblighi per gli accordi contrattuali tra fornitori terzi di servizi ICT ed entità finanziarie; un quadro di sorveglianza per i fornitori terzi di servizi ICT critici che forniscono servizi a entità finanziarie.

Da ultimo, nell'aprile 2023 la Commissione ha proposto un **Cyber Solidarity Act**, con l'obiettivo di migliorare il livello di preparazione e la capacità di risposta ai rischi di sicurezza informatica. In particolare, la proposta prevede l'istituzione di uno scudo informatico europeo, ovvero un'infrastruttura paneuropea composta da centri operativi di sicurezza (SOC) nazionali e transfrontalieri in tutta l'UE incaricati di rilevare e agire sulle minacce informatiche. Il Cyber Solidarity Act prevede anche la creazione di un meccanismo di emergenza informatica, per sostenere azioni di preparazione nei settori critici, servizi di risposta agli incidenti e supporto finanziario in ottica di mutua assistenza tra gli Stati membri. Infine, è previsto un meccanismo di riesame degli incidenti di cybersicurezza volto ad analizzare e valutare gli incidenti rilevanti.

Nel complesso, dunque, l'Unione Europea ha adottato diverse misure per allineare la normativa europea in materia di sicurezza informatica ai nuovi *trend*, rapidamente in evoluzione. Tuttavia, l'elevato numero di leggi sulla *cybersecurity* ha comportato un'alta

complessità normativa, sia dal lato dei Paesi membri che devono recepire norme e Direttive europee, sia dal lato delle imprese che devono adeguare repentinamente i loro modelli operativi e di *business* alle nuove esigenze, sia comunitarie sia nazionali.

Alle leggi in materia di sicurezza informatica si aggiungono infatti anche numerose **linee guida** definite a livello europeo, per esempio nell'ambito dell'EU Electronic Communications Code (EECC). Gli ambiti di azione su cui vengono concentrate tali linee guida sono: *governance* e gestione del rischio, sicurezza delle risorse umane, sicurezza di sistemi e strutture, gestione delle operazioni, gestione degli incidenti, gestione della continuità operativa, monitoraggio, *auditing* e test, consapevolezza delle minacce.

Queste numerose linee guida, non ancora vincolanti dal punto di vista giuridico, contribuiscono tuttavia ad aprire diversi scenari evolutivi sugli ulteriori sviluppi del quadro regolatorio, creando dunque **interrogativi e incertezze**, *in primis* per le imprese.

- **D1: GOVERNANCE E GESTIONE DEL RISCHIO**
- SO1: Politica di sicurezza delle informazioni
- SO2: Governance e gestione del rischio
- SO3: Ruoli e responsabilità per la sicurezza
- SO4: Sicurezza delle dipendenze di terzi
- **D2: SICUREZZA DELLE RISORSE UMANE**
- SO5: Controlli di base
- SO6: Conoscenza e formazione sulla sicurezza
- SO7: Cambiamenti del personale
- SO8: Gestione delle violazioni
- **D3: SICUREZZA DI SISTEMI E STRUTTURE**
- SO9: Sicurezza fisica e ambientale
- SO10: Sicurezza delle forniture
- SO11: Controllo degli accessi alla rete e ai sistemi informativi
- SO12: Integrità della rete e dei sistemi informativi
- SO13: Uso della crittografia
- SO14: Protezione dei dati critici per la sicurezza
- **D4: GESTIONE DELLE OPERAZIONI**
- SO15: Procedure operative
- SO16: Gestione delle modifiche
- SO17: Gestione delle risorse
- **D5: GESTIONE DEGLI INCIDENTI**
- SO18: Procedure di gestione degli incidenti
- SO19: Capacità di rilevamento degli incidenti
- SO20: Segnalazione e comunicazione degli incidenti
- **D6: GESTIONE DELLA CONTINUITÀ OPERATIVA**
- SO21: Strategia di continuità del servizio e piani di emergenza
- SO22: Capacità di disaster recovery
- **D7: MONITORAGGIO, AUDITING E TEST**
- SO23: Politiche di monitoraggio e registrazione
- SO24: Esercitazione dei piani di emergenza
- SO25: Test della rete e dei sistemi informativi
- SO26: Valutazioni della sicurezza
- SO27: Monitoraggio della conformità
- **D8: CONSAPEVOLEZZA DELLE MINACCE**
- SO28: Informazioni sulle minacce
- SO29: Informazione agli utenti sulle minacce

Figura 2.5. Le linee guida europee sulle misure di sicurezza identificate nell'ambito dell'EECC. *Fonte: elaborazione The European House – Ambrosetti su ENISA, 2023.*

In conclusione, il quadro normativo europeo sulla *cybersecurity* riflette la crescente attenzione dell'Unione Europea verso i temi di sicurezza informatica e digitalizzazione, presentando ancora oggi alcuni punti di attenzione legati soprattutto alla capacità delle imprese di implementare le misure richieste, con ricadute importanti sulla loro competitività. I **fattori di costi**, i **tempi** e lo **scopo di azione** delle misure messe in campo dall'Unione Europea rappresentano i principali ostacoli per favorire l'applicazione della normativa senza gravare eccessivamente sulle funzioni e sui processi delle imprese.

Garantire la capacità di innovazione, accrescendo allo stesso tempo la capacità di resilienza delle aziende agli attacchi informatici, resta dunque il nodo principale da sciogliere per garantire uno sviluppo sostenibile e competitivo del mercato digitale europeo.

Gli ambiti critici della normativa	Le criticità che emergono nel quadro regolatorio della *cybersecurity*
Costi	- Costi per la *compliance* (investimenti, risorse umane, ecc.) - Costi per la supervisione
Tempi	- Ampie tempistiche di elaborazione delle normative e di recepimento a livello nazionale rispetto alla rapidità dell'evoluzione tecnologica - Tempistiche per l'implementazione a livello di singola impresa
Scopo d'azione	- Focalizzazione su *provider* o *user* - Discrezionalità tra Paesi nel perimetro e nelle misure

Figura 2.6. Schema riassuntivo delle criticità che emergono nel quadro regolatorio della *cybersecurity* in Europa. *Fonte: elaborazione The European House – Ambrosetti, 2023.*

All'interno del contesto europeo, l'Italia è stato uno dei primi Paesi a muoversi verso la definizione di norme e strutture per garantire la sicurezza informatica.

In termini temporali, nel 2008 avviene la costituzione del **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche** (**Cnaipic**), già operante dal 2005, su impulso della Direttiva ECI (European Critical Infrastructure) che evidenziava la necessità di proteggere le infrastrutture critiche dal punto di vista fisico (data la recrudescenza degli attacchi terroristici), ma anche informatico. Successivamente, a seguito dell'approvazione della prima Cybersecurity Strategy dell'Unione Europea nel 2013, l'Italia si dota della prima architettura nazionale per la sicurezza informatica tramite il **Decreto Monti** nello stesso anno. Nel 2015 viene emanata la **Direttiva Renzi**, che mette ordine all'architettura ideata nel precedente decreto e inserisce il tema della *cybersecurity* nel più ampio contesto della sicurezza nazionale, attribuendone la competenza alla Presidenza del Consiglio dei Ministri. Nel 2017 il **Decreto Gentiloni** implementa le indicazioni della direttiva Renzi, introducendo una novità: seppur le competenze strategiche in materia di *cybersecurity* fossero rimaste in capo alla Presidenza del Consiglio dei Ministri, le competenze operative in materia passano ai servizi di *intelligence*.

Il Decreto Gentiloni rappresenta un primo tentativo da parte dell'Italia di recepire la normativa NIS del 2016, che sarà poi ufficialmente recepita nel 2018. Il Decreto legislativo n.65 del 18 maggio 2018 (**Decreto legislativo NIS**), entrato in vigore il 26 giugno 2018, rappresenta infatti il Decreto attuativo della Direttiva NIS, che si limita a incorporare nel quadro normativo nazionale quanto già stabilito dalla Direttiva, facendo dunque rientrare nella normativa i seguenti settori: Energia, Trasporti, Banche, Mercati finanziari, Sanità, Fornitura e distribuzione di acqua potabile, Infrastrutture digitali, Motori di ricerca, Servizi cloud e Piattaforme di commercio elettronico.

Tra le principali azioni messe in campo dal Governo italiano sui temi di sicurezza informatica è importante menzionare l'istituzione del **Perimetro di Sicurezza Nazionale Cibernetica** (**PSNC**), emanato con il Decreto legge n.105, 2019, con l'obiettivo di elevare la sicurezza dei sistemi ICT per le Pubbliche Amministrazioni e alcune imprese private selezionate. Nello specifico, il Perimetro di sicurezza cibernetica nazionale è finalizzato ad assicurare un **livello**

elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle pubbliche amministrazioni, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali, o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Il Perimetro agisce integrando il Decreto legislativo NIS, aggiungendo **nuovi settori al perimetro di sicurezza nazionale** sulla *cybersecurity*, ovvero: Settore governativo, Interno, Difesa, Spazio e aerospazio, Previdenza e lavoro, Tecnologie critiche, tra cui IA, robotica, semiconduttori, sicurezza informatica, nanotecnologie e biotecnologie. In generale, i settori inclusi nel perimetro di sicurezza nazionale cibernetica sono in parte diversi e più estesi rispetto a quelli previsti dalla Direttiva NIS, implicando difficoltà per le imprese che operano i più Paesi.

Secondo la normativa nazionale, infatti, le imprese rientranti nel Perimetro sono soggetti a specifici obblighi, ovvero:

- predisporre annualmente l'**elenco degli *asset*** "**strategici**" per la fornitura dei servizi essenziali e funzioni essenziali di pertinenza;
- con riferimento a tali *asset*, **adottare misure per assicurare elevati livelli di sicurezza e notificare** eventuali incidenti al CSIRT;
- **segnalare gli incidenti** che impattano su un bene ICT, su un sistema informativo e informatico connesso a un bene ICT, oltre che su tutti gli altri servizi, reti e sistemi dei soggetti del Perimetro;
- **comunicare** al Centro di Valutazione e Certificazione l'**intenzione di acquisire strumenti ICT** da impiegare sui propri *asset* "strategici".

Con riferimento al primo punto, i soggetti inclusi nel Perimetro predispongono e aggiornano, con cadenza almeno annuale, l'**elenco di beni ICT** di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono. Per ogni funzione essenziale, provvedono:

- a **individuare i beni ICT** necessari a svolgere la funzione essenziale o il servizio essenziale. A tal fine sono valutati: a) **l'impatto di un incidente** sul bene ICT, in termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziale; b) le **dipendenze** con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti;
- a predisporre l'**elenco dei beni ICT**.

In questo quadro, l'**Agenzia per la Cybersicurezza Nazionale** e, in particolare, il Computer Security Incident Response Team (CSIRT) e il Centro di Valutazione e Certificazione Nazionale (CVCN), svolgono un'attività di monitoraggio, controllo e certificazione sulle imprese che rientrano nel Perimetro.

Con l'entrata in vigore della nuova Direttiva NIS2 nel gennaio 2023, vengono **ulteriormente ampliati il perimetro delle aziende coinvolte nonché le obbligazioni** che queste devono adempiere per garantire gli *standard* di sicurezza comunitari. La NIS2 interviene in diversi ambiti che, anche a livello nazionale, sono già **ampiamente coperti da altre disposizioni normative**, tra cui l'adozione di misure di sicurezza e la segnalazione di incidenti.

Per questa ragione, l'attività di recepimento della Direttiva da parte del Governo italiano dovrà rispondere a due principali esigenze:

- **Armonizzazione** tra il tessuto normativo europeo e quello italiano. Le nuove disposizioni dovrebbero basarsi su quanto già attuato dagli enti (che rientrano nell'ambito di applicazione della legislazione) in conformità agli obblighi nazionali preesistenti e non dovrebbero costituire un onere aggiuntivo.
- **Semplificazione** dei requisiti e delle disposizioni nazionali in materia di sicurezza informatica. I principi che guidano i requisiti della direttiva europea dovrebbero servire anche come ispirazione per rivedere le disposizioni nazionali che sono eccessivamente onerose per i destinatari delle norme (ad esempio, il principio della gravità degli incidenti).

Infine, a maggio 2022 è stata approvata la nuova **Strategia nazionale di cybersicurezza** (2022-2026) e l'annesso Piano di implementazione. La Strategia intende perseguire **3 obiettivi** fondamentali, collegati a **82 misure** e supportati da **fattori abilitanti** (formazione, promozione della cultura della sicurezza cibernetica e cooperazione), con un ruolo chiave giocato dalle ***partnership* pubblico private**. Nello specifico, gli obiettivi sono:

- la **protezione degli *asset* strategici nazionali**, attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese;
- la **risposta alle minacce**, agli incidenti e alle crisi *cyber* nazionali, attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale;
- lo **sviluppo consapevole e sicuro** delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato.

La **migrazione in *Cloud*** della P.A. rappresenta un nodo prioritario per favorire la transizione digitale dell'Italia. Il *Cloud* è infatti l'infrastruttura abilitante per la *Data Economy* e la piena interoperabilità dei dati nella Pubblica Amministrazione. In questo contesto, un ruolo chiave è svolto dal **Polo Strategico Nazionale** (PSN), una struttura informatica per la P.A. localizzata in Italia a garanzia di continuità operativa e sicurezza. Il PSN ha l'obiettivo di **dotare la P.A. di tecnologie e infrastrutture *Cloud*** che possano beneficiare delle più alte garanzie di **affidabilità, resilienza e indipendenza**. Il PSN ospiterà principalmente **dati e servizi strategici**, la cui compromissione può avere un **impatto sulla sicurezza nazionale**. A tal

proposito, il PNRR prevede 900 milioni di Euro per la realizzazione del PSN e *milestone* che prevedono **280 migrazioni** al suo interno entro giugno 2026.

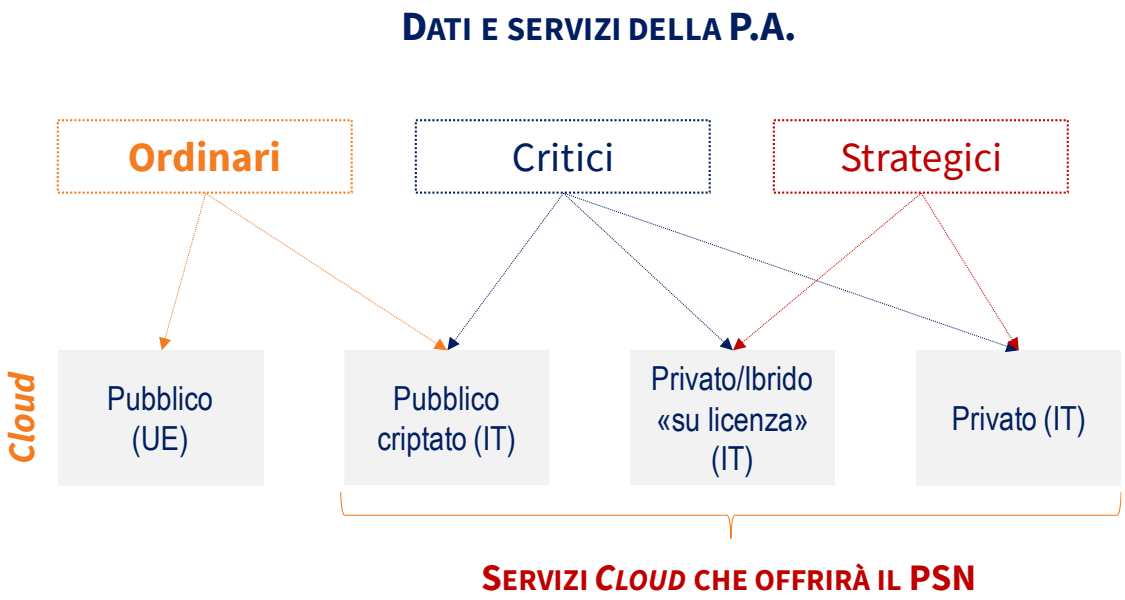

Figura 2.7. Dati e servizi in cloud della P.A. e i servizi *Cloud* che offrirà il PSN. *Fonte: elaborazione The European House – Ambrosetti su dati Strategia Cloud Italia, 2023.*

Il quadro degli investimenti in *cybersecurity* in Europa e Italia

Parallelamente all'attività normativa, l'impegno dell'Unione Europea in ambito di *cybersecurity* si sta sostanziando anche in importanti programmi di investimento per abilitare una maggiore sicurezza diffusa tra le aziende dei Paesi membri. Tra questi è possibile menzionare l'investimento di **236 milioni di Euro** tramite Horizon Europe[11], **1,6 miliardi di Euro** tramite Digital Europe[12] e **62,2 milioni di Euro** tramite Connecting Europe Facility[13]. Infine, è stato istituito a livello comunitario l'**European Cybersecurity Competence Center** (**ECCC**), un centro finalizzato a erogare sostegno finanziario per la *cybersecurity* proveniente dai programmi UE e composto dalla rete dei centri nazionali di coordinamento.

Dal punto di vista delle risorse finanziarie a disposizione in Italia, è previsto che l'**1,2% degli investimenti nazionali** su base annuale venga destinato a specifiche progettualità volte a traguardare il conseguimento dell'autonomia tecnologica in ambito digitale, oltre che l'ulteriore innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali. A ciò si

[11] Il programma europeo per sostenere la ricerca e l'innovazione dell'Unione Europea. Finora i relativi fondi sono stati stanziati nei programmi 2021-2022 e 2023-2024.

[12] Il programma europeo per sostenere la trasformazione digitale dell'UE.

[13] Il programma europeo per collegare l'UE in termini di trasporti, TLC ed energia. In questo caso i fondi sono stanziati nel ciclo di programmazione 2014-2020.

aggiungono una serie di importanti iniziative di investimento da parte del Governo italiano nel quadro del Piano Nazionale di Ripresa e Resilienza, tra cui:

- i **6,14 miliardi di Euro** per la **digitalizzazione della Pubblica Amministrazione**, di cui **623 milioni** per la ***cybersecurity***, nell'ambito della Missione 1 Componente 1 "Digitalizzazione, Innovazione e Sicurezza nella PA";
- gli **1,61 miliardi di Euro** per la creazione di almeno 10 **partenariati** tra 15 temi, tra cui è stato identificato un Partenariato sul tema *cybersecurity*, nell'ambito della Missione 4 Componente 2 "Dalla ricerca all'impresa".

A queste misure si aggiunge poi un aumento programmato delle **assunzioni** all'interno dell'Agenzia per la cybersicurezza nazionale di circa 300 specialisti entro dicembre 2023 e 800 entro il 2026.

Nell'ultimo ventennio in Europa sono proliferati i corsi sulla *cybersecurity*, con l'Italia che si attesta 2° Paese nell'UE per numerosità. Tra il 2000 e il 2020 sono stati istituiti **119 corsi sulla *cybersecurity*** in Europa, suddivisi in programmi di ***Master*** (**77%**), **lauree triennali** (**17%**) e programmi ***post-graduate*** (**6%**). Di questi programmi, il **57%** è stato tenuto **in presenza**, il 14% interamente in remoto e il **29% in modalità mista.**

A livello europeo, i corsi sulla sicurezza informatica possono essere classificati in:

- Sicurezza, calcolo e ingegneria (48,45% del totale)
- Organizzazione, gestione del rischio, *business* e *compliance* (12,11% del totale)
- Legge, etica, *policy*, *privacy* e *cybercrime* (9,55% del totale)
- *Interships* (4,49% del totale)
- Altro (25,4% del totale)

Figura 2.8. Programmi sulla *cybersecurity* in Europa (valori assoluti), 2021. *Fonte: elaborazione The European House – Ambrosetti su dati ENISA, 2023.*

Inoltre, per promuovere lo sviluppo dei talenti, il 18 aprile 2023 la Commissione Europea ha presentato la **Cybersecurity Skills Academy**, che rappresenta un approccio coordinato per colmare il divario di competenze nel campo della sicurezza informatica.

L'Academy sarà ospitata sulla **Piattaforma delle Competenze Digitali e dell'Occupazione**, in uno spazio *online* dedicato che fornisce tutte le informazioni rilevanti per gli europei interessati a una carriera nella sicurezza informatica

L'Accademia sarà organizzata in **4 pilastri** specifici:

- generazione di conoscenze attraverso **offerte di formazione**, stabilendo un approccio comune dell'UE alla formazione in sicurezza informatica;
- invito gli attori interessati a **presentare impegni**, migliorare l'**equilibrio di genere** nella sicurezza informatica e includere misure per affrontare il **divario di competenze**;
- maggiore **visibilità delle opportunità di finanziamento** e dei progetti per le attività legate alle competenze;
- sviluppo di una metodologia per monitorare la **valutazione del mercato** e misurare i progressi compiuti per colmare il divario di competenze nella sicurezza informatica.

L'obiettivo finale della Cyber Academy sarà la creazione di una **piattaforma condivisa** per l'accademia, i fornitori e l'industria al fine di **collaborare su programmi educativi**, **opportunità di formazione**, **iniziative di finanziamento** e **monitorare gli sviluppi nel mercato** del lavoro della sicurezza informatica.

Tale ambizione risulta particolarmente importante per l'Italia che, ad oggi, registra un'elevata difficoltà in Italia nel **trattenere i profili già formati**, a causa dei livelli di investimento relativamente bassi delle imprese nel personale dedicato alla *cybersecurity*.

Le tecnologie per la *cybersecurity* in Italia

L'esigenza di una riorganizzazione del quadro normativo e, più in generale, di uno sviluppo armonioso della *cybersecurity* in Italia risulta essere particolarmente pressante alla luce di **livelli di sicurezza informatica fortemente eterogenei** nei diversi settori.

Con riferimento alle imprese che usano almeno **5 misure di sicurezza ICT**, emerge come soltanto quelle operati nel settore informatico presentino livelli elevati, con un'incidenza sul totale dell'84%. In numerosi settori, le imprese con almeno 5 misure di sicurezza sono meno della metà: particolarmente critico risulta il settore dell'alloggio e ristorazione, collegato al turismo, in cui l'incidenza non supera il 30%. Questo punto di attenzione riguarda anche settori altamente strategici per il funzionamento del sistema-Paese: ad esempio, il settore della logistica e l'agroalimentare registrano un'incidenza del 45%, mentre quello delle costruzioni solo il 41%.

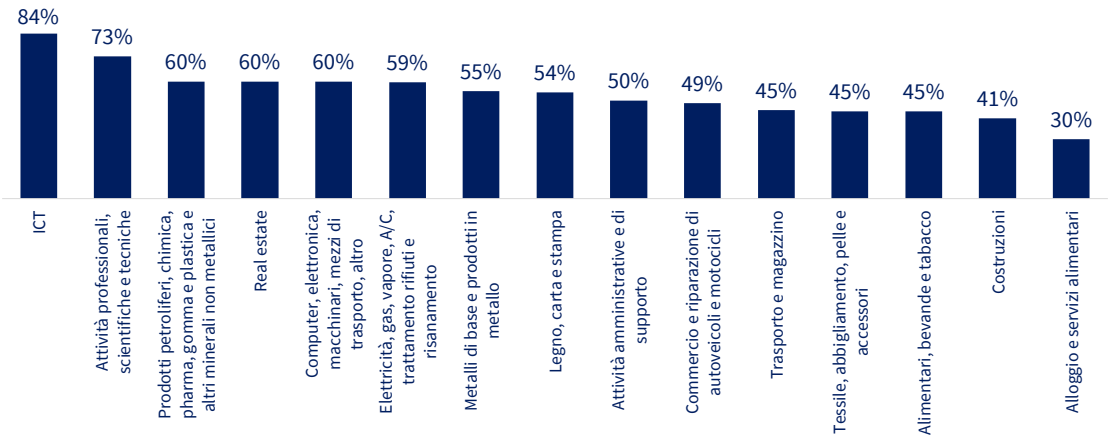

Figura 2.9. Imprese che usano almeno 5 misure di sicurezza ICT in Italia (percentuale), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Eurostat, 2023.*

La difficoltà di diffusione dei sistemi di sicurezza informatica, nella maggior parte dei casi, è riconducibile alla **piccola dimensione delle imprese** che caratterizza l'Italia. Guardando ai sistemi di sicurezza nelle imprese, è possibile notare che le imprese con oltre 250 addetti registrano livelli nettamente superiori rispetto a quelle con oltre 10 addetti.

Ad esempio, l'**utilizzo della VPN** è diffuso nell'89,4% delle grandi imprese, mentre la stessa incidenza si riduce al 41,7% considerando anche le imprese di più piccola dimensione. In questo contesto l'utilizzo di una *password* forte e di sistemi di *backup* è presente in una quota maggiore di imprese, con livelli ancora significativamente diversi a seconda delle dimensioni: le imprese con oltre 10 addetti che hanno una ***password* forte** sono l'83,9% del totale (rispetto al 96,2% delle imprese con oltre 250 addetti), mentre quelle con **sistemi di *backup*** sono l'80% (rispetto al 95,5% delle imprese con oltre 250 addetti).

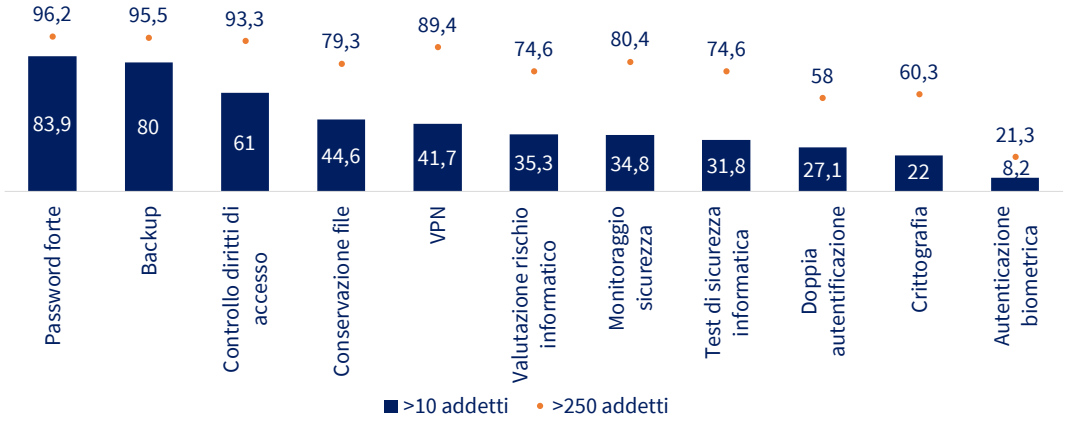

Figura 2.10. Sistemi di sicurezza nelle imprese, per classe dimensionale (percentuale), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Istat, 2023.*

Con particolare riferimento al ruolo dei settori del Perimetro di sicurezza cibernetica, secondo i dati Istat tali settori si caratterizzano per **6,2 miliardi di Euro di investimenti ICT**, con una forte trazione da parte del settore delle telecomunicazioni che registra più elevati valori di investimento pari a 3,2 miliardi di Euro, pari al 40% del totale degli investimenti del settore.

Particolarmente basso è il valore registrato dal settore energetico e delle *utilities*, in cui l'investimento in ICT raggiunge i 230 milioni, pari a circa il 2% del totale degli investimenti del settore.

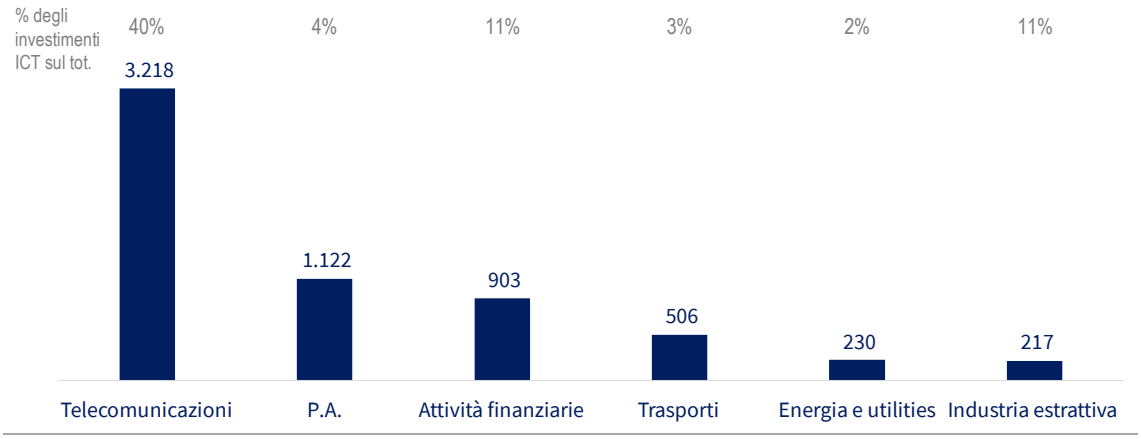

Figura 2.11. Investimenti fissi lordi in apparecchiature ICT dei settori rientranti nel Perimetro di sicurezza cibernetica nazionale in Italia (milioni di Euro), 2021 o ultimo anno disponibile. *Fonte: elaborazione The European House – Ambrosetti su dati Istat, 2023.*

A fronte di questi investimenti, la Figura 2.11 evidenzia lo *stock* di capitale fisso connesso ad apparecchiature ICT, impianti e macchinari, e prodotti di proprietà intellettuale dei settori rientranti nel Perimetro di sicurezza cibernetica nazionale in Italia. Dal grafico emerge come, cumulativamente, il valore degli *asset* la cui operatività dipende, anche in parte, dai sistemi ICT può arrivare fino a **195 miliardi di Euro**. In particolare, di questo valore:

- 18 miliardi di Euro sono connessi ad **apparecchiature ICT**;
- 140 miliardi di Euro sono connessi a **impianti e macchinari**;
- 37 miliardi di Euro connessi a prodotti di **proprietà intellettuale**.

In altre parole, a fronte di investimenti complessivi in ambito ICT pari a 6,2 miliardi di Euro, il **valore tutelato** da tali settori risulta ben più elevato (195 miliardi di Euro), a ulteriore testimonianza del ruolo ricoperto dalle infrastrutture critiche nell'economia del sistema-Paese.

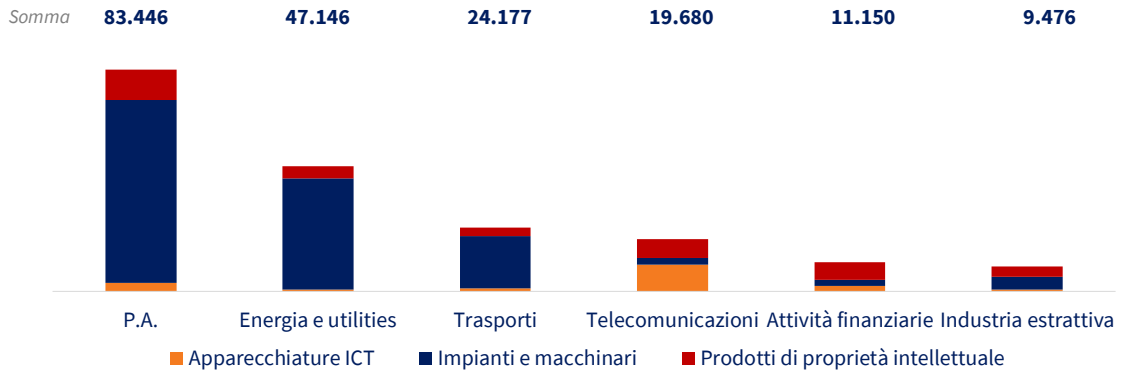

Figura 2.12. *Stock* di capitale fisso connesso ad apparecchiature ICT, impianti e macchinari, e prodotti di proprietà intellettuale dei settori rientranti nel Perimetro di sicurezza cibernetica nazionale in Italia (milioni di Euro), 2019. *Fonte: elaborazione The European House – Ambrosetti su dati Istat, 2023.*

In altri termini, la mancata tutela di questi *asset*, tramite il potenziamento di sistemi di sicurezza informatica e ICT, può risultare dunque in **grosse perdite da parte delle imprese e di tutto il Paese**, a seguito del **blocco delle attività** causati da eventuali attacchi *hacker*.

Alcuni esempi virtuosi, nati allo scopo di tutelare gli *asset* e migliorare il livello di sicurezza del *network*, sono il **GESMA Network Equipment Security Assurance Scheme** e il **5G Cybersecurity Knowledge Base**, due *standard* UE con la funzione rispettivamente di effettuare controlli e *test* sugli equipaggiamenti di rete e fornire una panoramica completa delle minacce alla sicurezza delle reti 5G.

Focus*: alcuni *standard* UE per tutelare gli *asset* e migliorare il livello di sicurezza del *network

GSMA Network Equipment Security Assurance Scheme

Il GSMA Network Equipment Security Assurance Scheme (NESAS) facilita il miglioramento dei livelli di sicurezza degli equipaggiamenti di rete nell'industria mobile, fornendo un **quadro di sicurezza unico e globale**

Lo scopo del programma è quello di effettuare ***audit*** **e** ***test*** sugli fornitori di equipaggiamenti di rete e sui loro prodotti, confrontandoli con un livello di sicurezza di base

Inoltre, con un unico schema si **riduce la duplicazione di lavoro** e di *test* di sicurezza quando si serve una varietà di mercati, aumentando inoltre la **trasparenza** e la **comparabilità dei prodotti** offerti agli operatori di rete

5G Cybersecurity Knowledge Base

La 5G Cybersecurity Knowledge Base fornisce una **panoramica delle minacce** per aiutare gli attori chiave a comprendere in modo sistematico e oggettivo le minacce alla sicurezza poste dalle reti 5G

Fornisce informazioni essenziali per la **strategia di gestione dei rischi**, indicazioni sulle ***best practice*** e misure di mitigazione del rischio, favorendo la **collaborazione** per proteggere le reti e i servizi da interruzioni e accessi non autorizzati, prevenendo e mitigando dei rischi

In questo modo, potrà contribuire ad **aumentare le competenze e le capacità di sicurezza del 5G** e rafforzare il lavoro degli operatori

Fonte: elaborazione The European House – Ambrosetti su fonti varie, 2023.

3. Le imprese italiane e la *cybersecurity*: stato dell'arte ed esigenze prospettiche

Per indagare la **consapevolezza** e il **ruolo delle *cybersecurity*** all'interno delle imprese italiane – e in particolare quelle appartenenti ai settori strategici – e identificare le **esigenze** prospettiche, è stata realizzata una *survey* strutturata. Il campione dell'indagine è costituito da **500 aziende**, appartenenti ai seguenti settori: *utility* ed energia, servizi finanziari, trasporti, infrastrutture, telecomunicazioni e digitale, sanità, aerospazio e difesa. Nella figura successiva sono evidenziate le statistiche di sintesi del campione, dalle quali emerge una copertura territoriale omogenea e – coerentemente con l'universo di riferimento – una particolare incidenza di piccole imprese (71% del totale) e medie (23%).

Settore di attività	%
Utility ed Energia	12%
Servizi finanziari	5%
Trasporti	49%
Infrastrutture	15%
Telecomunicazioni e digitale	12%
Sanità	4%
Aerospazio e difesa	2%

Dimensione	%
10-49 addetti	71%
50-249 addetti	23%
250 e più addetti	6%

Ripartizione geografica degli intervistati (percentuale)

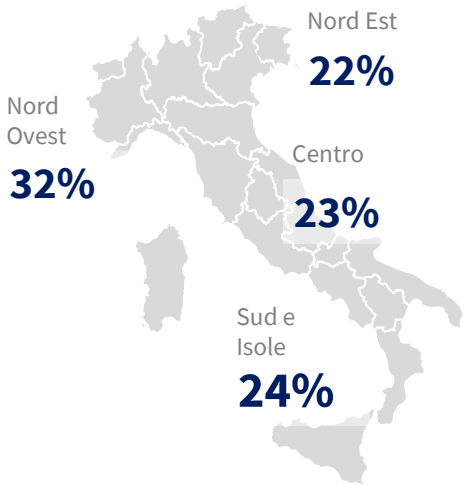

Figura 3.1. Statistiche di sintesi del campione dell'indagine. *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

La consapevolezza e il ruolo della *cybersecurity* all'interno delle aziende

La prima parte dell'indagine ha approfondito gli **ambiti di investimento** connessi al digitale e alla *cybersecurity*, la consapevolezza delle imprese e l'esposizione nei confronti degli attacchi informatici. Complessivamente, dalle evidenze della *survey* emerge come negli ultimi anni le imprese hanno concentrato i loro investimenti digitali sullo **sviluppo di *software* gestionali** (57,8% delle imprese), a cui seguono **investimenti in piattaforme e servizi in *Cloud*** (41,3%) e sistemi di ***Information Security* e *Cyber Security***. A livello settoriale, è interessante notare come i servizi finanziari si discostino dal dato medio, con una preponderanza degli investimenti di *Information Security* e *Cyber Security* (78,4% delle imprese). Per quanto riguarda il settore TLC e digitale, il primo ambito di investimento negli ultimi anni è stato rappresentato dalle piattaforme e servizi in *Cloud* (73,3%).

Ambiti	*Utility* ed energia	Servizi finanziari	Trasporti	Infrastrutture	Telecom e digitale	Sanità	Aerospazio e difesa	Totale
Software gestionali	**64,2%**	54,7%	**66,5%**	**57,6%**	35,6%	**78,5%**	57,7%	**57,8%**
Piattaforme e servizi in Cloud	33,0%	59,7%	32,7%	39,1%	**73,3%**	2,8%	11,5%	41,3%
Sistemi di Information Security e Cyber Security	36,7%	**78,4%**	23,4%	28,8%	29,3%	63,6%	**61,5%**	34,7%
Business Intelligence, Big Data and Analytics	4,8%	17,2%	3,4%	6,1%	49,5%	36,4%	11,5%	21,2%
Software di profilazione e gestione dei contatti	5,7%	9,1%	8,9%	4,6%	11,9%	15,3%	42,3%	9,7%
Nessuno	8,9%	0,0%	17,0%	19,1%	4,6%	0,0%	0,0%	10,3%
Altro	7,2%	2,3%	0,6%	0,5%	0,6%	1,3%	0,0%	1,4%

Figura 3.2. Risposte alla domanda «Su quali ambiti di investimento legati al digitale ha concentrato l'attenzione la vostra azienda negli ultimi anni?» (risposta multipla, massimo 3 risposte, ripartizione per ambiti e settori). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Analizzando le differenze, a seconda della classe dimensionale, **emerge come le piccole e le medie imprese tendano a investire di più in *software* gestionali** (59% tra le piccole imprese, 54% tra le medie), a differenza delle grandi imprese, dove il principale ambito di investimento è rappresentato dai sistemi di *Information Security* e *Cyber Security*. Per tutte le tipologie di impresa, il secondo ambito di investimenti è rappresentato dalle piattaforme e servizi in *Cloud*.

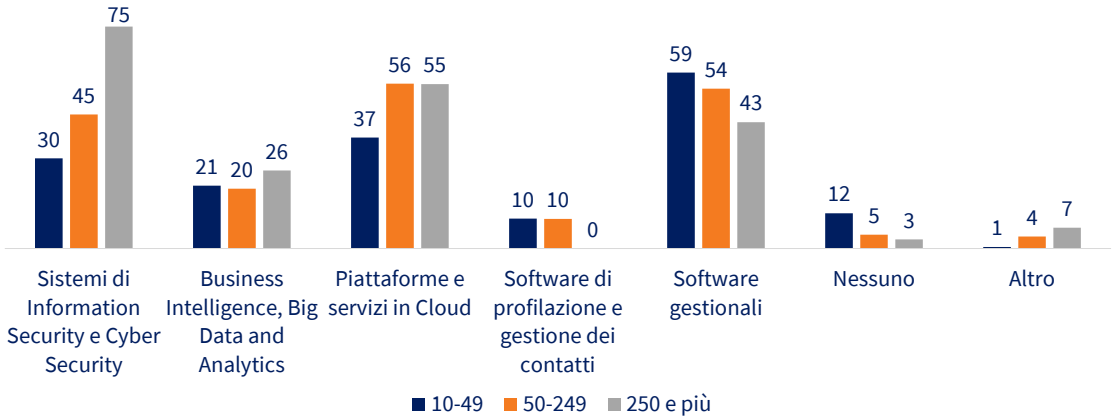

Figura 3.3. Risposte alla domanda «Su quali ambiti di investimento legati al digitale ha concentrato l'attenzione la vostra azienda negli ultimi anni?» (risposta multipla, massimo 3 risposte, ripartizione per classe dimensionale). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Focalizzando l'attenzione specificatamente sulle **soluzioni di *cyber security***, le imprese dei settori strategici stanno investendo soprattutto in ***firewall*** (ovvero il 64,9% delle imprese) e *software antivirus* (ovvero il 61,1% delle imprese). In entrambi i casi, oltre 6 aziende su 10 hanno investito o stanno investendo in queste soluzioni. Le altre soluzioni seguono con un ampio distacco: in particolare, il 17% delle imprese adotta *network security monitoring tools* e sistemi di *penetration testing*.

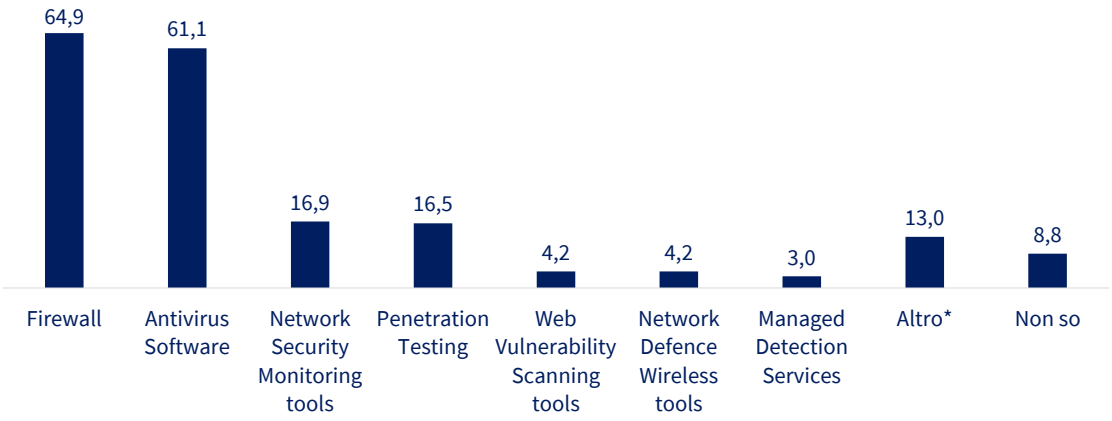

Figura 3.4. Risposte alla domanda «In quali soluzioni di *cybersecurity* ha investito/sta investendo la vostra azienda?» (risposta multipla, massimo 3 risposte). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

In termini di **spesa complessiva**, il **67,1%** delle aziende del campione ha dichiarato di **investire in *cybersecurity,* in media, meno del 10% del proprio *budget* IT**. Un particolare scostamento è rinvenibile nelle **grandi imprese**, dove il **52%** delle realtà investe in *cybersecurity*, in media, **oltre il 10% del proprio *budget* IT**, e in particolare **oltre il 20% per il 28% delle imprese**. In termini settoriali, inoltre, emerge come una maggiore propensione a investire in *cybersecurity* nelle imprese afferenti ai servizi sanitari (52,5% investono oltre il 10% del proprio *budget* IT), alla sanità (44,6%) e all'aerospazio e difesa (42,3%).

Sempre nell'ambito della spesa allocata nella *cybersecurity*, nei prossimi anni è attesa una **forte crescita degli investimenti**: entro il +10% per il 28,1% delle imprese che prevedono un aumento, tra il +10% e il 20% per il 32,4%, **oltre il +30% per il 32% delle imprese**[14]. In particolare, emerge un'ampia differenza a seconda della **classe dimensionale d'impresa**: nelle piccole imprese, per il 46,6% delle realtà è atteso un andamento costante della spesa, mentre per il 41,1% esso aumenterà; nelle medie imprese, la quota di coloro che dichiarano un aumento della spesa cresce al 52,9% (per il 35% rimarrà costante); infine, per il 74,1% delle grandi imprese nei prossimi 5 anni si attende un aumento degli investimenti e solo per il 18,6% la spesa rimarrà costante. Tra le grandi imprese che prevedono un aumento, inoltre, per 1 su 2 questo sarà compreso tra il +10% e il +20%.

[14] Il 7,5% delle imprese ha risposto "non so".

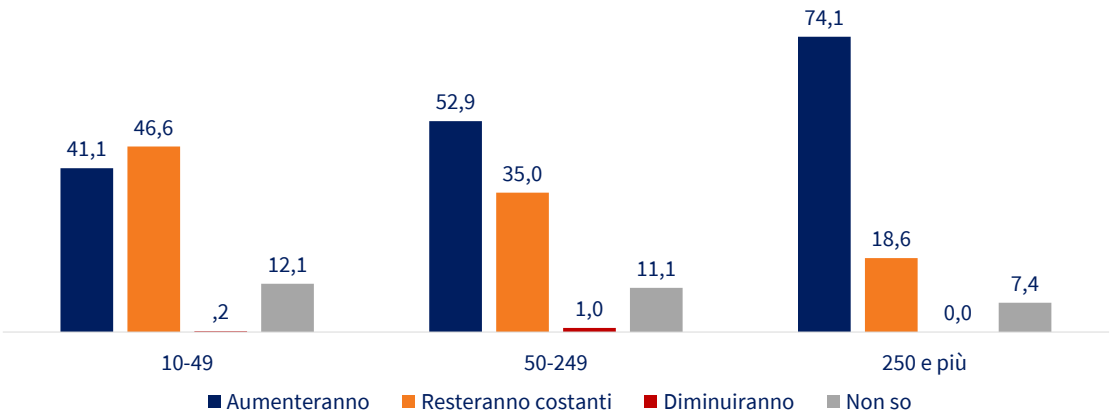

Figura 3.5. Risposte alla domanda «Come prevedete che cambieranno i vostri investimenti in *cybersecurity* nei prossimi 5 anni?» (percentuale, per classe di addetti). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Successivamente, è stato indagato il **grado di consapevolezza** delle imprese nei confronti della *cybersecurity*. In questo ambito, il **53,9%** delle imprese ha dichiarato di avere un'**attenzione alta o molto alta verso la *cybersecurity*** all'interno della propria organizzazione aziendale. Anche in questo caso emergono alcune differenze – seppure marginali – tra piccole imprese (dove il 52,6% reputa di avere un'attenzione alta o molto alta) e grandi (dove la percentuale sale al 65,1%). Connesso a questo aspetto, secondo quasi 9 aziende su 10 (87%), **il modello organizzativo è adeguato** a gestire le sfide attuali e prospettiche in termini di *cybersecurity*.

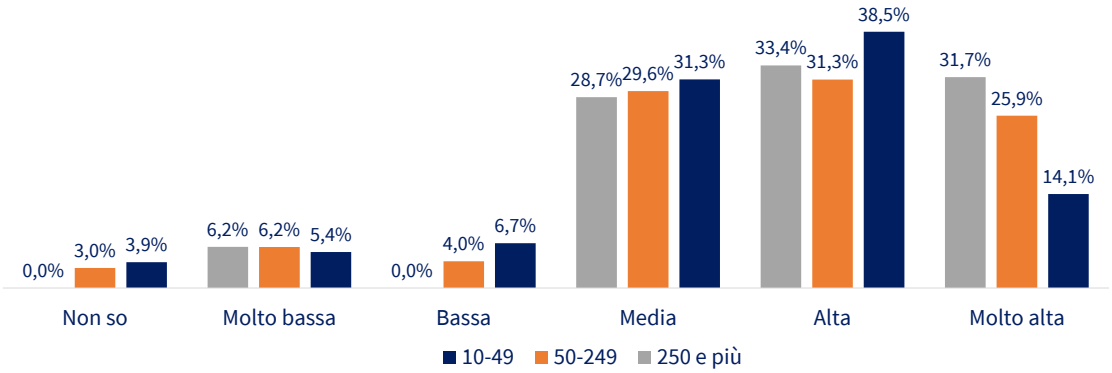

Figura 3.6. Risposte alla domanda «All'interno della vostra organizzazione aziendale come giudicate l'attenzione verso la *cybersecurity*?» (percentuale, per classe di addetti). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

La percezione delle imprese coinvolte nella *survey* sembra essere confermata dalle evidenze empiriche. Infatti, secondo i dati Eurostat, l'Italia è al **quarto posto nell'Unione Europea** per minor quota di imprese che hanno sperimentato almeno una volta **problemi derivanti da incidenti di sicurezza informatica**, con un valore pari al **10,1%**. Si tratta di un valore inferiore di 3,5 punti percentuali inferiore rispetto alla media europea (13,3%) e di 5,4 p.p. inferiore rispetto, per esempio, alla Francia (15,5%).

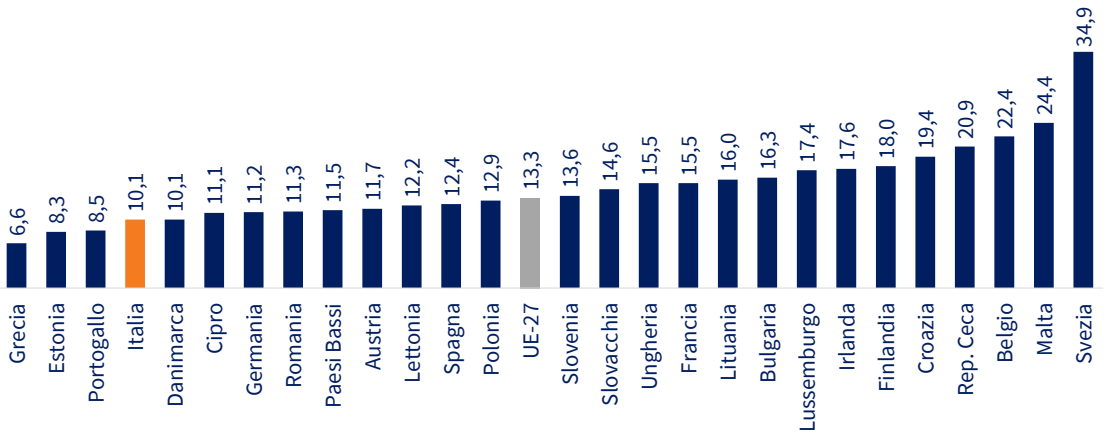

Figura 3.7. Imprese che hanno sperimentato almeno una volta problemi derivanti da incidenti di sicurezza informatica (percentuale), 2019. *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

In questa prospettiva, occorre sottolineare un elemento di attenzione. Infatti, secondo i dati Eurostat, l'Italia è tra i Paesi europei con la maggiore quota di imprese che hanno **definito o aggiornato la propria *policy* di sicurezza informatica oltre 2 prima** rispetto alla rilevazione (2022). In particolare, il 6,9% delle imprese italiane si trova in questa situazione, rispetto a una media europea del 4,8% e a valori ben più bassi nei Paesi *benchmark* europei, quali per esempio la Francia (2,8%) e la Germania (2,4%). Da questo punto di vista, occorre sottolineare come – in un quadro di forti cambiamenti tecnologici e normativi – strategie aziendali aggiornate in ambito di *cybersecurity* rappresentino uno strumento essenziale per garantire efficacemente la ***cyber*-resilienza** delle attività.

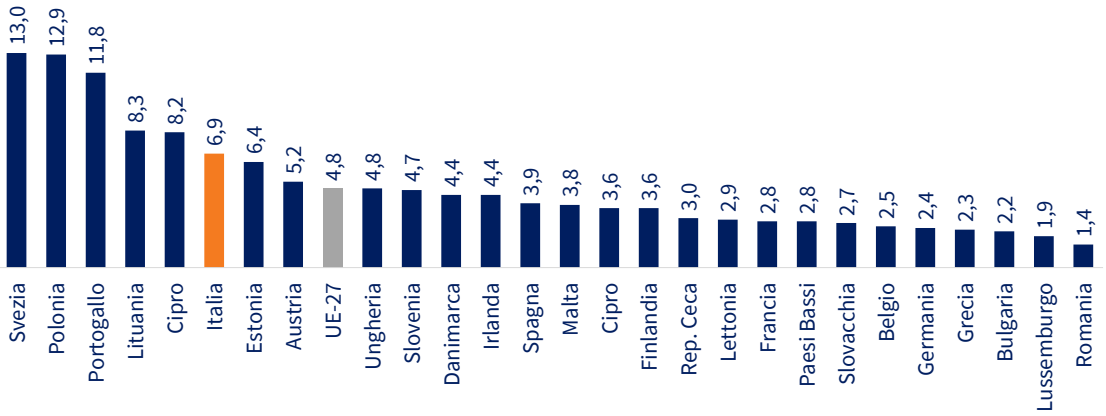

Figura 3.8. Imprese che hanno definito o aggiornato la propria *policy* di *cybersecurity* oltre 2 anni prima (percentuale), 2022. *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Come ulteriore ambito di approfondimento, è stata indagata l'esposizione delle imprese appartenenti ai settori strategici verso gli attacchi informatici. Dalla rilevazione, è emerso come il **numero medio di attacchi** nell'ultimo triennio sia stato pari a **5,5**, con alcune differenze tra le diverse tipologie di imprese. In particolare, le **imprese del Sud e delle Isole** hanno registrato un valore tre volte superiore rispetto alla media (15,6); similmente, anche medie e grandi imprese hanno subito un numero di attacchi superiore (7,6 e 7,3 rispettivamente).

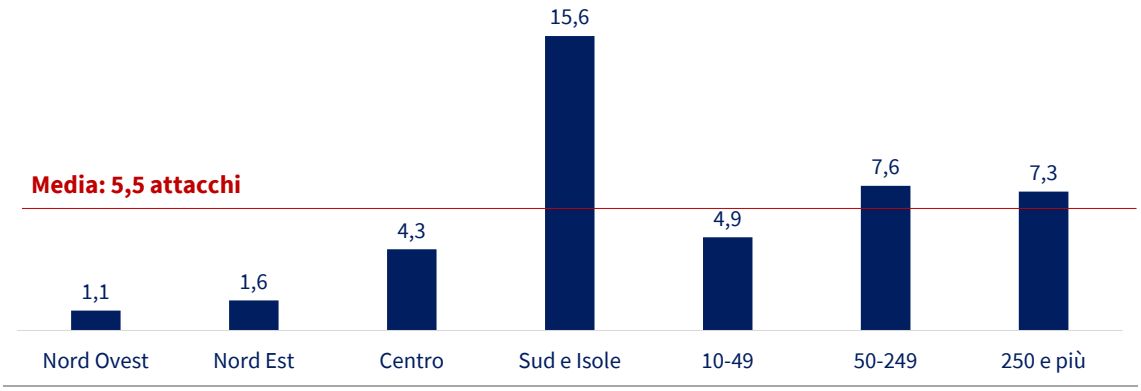

Figura 3.9. Risposte alla domanda «Quanti attacchi informatici avete registrato nell'ultimo triennio?» (numero medio, per ripartizione geografica e classe di addetti). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Secondo le imprese della *survey*, inoltre, il **furto di denaro** è l'obiettivo più frequente degli attacchi informatici per tutte le tipologie di imprese, con una quota compresa **tra il 43,4% nelle piccole imprese e il 31,9% delle grandi**. A seguire, per le piccole e medie imprese, si colloca l'**interruzione delle principali attività aziendali** (es. transazioni *online*, commerciali, funzionamento del *computer*, ecc.). Per le grandi imprese, invece, il secondo obiettivo risulta essere il **furto di informazioni aziendali** (es. coordinate bancarie o dati delle carte di pagamento). Per una quota rilevante delle grandi imprese (18%), inoltre, l'obiettivo degli attacchi informatici è stato rappresentato dall'**interruzione del funzionamento degli *asset* strategici** gestiti dall'azienda (es. blocco delle infrastrutture, interruzione dei servizi, ecc.). Infine, per il 23,9% delle grandi imprese, il motivo dell'attacco rimane sconosciuto.

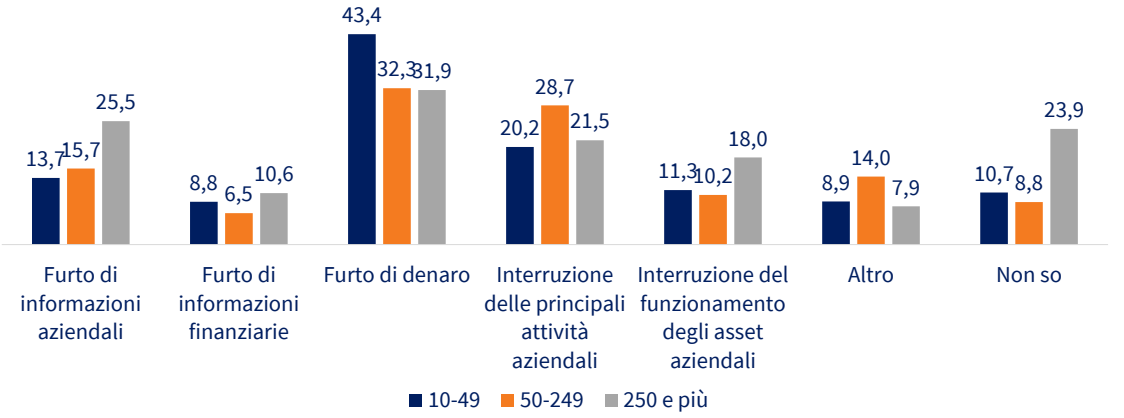

Figura 3.10. Risposte alla domanda «Quali obiettivi hanno avuto gli attacchi informatici ricevuti dalla vostra azienda?» (possibile risposta multipla, massimo 2 risposte, per classe di addetti). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Nell'ambito degli attacchi informatici subiti dall'azienda, è interessante rilevare come per il 42,4% delle imprese la **fonte principale** sia rappresentata dall'**errore umano**, contrapposto al 22,7% delle imprese secondo cui esso sia imputabile principalmente ad un attacco forzato dei sistemi. L'errore umano risulta **particolarmente comune tra le PMI**: secondo il **48,3%** delle medie imprese la fonte dell'attacco è attribuibile esclusivamente all'errore umano, una

quota superiore sia alle piccole imprese (41,8%), nonché alle grandi (32,5%) di circa 15,8 punti percentuali.

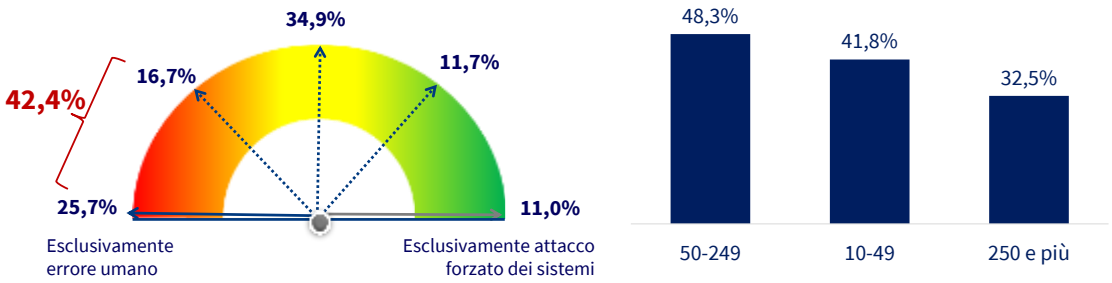

Figura 3.11. Grafico di sinistra: risposte alla domanda «Quale è la principale fonte di attacchi informatici?» (Esclusivamente errore umano = 1; Esclusivamente attacco forzato dei sistemi informatici aziendali = 5). Grafico di destra: risposte alla domanda «Quale è la principale fonte di attacchi informatici?» (Principalmente errore umano). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Tali evidenze trovano conferma anche nelle principali rilevazioni di Eurostat sul tema. In ambito di **competenze digitali**, infatti, l'Italia è al **quartultimo posto nell'Unione Europea** per persone con competenze digitali almeno di base, con una quota pari al **45,6%**, inferiore di 8,3 punti percentuali rispetto alla media europea (53,9%). Le competenze digitali diffuse rappresentano una precondizione fondamentale per evitare gran parte degli attacchi, ovvero quelli riconducibili ad errori umani.

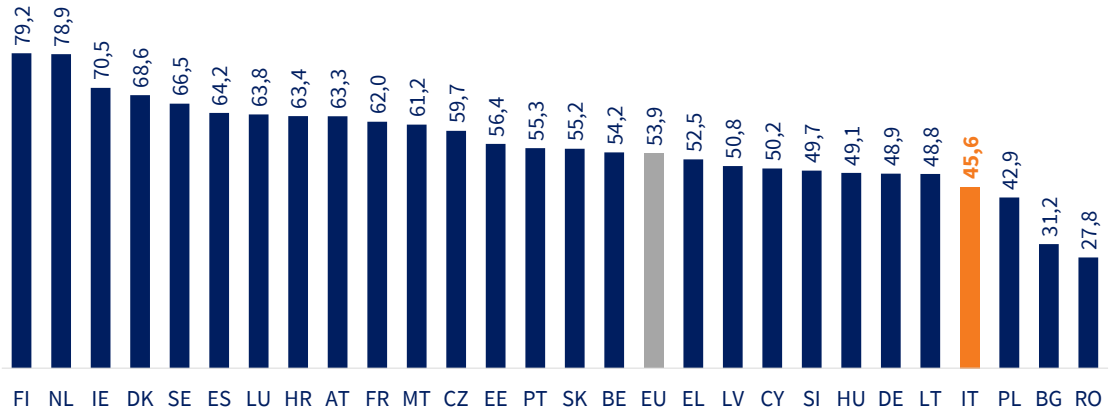

Figura 3.12. Persone con competenze digitali almeno di base (percentuale), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Eurostat, 2023.*

Oltre a queste competenze di base, è fondamentale poter fare affidamento su **competenze tecniche specialistiche**, per poter gestire efficacemente le sfide di *cybersecurity*: anche da questo punto di vista, l'Italia presenta alcuni *gap*. Gli **esperti ICT** nelle imprese italiane pesano, infatti, per il **3,8%** della forza lavoro, una quota inferiore sia alla media europea (4,5%) sia ai Paesi *benchmark* come Francia (4,5%) e Germania (4,9%).

In Italia, inoltre, si registra un **basso livello di formazione in ambito ICT**, contribuendo ad aumentare l'esposizione verso i potenziali attacchi: la quota di imprese che offrono corsi di ICT al personale è inferiore rispetto alla media europea per ciascuna classe dimensionale, con

differenze comprese tra i 4,1 punti percentuali per le grandi imprese e gli 1,6 p.p. nelle piccole imprese.

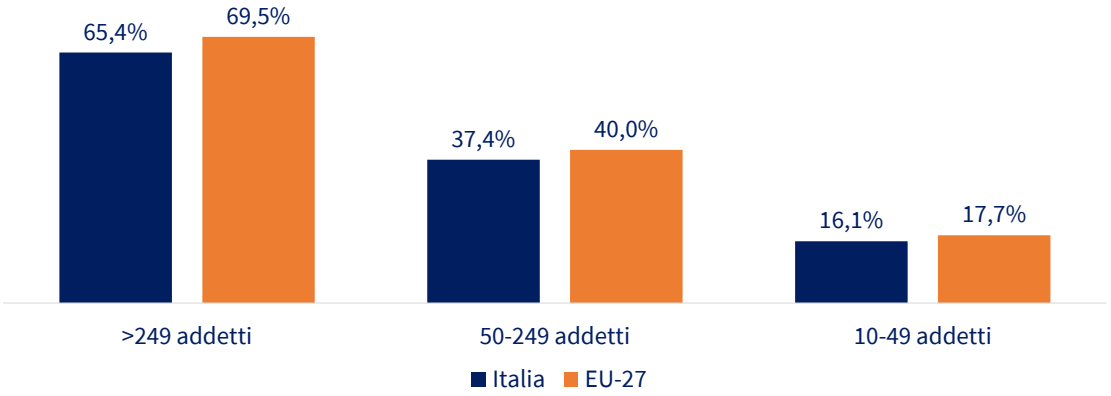

Figura 3.13. Imprese che offrono corsi di ICT al personale per dimensione (percentuale), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Eurostat, 2023.*

Focus: il Quadro europeo delle competenze in materia della cybersicurezza

ENISA ha lavorato allo sviluppo dell'European Cybersecurity Skills Framework (ECSF), ossia al **Quadro europeo delle competenze in materia della cybersicurezza,** che ha lo scopo di rafforzare la cultura europea della cybersicurezza fornendo un linguaggio europeo comune a tutte le comunità, compiendo un passo avanti essenziale verso il futuro digitale dell'Europa.

L'ECSF fornisce uno strumento pratico per supportare l'identificazione e l'articolazione di compiti, competenze, abilità e conoscenze associate ai ruoli dei professionisti europei della cybersicurezza. Lo scopo principale del quadro è creare un'intesa comune tra individui, datori di lavoro e fornitori di programmi di apprendimento negli Stati membri dell'UE, rendendolo uno strumento prezioso per colmare il divario tra la domanda professionale di cybersicurezza (reclutamento e avanzamento professionale) e l'offerta formativa in tutta l'Unione Europea.

Il quadro definisce una serie di **12 profili professionali** tipici della cybersicurezza, in particolare: *Chief Information Security Officer* (CISO); *Cyber Incident Responder*; *Cyber Legal, Policy and Compliance Officer*; *Cyber Threat Intelligence Specialist*; *Cybersecurity Architect*; *Cybersecurity Auditor*; *Cybersecurity Educator*; *Cybersecurity Implementer*; *Cybersecurity Researcher*; *Cybersecurity Risk Manager*; *Digital Forensics Investigator*; *Penetration Tester*.

Fonte: elaborazione The European House – Ambrosetti su dati ENISA e Agenda Digitale, 2023.

La *cybersecurity* come leva di sviluppo e innovazione aziendale

La seconda parte della *survey* ha voluto approfondire il **legame tra *cybersecurity* e innovazione** dal punto di vista delle imprese. Come punto di partenza, le aziende del campione si sono espresse sul proprio grado di conoscenza delle principali normative sulla *cybersecurity* a livello italiano ed europeo: dalla rilevazione, emerge come il **43,1%** delle imprese reputino di avere una **conoscenza bassa o molto bassa del quadro di riferimento**, con una particolare **incidenza delle piccole imprese** (dove la percentuale sale al 44,3%); dall'altro lato, un alto (o molto alto) livello di conoscenza sulle normative è presente principalmente tra le grandi imprese, con una quota pari al 44,3% (rispetto, per esempio, al 12,9% delle piccole imprese o al 18,2% delle medie).

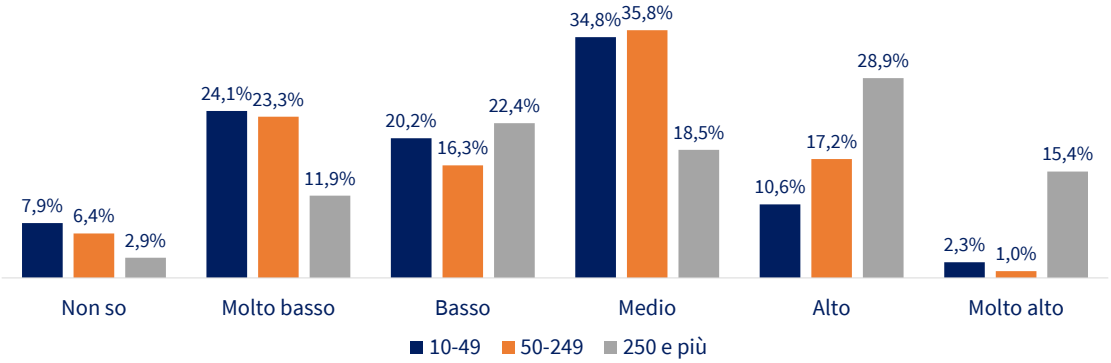

Figura 3.14. Risposte alla domanda «Come giudicherebbe il livello di conoscenza delle principali normative sulla *cybersecurity* a livello italiano ed europeo nella vostra azienda?» (percentuale, per classe di addetti). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Successivamente, è stato approfondito in quale modalità lo sviluppo della *cybersecurity* possa rappresentare una **leva di sviluppo e innovazione** per l'azienda. Da questo punto di vista, emerge come, in media, per circa **un terzo delle imprese** la *cybersecurity* permetta di **investire maggiormente in nuove soluzioni digitali** grazie ai più alti livelli di sicurezza garantiti. Il secondo ambito in cui si dispiega tale relazione positiva riguarda il fatto che la *cybersecurity* garantisce **processi aziendali e commerciali più efficienti** grazie a una maggiore resilienza, dovuta alla riduzione delle interruzioni causate dagli attacchi informatici: ciò si verifica per il 31,8% delle aziende coinvolte nella *survey*, con una quota che sale al 56% nei servizi finanziari e nelle telecomunicazioni. Per questi due settori, inoltre, la *cybersecurity* assume un ruolo strategico (per il 32,8% delle imprese TLC e per il 34,5% dei servizi finanziari) in quanto migliora il posizionamento in termini di immagine dell'azienda, aumentando la affidabilità e fiducia nei confronti dei *partner*. Non da ultimo, nel settore sanitario per oltre 1 azienda su 4 la *cybersecurity* consente di **ottimizzare la gestione dei propri *asset*** strategici.

Ambiti	*Utility* ed energia	Servizi finanziari	Trasporti	Infrastrutture	Telecom e digitale	Sanità	Aerospazio e difesa	Totale
Permette di investire in nuove soluzioni digitali grazie ai più alti livelli di sicurezza	**30,4%**	28,4%	**21,2%**	**33,9%**	47,9%	**33,2%**	**38,5%**	**33,3%**
Garantisce processi più efficienti grazie a una maggiore resilienza	17,6%	**56,4%**	20,0%	24,3%	**56,1%**	23,6%	19,2%	31,8%
Migliora il posizionamento di immagine aumentando la propria affidabilità	26,7%	34,5%	18,2%	24,0%	32,8%	17,4%	26,9%	24,4%
Consente di ottimizzare la gestione degli asset strategici dell'azienda	18,7%	8,6%	13,5%	13,2%	7,1%	27,8%	19,2%	14,1%
Favorisce collaborazioni tra realtà simili per implementare sistemi di sicurezza comuni	10,1%	16,8%	12,1%	5,0%	10,1%	1,2%	0,0%	8,7%

Figura 3.15. Risposte alla domanda «In che modo la *cybersecurity* può essere una leva di sviluppo e innovazione per l'azienda?» (risposta multipla, massimo 2 risposte). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

In questo quadro, quasi 1 impresa del campione su 2 (45,1%) ritiene che l'attuale quadro regolatorio in materia di *cybersecurity* impatti sulla **capacità di innovare e generare crescita** per l'azienda. Approfondendo le motivazioni sottostanti, si rileva che per oltre la metà delle

imprese (**55%**), la capacità innovativa è **impattata dai fattori di costo**, ovvero in quanto causa un aumento della burocrazia e dei costi amministrativi per adempiere agli *standard* (30%) e perché comporta costi significativi sia in termini di tecnologie sia in termini di personale da dedicare alle attività di *cybersecurity* (29%). Le restanti motivazioni afferiscono alla creazione di **barriere all'ingresso** per le imprese di più piccola dimensione che non hanno le stesse risorse per adempiere agli *standard* (30%) e alle **restrizioni alle attività** delle imprese (es. raccolta e utilizzo di dati), per il 15% delle imprese.

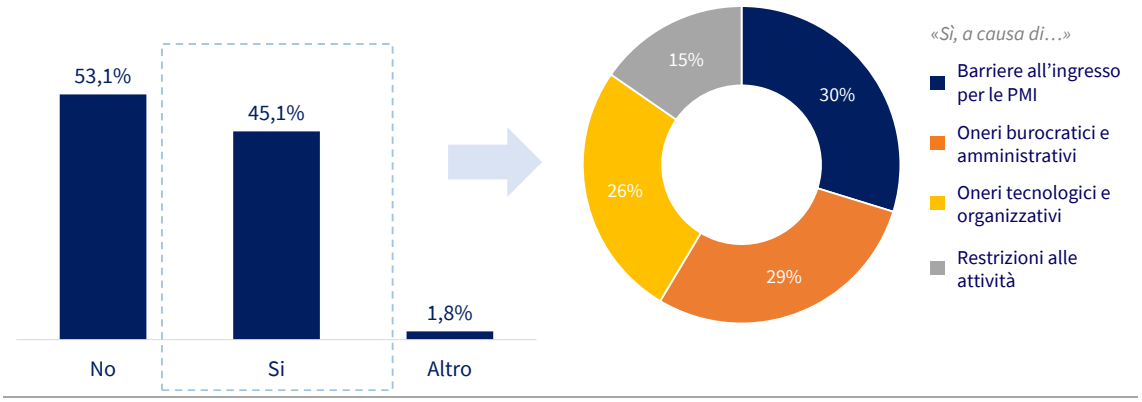

Figura 3.16. Risposte alla domanda «Reputa che il quadro regolatorio in materia di *cybersecurity* impatti sulla capacità di innovare e generare crescita per l'azienda?» (risposta multipla, massimo 2 risposte). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Connesso a tale quesito, alle imprese è stato chiesto quali fossero i **principali problemi** riscontrati nel conformarsi alla normativa di riferimento. Dalla rilevazione emergono problematiche differenziate: per i settori delle infrastrutture e delle telecomunicazioni le criticità principali sono relative alle **necessità di adeguamento in termini di infrastrutture** informatiche (62,0% e 67,7% rispettivamente). Nel settore dei trasporti, invece, sono emerse criticità con riferimento alle **necessità di adeguamento delle competenze** del personale IT (53,2% delle imprese). Non da ultimo, per il settore delle *utility* ed energia la principale problematica afferisce al **disallineamento tra normativa europea e italiana**, come rilevato dal 52,8% delle aziende.

Ambiti	*Utility* ed energia	Trasporti	Infrastrutture	Telecom. e digitale
Necessità di adeguamento delle competenze del personale IT	9,2%	**53,2%**	30,8%	45,7%
Necessità di adeguamento in termini di infrastrutture informatiche	29,1%	26,9%	**62,0%**	**67,7%**
Necessità di riorganizzazione delle strategie di sicurezza aziendale	24,2%	0,0%	15,3%	13,3%
Normativa poco chiara	8,9%	37,4%	31,9%	0,0%
Le azioni richieste eccedono le esigenze di sicurezza dell'azienda	13,8%	9,1%	15,6%	8,7%
Le azioni richieste non garantiscono la sicurezza informatica	0,0%	9,1%	0,0%	0,0%
Gli *standard* ledono la capacità di innovazione e offrire nuovi servizi	0,0%	0,0%	12,9%	0,0%
Disallineamento tra normativa europea e italiana	**52,8%**	9,4%	15,9%	0,0%
Altro (specificare)	52,8%	0,0%	0,0%	32,3%

Figura 3.17. Risposte alla domanda «Quali sono i principali problemi riscontrati dalla vostra azienda nel conformarsi alla normativa di riferimento sulla *cybersecurity*?» (risposta multipla, massimo 2 risposte). Nota: servizi finanziari, Sanità, Aerospazio e Difesa sono stati esclusi a causa della base non statisticamente significativa. *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Nel complesso, quella dell'adeguamento a diverse normative rappresenta una necessità comune per molteplici imprese. In particolare, **un terzo delle realtà** operanti in più Paesi ha riportato **difficoltà nel gestire la sicurezza informatica nelle attività condotte in più Paesi europei**, alla luce dei diversi requisiti di sicurezza richiesti.

Focalizzando l'attenzione sulle motivazioni, si tratta soprattutto di **risorse aggiuntive per adattare i prodotti** alle differenti normative dei Paesi (54,7%), a cui segue la difficoltà di adattare l'offerta ai diversi contesti regolatori (37,3%).

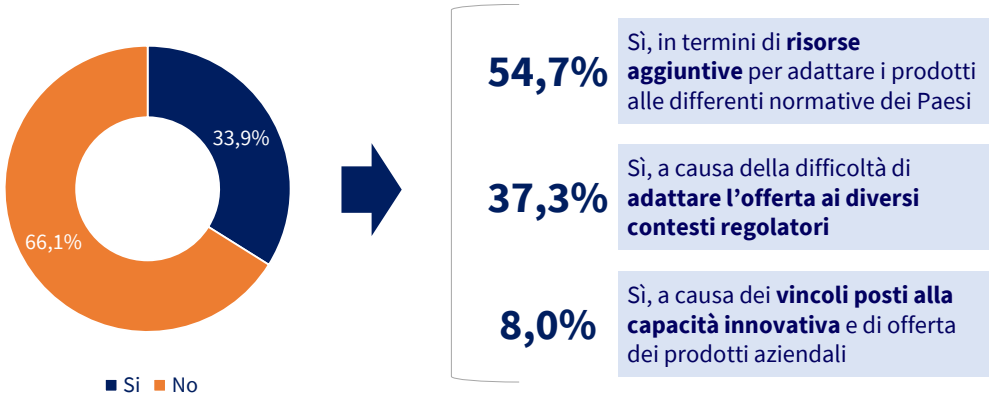

Figura 3.18. Risposte alla domanda «Riscontrate difficoltà nel gestire la sicurezza informatica nelle attività condotte in più Paesi europei, alla luce dei diversi requisiti di sicurezza richiesti dai Paesi membri?» (Una risposta). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Infine, sono stati approfonditi gli ambiti di *cybersecurity* che, dal punto di vista delle imprese, consentono di avere una **maggiore flessibilità e innovazione**. Dalle risposte a tale quesito sono emersi alcuni ambiti strategici, in particolare la **crittografia** e i ***backup*** per proteggere i dati sensibili (30,6% delle imprese), a cui segue la **sicurezza delle reti aziendali** (30,4%) e i **sistemi di sicurezza *cloud-based*** (28,7%). Anche in questo caso emergono alcune differenze settoriali, rinvenibili, per esempio, nei settori delle telecomunicazioni e della sanità, dove un

ruolo strategico è ricoperto proprio dai sistemi *cloud-based*. Per i servizi finanziari, inoltre, un contributo chiave è affidato alla gestione dell'identità e degli accessi (50,7%).

Ambiti	*Utility* ed energia	Servizi finanziari	Trasporti	Infrastrutture	Telecom e digitale	Sanità	Aerospazio e difesa	Totale
Crittografia e backup per proteggere dati sensibili	19,7%	**51,7%**	21,5%	36,2%	41,2%	25,0%	11,5%	**30,6%**
Sicurezza delle reti aziendali	**39,9%**	42,1%	**29,4%**	**41,9%**	26,2%	16,7%	**42,3%**	30,4%
Sistemi di sicurezza cloud-based	5,6%	9,0%	17,0%	8,8%	**58,9%**	**41,7%**	11,5%	28,7%
Gestione dell'identità e degli accessi	20,7%	50,7%	14,9%	16,3%	26,9%	17,1%	26,9%	20,4%
Analisi periodiche della sicurezza	26,1%	14,3%	15,3%	22,8%	10,2%	14,6%	0,0%	16,1%
Sicurezza dei dispositivi mobili dei dipendenti	15,4%	7,9%	11,3%	17,5%	11,8%	0,0%	**42,3%**	11,3%
Non so	20,3%	3,0%	25,4%	15,8%	9,0%	40,1%	19,2%	20,1%

Figura 3.19. Risposte alla domanda «Quali ambiti di *cybersecurity* consentono di avere una maggiore flessibilità e innovazione dell'azienda e dei suoi processi?» (risposta multipla, massimo 2 risposte, ripartizione per ambiti e settori). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Le proposte di ottimizzazione del *framework* della *cybersecurity* per l'Italia

Dopo aver analizzato nei capitoli precedenti il contesto di riferimento della *cybersecurity* in Italia nel quadro europeo, il presente capitolo conclusivo intende delineare gli ambiti d'azione per **ottimizzare il *framework* della *cybersecurity*** per il Paese.

A tal fine, le proposte sono state ricondotte a tre diversi ambiti di focalizzazione, ovvero:

1. **Competenze e *awareness***;
2. **Supporto alle imprese e alla capacità innovativa**;
3. ***Governance* e modelli collaborativi**.

Competenze e *awareness*

Le competenze digitali, diffuse e tecniche, rappresentano una precondizione fondamentale per poter gestire efficacemente il processo di trasformazione digitale e, in particolare, per poter promuovere la *cybersecurity*.

Da un lato, le competenze digitali tecniche possono contribuire positivamente allo **sviluppo di nuove soluzioni innovative** di sicurezza (per esempio grazie a competenze di programmazione, gestione dei dati, progettazione e analisi) e alla gestione dei sempre più complessi e sofisticati **rischi di sicurezza informatica**.

Le competenze digitali diffuse, invece, risultano necessarie a garantire livelli di sicurezza adeguati lungo tutta la filiera digitale (di un'impresa o di una Pubblica Amministrazione), evitando che falle riconducibili a un errore umano determinino ripercussioni critiche. Basti pensare che, tra le aziende coinvolte nella *survey* realizzata nel presente *Position Paper*, per il 42,4% delle imprese (48,3% tra quelle di medie dimensioni) la **fonte principale** degli attacchi informatici è rappresentata dall'**errore umano**, contrapposto al 22,7% delle imprese secondo cui esso è imputabile principalmente ad un attacco forzato dei sistemi.

Nell'ambito delle competenze digitali, tuttavia, il sistema-Paese presenta ancora notevoli *gap*: secondo i dati Eurostat l'Italia si trova al **quartultimo posto nell'Unione Europea** per persone con competenze digitali almeno di base, con una quota pari al **45,6%**. Allo stesso tempo, gli **esperti ICT** nelle imprese italiane pesano solo per il **3,8%** della forza lavoro, una quota inferiore sia alla media europea (4,5%) sia ai Paesi *benchmark* come Francia (4,5%) e Germania (4,9%).

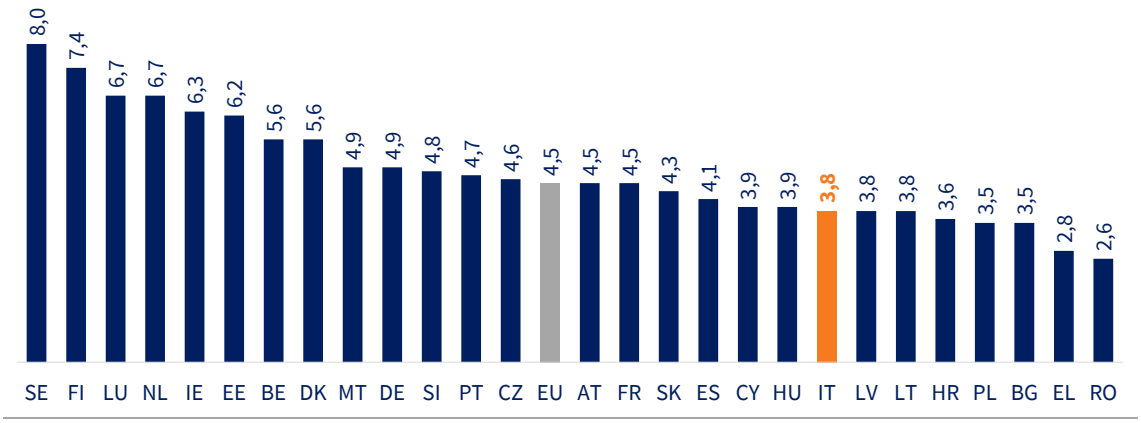

Figura 4.1. Esperti ICT nelle imprese (percentuale), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Eurostat, 2023.*

Oltre alle competenze in senso stretto, un ruolo chiave è assunto anche dalla **consapevolezza** rispetto ai temi di *cybersecurity*, ovvero dalla conoscenza delle sue dinamiche fondamentali e dalla capacità di un'organizzazione di definire e perseguire una chiara visione di sviluppo delle proprie strategie di sicurezza informatica, dotandosi di adeguate procedure e *policy*. In un contesto che – come evidenziato nei passaggi precedenti – vede una crescente complessità (sia sul fronte della normativa, sia sul fronte tecnologico), risulta dunque fondamentale porre in essere strategie che sappiano essere flessibili rispetto agli scenari di evoluzione normativo-tecnologica e che pongano al centro le tematiche connesse alla *governance* e alla gestione dei processi di *cybersecurity*.

Per rispondere all'esigenza di promuovere le **competenze tecniche** in ambito di *cybersecurity* e le **competenze digitali diffuse** nella popolazione, la proposta è quella di promuovere appositi **quadri di certificazione** delle competenze. Si tratta, in particolare, di dare concreta attuazione a quanto già previsto dalla Strategia Nazionale di Cybersicurezza (nella Misura n. 61), assicurando coerenza con il nuovo Quadro europeo delle competenze in materia della cybersicurezza definito a livello europeo.

In questo contesto, si rende necessario anche promuovere la **collaborazione tra sistema formativo e delle imprese**, per esempio prevedendo degli incentivi per le imprese che partecipano alle ITS Academy (ovvero le scuole che erogano percorsi di formazione *post*-diploma ad alta specializzazione) focalizzate in ambito di *cybersecurity*.

La seconda proposta intende rafforzare la consapevolezza delle organizzazioni, *in primis* le imprese, nei confronti della *cybersecurity*, per esempio introducendo **requisiti di *disclosure* sulle capacità dei vertici aziendali**. Una fonte di ispirazione in questo senso è rappresentata dalla "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" della SEC, l'ente federale statunitense preposto alla vigilanza delle borse valori.

Focus: "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"

Nel 2022, per far fronte all'evoluzione dei rischi e delle esigenze degli investitori, la Securities and Exchange Commission (SEC) degli USA nel 2022 ha proposto nuove regole per migliorare e standardizzare le informazioni sulla gestione del rischio di *cybersecurity*, sulla strategia, sulla *governance* e sulla segnalazione degli incidenti da parte delle società pubbliche.

Oltre a requisiti in termini di segnalazione degli incidenti di *cybersecurity*, le nuove regole riguardano anche la presentazione di **relazioni periodiche** su:

- Le **politiche** e le **procedure** delle aziende **per identificare e gestire i rischi di *cybersecurity***, incluso se l'ente considera la *cybersecurity* all'interno della propria strategia di *business*, della propria programmazione finanziaria e della *capital allocation*;
- La **supervisione del rischio di *cybersecurity* da parte del Consiglio di Amministrazione**, nonché il ruolo e l'*expertise* del *management* nella valutazione e nella gestione del rischio di *cybersecurity* e nell'attuazione delle politiche, delle procedure e delle strategie di *cybersecurity*.

Le nuove regole richiedono inoltre la presentazione di relazioni annuali o di alcune informazioni sulle **competenze del Consiglio di Amministrazione** in materia di *cybersecurity*, se esistenti.

Fonte: elaborazione The European House – Ambrosetti su dati SEC, 2023.

La terza proposta consiste nel supportare lo **scambio di competenze** nel campo della sicurezza informatica, promuovendo la collaborazione tra professionisti e istituzioni e rafforzando le capacità nel settore di affrontare le nuove sfide.

Supporto alle imprese e alla capacità innovativa

Dall'attività di ascolto degli *stakeholder* e delle imprese sono emerse alcune esigenze fondamentali per promuovere la *cybersecurity* e la capacità innovativa. Basti pensare che quasi 1 impresa del campione su 2 (45,1%) ritiene che l'attuale quadro regolatorio in materia di *cybersecurity* impatti sulla **capacità di innovare e generare crescita** per l'azienda (soprattutto per fattori di costo) e che **un terzo delle realtà** operanti in più Paesi ha riportato **difficoltà nel gestire la sicurezza informatica nelle attività condotte in più Paesi europei**, alla luce dei diversi requisiti di sicurezza richiesti.

Inoltre, in termini di ambiti di intervento prioritari per migliorare la *cybersecurity*, le imprese hanno messo al primo posto il **supporto economico** per l'*upgrade* della sicurezza informatica (47,1%), seguito dalla **semplificazione della normativa** di riferimento e delle procedure di certificazione (28,5%). Approfondendo le risposte rispetto alla classe dimensionale, emerge come tra le imprese di grandi dimensioni la semplificazione della normativa rappresenta l'intervento prioritario (40,4%), al contrario delle piccole e medie imprese dove il supporto economico si conferma l'esigenza primaria (50,7% e 34,1% delle imprese rispettivamente).

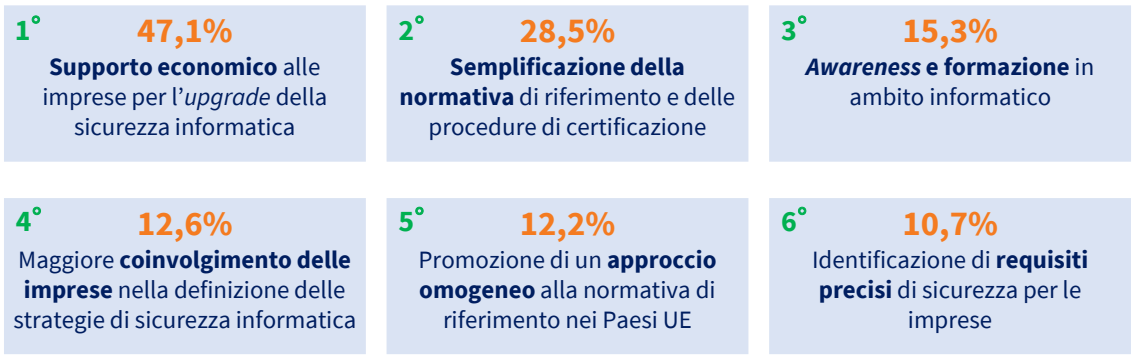

Figura 4.2. Risposte alla domanda «*Quali ritiene essere gli ambiti di intervento prioritari per migliorare la sicurezza informatica, promuovendo approcci flessibili e innovativi delle aziende?*» (risposta multipla, massimo 2 risposte). *Fonte: elaborazione The European House – Ambrosetti su risultati della survey, 2023.*

Alla luce di tali evidenze, come precondizione fondamentale, si reputa necessario promuovere un maggiore **allineamento della normativa italiana di *cybersecurity* a *standard* comunitari** e la **semplificazione del quadro corrente**, evitando la duplicazione di obblighi in capo agli attori, con riferimento sia all'implementazione della Direttiva NIS 2 sia allo sviluppo di sistemi di certificazione. Relativamente al tema delle certificazioni, inoltre, si suggerisce la definizione di schemi di **mantenimento delle certificazioni** e di **certificazione dei processi**, secondo paradigmi di *security-by-design* e *certification-by-design*, volti ad attenuare gli oneri in campo alle imprese e dunque a stimolare la capacità di sviluppo di nuovi prodotti e soluzioni. Un metodo per incentivare l'acquisizione di certificazioni di *cybersecurity* potrebbe essere la valorizzazione di tali investimenti (sul modello delle certificazioni della parità di genere recentemente introdotte dal PNRR) nei meccanismi di valutazione connessi agli appalti pubblici.

Contestualmente, si propone di sviluppare specifiche attività di accompagnamento alle imprese nei loro percorsi di rafforzamento della sicurezza informatica, per esempio tramite **incentivi per l'acquisto di soluzioni di *cybersecurity***, *in primis* per le imprese coinvolte nello *scope* della NIS e con particolare riguardo alle PMI. In questa prospettiva, e vista che la *cybersecurity* prevede per sua natura una forte interconnessione tra tutti gli attori economici (a partire da quelli appartenenti alle stesse filiere), occorre promuovere **modelli di collaborazione di filiera**, per esempio incentivando la partecipazione a iniziative congiunte su ambiti quali la formazione, la condivisione di *best practice*, la ricerca e l'innovazione.

Inoltre, si propone di identificare e creare uno *standard* unificato per la **certificazione tecnica** (come ad esempio EUCC/GSMA 5G NESAS, ecc.), al fine di semplificare il processo – ad oggi ancora complesso – di certificazione.

Infine, è possibile realizzare un nuovo modello di servizio per la *cybersecurity* "***CISO as a Service***" (*Chief Information Security Officer* come servizio), prevedendo l'*outsourcing* del ruolo di CISO a un fornitore di servizi specializzato in sicurezza informatica, permettendo soprattutto alle PMI che si avviano ai processi di digitalizzazione e sicurezza informatica di avere accesso a competenze e risorse esperte in *cybersecurity* senza la necessità di assumere un CISO a tempo pieno. Tale modello potrebbe evolvere, per le PMI più strutturate dal punto di vista digitale e di *cybersecurity*, in **consorzi** per offrire una gamma completa di servizi di

sicurezza informatica. Questi consorzi potrebbero comprendere diverse competenze e specializzazioni, consentendo alle aziende di accedere a un'ampia gamma di servizi di sicurezza (*in primis* sulle componenti esecutive) in un unico punto di contatto. L'obiettivo finale di questa proposta è quello di fornire alle aziende di tutte le dimensioni un accesso più conveniente e flessibile alle competenze di sicurezza informatica, consentendo loro di migliorare la propria sicurezza e mitigare i rischi legati alle minacce informatiche sempre più sofisticate.

Governance e modelli collaborativi

L'ultimo ambito è strettamente legato alla **natura fortemente trasversale** della *cybersecurity*, che interconnette attori economici pubblici e privati, di piccole e grandi dimensioni, afferenti a una pluralità di settori e Paesi. Tutti questi attori, che sono naturalmente associati ad **esigenze** diverse, sono nondimeno accomunati dall'obiettivo di garantire sempre crescenti livelli di sicurezza, a supporto dei propri sistemi economici e sociali.

Per questo motivo, e traendo ispirazione dalle migliori pratiche già presenti, si suggerisce di attivare **meccanismi di consultazione degli *stakeholder*** nell'ambito dell'attività normativa della *cybersecurity*. Si fa per esempio riferimento ai meccanismi di consultazione previsti dall'Unione Europea, dove le iniziative di *policy* prevedono un'intensa attività di raccolta delle istanze delle parti interessate. Con specifico riferimento alla *cybersecurity*, possono essere ricordati i casi di Regno Unito e Canada, che per garantire un risultato ottimale delle loro Strategie Nazionali di Cybersicurezza hanno messo a disposizione un processo di consultazione aperta per consentire a tutti di fornire un *feedback* sulla strategia, ma anche la Francia che ha redatto la lista delle infrastrutture in accordo con gli operatori stessi[15].

[15] Fonte: DCAF – Geneva Centre for Security Sector Governance, "Guide to Good Governance in Cybersecurity", 2022.

Focus: I processi di *stakeholder engagement* dell'Unione Europea

Esistono due modalità principali per **partecipare al processo legislativo** dell'Unione Europea: la prima riguarda la definizione delle politiche o il loro miglioramento; la seconda invece offre la possibilità di suggerire miglioramenti e semplificazioni in generale anche su leggi e direttive già in essere con lo scopo di ridurre gli oneri che queste possono comportare.

Il primo percorso prevede che durante il processo che trasforma le idee in testi normativi i cittadini possano intervenire più volte, in ogni passaggio, **inviando commenti** alle idee, **esprimendo pareri** su questionari relativi alla bozza di norma, mandando commenti al testo legislativo prima dell'approvazione. Inoltre, spesso le norme sono seguite da altri testi che le integrano ("atti delegati") o ne dettagliano l'applicazione ("atti di esecuzione"); anche su questi testi è possibile, prima della loro adozione, esprimere pareri e commenti. **Ciò che i cittadini inviano viene valutato** rispetto alle regole di pubblicazione, ma poi immediatamente **reso pubblico** in modo che anche gli altri cittadini possano rendersi conto degli argomenti posti in essere rispetto al tema in discussione; il cittadino per commentare si deve iscrivere al sito, ma in questo modo ha la possibilità di ricevere gli avvisi ogni qual volta ci sono sviluppi sulla questione a cui ha partecipato o nuove consultazioni sui temi di suo interesse. Diversamente **le associazioni, le organizzazioni e coloro che agiscono per influire sui processi decisionali** della Commissione a livello professionale devono preventivamente registrarsi sul "**Registro per la Trasparenza**" per poter poi inviare i loro commenti.

Il secondo percorso è molto più generico e aperto, in quanto **ogni cittadino può inviare suggerimenti e osservazioni su qualsiasi legge o regolamento in essere da almeno 2 anni**, al fine di rendere tale provvedimento più efficiente o ridurre il carico normativo che comporta. Tutte le osservazioni vengono prese in carico attraverso la piattaforma REFIT che, dopo una valutazione, provvederà ad inserire il suggerimento nelle sue raccomandazioni alla Commissione oppure, nel caso non sia applicabile, a rispondere al cittadino o organizzazione con una spiegazione in merito. Per garantire la massima partecipazione tale strumento prevede che il cittadino, al momento di inviare i commenti, può scegliere se rimanere anonimo o no.

Fonte: elaborazione The European House – Ambrosetti su dati Dipartimento per la Funzione Pubblica, 2023.

La seconda proposta attiene invece al supporto alle ***partnership* con Paesi terzi**, potenzialmente afferenti a una pluralità di ambiti e finalizzate all'aumento della capacità europea in ambito di sicurezza informatica. Tali soluzioni di collaborazione internazionale sono infatti in grado di generare modelli virtuosi per affrontare le sfide comuni della *cybersecurity*, da quelle formative e di *governance*, fino a quelle normative e tecnologiche. Si tratta, inoltre, di un'indicazione coerente con la Strategia Nazionale di Cybersicurezza, che evidenzia la necessità di incrementare la cooperazione sul fronte nazionale partecipando in modo proattivo alle iniziative europee e internazionali e promuovendo collaborazioni bilaterali.

Infine, si propone di definire **meccanismi trasparenti** per le attività di valutazione dei rischi di sicurezza *end-to-end*, ovvero basati su criteri e *standard* scientificamente applicabili.

Bibliografia di riferimento

- Accredia, “Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata”, 2022
- Aica, Anitec-Assinform, Assintel, Assinter Italia, “Osservatorio delle Competenze Digitali 2019”, 2019
- Agenzia per la cybersicurezza nazionale, “Strategia nazionale di Cybersicurezza 2022-2026”, 2022
- Anderton, R., Jarvis, V., Labhard, V., Petroulakis, F., Rubene, I. & Vivian, L., “The digital economy and the euro area”, 2020
- Assintel, “Il mercato ICT e l’evoluzione digitale in Italia”, 2022
- Banca europea per gli investimenti e Commissione europea, “La digitalizzazione delle piccole e medie imprese in Italia. Modelli per il finanziamento di progetti digitali”, 2021
- Castellani D., Lamperti F., Lavoratori K., “Measuring adoption of industry 4.0 technologies via international trade data: insights from European countries”, 2022
- Cefriel – Politecnico di Milano, White Paper “Come governare il patrimonio informativo aziendale per estrarne il valore”, 2023
- Centro Economia Digitale, “Sovranità Tecnologica”, 2021
- Clusit, “Rapporto Clusit 2022 sulla sicurezza ICT in Italia”, 2022
- Commissione Europea e European Investment Bank, “European Cybersecurity Investment Platform”, 2022
- Commissione Europea, “Allegati della proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148”, 2016
- Commissione Europea, “Allegati della Proposta di regolamento del parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020”, 2022
- Commissione Europea, “Comunicazione congiunta al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni. Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro”, 2013
- Commissione Europea, “Data market study 2021-2023. D2.1 First report on facts and figures”, 2022
- Commissione Europea, “Digital Economy and Society Index (DESI) 2022”, 2022

- Commissione Europea, “Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione”, 2016
- Commissione Europea, “Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148”, 2020
- Commissione Europea, “Overview of cybersecurity policies in the EU”, 2021
- Commissione Europea, “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”, 2019
- Commissione Europea, “Regolamento Del Parlamento Europeo E Del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020”, 2022
- Commissione Europea, “Relazione della Commissione al Parlamento Europeo e al Consiglio di valutazione della coerenza degli approcci adottati dagli Stati membri per l'identificazione degli operatori di servizi essenziali conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi”, 2019
- Commissione Europea, “Strategia dell'UE sull'Unione della sicurezza: integrare le singole misure un nuovo ecosistema della sicurezza”, 2020
- Commissione Europea, “The EU’s Cybersecurity Strategy for the Digital Decade”, 2020
- Confindustria Digitale, Anitec – Assiform, “Il digitale in Italia 2022. Mercati, dinamiche, Policy”, 2022
- Cordella A., Paletti A., “Government as a platform, orchestration, and public value creation: The Italian case”, 2019
- DCAF – Geneva Centre for Security Sector Governance, “Guide to Good Governance in Cybersecurity”, 2022
- Eurofound, “Anticipating and managing the impact of change. Ethics in the digital workplace”, 2022
- European Union Agency for cybersecurity (ENISA), “ENISA thread landscape 2022”, 2022
- European Union Agency for cybersecurity (ENISA), “NIS Investments”, 2022
- Foreign, Commonwealth & Development Office, DCAF e DCSD, “Guide to Good Governance in Cybersecurity”, 2019

- Fraunhofer Institute for Software and Systems Engineering, “Industrial Data Space: Digital Sovereignty Over Data”, 2016
- Governo italiano, “Piano Nazionale di Ripresa e Resilienza #NextGeneration Italy”, 2021
- Huawei, “Huawei's Position Paper on Cyber Security”, 2019
- Istat, “Digitalizzazione e tecnologia nelle imprese italiane”, 2020
- Istituto per la competitività (i-com), “Rapporto Osservatorio sulla cibersicurezza. L’ecosistema italiano della sicurezza informatica tra regolazione, competitività e consapevolezza”, 2023
- Joint Research Centre, “Application Programming Interfaces in Governments: Why, what and how”, 2020
- Organization for Economic Co-operation and Development (OECD), “Digital technology adoption, productivity gains in adopting firms and sectoral spill-overs: Firm-level evidence from Estonia”, 2020
- Organization for Economic Co-operation and Development (OECD), “Digital Dividend: Policies to Harness the Productivity Potential of Digital Technologies”, 2019
- Organization for Economic Co-operation and Development (OECD), “Digitalisation and productivity: In search of the holy grail – Firm-level empirical evidence from EU countries”, 2019
- Organization for Economic Co-operation and Development (OECD), “Measuring the Digital Transformation: A Roadmap for the Future”, 2019
- Organization for Economic Co-operation and Development (OECD), “Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies”, 2019
- Organization for Economic Co-operation and Development (OECD), “Better Regulation Practices across the European Union”, 2019
- Organization for Economic Co-operation and Development (OECD), “Tax Challenges Arising from Digitalisation”, 2018
- Parlamento Europeo, “European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))”, 2022
- Pope R., “Playbook: Government as a Platform”, 2019
- Securities and Exchange Commission, “Factsheet – Public Company Cybersecurity; Proposed Rules”, 2022
- Stigler Center, “Stigler Committee on Digital Platforms – Final Report”, 2019
- UNCTAD, “Digital Economy Report 2021. Cross-border data flows and development: For whom the data flow”, 2021