EXECUTIVE SUMMARY

CAPITOLO 1
Lo stato della cibersicurezza in Europa

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPITOLO 2
Lo stato della cibersicurezza in Italia

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

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

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

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

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

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

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

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

difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, assumere tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi di cui si dirà nei paragrafi successivi, incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale (comprese le attività di ispezione e verifica e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative), acquisire le competenze attribuite al DIS dal decreto-legge perimetro e dai relativi provvedimenti attuativi, quelle relative alla sicurezza e all'integrità delle comunicazioni elettroniche di cui al D.Lgs. n. 259/03 e svolgere tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, nonché tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti.

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

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

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

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

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

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

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

Il decreto legge n. 105/2019, convertito con la legge n. 133/2019, ha istituito il **perimetro di sicurezza nazionale cibernetica** al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Per raggiungere tale obiettivo, la disciplina istitutiva del perimetro ha tracciato un percorso attuativo frazionato con scadenze temporali diversificate, che si snoda attraverso cinque decreti del Presidente del Consiglio dei ministri ed un regolamento governativo di esecuzione e che, seppur in ritardo, è finalmente giunto a completamento con l'adozione del DPCM 18 maggio 2022, n. 92 (pubblicato sulla G.U. del 15 luglio 2022) con il quale è stato adottato il regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra il CVCN, i laboratori di prova accreditati ed i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa.

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

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

Esercizio dei poteri speciali e il perimetro di sicurezza cibernetica

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPITOLO 4
L'offerta formativa in materia cibersicurezza

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

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

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

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

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

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

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

La riforma degli ITS

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

CAPITOLO 5
Le certificazioni

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

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

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

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

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

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

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

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