LUISS

Dipartimento
di Scienze Politiche

Cattedra di Politica Economica

La sicurezza informatica nell'ambito del Mercato Unico Digitale: uno strumento di crescita economica

Prof. Paolo Garonna

RELATORE

Federica Pizzuti Matr. 087882

CANDIDATO

Anno Accademico 2020/2021

INDICE

INTRODUZIONE

"Voglio che proteggiamo meglio gli europei nell'era digitale"

Jean-Claude Juncker[1]

Con l'inizio dell'Era Digitale, il tema della protezione dei dati *online,* e più in generale della sicurezza informatica, si è esteso a quasi tutti gli ambiti della società odierna, andando ad influenzare ogni aspetto dei sistemi internazionali di *governance* economica e politica. Con l'approdo in Europa della digitalizzazione, l'illegalità e i crimini informatici si sono evoluti considerevolmente, e di conseguenza è cresciuta l'attenzione alla *cybersecurity* da parte delle istituzioni europee e degli Stati Membri, che hanno cominciato a percepirla come un'emergenza da affrontare su diversi fronti. Gli investimenti nel settore della sicurezza informatica rappresentano un passaggio essenziale all'interno del processo di trasformazione digitale intrapreso dall'Unione e dagli Stati Membri. Il sistema europeo di monitoraggio e di risposta agli attacchi cibernetici si basa su azioni multidimensionali e trasversali, volte alla formazione e sensibilizzazione al tema della *cybersecurity*, allo sviluppo di un linguaggio *cyber* comune, ma soprattutto alla certificazione e all'impiego di *best practices*, che vedono un coinvolgimento sia da parte degli attori pubblici che di quelli privati. Il ciberspazio è caratterizzato da una geografia poco conosciuta ed in continua evoluzione e stare al passo con un processo trasformativo di tale portata richiede un costante aggiornamento e potenziamento in termini di investimenti nel settore della ricerca e dell'innovazione, il quale è strettamente correlato a quello della sicurezza informatica. In particolare, nel contesto dell'Unione Europea i fondi e i finanziamenti a disposizione per la *cybersecurity* sono aumentati negli ultimi anni, così come è aumentata la collaborazione tra la ricerca, le imprese e i governi, al fine non solo di accrescere il livello di protezione degli utenti *online*, ma anche di salvaguardare le economie mondiali.

Il presente studio intende approfondire il percorso strategico e normativo che l'Unione Europea ha intrapreso nel contesto del Mercato Unico Digitale (*Single Digital Market*) al fine di rafforzare la sicurezza informatica in quei settori chiave per la crescita economica e sociale europea. In particolare, l'attenzione è posta sul settore finanziario, uno dei campi più influenzati e dipendenti dal processo di transizione digitale, e di conseguenza

[1] Juncker, JC. (2017, settembre 13). *Discorso sullo stato dell'Unione 2017*. Commissione Europea (Discorso).

maggiormente esposto alle crescenti minacce informatiche. L'interesse per tale argomento è frutto dell'esperienza acquisita durante il mio tirocinio universitario, che mi ha dato l'opportunità di investigare su molte tematiche relative agli obiettivi e alle priorità dell'Unione Europea, soprattutto nell'ambito della *cybersecurity*, la cui rilevanza non può più essere esclusa, né a livello europeo né a livello mondiale. L'elaborato fa riferimento a dati e studi statistici rilevanti, al fine di aiutare il lettore a comprendere la strategia europea di sicurezza informatica ed a sviluppare una maggiore consapevolezza delle sfide che il mercato globale, ma anche i singoli individui devono affrontare di fronte all'espansione del ciberspazio e delle pericolosità ad esso connesse.

Innanzitutto, l'elaborato intende ripercorrere i punti salienti del percorso di realizzazione del quadro legislativo dell'Unione Europea nel campo della sicurezza informatica, partendo da un'analisi delle misure adottate sin dai primi anni 2000, fino a toccare il quadro normativo più recente. La strategia europea in ambito *cyber* si inserisce all'interno del piano di crescita del Mercato Unico Digitale europeo, il cui funzionamento è essenziale per la sopravvivenza e lo sviluppo dell'economia europea. Difatti, le dimensioni interne al sistema economico europeo stanno da tempo subendo una crescente influenza, per lo più positiva, da parte del processo di digitalizzazione, richiedendo un intervento maggiore delle istituzioni europee e dei singoli Stati Membri. Fondamentali sono anche i rapporti cooperativi che intercorrono tra i diversi attori interni ed esterni all'Unione nell'implementazione delle misure previste da tale strategia europea, in quanto è proprio sulla base di questa rete relazionale che la prevenzione e la protezione ai crimini informatici vengono garantite su tutto il territorio comunitario.

Il secondo capitolo si focalizza in primo luogo sui fondi e sugli strumenti finanziari messi a disposizione dall'Unione Europea al fine di sostenere la spesa prevista per le misure di sicurezza informatica. Nonostante il quadro di politica economica relativo alla spesa europea in ambito *cyber* sia particolarmente frammentato, i programmi finanziari previsti offrono budget elevati, dimostrando la volontà dell'Unione di accelerare il processo di digitalizzazione in tutti i settori, oltre che a quello della *cybersecurity*. In secondo luogo, questa sezione dell'elaborato si concentra sull'analisi delle principali iniziative *cyber* intraprese per il settore finanziario e per quello industriale. L'elevata criticità del settore finanziario, legata ad una sua maggiore esposizione alla criminalità informatica rispetto ad altri settori chiave, ha spinto le istituzioni e le agenzie europee coinvolte a dare vita ad una nuova strategia di finanza digitale, basata su un rigido sistema di regolamentazione e

vigilanza. Alla base vi è la consapevolezza che la protezione del settore finanziario sul fronte digitale è propedeutica alla protezione della stabilità finanziaria europea.

Il terzo e ultimo capitolo entra più nel dettaglio, fornendo una panoramica della strategia di sicurezza informatica adottata da uno dei paesi membri dell'Unione Europea più all'avanguardia nel settore della digitalizzazione: l'Estonia. Sulla base del contesto normativo nazionale estone e di alcune analisi statistiche è stato possibile individuare le sfide future che l'Estonia dovrà affrontare nel settore della *cybersecurity*, e allo stesso tempo di proporre un profilo evolutivo della strategia estone nel processo di digitalizzazione.

CAPITOLO 1
LA STRATEGIA EUROPEA PER LA SICUREZZA INFORMATICA

1.1 IL QUADRO LEGISLATIVO EUROPEO SULLA *CYBERSECURITY*

1.1.1 I primi passi verso un'Europa digitale più sicura

Negli ultimi vent'anni il ruolo dell'Unione Europea nell'ambito della sicurezza informatica ha subito una notevole trasformazione. Pur rimanendo un punto di riferimento per gli Stati Membri nello sviluppo del loro *framework* nazionale in ambito *cyber*, il concetto di uniformità e di cooperazione tra i vari Stati europei risulta ancora poco definito, al punto da rendere più complesso l'aggiornamento delle politiche europee nel settore della *cybersecurity*.

La sicurezza cibernetica è stata inserita per la prima volta nelle discussioni politico-economiche europee solamente a partire dagli anni 2000, a seguito dell'elaborazione da parte della Commissione Europea di due comunicazioni: la prima comunicazione rivolta alla sicurezza delle reti e dell'informazione nel panorama europeo[2]; l'altra relativa al miglioramento della sicurezza delle infrastrutture dell'informazione e alla lotta al *cybercrime*[3]. In queste comunicazioni è stata sottolineata la crescente interconnessione tra lo sviluppo socioeconomico e lo sviluppo del mondo delle comunicazioni e delle informazioni. Da questa importante correlazione deriva che i numerosi attacchi che colpiscono il mondo digitale rischiano di compromettere anche gran parte delle economie mondiali. Per far fronte a questi rischi, la Commissione Europea ha ritenuto necessario un avanzamento nel campo della sicurezza informatica, con lo scopo di garantire una transizione affidabile dell'Europa verso una società dell'informazione[4]. L'approccio strategico europeo in materia di protezione delle reti e dell'informazione è stato considerato

[2] Commissione Europea. (2001). *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM/2001/0298). Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

[3] Commissione europea. (2001). *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002* (COM/2000/890). Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

[4] Per una definizione accurata del termine "società dell'informazione" cfr.: Giorgio Sirilli, *Enciclopedia della Scienza e della Tecnica,* https://www.treccani.it/enciclopedia/societa-dell-informazione_%28Enciclopedia-della-Scienza-e-della-Tecnica%29.

prioritario fin dall'inizio, vista l'elevata correlazione con il funzionamento dell'economia dell'Unione. Nella comunicazione di giugno 2001, relativa alla sicurezza delle reti e dell'informazione, la Commissione ha riportato che "la sicurezza delle reti e dell'informazione è una merce comprata e venduta sul mercato ed è ormai parte integrante delle clausole contrattuali siglate tra le parti[5]". Già all'epoca, la presenza di imperfezioni nel mercato di tali servizi rendeva complicata l'attuazione di investimenti necessari e sufficienti e per questo motivo un approccio strategico europeo basato su soluzioni comuni e su una cooperazione mondiale[6] era considerato essenziale da parte della Commissione. Tale strategia europea avrebbe rappresentato un'aggiunta al quadro di riferimento esistente all'epoca, caratterizzato dalla fusione fra "politiche delle telecomunicazioni, della protezione dei dati e della criminalità informatica[7]", come illustrato nel grafico che segue.

Fonte: Commissione Europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM/2001/0298), 6 giugno 2001.

Entrambe le comunicazioni della Commissione Europea sono state propedeutiche alla definizione del quadro di riferimento comune europeo nell'ambito della cibersicurezza.

[5] Commissione Europea. (2001). *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo. Op. cit.,* pag. 19.
[6] Commissione europea. (2001). *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002,* pag. 3.
[7] Commissione Europea. (2001). *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo. Op. cit.,* pag. 3.

Infatti, il termine "*cybersecurity*" non compare nei rispettivi documenti, lasciando intendere l'iniziale arretratezza delle istituzioni europee e degli Stati Membri in tale settore[8].

1.1.2 L'Agenzia dell'Unione Europea per la cibersicurezza (ENISA)

Nel 2004, l'Unione Europea ha fatto un ulteriore passo avanti nella creazione di una strategia europea sulla sicurezza informatica, approvando il regolamento n. 460/2004, con il quale è stata istituita l'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA, *European Network and Information Security Agency*). ENISA è un organismo consultivo che si occupa di affiancare la Commissione Europea nel processo di creazione di un contesto europeo più sicuro ed affidabile in ambito *cyber*. L'Agenzia fornisce assistenza a tutti gli Stati Membri già in possesso di un quadro normativo in ambito di cibersicurezza, mentre, per gli Stati rimasti ancora indietro, ENISA agisce diffondendo la cultura della sicurezza informatica. L'obiettivo primario è quello di raggiungere un adeguato livello di cooperazione nell'attuazione delle politiche comuni europee e per questo motivo uno dei compiti principali dell'Agenzia è quello di fare in modo che la sicurezza informatica non sia un campo riservato esclusivamente ad un gruppo di specialisti, ma che diventi una colonna portante delle politiche nazionali dei singoli Stati europei, cosicché essi abbiano gli strumenti adatti per poter combattere i crescenti attacchi cibernetici. Al momento, tutti gli Stati dell'Unione Europea sono dotati di una *National Cybersecurity Strategy* (NCSS), ovvero un piano nazionale in cui vengono indicati gli obiettivi primari e i target da raggiungere nel campo della sicurezza informatica. ENISA si occupa di supportare questi piani d'azione, in particolar modo fornendo delle linee guida agli Stati Membri, in modo che essi possano implementare e sviluppare le proprie strategie in parallelo con i progressi svolti dall'Unione Europea.

ENISA è un'entità neutrale che agisce in modo trasparente per aiutare individui, organizzazioni e industrie, che investono nelle nuove infrastrutture e tecnologie digitali. I costi e i benefici della digitalizzazione devono essere costantemente monitorati, ed è proprio qui che ENISA interviene: valuta i livelli di sicurezza dei servizi e dei prodotti digitali, utilizzando un approccio volto a bilanciare i bisogni sia economici che di sicurezza informatica degli enti coinvolti. In questa attività di monitoraggio è importante la cooperazione con i *Computer Security Incident Response Teams* (CSIRTs), ossia degli

[8] C. Cencetti. (2014). *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Nuova Cultura. p. 25.

istituti attivi nell'analisi, nel monitoraggio e nell'intervento in caso di attacchi cibernetici rivolti ad aziende o alla Pubblica Amministrazione. I principali servizi offerti dai CSIRTs sono:

1. **Servizi reagenti:** consistono in relazioni scritte a seguito di incidenti cibernetici;
2. **Servizi proattivi:** rilevano la presenza di attacchi cibernetici e li prevengono ancor prima che eventuali effetti negativi si generino;
3. **Servizi di gestione della qualità della sicurezza:** possono essere richiesti da enti esterni ai CSIRTs per effettuare una revisione o un miglioramento dei servizi di sicurezza offerti dall'ente stesso[9].

Il ruolo dell'Agenzia dell'Unione Europea per la cybersecurity è cresciuto e continua a crescere tutt'oggi, ed è affiancato da nuove agenzie altamente qualificate, le quali rappresentano un valore aggiunto nella promozione della salvaguardia e della sicurezza della società digitale[10].

1.1.3 Dall'Agenda digitale alla strategia europea per la cybersecurity

A partire dalla "Relazione sull'attuazione della Strategia europea in materia di sicurezza[11]", presentata nel 2008 dal Consiglio dell'Unione Europea con lo scopo di rinforzare la "Strategia europea in materia di sicurezza del dicembre 2003[12]", il termine "*cybersecurity*" è stato inserito nelle analisi e nel corpus normativo dell'Unione Europea[13]. Nella relazione il Consiglio ha sottolineato che "*more work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation*[14]".

[9] ENISA: https://www.enisa.europa.eu/topics/csirt-cert-services (Ultimo accesso 8 aprile 2021).
[10] Per approfondimenti cfr. Paragrafo 1.2 "La comunità *cyber*".
[11] Council of the EU. (2008). *Report on the Implementation of the European Security Strategy*. (S407/08). https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf (Ultimo accesso 8 Aprile 2021).
[12] Consiglio dell'Unione Europea. (2003). *Strategia Europea in materia di sicurezza*. Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea. La strategia europea in materia di sicurezza viene inserita all'interno del quadro europeo della Politica di sicurezza e di difesa comune (PSDC).
[13] https://www.enisa.europa.eu/topics/csirt-cert-services (Ultimo accesso 8 aprile 2021).
[14] Council of the EU. (2008). *Report on the Implementation of the European Security Strategy*, pag. 5.

Nel 2010 la Commissione Europea ha pubblicato un'importante comunicazione intitolata "Un'Agenda digitale europea[15]", la quale rappresenta una delle sette iniziative faro della strategia Europa 2020[16]. Lo scopo di questa strategia era quello di accompagnare gli Stati Membri nella ripresa a seguito della crisi finanziaria del 2008 e di seguirli nel percorso di crescita intelligente, sostenibile e inclusiva entro il 2020. L'Agenda digitale europea è stata posta alla base di un processo di digitalizzazione economico e sociale, volto a valorizzare e diffondere le moderne tecnologie, in modo da poter migliorare la qualità della vita di tutti i cittadini europei. Le nuove tecnologie dell'informazione e della comunicazione (TIC), che rappresentano una risorsa fondamentale dell'economia digitale, non sono ancora state sfruttate a pieno nel panorama europeo, a causa della presenza di svariati ostacoli (Figura 1):

1. Frammentazione dei mercati digitali;
2. Mancanza di interoperabilità;
3. Aumento della criminalità informatica e rischio di un calo di fiducia nelle reti;
4. Mancanza di investimenti nelle reti;
5. Impegno insufficiente nella ricerca e nell'innovazione;
6. Mancanza di alfabetizzazione digitale e competenze informatiche;
7. Opportunità mancate nella risposta ai problemi della società[17].

L'Agenda digitale europea ha proposto un piano d'azione incentrato sulla risoluzione di questi sette ostacoli, attraverso un elevato livello di cooperazione sia a livello dell'Unione che a livello regionale. L'Agenda "non può avere successo senza un contributo sostanziale da parte delle altre parti interessate, compresi i giovani "figli dell'era digitale", dai quali abbiamo molto da imparare[18]". Tra le varie problematiche evidenziate dalla Commissione Europea è importante soffermarsi su quella relativa alla criminalità cibernetica e al calo di fiducia nel progresso tecnologico europeo. Secondo la Commissione Europea, la sicurezza

[15] Commissione Europea. (2010). *Un'Agenda digitale europea*, (COM/2010/245). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[16] Commissione Europea. (2010). *EUROPA 2020 Una strategia per una crescita intelligente, sostenibile e inclusiva,* (COM/2010/2020). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[17] Commissione Europea. (2010). *Un'Agenda digitale europea*, (COM/2010/245). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[18] Commissione Europea. (2010). *EUROPA 2020 Una strategia per una crescita intelligente, sostenibile e inclusiva,* (COM/2010/2020). *Op. cit*., pag. 7. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea

informatica è un diritto di tutti i cittadini europei, che deve essere necessariamente tutelato da eventuali minacce o attacchi informatici. Le azioni previste dall'agenda digitale in questo campo sono molteplici e possono essere riassumibili in alcuni punti:

- Adottare misure nuove volte a rafforzare la politica di sicurezza delle reti e delle informazioni. Ad esempio, rinnovare l'Agenzia dell'Unione Europea per la cibersicurezza (ENISA), oppure rafforzare il sistema dei CSIRTs, non solo in relazione alle aziende o alla Pubblica Amministrazione, ma anche in funzione delle istituzioni europee;
- Adottare un quadro normativo che preveda nuove misure da intraprendere in caso di attacchi informatici, e ampliare il quadro normativo vigente in ambito cyber;
- Istituire un centro europeo per il *cybercrime*;
- Migliorare la collaborazione a livello globale, in modo da permettere una gestione dei rischi condivisa e da migliorare l'azione di risposta alle minacce informatiche;
- Fornire degli strumenti di prevenzione e preparazione ai *cyber-attacks*.

Gli Stati Membri, invece, sono chiamati a:

- Istituire sui propri territori nazionali delle reti efficienti di analisi e monitoraggio degli attacchi cibernetici;
- Installare delle linee telefoniche dirette per denunciare contenuti *online* irregolari[19].

Il 2013 ha rappresentato un anno di svolta per l'Unione Europea nel campo della cibersicurezza, in quanto è stata approvata la "Strategia dell'Unione Europea per la cybersicurezza[20]", proposta dalla Commissione Europea e dall'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza. L'arretratezza dell'Europa nel campo della *cybersecurity* rispetto agli altri paesi industrializzati e la necessità di trasformare l'Europa in un luogo digitalizzato e al contempo sicuro hanno spinto le istituzioni europee a delineare le misure e gli interventi idonei nel campo della cibersicurezza, e a formalizzarli inserendoli all'interno di una strategia nuova basata sul coinvolgimento attivo sia a livello comunitario che a livello internazionale. Per la prima volta l'Unione Europea si è dotata di un piano d'azione interamente rivolto alla sicurezza informatica e alla creazione di un

[19] *Ibidem*, pag. 19-20.
[20] Commissione Europea (2013). *Strategia dell'Unione Europea per la cybersicurezza.* Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

"ciberspazio aperto e sicuro[21]".

La strategia evidenzia innanzitutto i principi fondanti del *framework* legislativo sulla cibersicurezza. Affinché si possa parlare di un ciberspazio efficiente è necessario che i valori, i diritti e le libertà fondamentali sancite dall'Unione Europea vengano rispettati, soprattutto in materia di protezione dei dati personali, e che l'accesso ad Internet sia garantito a tutta la popolazione europea. Nella seconda parte del documento vengono trattate cinque priorità strategiche da seguire per poter affrontare le sfide enunciate dalla Commissione nel campo della sicurezza informatica. Infine, nell'ultima parte si fatto riferimento agli attori da coinvolgere e alle differenti attività di coordinamento tra di essi.

La prima priorità strategica è relativa al raggiungimento della ciberresilienza. Con il termine *cyber resilience* si fa riferimento a "*the ability to continuously deliver the intended outcome despite adverse cyber events*[22]". Al fine di raggiungere tale obiettivo è necessaria un'attuazione costante e aggiornata delle misure di sicurezza informatica. Per questo motivo, all'interno della strategia per la cibersicurezza, la Commissione ha chiesto all'Agenzia dell'Unione Europea per la cibersicurezza di rafforzare il proprio ruolo assistenziale e di promuovere la resilienza informatica, anche nel rapporto con il settore privato. La realizzazione della ciberresilienza all'interno dell'Unione necessita di una campagna di sensibilizzazione, affinché tutti gli attori coinvolti siano consapevoli dei rischi e dei benefici legati al processo di digitalizzazione. La seconda priorità definita all'interno della strategia concerne la lotta contro gli attacchi cibernetici. La criminalità informatica è un fenomeno in rapida crescita, che necessita di un'attenzione maggiore da parte delle istituzioni europee e degli Stati Membri. All'interno della strategia la Commissione ha chiesto pertanto agli Stati europei di implementare le politiche nazionali di difesa in materia *cyber* e, per gli Stati che ancora non avevano ratificato la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica[23], di farlo al più presto. Inoltre, la Commissione ha chiesto un miglioramento delle attività di monitoraggio e di risposta ai *cyber-attacks* da parte delle entità coinvolte, in particolar modo il Centro europeo per la lotta alla criminalità informatica

[21] *Ibidem*, pag. 2.
[22] Björck F., Henkel M., Stirna J., Zdravkovic J. (2015). *Cyber Resilience – Fundamentals for a Definition*, pag. 2. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol 353. Springer, Cham.
[23] Consiglio d'Europa, *Convenzione sulla criminalità informatica*, aperta alla firma a Budapest il 23 novembre 2001, entrata in vigore il 1° luglio 2004, STE n. 185. La Convenzione è il primo trattato internazionale in materia di criminalità informatica, con lo scopo di raggiungere un *framework* legislativo comune in relazione alla lotta al *cyber-crime*. La Convenzione presenta le misure idonee da adottare, in regime di cooperazione internazionale, per combattere le infrazioni penali commesse *online*. Attualmente, gli unici Stati Membri che non hanno ratificato la Convenzione sono la Svezia e l'Irlanda.

(EC3), oltre che un maggiore coordinamento tra di esse. La terza priorità strategica fa riferimento all'implementazione di una politica di ciberdifesa connessa alla Politica europea di difesa e sicurezza comune (PSDC). Il rapporto tra le istituzioni europee e le istituzioni militari è fondamentale in ambito di sicurezza informatica e per questo la Commissione ha chiesto di rafforzare il regime di cooperazione tra UE e NATO[24]. La quarta priorità strategica riguarda lo sviluppo delle risorse industriali e tecnologiche per la cibersicurezza, il cui raggiungimento richiede innanzitutto una partnership tra il settore pubblico e quello privato. Dato il carattere extra-territoriale della produzione di prodotti e servizi TIC, la Commissione ha chiesto al settore privato europeo di rafforzare le tecniche di sicurezza dei prodotti TIC, attraverso investimenti nel campo della ricerca e dell'innovazione. Infine, la strategia per la cibersicurezza ha imposto l'attuazione da parte dell'UE di un piano d'azione internazionale sul ciberspazio. Attraverso le misure presenti all'interno del piano "l'UE dovrà proporsi di promuovere l'apertura e la libertà di Internet, di incoraggiare le iniziative per l'elaborazione di regole di condotta e di applicare nel ciberspazio le leggi internazionali vigenti[25]" e di "aumentare l'impegno con i principali partner e le principali organizzazioni internazionali, per inserire le materie connesse alla cibersicurezza nella PESC e per migliorare il coordinamento di aspetti di portata globale[26]". L'ultima parte della strategia è rivolta agli attori da coinvolgere e alle responsabilità che essi devono assumere. La gestione degli attacchi è più efficace a livello nazionale, sia in termini di tempo che di azione. Tuttavia, un coinvolgimento unionale potrebbe essere utile in specifici casi[27].

1.1.4 Il quadro normativo recente

A partire dalla Strategia per la *cybersecurity* del 2013 il quadro normativo europeo in ambito di sicurezza informatica si è evoluto, assumendo un carattere maggiormente definito. Prima di poter analizzare la nuova legislazione europea sulla cibersicurezza è necessario soffermarsi su alcuni dei progetti comunitari che ne hanno ispirato la creazione. Una delle priorità del programma della Commissione Europea Juncker per il periodo 2014-2019 era quella relativa alla realizzazione di un Mercato Unico Digitale (*Single Digital*

[24] Per approfondimenti cfr. Paragrafo 1.2.2.
[25] Commissione Europea. (2013). *Strategia dell'Unione Europea per la cybersicurezza*. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea, p. 16.
[26] *Ibidem*, p. 18.
[27] Per approfondimenti cfr. Paragrafo 1.2 "La comunità *cyber*".

Market) connesso e moderno. Il *Single Digital Market* è un mercato in cui "è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui (…) persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività *online* in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali[28]". Il funzionamento di tale mercato è fondamentale per l'economia digitale europea e per la sua società, in quanto esso potrebbe migliorare le condizioni di accesso ai prodotti digitali e permettere di raggiungere livelli elevati di crescita e innovazione in campo informatico. La media europea di accesso ai servizi di Internet (Figura 1) ammontava a circa l'80% delle famiglie nel 2014, per poi crescere approssimativamente al 90% nel 2019. A partire da questi dati è possibile concludere che il processo di digitalizzazione è iniziato in quasi tutti i paesi dell'Unione Europa ed è attualmente in rapida crescita, dimostrando l'efficacia delle politiche e delle strategie europee in campo digitale.

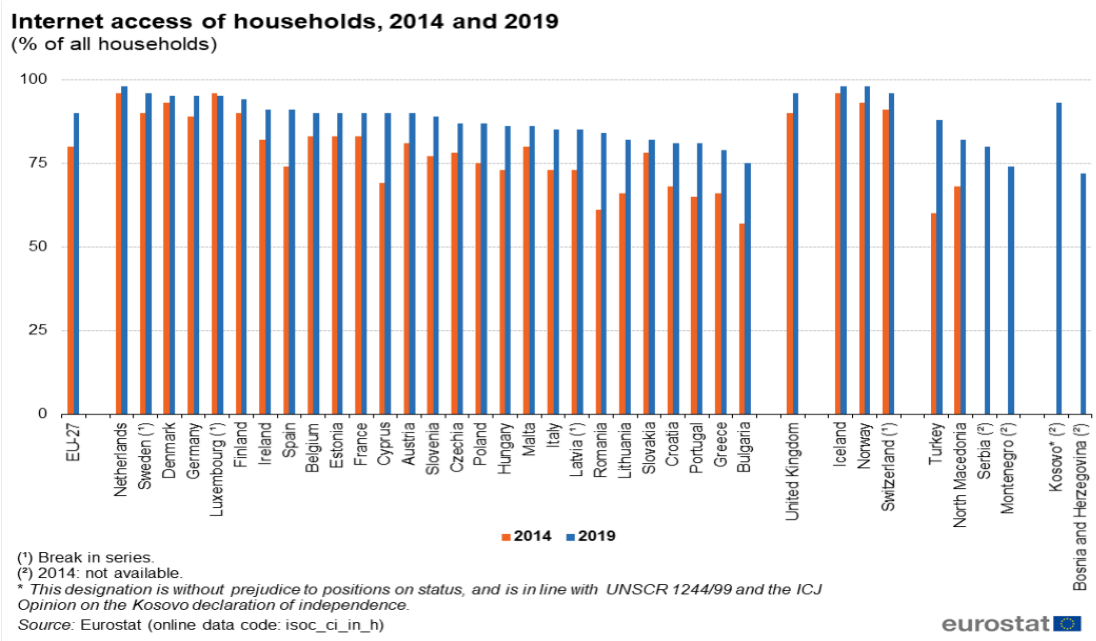

Figura 1: Accesso ad Internet delle famiglie nei 27 Stati Membri nel 2014 e 2019.

Fonte: Eurostat.

La sicurezza informatica è considerata uno degli elementi principali del Mercato Unico Digitale europeo. La rapidità dei processi di digitalizzazione e la crescente

[28] Commissione Europea. (2015). *Strategia per il mercato unico digitale in Europa*, (COM/2015/192 final). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea, pag. 3.

interconnessione delle economie digitali degli Stati Membri, entrambe conseguenze della creazione del Single Digital Market, hanno spinto l'Unione Europea a rafforzare il proprio approccio normativo in ambito *cyber*, attraverso l'aggiornamento del *framework* legislativo preesistente[29]. Un primo passo verso questa direzione è stato fatto con l'approvazione, nel 2016, della Direttiva NIS (*Network and Information System*, tradotto in rete e sistema informativo), la quale rappresenta la prima normativa europea in ambito *cybersecurity*. "Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno[30]". Trattandosi di una direttiva europea, quindi non direttamente applicabile nel territorio degli Stati Membri, la direttiva NIS è stata trasposta in ciascuno Stato europeo attraverso l'adozione di una specifica legislazione nazionale, con un termine temporale stabilito per il 9 novembre 2018. La direttiva è nata con l'intento di proteggere l'economia dell'Unione europea, assieme al benessere sociale dei suoi cittadini, da incidenti ed attacchi informatici rivolti alle reti e ai sistemi di informazione. La sicurezza di tali prodotti è fondamentale per la salute economica di specifici settori[31] e deve essere garantita attraverso un elevato livello di armonizzazione tra gli Stati UE.

La direttiva ha definito particolari misure per gli Stati Membri. Innanzitutto, è richiesta l'attuazione di una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi[32]. Entro un certo termine, gli Stati UE devono indentificare gli "operatori di servizi essenziali[33]" e i "fornitori di servizi digitali[34]", a cui si applica la direttiva NIS, e devono stabilire degli obblighi di sicurezza e di notifica nei loro confronti[35]. Un altro punto fondamentale della direttiva è quello che fa riferimento alle istituzioni nazionali che ogni Stato Membro deve designare. In base all'articolo 1 gli Stati devono istituire delle autorità nazionali competenti, dei punti di contatto unici e dei CSIRTs, che devono occuparsi rispettivamente del controllo dell'applicazione della direttiva a livello nazionale[36], del

[29] Mensi M. (2017). *Cybersecurity and the European digital market*, ISPI, https://www.ispionline.it/it/pubblicazione/cybersecurity-and-european-digital-market-18234.
[30] Direttiva (UE) 2016/1148, 6 luglio 2016, pag. 1.
[31] Cfr. Allegato II della Direttiva NIS (2016/1148).
[32] Cfr. Art. 7, Direttiva NIS (2016/1148).
[33] Per una definizione specifica cfr. Art. 5.2 Direttiva NIS.
[34] L'Allegato III della Direttiva NIS definisce tre tipi di servizi digitali: il mercato online, il motore di ricerca online e i servizi della nuvola (*cloud computing*).
[35] Mensi, M. *Cybersecurity and the European digital market*, *op. cit*.
[36] In caso di violazione della normativa nazionale di attuazione della direttiva NIS, l'Art. 21 prevede delle sanzioni.

collegamento con le autorità competenti degli altri Stati Membri e del monitoraggio e intervento in caso di attacchi informatici[37].

Il quadro normativo europeo in ambito di cibersicurezza è stato allargato ulteriormente con l'adozione del regolamento UE 2016/679, intitolato "Regolamento generale per la protezione dei dati[38]" (*General Data Protection Regulation* – GDPR), che ha imposto un modello di trattamento e di difesa dei dati personali comune per tutto il territorio dell'Unione, con lo scopo di rassicurare i cittadini sul funzionamento del Mercato Unico Digitale.

Nel 2017, la Commissione Europea ha presentato al Parlamento europeo e al Consiglio un pacchetto intitolato "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE[39]". Lo scopo di tale comunicazione era quello di riformare e rafforzare il quadro normativo europeo in materia di sicurezza informatica, in particolar modo la strategia sulla cibersicurezza del 2013 e la direttiva NIS del 2016. L'obiettivo prefissato nel pacchetto della Commissione è stato tuttavia raggiunto solamente nell'aprile del 2019, con l'approvazione del regolamento relativo all'Agenzia dell'UE per la cibersicurezza (ENISA) e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, noto anche come "*Cybersecurity Act*[40]". La prima parte del regolamento è rivolta al ruolo di ENISA, rimasto fino ad allora secondario, rispetto a quello degli Stati Membri, nell'elaborazione delle misure nazionali e settoriali in materia di cibersicurezza[41]. Il *Cybersecurity Act* ha rafforzato i compiti dell'Agenzia sotto ogni aspetto: dall'assistenza alle istituzioni europee e agli Stati UE, al compito di effettuare analisi strategiche, fino all'obbligo di promuovere la cooperazione internazionale sulle questioni relative alla sicurezza informatica[42]. La seconda parte del regolamento ha istituito "il quadro europeo di certificazione della cibersicurezza al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione

[37] Holzleitner MT., Reichl J. (2017). *European provisions for cyber security in the smart grid – an overview of the NIS-directive.* In *Elektrotech. Inftech.* 134**,** pag. 14–18. https://doi.org/10.1007/s00502-017-0473-7.
[38] Parlamento Europeo e Consiglio. (2016). *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio*.
[39] Commissione Europea. (2017). *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE*. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[40] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, 17 aprile 2019.
[41] Il *Cybersecurity Act* ha abrogato il regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).
[42] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, 17 aprile 2019, *op. cit.*

della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC[43]". Prima dell'adozione del regolamento, la maggior parte dei certificati di sicurezza informatica dei prodotti TIC e dei servizi digitali erano riconosciuti a livello nazionale, senza assumere alcun rilievo a livello comunitario. Con il *Cybersecurity Act*, invece, è stato istituito uno schema unitario di certificazione, che prevede la creazione di diversi sistemi europei di certificazione della cibersicurezza (Di Biagio, 2019). Questi nascono con lo scopo di proteggere i dati conservati, trasmessi o trattati, e di monitorare e valutare i livelli di sicurezza e affidabilità dei prodotti e servizi TIC messi sul mercato digitale. "La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati (…), al fine di garantire l'opportuno livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e migliorare il funzionamento del mercato interno[44]". Lo scopo di questa seconda parte del regolamento è quello di fare in modo che i diritti digitali dei cittadini vegano tutelati, ma allo stesso tempo è anche quello di aumentare i livelli di fiducia dei consumatori nei confronti dei produttori e fornitori europei di servizi di digitali, i quali si ritrovano ad operare all'interno di un Mercato Unico Digitale fondato sulla trasparenza e sulla controllabilità.

Sulla base della Strategia per l'Unione della sicurezza 2020-2025[45], dell'agenda strategica del Consiglio europeo per il periodo 2019-2024[46] e della strategia digitale definita dalla Commissione Europa e intitolata "Un'Europa pronta per l'era digitale[47]", la stessa Commissione ha presentato, lo scorso dicembre 2020, una nuova strategia sulla cibersicurezza[48], al fine di attuare "tre strumenti principali – normativi, di investimento e politici – per tre settori di intervento dell'UE: 1) resilienza, sovranità tecnologica e leadership, 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta e 3) promozione di un ciberspazio globale e aperto[49]". La nuova strategia in materia di cibersicurezza è nata dalla volontà di migliorare la qualità del processo di digitalizzazione

[43] Art. 46 del *Cybersecurity Act*.
[44] Art. 56.3 del *Cybersecurity Act*.
[45] Commissione Europea. (2020). *La strategia dell'UE per l'Unione della sicurezza 2020-2025*, COM (2020) 605 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[46] Una nuova agenda strategica 2019–2024. (2019). [Comunicato stampa]. https://www.consilium.europa.eu/it/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/ (Ultimo accesso 9 aprile 2021).
[47] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_it (Ultimo accesso 9 aprile 2021).
[48] Commissione Europea. (2020). *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN (2020) 18 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[49] *Ibidem*, pag. 5.

europeo, il quale richiede un livello di sicurezza, di difesa e di affidabilità ancor più elevato rispetto a qualche decennio fa.

Con l'approdo in Europa della trasformazione digitale l'illegalità e i crimini informatici sono cresciuti considerevolmente, e di conseguenza anche l'attenzione alla *cybersecurity* da parte delle istituzioni europee e degli Stati Membri. Al fine di garantire una tutela adeguata dei diritti digitali dei cittadini e delle imprese europee, la Commissione Europea ha presentato, in aggiunta alla nuova strategia europea in materia di sicurezza informatica, due nuove proposte legislative: la legge sui servizi digitali (*Digital Service Act*)[50] e la legge sui mercati digitali (*Digital Market Act*)[51]. L'obiettivo di questo nuovo pacchetto normativo è quello di modificare la natura dei mercati digitali e delle piattaforme *online* fornitrici di servizi digitali, attraverso un controllo più approfondito, sia a livello comunitario che nazionale, degli obblighi stabiliti dall'Unione Europea nei loro confronti, e tramite la totale eliminazione delle irregolarità e delle pratiche sleali *online*. Nonostante il pacchetto di legge non sia ancora stato approvato, esso rappresenta un ulteriore passo avanti nella definizione della legislazione *cyber* europea, la quale continua a trasformarsi e migliorarsi nell'interesse generale dell'intera comunità.

1.2 LA COMUNITÀ *CYBER*

Oltre alla figura dell'Agenzia dell'Unione Europea per la cybersecurity (ENISA)[52] vi sono diversi altri organi attivi nell'ambito della sicurezza informatica. Elevati livelli di cooperazione, sia a livello unionale, sia a livello internazionale sono essenziali per il raggiungimento di una comunità *cyber* efficiente.

1.2.1 La cooperazione interna

La cooperazione interna all'UE in materia di cibersicurezza è svolta principalmente da tre agenzie: il Centro europeo per la lotta alla criminalità informatica (*European Cybercrime*

[50] Commissione Europea. (2020). *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, COM (2020) 825 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[51] Commissione Europea. (2020). *Proposta di regolamento del parlamento europeo e del consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*, COM (2020) 842 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[52] Per approfondimenti cfr. Paragrafo 1.1.2.

Centre – EC3), il *Computer Emergency Response Team* per le istituzioni europee (CERT-UE) e l'Unità di cooperazione giudiziaria dell'Unione Europea (*European Union Agency for Criminal Justice Cooperation – Eurojust*).

Il Centro Europeo per la lotta al *cybercrime* è nato nel 2013 da una proposta della Commissione Europea. Esso è parte integrante dell'Ufficio europeo di polizia (Europol) e funge da "punto di riferimento europeo per le informazioni sulla criminalità informatica[53]. L'EC3 si occupa di sostenere gli Stati Membri nell'indagine e nella lotta contro i crimini informatici. Le informazioni recepite dal centro europeo vengono immediatamente inviate alle autorità nazionali competenti, affinché esse possano agire in tempo contro qualsiasi minaccia o attacco *online*. Oltre a collaborare con gli Stati Membri, l'EC3 interagisce con il settore privato, la comunità dei ricercatori e le organizzazioni della società civile[54], attraverso uno scambio di informazioni utile per mantenere elevati i livelli di sicurezza informatica.

L'EC3 lavora congiuntamente ad ENISA e al CERT-UE. Quest'ultimo è stato istituito nel 2012 ed è composto da un insieme di esperti delle istituzioni europee, incaricati di rispondere in modo efficace al *cybercrime*. Il CERT-UE svolge un lavoro di monitoraggio, prevenzione e risposta agli attacchi informatici, in collaborazione con i CERTs e CSIRTs[55] presenti sul territorio di ogni Stato Membro. "*The incident support and coordination activities include evaluating available information, validating and verifying it, gathering additional evidence if required, communicating with relevant parties, and finally proposing solutions in order to resolve the incident*"[56].

Un altro importante attore coinvolto nella sensibilizzazione e diffusione delle giuste pratiche di sicurezza informatica è Eurojust, istituito nel 2002 e rafforzato nel 2009. Si tratta di un organismo composto da esperti giudiziari nazionali, i quali si occupano di affrontare e combattere crimini transnazionali di ogni tipo, compresi i crimini informatici. Anche nel caso di Eurojust, la collaborazione con gli Stati Membri e le altre entità europee è fondamentale, in particolare nelle attività di investigazione. Nel 2019, Eurojust ed

[53] Commissione Europea. (2012). *Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica*, COM (2012) 140 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.
[54] *Ibidem*, pag. 8.
[55] Per approfondimenti cfr. Paragrafo 1.1.2.
[56] RFC 2350 CERT-EU, versione 5.1, settembre 2019.

Europol/EC3 hanno presentato un documento congiunto relativo alle attuali sfide e sviluppi della lotta al cybercrime[57]. Le aree di identificazione di queste nuove sfide sono cinque:

1. Perdita di dati;
2. Perdita di localizzazione;
3. Sfide legate ai quadri giuridici nazionali;
4. Ostacoli alla cooperazione internazionale;
5. Sfide dei partenariati pubblico-privato[58].

Il documento considera gli scenari evolutivi possibili nel riguardo del *cybercrime* e sottolinea la necessità di accrescere il livello di specializzazione delle entità coinvolte nella lotta ai crimini informatici, in particolare per quanto riguarda le pratiche di *law enforcement* e di "investigazione, prosecuzione, protezione e prevenzione del *cybercrime*[59]".

1.2.2 La cooperazione internazionale

La gestione della *cybersecurity* e del ciberspazio richiede una cooperazione non solo interna all'Unione, ma anche esterna, con paesi terzi, organizzazioni internazionali e organizzazioni regionali. Affinché si possano raggiungere gli obiettivi di sicurezza dello spazio informatico e di resilienza informatica, che sono alcuni dei pilastri della nuova strategia europea sulla cybersecurity, è necessario un dialogo multilaterale, fondato sui principi della *cyberdiplomacy*. Attualmente, la cooperazione internazionale in ambito *cyber* è gestita congiuntamente dalla Commissione Europa, dagli Stati Membri e dal SEAE (Servizio Europeo per l'Azione Esterna), i quali collaborano maggiormente con le Nazioni Unite (Onu), la NATO e l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE)[60].

Nel quadro della collaborazione con le Nazioni Unite è importante il ruolo dell'Unione internazionale delle telecomunicazioni (ITU), la quale è coinvolta in numerose

[57] https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime. (Ultimo accesso 10 aprile 2021).
[58] Eurojust e Europol. (2019). *Common challenges in combating cybercrime, as identified by Eurojust and Europol*, joint report Europol and Eurojust Public Information.
[59] *Ibidem*, pag. 4. Citazione tradotta dall'inglese.
[60] European Commission. (2017). *EU cybersecurity initiatives working towards a more secure online environment – Factsheet*. https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment. (Ultimo accesso 10 aprile 2021).

attività di cooperazione e supporto degli Stati nell'elaborazione delle loro politiche sulla cibersicurezza. L'ITU si è dedicata all'elaborazione del *Global Cybersecurity Index* (GCI), un'iniziativa che misura l'impegno degli Stati e delle regioni del mondo rivolto alla cibersicurezza[61]. L'indice calcola il livello di benessere informatico dei singoli paesi, sulla base di cinque pilastri della *Global Cybersecurity Agenda*[62], ovvero il quadro normativo su cui si fonda lo stesso GCI. I pilastri presi in considerazione sono: misure legali, misure tecniche, misure organizzative, *capacity building* e cooperazione[63].

In ambito di difesa cibernetica, invece, è importante la cooperazione UE-NATO. L'obiettivo stabilito all'interno della strategia europea è quello di sviluppare una "visione e strategia militari dell'UE sul ciberspazio come dominio operativo per le missioni e le operazioni militari della PSDC[64]", la cui realizzazione necessita una *partnership* tra l'Unione e la NATO. Fino ad ora, la collaborazione è avvenuta principalmente attraverso lo scambio di informazioni e la partecipazione ad esercitazioni congiunte (Barbieri, 2020), i quali hanno permesso un miglioramento della risposta internazionale alle minacce ibride[65].

Nonostante la cooperazione internazionale in materia di sicurezza informatica sia un pilastro dell'agenda politico-economica dell'Unione Europa, essa non deve sostituire l'attuale quadro europeo, bensì deve limitarsi ad affiancarlo ed integrarlo (Barbieri, 2020).

---

[61] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. (Ultimo accesso 13 aprile 2021).

[62] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. (Ultimo accesso 13 aprile 2021).

[63] Trimintzios, P., et al. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU*. EPRS/STOA/SER/16/214N. https://doi:10.2861/853031.

[64] Commissione Europea. (2020). *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN (2020) 18 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

[65] Council of the EU. (2018). Joint *declaration on EU-NATO cooperation by President of the European Council Donald Tusk, President of the European Commission Jean-Claude Juncker, and Secretary General of NATO Jens Stoltenberg*. https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/. (Ultimo accesso 13 aprile 2021).

CAPITOLO 2
ECONOMIA EUROPEA E *CYBERSECURITY*

2.1 I FINANZIAMENTI PER LE POLITICHE EUROPEE DI SICUREZZA INFORMATICA

La spesa nel settore della cibersicurezza è frammentata a livello mondiale. Nel periodo 2017-2021, il costo delle *policies* nell'ambito della sicurezza informatica è aumentato considerevolmente, soprattutto a seguito della diffusione del virus COVID-19. La pandemia, che ha costretto famiglie e aziende in tutto il mondo a lavorare da casa, ha causato un aumento delle minacce e degli attacchi informatici, con la conseguenza di aver compromesso i diritti digitali fondamentali dell'intera popolazione globale. La spesa per la *cybersecurity* è dunque passata da circa 34 miliardi di dollari a ben 60 miliardi di dollari in soli quattro anni (Figura 2).

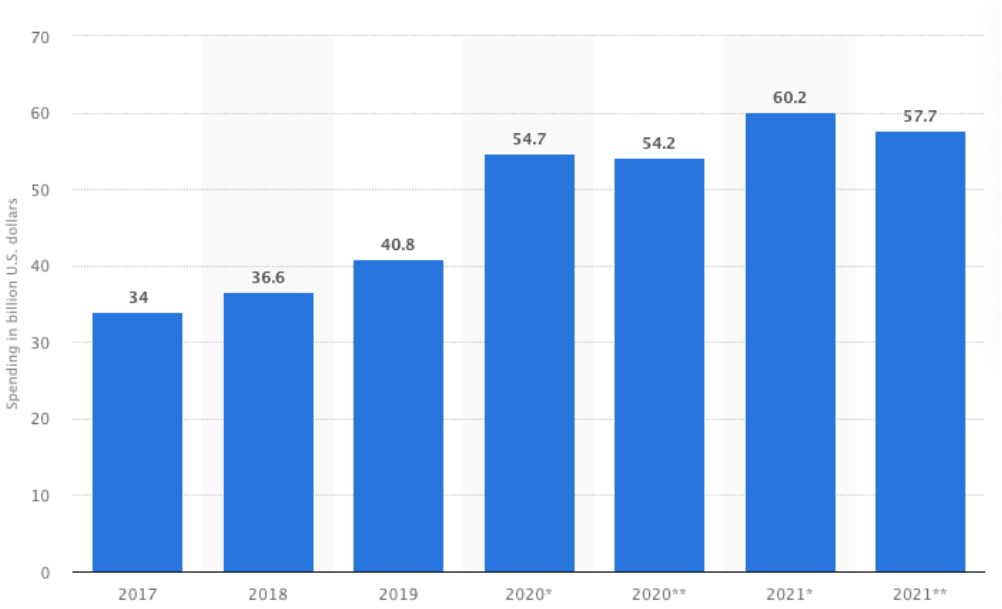

Figura 2: Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted) (in billion U.S. dollars).

Fonte: Statista, https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

A livello dell'Unione Europea il calcolo esatto della spesa annuale per la cibersicurezza è ostacolato da una serie di fattori. L'assenza di statistiche esaustive, dovuta alla trasversalità della stessa *cybersecurity* e alla difficoltà nel distinguere la spesa per la

sicurezza informatica dalla spesa per il settore informatico in generale[66], provoca un peggioramento della capacità delle istituzioni europee di calcolare i costi della sicurezza informatica, e di conseguenza un aggravamento del sistema economico digitale europeo.

2.1.1 Orizzonte 2020, cPPP e Orizzonte Europa

La spesa per la sicurezza informatica nell'ambito dell'Unione Europea ha cominciato ad accrescere a partire dal 2014, con l'elaborazione del programma "Orizzonte 2020" (H2020), ovvero il programma quadro dell'Unione Europea per la ricerca e l'innovazione relativo al periodo 2014-2020. Il programma è composto da un budget di 80 miliardi di euro, il quale è rivolto a specifici destinatari promotori di progetti nell'ambito delle priorità definite dal programma stesso.

Il settore della ricerca e dell'innovazione (R&I) è un elemento chiave della crescita economica e produttiva dell'Unione Europea. A partire da uno studio svolto dalla Direzione Generale per la Ricerca e l'Innovazione della Commissione Europea, è stato rilevato che circa i due terzi della crescita economica in Europa dal 1995 al 2007 è derivato dal settore R&I, in particolare dagli investimenti positivi effettuati dalle aziende proprio in questo ambito (Direzione Generale per la Ricerca e l'Innovazione, 2017). L'ottenimento dei fondi di Orizzonte 2020 per progetti relativi alla sicurezza informatica è regolato all'interno di due sezioni specifiche del programma, denominate "Società sicure - proteggere la libertà e la sicurezza dell'Europa e dei suoi cittadini" e "Leadership nelle tecnologie di supporto e industriali", dotate rispettivamente di 1,695 miliardi di euro e 13,557 miliardi di euro (di cui almeno 3 miliardi destinati alle PMI) di finanziamenti. La Corte dei Conti europea ha affermato che i propri auditori "hanno individuato 279 progetti appaltati in materia di cibersicurezza fino a settembre 2018, per un finanziamento UE complessivo di 786 milioni di euro[67]". Nell'ambito della ricerca e dell'innovazione, su cui ruota tutto il programma Orizzonte 2020, si inserisce dunque lo sviluppo delle tecnologie necessarie per garantire elevati livelli di sicurezza informatica e una giusta protezione dei diritti digitali dei cittadini europei. Nei primi mesi del 2020, la Commissione Europea ha annunciato di voler

[66] Corte dei Conti Europea. (2019). *Analisi n. 02/2019: Le sfide insite in un'efficace politica dell'UE in materia di cybersicurezza (Documento di riflessione)*, pag. 24. https://www.eca.europa.eu/it/Pages/DocItem.aspx?did=49416 (Ultimo accesso 15 aprile 2021).
[67] *Ivi*, pag. 26.

impegnare circa 41 milioni di euro, tramite Orizzonte 2020, per supportare nove progetti volti a valorizzare il settore della cibersicurezza[68].

Il contributo di Orizzonte 2020 allo sviluppo di progetti e politiche innovativi di sicurezza informatica si è rafforzato nel 2016, con la creazione di un partenariato pubblico-privato contrattuale (*contractual Public-Private Partnership* – cPPP) tra la Commissione Europea e la *European Cyber Security Organization* (ECSO). L'obiettivo di questo partenariato è quello di "promuovere la cooperazione tra attori pubblici e privati nelle prime fasi del processo di ricerca e innovazione, al fine di consentire ai cittadini europei di accedere a soluzioni europee innovative e affidabili (prodotti, servizi e software TIC)[69]", e di rafforzare l'industria europea della sicurezza informatica. Grazie a questa partnership, il contributo dell'UE tramite Horizon 2020 è aumentato da 200 a 450 milioni di euro[70] (Figura 3).

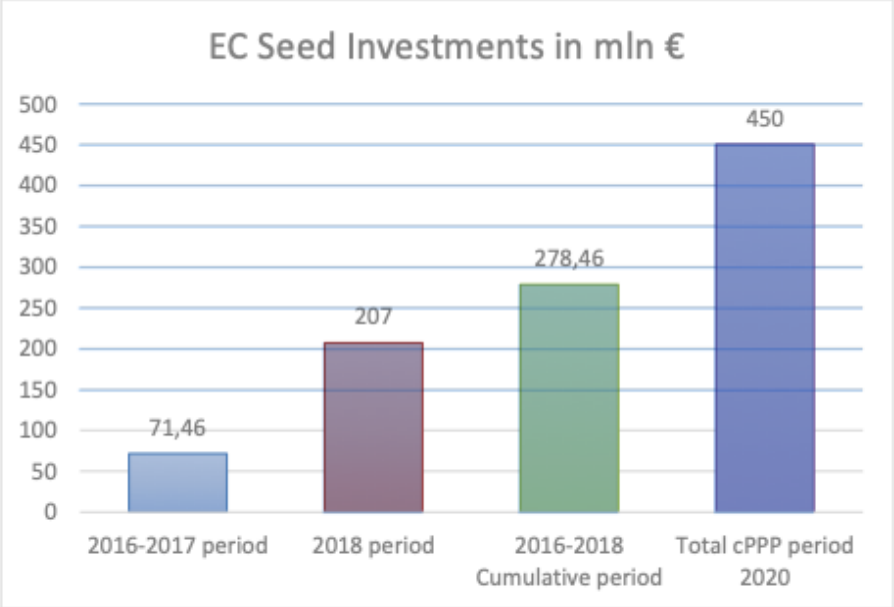

Figura 3: European Commission Investments in mln €.

Fonte: ECS, ECS cPPP Progress Monitoring Report 2018, 22 ottobre 2019, https://www.ecs-org.eu/documents/uploads/cppp-progress-monitoring-report-2018.pdf.

[68] https://digital-strategy.ec.europa.eu/en/node/925/printable/pdf.
[69] https://ecs-org.eu/cppp.
[70] ECS. (2016). *European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP)*, pag. 17. https://www.ecs-org.eu/documents/uploads/sria.pdf. (Ultimo accesso 16 aprile 2021).

Il lavoro intrapreso dall'Unione Europa nel campo della ricerca e dell'innovazione per il periodo 2014-2020 continuerà anche nel periodo 2021-2017, in vista dell'elaborazione di un nuovo programma quadro Orizzonte Europa. Questo nuovo programma di ricerca e innovazione, ancora in fase di approvazione da parte del Parlamento europeo e del Consiglio, disporrà di una dotazione maggiore del 30% rispetto al programma Orizzonte 2020, passando quindi da un budget di 80 miliardi di euro ad uno di 95,5 miliardi di euro (Commissione Europea, 2020). La struttura del programma Orizzonte Europa è composta da tre pilastri fondamentali:

1. Eccellenza scientifica;
2. Sfide globali e competitività industriale europea;
3. Europa innovativa.

Il tema della cibersicurezza è affrontato all'interno del pilastro "Sfide globali e competitività industriale europea" ed è stato inserito nel polo tematico definito "Sicurezza civile per la società". Garantire la sicurezza dei cittadini e in generale del contesto europeo è sinonimo di garantire un elevato livello di sicurezza informatica, data la crescente possibilità di accesso dei cittadini europei, su tutto il territorio dell'Unione, ai servizi e prodotti digitali. Con Orizzonte Europa l'UE vuole puntare a sviluppare l'industria europea della sicurezza informatica, a rafforzare le infrastrutture digitali coinvolte nella lotta ai crimini cibernetici e a difendere l'integrità del Mercato Unico Digitale. Al fine di proteggere i dati e le attività dei cittadini, delle pubbliche autorità e delle aziende, i «principi fondamentali della "*security-by-design*[71]" e della "*privacy-by-design*" saranno implementati nelle tecnologie digitali e nelle loro applicazioni, come il 5G, l'industria 4.0, l'intelligenza artificiale, l'*Internet of Things*, la *blockchain*, le tecnologie quantistiche, i dispositivi mobili e mobilità ed energia connesse, cooperative ed autonome[72]». Per il secondo pilastro la Commissione Europea ha avanzato una proposta di budget di circa 53 miliardi di euro, da

[71] "Le aziende e le organizzazioni sono incoraggiate a mettere in atto misure tecniche e organizzative, fin dalle prime fasi della progettazione delle operazioni di trattamento, in modo da salvaguardare fin dall'inizio i principi di tutela della vita privata e di protezione dei dati personali («protezione dei dati fin dalla progettazione»)". https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_it (Ultimo accesso 16 aprile 2021).

[72] Directorate-General for Research and Innovation (European Commission). (2021). *Horizon Europe Strategic Plan 2021-2024*. Luxembourg: Publications Office of the European Union, pp. 59-60.

ripartire nei poli tematici previsti. Del totale del budget, circa 1,6 miliardi di euro spetteranno al polo "Sicurezza civile per la società" e di conseguenza alla *cybersecurity*[73].

2.1.2 Altre spese per la cybersecurity nell'UE

Nel periodo 2014-2020 l'Unione Europea ha investito nell'ambito della sicurezza informatica, non solo attraverso il programma Orizzonte 2020, ma anche attraverso il "Meccanismo per collegare l'Europa" (*Connecting Europe Facility* – CEF). Si tratta di uno strumento finanziario di 33 miliardi di euro, volto a stimolare gli investimenti sia pubblici che privati nei settori dell'energia, dei trasporti e delle telecomunicazioni. Al settore delle telecomunicazioni, all'interno del quale si inseriscono anche gli investimenti per la cibersicurezza, sono stati previsti circa 1,05 miliardi di euro, rivolti al sostegno di progetti europei di sviluppo dei servizi di connettività e delle infrastrutture digitali[74]. Dal 2014 al 2020 sono stati messi a disposizione circa 85 milioni di euro per finanziare progetti nel campo della cibersicurezza ("CEF Telecom - *Innovation And Networks Executive Agency - European Commission*" 2021), come conseguenza dell'elevato interesse da parte delle istituzioni europee per il progresso in questo settore, il quale è strettamente collegato alla crescita economica dell'Unione stessa. Il Meccanismo per collegare l'Europa sarà funzionante anche a partire dal 2021 e fino al 2027, con una dotazione complessiva pari a 33,71 miliardi di euro. Il budget proposto per il settore della connettività digitale ammonta a 2,06 miliardi di euro e "per poter beneficiare del sostegno a titolo dell'MCE 2.0, i progetti dovranno contribuire al mercato unico digitale e agli obiettivi dell'UE in materia di connettività[75]".

A sostegno del programma Orizzonte Europa e del Meccanismo per collegare l'Europa, l'UE ha predisposto un altro strumento finanziario, il programma Europa Digitale (*Digital Europe*), inserito all'interno del bilancio a lungo termine dell'Unione Europea (Quadro Finanziario Pluriennale – QFP) per il periodo 2021-2027. Tra i poli tematici che

[73] Agenzia per la Promozione della Ricerca Europea (APRE): https://www.versohorizoneurope.it/articoli/95-miliardi-horizon-europe/.
[74] *Meccanismo Per Collegare L'Europa*. (2021). Il Sole 24 ORE. https://st.ilsole24ore.com/art/osservatorio-finanziamenti-ue/2014-02-21/meccanismo-collegare-europa-113016.shtml?uuid=ABPMO9x (Ultimo accesso 16 aprile 2021).
[75] Consiglio dell'UE. (2021). *Meccanismo Per Collegare L'Europa: Accordo Informale Con Il Parlamento Europeo Sul Programma Dopo Il 2020*. [Comunicato stampa]. https://www.consilium.europa.eu/it/press/press-releases/2021/03/11/connecting-europe-facility-informal-agreement-with-european-parliament-on-the-post-2020-programme/ (Ultimo accesso 17 aprile 2021).

riceveranno i finanziamenti del programma Europa Digitale si inserisce quello della cibersicurezza, al quale verranno erogati circa 1,6 miliardi di euro[76]. Le PMI saranno le beneficiarie prioritarie dei fondi *Digital Europe* per la *cybersecurity*, in quanto si tratta di una delle categorie maggiormente colpite da attacchi cibernetici, soprattutto a partire dalla pandemia di COVID-19. Europa Digitale mira ad implementare il *framework* legislativo europeo sulla cibersicurezza, in particolare la *Cybersecurity Strategy* e la Direttiva NIS, focalizzandosi sul ruolo e sulle capacità degli Stati Membri nello sviluppo dei livelli adeguati di sicurezza digitale. Il programma, ancora in fase di approvazione, "sarà attuato attraverso programmi di lavoro pluriennali che copriranno uno o più dei cinque ambiti d'intervento. È previsto il cofinanziamento con gli Stati membri e, se necessario, con il settore privato. Il tasso di cofinanziamento sarà stabilito nei programmi di lavoro che definiranno anche i criteri di ammissibilità per le azioni nell'ambito del programma Europa digitale. Le sovvenzioni nell'ambito del programma potranno coprire fino al 100 % dei costi ammissibili[77]".

I Fondi strutturali e di investimento europei (Fondi SIE) rappresentano un'altra importante fonte di finanziamento per gli investimenti nel settore *cyber*, in particolare in ambito regionale. Per il periodo 2014-2020 è stata prevista una dotazione massima di 400 milioni di euro, da gestire in maniera concorrente, ovvero sia a livello dell'Unione, con la Commissione Europea come punto di riferimento, sia a livello degli Stati Membri, con la partecipazione attiva delle specifiche autorità nazionali e regionali competenti, incaricate di presentare alla Commissione Europea i progetti di investimento[78].

[76] Il budget totale del programma Europa Digitale ammonta a 7 588 miliardi di euro (a prezzi correnti).
[77] Consiglio dell'UE. (2021). *Programma Europa Digitale – Accordo Informale Con Il Parlamento Europeo*. [Comunicato stampa]. https://www.consilium.europa.eu/it/press/press-releases/2020/12/14/digital-europe-programme-informal-agreement-with-european-parliament/. (Ultimo accesso 17 aprile 2021).
[78] Agenzia per l'Italia Digitale. (2020). *Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali*, pag. 106. https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/modelli-di-finanziamento.html (Ultimo accesso 17 aprile 2021).

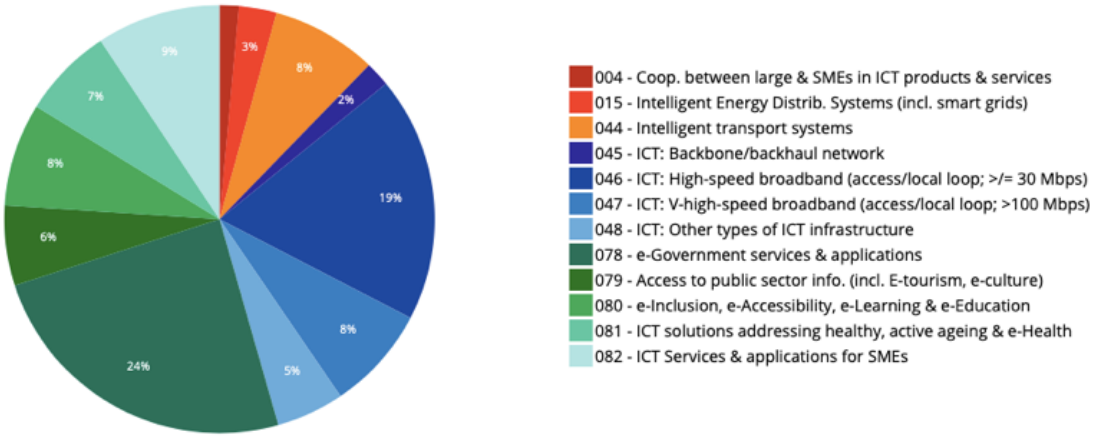

Figura 4: Planned ERDF Digital Investment 2014-2020.

Fonte: Cohesion Data

Nonostante la cibersicurezza sia stata inserita tra gli ambiti previsti per i Fondi SIE, questi ultimi si sono concentrati maggiormente su altri tipi di investimenti digitali, in particolare sulle soluzioni e sui servizi TIC per le PMI europee, ma anche sui servizi di *e-Government*, *e-Inclusion* e *e-Accessibility*. La sicurezza informatica è stata integrata nella categoria di intervento denominata "Servizi e applicazioni di *e-Government*", la più grande fra i campi di intervento dei fondi (Figura 4).

La crisi generata dalla pandemia di COVID-19 ha costretto l'Unione Europea ad allocare ulteriori risorse finanziare a sostegno della digitalizzazione e della cibersicurezza, dato l'aumento del numero di utenti *online* e di conseguenza degli attacchi informatici. Gli investimenti aggiuntivi per il settore della sicurezza informatica verranno finanziati in parte attraverso lo strumento temporaneo per la ripresa dell'Europa dopo la crisi pandemica, definito "*NextGenerationEU"*, il quale ammonta a 750 miliardi di euro. Al fine di affrontare al meglio la ripresa economica europea, questo strumento temporaneo si unisce al bilancio a lungo termine dell'UE, raggiungendo un importo totale di 1 824,3 miliardi di euro, i quali verranno ripartiti in sette rubriche diverse. Per la rubrica "Mercato unico, innovazione e agenda digitale", al cui interno si inserisce anche la spesa per la sicurezza informatica, *NextGenerationEU* prevede un contributo totale di 10,6 miliardi di euro[79]. Circa il 90% dello strumento finanziario temporaneo è coperto dal dispositivo per la ripresa e la resilienza

[79] *Piano per la ripresa dell'Europa*. (2020). Commissione europea - European Commission. https://ec.europa.eu/info/strategy/recovery-plan-europe_it#un-pacchetto-di-stimolo-senza-precedenti (Ultimo accesso 17 aprile 2021).

(672,5 miliardi di euro), un piano composto da prestiti e sovvenzioni, volto a finanziare le riforme e i programmi illustrati dagli Stati Membri all'interno dei propri piani nazionali di ripresa e resilienza. In base alle linee guida definite dalla Commissione Europea, i settori in cui gli Stati Membri dovranno intervenire, utilizzando le risorse fornite dallo stesso dispositivo europeo, sono sei, tra cui anche il settore della trasformazione digitale[80]. "Il fondo dovrà essere di entità adeguata, mirato ai settori e alle aree geografiche dell'Europa maggiormente colpiti e destinato a far fronte a questa crisi senza precedenti" (Michel, 2020).

2.2 LA *CYBERSECURITY* E IL SETTORE FINANZIARIO EUROPEO

Il settore finanziario è uno degli ambiti più coinvolti nel processo di digitalizzazione. "*The financial sector is the largest user of information and communications technology (ICT) in the world, accounting for about a fifth of all ICT expenditure*[81]". L'utilizzo dei servizi digitali, dell'intelligenza artificiale o della crittografia espone il settore finanziario al rischio di minacce ed attacchi cibernetici, rendendo indispensabile la costruzione di un elevato livello di sicurezza informatica, da garantire attraverso un quadro normativo di prevenzione e protezione ben definito. "*Whether we talk about online banking or insurance services, mobile payment applications, digital trading platforms […], financial services delivered today rely on digital technologies and data*[82]".

2.2.1 Le principali iniziative cyber europee per il settore finanziario

Le iniziative *cyber* europee per il settore finanziario sono particolarmente complesse e frammentate, a causa dell'esistenza di un'ampia varietà di istituzioni finanziarie e a causa dei differenti quadri normativi e di sorveglianza in cui le stesse ricadono[83]. Di fronte all'avanzamento della digitalizzazione, l'Unione Europea si è impegnata a completare il quadro normativo europeo in ambito *cyber*, attraverso la creazione di un *framework*

[80] *Un piano per la ripresa dell'Europa*. (2021). European Council. https://www.consilium.europa.eu/it/policies/eu-recovery-plan/ (Ultimo accesso 17 aprile 2021).
[81] European Commission (2019). *Consultation Document - Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*, pag. 3.
[82] *Ibidem*.
[83] Brauchle, J. and Krüger, P. S. (2021*) The European Union, Cybersecurity, and the Financial Sector: A Primer*. Cyber Policy Initiative Working Paper Series "Cybersecurity and the Financial System" No. 9, pp, 8-9. https://carnegieendowment.org/files/Krueger_Brauchle_Cybersecurity_legislation.pdf (Ultimo accesso 18 aprile 2021).

legislativo specifico per l'ambito finanziario, definito come un settore critico assieme a quello energetico e a quello sanitario[84].

La Commissione Europea ha assunto un ruolo chiave nello sviluppo di tale strategia normativa. Nel 2018 ha presentato il *FinTech Action Plan*[85], il piano d'azione per le tecnologie finanziarie, con lo scopo di aumentare il livello di sicurezza dei nuovi prodotti *fintech*, i quali hanno rivoluzionato la modalità d'azione del settore finanziario, ma allo stesso tempo lo hanno esposto a rischi connessi alla sicurezza informatica. "Aumentare la resilienza del settore finanziario nei confronti degli attacchi informatici è di fondamentale importanza per garantirne una protezione adeguata, per fare in modo che i servizi finanziari siano forniti in modo efficace e ordinato in tutta l'UE e per preservare la fiducia dei consumatori e degli operatori del mercato[86]". Secondo la Commissione, un'adeguata ciberresilienza nel settore finanziario può essere garantita attraverso la cooperazione tra gli istituti finanziari che fanno uso delle nuove tecnologie *fintech*, e in particolare attraverso lo scambio di informazioni sugli eventuali attacchi cibernetici e tramite un coordinamento di prevenzione e di risposta agli attacchi.

Nel 2020 la Commissione Europea ha presentato una nuova strategia europea in materia di finanza digitale[87], con lo scopo di migliorare la finanza digitale sulla base del quadro strategico europeo già consolidato. Ad esempio, sulla base della normativa relativa al nuovo Mercato Unico Digitale, l'Unione Europea dovrà impegnarsi ad impedirne la frammentazione, avviando un processo di digitalizzazione anche per le imprese finanziarie europee. La nuova strategia punta inoltre alla realizzazione di una "finanza aperta", all'interno della quale è possibile la "condivisione e l'uso dei dati, con il consenso del cliente, da parte di banche e fornitori terzi per creare nuovi servizi[88]". Il raggiungimento degli obiettivi prefissati all'interno della strategia europea per lo sviluppo della finanza digitale è fondamentale per la crescita economica dell'Unione Europea.

Nel contesto europeo esistono diversi attori coinvolti nella garanzia della stabilità finanziaria. Si tratta di agenzie e autorità indipendenti che si occupano di vigilare e

---

[84] *Ivi*, pag. 7.
[85] Commissione Europea. (2018). *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, COM (2018) 109 final. Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.
[86] *Ibidem*, pag. 3.
[87] Commissione Europea. (2020). *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE*, COM (2020) 591 final. Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.
[88] *Ibidem*, pag. 16.

supportare gli istituti finanziari, in particolare nel settore bancario e nel settore delle assicurazioni. Il lavoro di vigilanza di tali agenzie si è esteso nel tempo anche al campo TIC e a quello della gestione dei rischi di sicurezza, come conseguenza dell'aumento degli incidenti e degli attacchi cibernetici connessi a questi stessi settori, di cui gli istituti finanziari sono fortemente interdipendenti. Al centro di questo complesso sistema di controllo vi è il Sistema europeo di vigilanza finanziaria (SEVIF), che si occupa di verificare che gli istituti finanziari applichino correttamente le norme che compongono il quadro europeo di regolamentazione e vigilanza, volto "a promuovere la stabilità finanziaria e a proteggere gli utilizzatori dei servizi finanziari[89]". Il SEVIF è composto al suo interno dall'Autorità europea degli strumenti finanziari e dei mercati (ESMA), dall'Agenzia Bancaria Europea (ABE), dall'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA), e infine dal Comitato europeo per il rischio sistemico (CERS).

Negli ultimi anni, l'ABE e l'EIOPA hanno assunto un ruolo chiave nello sviluppo e nell'implementazione della *policy* europea in materia *cyber*. L'Agenzia Bancaria Europea fornisce linee guida, raccomandazioni e pareri agli istituti bancari e finanziari su temi relativi all'utilizzo delle nuove tecnologie digitali e al miglioramento della ciberresilienza. Innanzitutto, l'ABE partecipa alla creazione del *Single Rulebook*[90], un sistema di norme prudenziali armonizzate, di cui è richiesta la piena attuazione da parte degli Stati Membri. Lo scopo di questo *set* di regole è quello di fare in modo che gli effetti negativi di eventuali crisi finanziarie non si diffondano su tutto il territorio dell'Unione, data l'elevata interconnessione tra le diverse economie nazionali, ma vengano gestiti congiuntamente dagli Stati Membri attraverso un elevato livello di cooperazione. Il *Single Rulebook* è inteso a proteggere il settore bancario europeo da qualsiasi tipo di minaccia e a trasformarlo in un settore più resiliente, trasparente ed efficiente[91].

Per quanto riguarda i pareri e le raccomandazioni fornite dall'ABE, nel 2017 l'autorità ha pubblicato delle linee guida sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2)[92]. La direttiva europea PSD2 sui servizi di pagamento nasce con lo scopo di trasformare il mercato

[89] Parenti, R. (2020). Sistema europeo di vigilanza finanziaria (SEVIF). Parlamento Europeo, pag. 1. https://www.europarl.europa.eu/ftu/pdf/it/FTU_2.6.14.pdf (Ultimo accesso 20 aprile 2021).
[90] *The Single Rulebook*. (2021). European Banking Authority. https://www.eba.europa.eu/regulation-and-policy/single-rulebook (Ultimo accesso 20 aprile 2021).
[91] *Ibidem*.
[92] European Banking Authority (2017). *Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2*. EBA/GL/2017/17.

dei pagamenti, in particolare di quelli elettronici, in una piattaforma sicura e regolamentata. "*PSD2 provides that payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide*[93]". Sulla base della direttiva PSD2, l'ABE e la Banca Centrale Europea (BCE) devono indicare ai fornitori dei servizi di pagamento le modalità da seguire per prevenire e rispondere ad eventuali incidenti operativi e di sicurezza, inclusi quelli cibernetici, a seguito dell'emissione dei servizi (*online*) di pagamento sul mercato europeo.

Nel 2019 l'ABE ha pubblicato ulteriori linee guida rivolte agli istituti finanziari, questa volta sulla gestione dei rischi legati alle TIC e alla sicurezza[94]. Affinché si possa garantire un livello sufficiente di armonizzazione all'interno del Mercato Unico Digitale europeo, gli istituti finanziari devono rispettare le regole stabilite per la protezione dagli incidenti cibernetici e devono stabilire una *governance* interna efficiente ed un piano strategico per prepararsi ad un'eventuale gestione di rischi legati alla sicurezza informatica.

Sulla base della strategia europea per la cibersicurezza, del *FinTech Action Plan* e della strategia per il Mercato Unico Digitale, l'EIOPA ha pubblicato una strategia sul *cyber underwriting*[95], ovvero la gestione dei rischi della finanza digitale. Tale strategia è essenziale per lo sviluppo del mercato europeo delle assicurazioni informatiche e per migliorare la risposta agli attacchi *cyber*. L'obiettivo di EIOPA è quello di proteggere i consumatori e di promuovere la formazione degli istituti finanziari alle sane pratiche di gestione del rischio e di *cyber underwriting.*

2.2.2 L'impatto del cybercrime sull'economia mondiale e dell'Unione Europea

Oltre ad essere responsabile della crescita di gran parte delle economie mondiali, il processo di digitalizzazione è accompagnato da un aumento costante del *cybercrime*, i cui costi di prevenzione e di risposta provocano un impatto economico anche in quei paesi dotati di un'efficacie strategia per la cibersicurezza. Secondo l'ultimo *report* effettuato nel 2018 dall'azienda *McAfee*, in collaborazione con il *Center of Strategic and International Studies*

[93] *Ibidem*, pag. 4.
[94] European Banking Authority (2019). *Final report on guidelines on ICT and security risk management*, EBA/GL/2019/04.
[95] EIOPA (2020). *EIOPA strategy on cyber underwriting*. doi: 10.2854/793935.

(CSIS)[96], il *cybercrime* avrebbe un costo globale di circa 600 miliardi di dollari, che corrisponde allo 0,8% del PIL mondiale. Nel 2014, il costo degli attacchi informatici ammontava a circa 100 miliardi di dollari in meno rispetto al 2018, e secondo il *report* diverse sono le cause legate a questo aumento (CSIS, McAfee; 2018):

- Rapida adozione di nuove tecnologie da parte dei criminali informatici;
- L'aumento del numero di nuovi utenti *online* (provenienti da paesi a basso reddito e con scarsa sicurezza informatica);
- La maggiore facilità di commettere reati informatici;
- Un numero crescente di "centri" di criminalità informatica, ora anche in Brasile, India, Corea del Nord e Vietnam;
- Una crescente sofisticazione finanziaria tra i criminali informatici di alto livello, che rende più facile per loro la monetizzazione (CSIS, McAfee; 2018).

Dallo studio è emerso che nel 2017, l'Europa ha speso tra i 160 e i 180 miliardi di dollari, registrando una perdita di circa 0,8% del proprio PIL. Le regioni con i paesi più ricchi sono quelle che hanno registrato un impatto economico degli attacchi informatici maggiore, dato l'elevato livello di digitalizzazione e data la possibilità per i criminali informatici di avere accesso ad aziende e individui economicamente avvantaggiati.

Il *report* sottolinea anche le difficoltà riscontrate nel calcolo del costo economico del *cybercrime*. Innanzitutto, la rilevazione degli attacchi informatici da parte delle istituzioni governative è poco accurata e spesso erronea, e per questo motivo molti paesi stanno puntando al perfezionamento del coordinamento e dello scambio di informazioni tra istituzioni politiche e agenzie private. In secondo luogo, le stime sui costi sono generiche, ovvero non specificano i costi rivolti ai singoli individui o alle singole aziende all'interno di un paese, generando ulteriori problemi di valutazione. Nonostante i dati sugli attacchi informatici siano scarsi, diversi studi sono riusciti a quantificare i costi della criminalità informatica, che diverse aziende nel mondo devono affrontare. Secondo una ricerca condotta dal *Ponemon Institute*, l'impatto economico del *cybercrime* sulle aziende varia in base alla grandezza dell'azienda stessa e al tipo di attacco informatico (*malware, phishing,*

[96] CSIS, McAfee. (2018). *Economic Impact of Cybercrime - No Slowing Down*. https://www.mcafee.com/enterprise/en-us/forms/gated-form-thanks.html?docID=5fee1c652573999d75e4388122bf72f5&tag=ec&eid=18TL_ECGLQ1_CT_WW#form-download (Ultimo accesso 21 aprile 2021).

cryprocurrency theft, identity theft, ecc…), ed esso colpisce la maggior parte dei settori dell'industria. Il settore finanziario subisce un impatto del *cybercrime* maggiore rispetto ad altri settori, come quello dei servizi o quello sanitario[97].

All'interno del settore finanziario, le banche rappresentano le vittime maggiori di attacchi informatici. Nel 2020, la presidente della BCE Christine Lagarde ha dichiarato che vi è una possibile correlazione fra gli attacchi informatici rivolti alle banche europee e lo scoppio di una nuova crisi di liquidità all'interno dell'Unione Europea (Paganini, 2020). Prevenire tale sconvolgimento e aumentare la resilienza informatica del settore finanziario sono due degli obiettivi principali prefissati dalla BCE in ambito *cyber*. Un primo passo intrapreso dalla BCE in questa direzione è avvenuto nel 2018, con il lancio di un piano comune transnazionale per l'esecuzione di test di resilienza del settore finanziario agli attacchi informatici (*European framework for testing financial sector resilience to cyber attacks* – TIBER-EU). TIBER-EU "*is the first EU-wide guide on how authorities, financial entities, threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyberattack*[98]". All'interno del contesto della BCE, il Comitato di ciberresilienza dell'euro per le infrastrutture finanziarie paneuropee (*Euro Cyber Resilience Board for pan-European Financial Infrastructures* - ECRB) ha presentato la "*Cyber Information and Intelligence Sharing Initiative*", con lo scopo di aiutare gli istituti finanziari nella lotta e nella prevenzione agli attacchi informatici, puntando sulla cooperazione fra strutture finanziarie paneuropee, le banche centrali nazionali, l'ENISA, l'Europol e i fornitori di servizi critici[99].

Al di fuori del contesto dell'Unione Europea, il Forum Economico Mondiale (*World Economic Forum* – WEF) ha introdotto il concetto di "maturità cibernetica" degli istituti finanziari, per indicare il loro livello di efficacia nella prevenzione e nella risposta al *cybercrime*, fornendo allo stesso tempo delle indicazioni su come potenziarla:

- Riconoscere la *cybersecurity* come una priorità strategica;
- Combinare diversi approcci per migliorare la ciberresilienza;

[97] Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global*, pag. 4.
[98] ENISA. (2021). *EU cybersecurity initiatives in the finance sector*, pag. 7. https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector (Ultimo accesso 20 aprile 2021).
[99] https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html

- Insegnare le regole di "*cyber-hygiene*[100]";
- Migliorare le competenze dei proprio esperti;
- Introdurre metodi aggiuntivi di protezione;
- Affidare problemi di cibersicurezza a compagnie esperte[101].

Tra le iniziative *cyber* internazionali volte a ridurre l'impatto economico degli attacchi informatici sul settore finanziario vi sono quelle presentate dal *Financial Services Information Sharing and Analysis Center* (FS-ISAC)[102], il quale punta ad un miglioramento del coordinamento internazionale fra le agenzie coinvolte nello sviluppo della sicurezza informatica mondiale. A livello europeo, il lavoro di condivisione delle informazioni e di protezione del settore finanziario dalla criminalità informatica è svolto dall'*European Financial Institutes – Information Sharing and Analysis Centre* (FI- SAC)[103], un istituto indipendente supportato dall'ENISA, che organizza il proprio lavoro basandolo sulla cooperazione con i CERTs nazionali, le banche centrali, in particolare la BCE, e le forze di polizia.

La riduzione degli effetti negativi del *cybercrime* sull'economia europea richiede un'attenzione non solo al settore finanziario, ma anche al settore privato, e in particolare alle piccole-medie imprese (PMI), le quali rappresentano circa il 99,8% del totale delle imprese europee[104]. Da uno studio svolto per conto del Comitato economico e sociale europeo è emerso che, nonostante le PMI siano la fonte principale dell'innovazione e della modernizzazione europea, esse sono le imprese meno preparate alla lotta agli attacchi informatici nello scenario privato dell'Unione Europea, e di conseguenza ricadono tra le vittime principali del *cybercrime*. Le ragioni legate a questa mancanza di preparazione sono molteplici. Innanzitutto, le PMI non posseggono la "maturità cibernetica", ovvero non sono consapevoli della minaccia rappresentata dall'aumento del *cybercrime*. In secondo luogo, esse ricevono un supporto finanziario minore da parte delle entità europee rispetto alle grandi

[100] Con il termine "*cyber-hygiene*" si intende una serie di principi da seguire quotidianamente per minimizzare i rischi derivanti dall'utilizzo di sistemi informatici.
[101] Samartsev, D. (2020). *Cybercrime is maturing. Here's how organizations can keep up*. World Economic Forum. https://www.weforum.org/agenda/2020/11/how-to-protect-companies-from-cybercrime/ (Utlimo accesso 20 aprile 2021).
[102] https://www.fsisac.com.
[103] https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership.
[104] Bhattacharyya, K., Frinking, E., Kertysova, K., Maričić, A., van den Dool, K. (2018). *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, pp. 8-9. European Economic and Social Committee (EESC): "Visits and Publications" Unit. doi:10.2864/98090.

imprese multinazionali, e di conseguenza il costo da affrontare per la sicurezza informatica è maggiore e più difficile da gestire[105]. Per questo motivo, un miglioramento dell'allocazione delle risorse finanziarie per la sicurezza informatica da parte delle istituzioni europee è necessario per migliorare lo stato di salute delle PMI, così come è importante potenziare la cooperazione con gli istituti nazionali di accertamento e di risposta agli attacchi informatici, al fine di sviluppare il *capacity building* delle PMI in ambito di sicurezza informatica.

La salvaguardia dell'economia europea richiede un nuovo approccio strategico, ed in particolare le imprese europee "*must start preparing for an Internet that may be far less business- friendly, with more sovereign borders and more disruptive attacks*[106]".

[105] *Ivi,* pp. 67-70.
[106] Atltantic Council. (2015). *Risk Nexus - Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, pag. 32.

CAPITOLO 3
IL CASO DELL'ESTONIA

3.1 L'ATTACCO INFORMATICO DEL 2007

La definizione del percorso strategico intrapreso dall'Unione Europea in materia di sicurezza informatica non è stata semplicemente frutto di un attento lavoro decisionale e legislativo svolto dai vertici della stessa UE, ma è stata possibile grazie all'esperienza diretta di uno degli Stati Membri più piccoli della comunità europea: l'Estonia. Il crollo dell'Unione Sovietica e il conseguente distacco dalla Russia hanno permesso all'Estonia di poter acquisire un certo grado di indipendenza, anche se "*the only way for Estonia to balance Russian influence has been through collective security arrangements*[107]".

A partire dall'ingresso nella NATO e nell'Unione Europea, l'Estonia ha portato avanti numerose politiche di sviluppo e di gestione delle nuove tecnologie dell'informazione e della comunicazione, divenendo uno tra i paesi europei più all'avanguardia nel campo della digitalizzazione, ma allo stesso tempo esponendosi sempre di più a possibili attacchi informatici, che all'epoca non erano ancora avvertiti come una minaccia e per cui ancora non esistevano efficaci misure di prevenzione e di risposta. L'evento che ha stravolto completamente le necessità di sicurezza informatica dell'Estonia e dell'intera Unione Europea, e che ha spinto verso la creazione di un nuovo quadro strategico di cibersicurezza, è rappresentato dal primo caso di attacco cibernetico di carattere politico-economico, organizzato dalla Russia e diretto contro l'Estonia, espletatosi il 27 aprile 2007 e durato circa tre settimane. L'attacco russo è stato provocato a seguito della decisione del governo estone di rimuovere un monumento commemorativo sovietico situato a Tallin e risalente alla Seconda Guerra Mondiale. Questo provvedimento avrebbe causato lo scoppio di una serie di rivolte da parte della minoranza etnica russa presente in Estonia, e di conseguenza l'inizio di una vera e propria *cyber* guerra, il cui fondamento politico ed economico si è rivelato, tuttavia, ben più profondo. Vittime di questi crimini cibernetici sono state le istituzioni politiche estoni, ma anche le banche, i giornali e le televisioni (Dragosei, 2007), che hanno assistito ad un blocco totale dei propri servizi *online*. Le misure intraprese dal governo estone per rispondere agli attacchi informatici sono state caratterizzate da un coinvolgimento diretto

[107] Kohler, Kevin. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture*, pag. 4. Doi: 10.3929/ethz-b000438276.

delle autorità competenti nazionali, in particolare i CERTs estoni, i quali sono stati affiancati dai CERTs di altri paesi limitrofi, dalle agenzie interne alla NATO incaricate di gestire la criminalità informatica, dall'ENISA, ma anche da organizzazioni private esperte nell'ambito informatico[108].

A partire dall'attacco del 2007, l'Estonia ha rinnovato il proprio settore nazionale della sicurezza informatica, divenendo un punto di riferimento per la lotta al *cybercrime* e per lo sviluppo di politiche di cibersicurezza e ciberdifesa, sia in Europa che nel resto del mondo. "*The attacks have stuck in the national consciousness by proving to Estonians the importance of cyber security*[109]". Un primo passo verso la definizione di una strategia nazionale per la sicurezza informatica è avvenuto con la creazione dell'*Estonia Defence League's Cyber Unit* (EDL CU), un'organizzazione nazionale volontaria nata per migliorare la qualità della difesa cibernetica estone. Dal punto di vista della cooperazione internazionale *cyber*, nel 2008 Tallin si è trasformata nel cuore della lotta al *cybercrime* portata avanti dalla NATO, divenendo sede ufficiale del *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), il Centro di Eccellenza della NATO per la Difesa Cibernetica. Si tratta di un istituto di ricerca e di formazione, che funge da supporto ai propri Stati Membri e alla NATO nella realizzazione di un piano strategico nell'ambito della difesa cibernetica. Il CCDCOE organizza conferenze internazionali incentrate sulla ricerca nell'ambito dei conflitti cibernetici, le "CyCon", con l'obiettivo di riunire esperti di tecnologia, di economia e di politica in grado di guidare un dibattito e di trovare nuove soluzioni a potenziali attacchi informatici. A partire dal 2010, il centro *cyber* della NATO gestisce ogni anno i *Locked Shields*, le più grandi esercitazioni mondiali di ciberdifesa, al fine di preparare gli Stati ad una gestione efficace dei propri sistemi e programmi di sicurezza informatica di fronte ad incidenti *cyber* artificiali.

L'attacco cibernetico del 2007, che ha segnato l'inizio di una nuova epoca per la ricerca e l'implementazione delle politiche estoni di cibersicurezza, ha provocato un impatto economico di lieve portata alla nazione baltica. Le informazioni relative agli effetti economici dell'attacco informatico sono scarse e difficilmente reperibili, sia a causa dell'assenza di un monitoraggio adeguato dei sistemi Internet da parte delle istituzioni governative estoni, sia per la carenza di segnalazioni da parte delle agenzie incaricate di

[108] Herzog, Stephen (2011). *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. Journal of Strategic Security 4, no. 2: pp. 49-60.
[109] Mcguinness, Damien (2017). *How A Cyber Attack Transformed Estonia*. BBC News. https://www.bbc.com/news/39655415 (Ultimo accesso 3 maggio 2021).

gestire gli attacchi[110]. Gli attacchi rivolti contro l'Estonia sono stati di tipo *Distributed Denial of Service* (DDoS). Attacchi di questo genere, anche se di grande portata, hanno un impatto limitato sull'economia nazionale del paese interessato[111], proprio come è avvenuto nel caso dell'Estonia, che ha saputo gestire l'aggressione senza subire effetti economici estesi ed a lungo termine. Per meglio comprendere questo passaggio, è sufficiente analizzare l'andamento di crescita del Prodotto Interno Lordo (PIL) dell'Estonia, nel periodo compreso tra il 2000 e il 2019 (Figura 5).

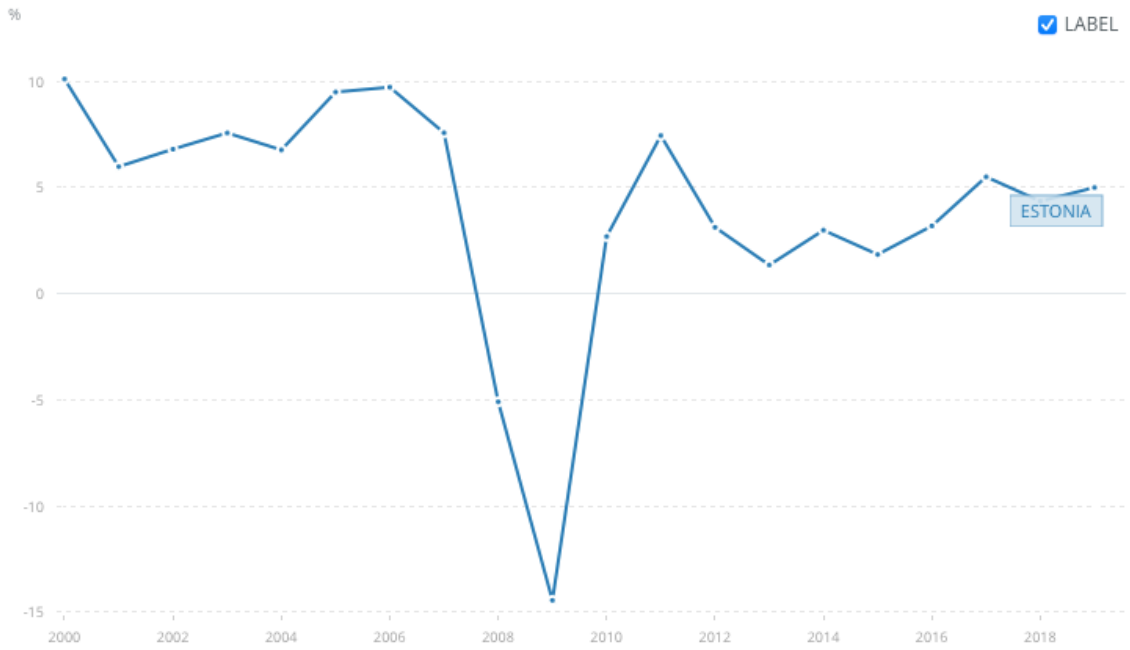

Figura 5: Crescita percentuale del PIL 2000-2019, Estonia.

Fonte: World Bank Data.

Il grafico illustra un lieve calo della crescita del PIL nel 2007, a dimostrazione del fatto che l'attacco subito non ha provocato un impatto significativo sull'economia nazionale estone. Il vertiginoso calo verificatosi tra il 2008 e il 2009 non mostra segni di correlazione

[110] Schmidt, Andreas. (2013). *The Estonian Cyberattacks*, pag. 14. Capitolo preparato per il libro "The fierce domain – conflicts in cyberspace 1986-2012", modificato da Jason Healey, Washington, D.C.: Atlantic Council, 2013.

[111] Center for Strategic and International Studies. (2013). *The Economic Impact of Cybercrime And Cyber Espionage*, pag. 10. McAfee. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf (Ultimo accesso 4 maggio 2021).

con le conseguenze del *cyber-attack*, ma può essere ricondotto allo scoppio della crisi finanziaria, che ha colpito in modo negativo tutti i paesi membri dell'Unione Europea.

3.2 LA STRATEGIA NAZIONALE ESTONE PER LA *CYBERSECURITY*: PRIMA E DOPO L'ATTACCO DEL 2007

3.2.1 E-Estonia: punti di forza e sfide future

A partire dall'indipendenza dalla Russia, ottenuta nel 1991, l'Estonia ha dato inizio ad un processo di ammodernamento della politica, dell'economia e della cultura, puntando su riforme ed approcci innovativi incentrati sullo sviluppo tecnologico e sulla digitalizzazione, divenendo una tra le prime società digitali avanzate al mondo. L'obiettivo principale, che è stato raggiunto con successo dal governo estone, è quello della totale digitalizzazione dei servizi statali, un processo basato su principi di sicurezza, efficienza e trasparenza. Diversi sono stati gli svolgimenti che hanno portato alla nascita di una vera e propria "E-Estonia": la creazione del primo servizio di *e-banking* nel 1996; l'istituzione dell'identificazione digitale nazionale nel 2022; l'introduzione del servizio di *e-voting* nel 2005; e infine, lo sviluppo di una nuova strategia nell'ambito della sicurezza informatica e della tecnologia *blockchain*, al fine di prevenire e combattere tutte le forme di minaccia informatica, compresa quella di manipolazione dei dati nazionali[112].

Nell'ambito della sicurezza informatica, lo sviluppo di un piano strategico digitale è iniziato ufficialmente solo dopo l'attacco informatico subito nel 2007. Prima di quell'anno, le minacce informatiche non rientravano tra le priorità del governo estone per quanto riguarda la politica di creazione di una nuova economia digitale, e solo a seguito dell'offensiva russa l'Estonia ha cominciato ad aprire gli occhi sul tema della *cybersecurity* e sull'importanza di sviluppare una strategia adeguata di difesa cibernetica. La Strategia Nazionale di Sicurezza Informatica dell'Estonia[113], presentata nel 2008 dal Ministero estone della Difesa, rappresenta una delle prime strategie nazionali in ambito di sicurezza informatica, e di conseguenza un modello di riferimento per la nascita delle strategie di altri paesi, in particolare dei paesi membri UE, i quali ancora oggi si ispirano al modello di economia digitale sviluppato dall'Estonia. "*The 2008 Cyber Security Strategy was Estonia's*

[112] https://e-estonia.com.
[113] Cybersecurity Strategy Committee. (2008). *Cybersecurity Strategy*. Tallin: Ministry of Defence.

first national strategy document that recognized the interdisciplinary nature of cybersecurity and the need for coordinated action in the area. It was also one of the first horizontal cybersecurity strategies in the world – it was only after the 2007 cyberattacks against Estonia that cybersecurity began to be perceived as an essential part of national security[114]".

La strategia *cyber* estone, rinnovata per i periodi 2014-2017 e 2019-2022, è stata creata con lo scopo di promuovere la sicurezza digitale dei propri cittadini e in linea con la legislazione europea in materia. Il piano strategico punta al rafforzamento della società digitale estone e dell'economia nazionale, ed è caratterizzato da un approccio multidimensionale, che richiede una cooperazione intersettoriale mirata[115]. Il programma si basa su quattro principi fondamentali:

1. La protezione e la promozione dei diritti e delle libertà fondamentali nel ciberspazio;
2. Il sostenimento della crescita socioeconomica dell'Estonia, attraverso misure innovative nel campo dello sviluppo digitale;
3. La promozione delle nuove tecniche di crittografia;
4. L'adesione ad una forma di comunicazione trasparente e aperta[116].

Il corretto funzionamento dell'economia estone nel contesto del Mercato Unico europeo è possibile a partire dalla promozione di misure adeguate di sicurezza informatica. Il Ministero degli Affari Economici e delle Comunicazioni dell'Estonia collabora attivamente con il *Cyber Security Council*, uno dei rami operativi del governo estone, con lo scopo di promuovere la strategia estone per la cibersicurezza.

La "*Digital Agenda 2020 for Estonia*[117]" dedica gran parte del programma alla sicurezza informatica, con un budget totale di 4,2 milioni di euro per il periodo 2019-2020[118]. L'agenda prevede quattro sotto-obiettivi:

1. La costruzione di una società digitale sostenibile attraverso la promozione di un'efficace ciberresilienza e di sistemi di prevenzione e gestione delle crisi informatiche;

[114] Republic of Estonia. Ministry of Economic Affairs and Communication. (2019). *Cybersecurity Strategy Republic of Estonia*, pag. 7.
[115] *Ivi*, pag. 8.
[116] *Ivi*, pag. 10.
[117] Government of the Republic of Estonia. (2018). *Digital Agenda 2020 for Estonia*.
[118] Ivi, p. 20.

2. L'implementazione delle attività di ricerca e innovazione nel campo della sicurezza informatica;
3. Il rafforzamento del ruolo internazionale dell'Estonia in ambito cyber, sia dal punto di vista della cooperazione strategica, che della *cyber-capability* nei paesi partner;
4. Lo sviluppo di attività di sensibilizzazione e di formazione alla difesa cibernetica, rivolte in particolare ai giovani[119].

La strategia *cyber* dell'Estonia è caratterizzata da elementi particolarmente innovativi ed offre delle soluzioni adeguate ed efficaci per lo sviluppo di una comunità informatica all'avanguardia. Nonostante i numerosi punti di forza nel campo della sicurezza informatica, l'Estonia non è ancora completamente immune alla cibercriminalità e deve affrontare una serie di sfide, al fine di garantire un livello di sicurezza digitale proporzionato alle esigenze della crescente comunità *cyber* estone[120]. La prima sfida riguarda la mancanza di personale specializzato nel settore della cibersicurezza, all'interno sia del settore pubblico che di quello privato, alla quale si affianca anche la scarsa formazione di nuovi esperti presenti nel mercato del lavoro della sicurezza informatica. La seconda sfida concerne la difficoltà delle istituzioni politico-economiche di comprendere l'importanza delle minacce e degli attacchi informatici ed in particolare la loro influenza negativa sui mercati e in generale sul benessere sociale dei cittadini, i quali rimangono indifferenti alla garanzia di una corretta *cybersecurity* e non la percepiscono come una responsabilità individuale[121]. Un altro problema è rappresentato dall'insufficiente collaborazione tra gli istituti di ricerca e le agenzie governative estoni, la quale crea problemi alla crescita economica del paese e rappresenta una barriera per le imprese nazionali che hanno appena intrapreso un percorso di innovazione nel settore della sicurezza informatica[122]. Infine, l'Estonia deve mostrarsi in grado di poter mantenere la reputazione che si è guadagnata negli anni sul campo internazionale, destinando un'ingente quantità di risorse finanziarie alla transizione digitale[123].

[119] *Ibidem*.
[120] Republic of Estonia. Ministry of Economic Affairs and Communication (2019*). Cybersecurity Strategy Republic of Estonia*, pag. 26.
[121] *Ivi*, pag. 27.
[122] *Ivi*, pag. 28.
[123] *Ibidem*.

3.2.2 Analisi statistiche rilevanti

Per meglio comprendere la capacità strategica dell'Estonia nel portare avanti politiche efficaci di digitalizzazione e di cibersicurezza è necessario analizzare alcuni dati statistici. Il *National Cybersecurity Index* (NCSI) è un indice globale con la quale viene misurata la capacità dei singoli Stati di sviluppare delle *policies* e dei programmi nazionali di prevenzione e lotta agli attacchi informatici[124]. A partire da una serie di indicatori, il NSCI si concentra su una serie di elementi quantificabili in materia di sicurezza informatica, realizzati dai governi centrali[125]. L'Estonia, con un punteggio di 90.91 su 100[126], si posiziona al terzo posto nella classifica mondiale, dimostrando nuovamente il proprio ruolo da *leader* nel processo di transizione verso una società digitale più sicura.

Il monitoraggio dello sviluppo del Mercato Unico Digitale europeo avviene attraverso la raccolta e la valutazione di numerosi dati relativi all'esperienza dei cittadini e delle imprese europee durante l'utilizzo di Internet e delle nuove tecnologie di informazione e comunicazione. In Estonia circa il 90% della popolazione fa uso di Internet[127] e diverse fonti hanno dimostrato elevati livelli di sicurezza informatica durante la navigazione *online*. Nel 2010, circa il 40% degli utenti estoni ha riscontrato problemi di sicurezza via Internet, rappresentando il 20% in più rispetto alla media europea (Figura 6). Nell'arco di quasi dieci anni, il dato estone è calato gradualmente, e nel 2019 solo circa il 3% degli utenti sia europei che estoni ha vissuto esperienze negative *online*. Il grafico evidenza, inoltre, una previsione dell'andamento futuro dei dati: entrambe le linee di tendenza rilevano uno sviluppo decrescente dei dati, mentre, fino al 2022, il profilo dell'Estonia sembrerebbe migliorare rispetto alla media europea.

[124] https://ncsi.ega.ee/methodology/.
[125] *Ibidem.*
[126] https://ncsi.ega.ee/ncsi-index/?order=-ncsi.
[127] https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2019&locations=EE&start=2019&view=bar.

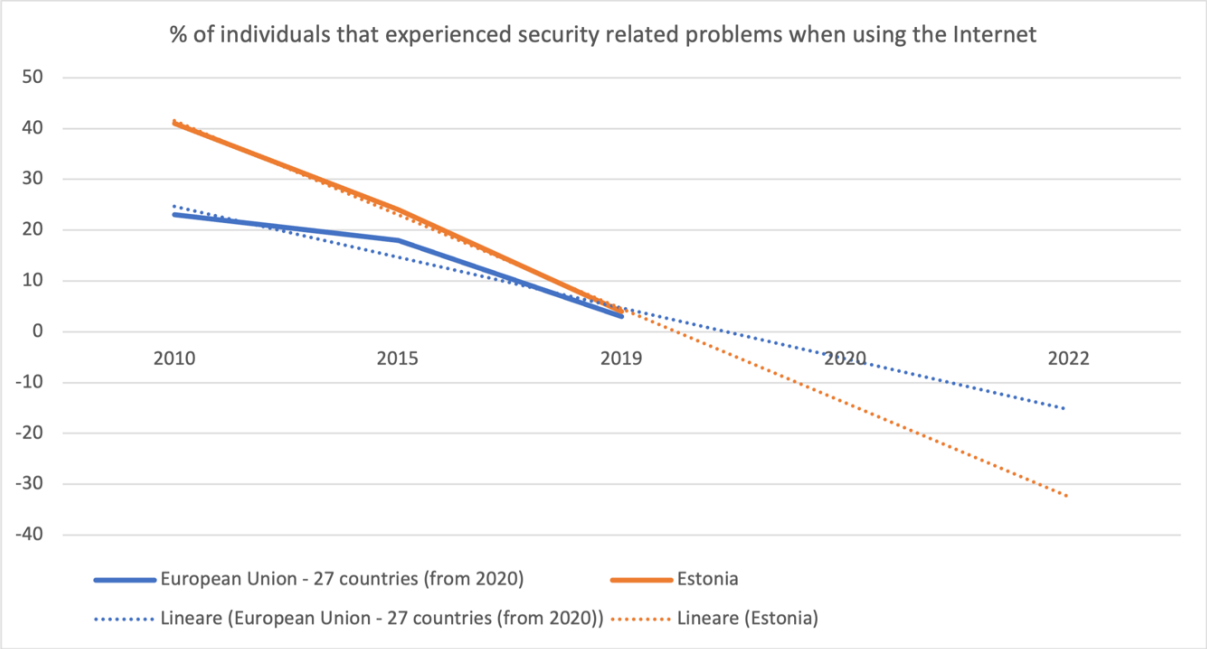

Figura 6: % degli utenti che ha riscontrato problemi di sicurezza *online*.

Fonte: Eurostat, dati rielaborati dall'autrice.

https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb$DV_538/default/line?lang=en.

Un altro importante dato è relativo alla percentuale di utenti estoni, di età compresa tra i 16 e i 74 anni, che tra il 2010 e il 2015 hanno subito "perdite finanziarie durante la navigazione *online*, causate dall'uso fraudolento della carta di pagamento oppure dalla ricezione di messaggi fraudolenti (*'phishing'*) o dal reindirizzamento forzato a siti falsi che richiedono informazioni personali (*'pharming'*)[128]" (Figura 7). Nuovamente, i dati rilevano l'elevato progresso effettuato dall'Estonia nel campo della sicurezza informatica e della *privacy*. A differenza dell'Unione Europea nel suo insieme, che ha registrato un aumento della percentuale di individui colpiti da attacchi informatici, l'Estonia è stata in grado di gestire con attenzione la prevenzione di tali incidenti finanziari, garantendo ai propri utenti un livello di protezione cibernetica maggiore.

[128] https://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-countries#chart={"indicator-group":"security-privacy","indicator":"i_secfl","breakdown":"ind_total","unit-measure":"pc_ind_ilt12","ref-area":["EE","EU"]}.

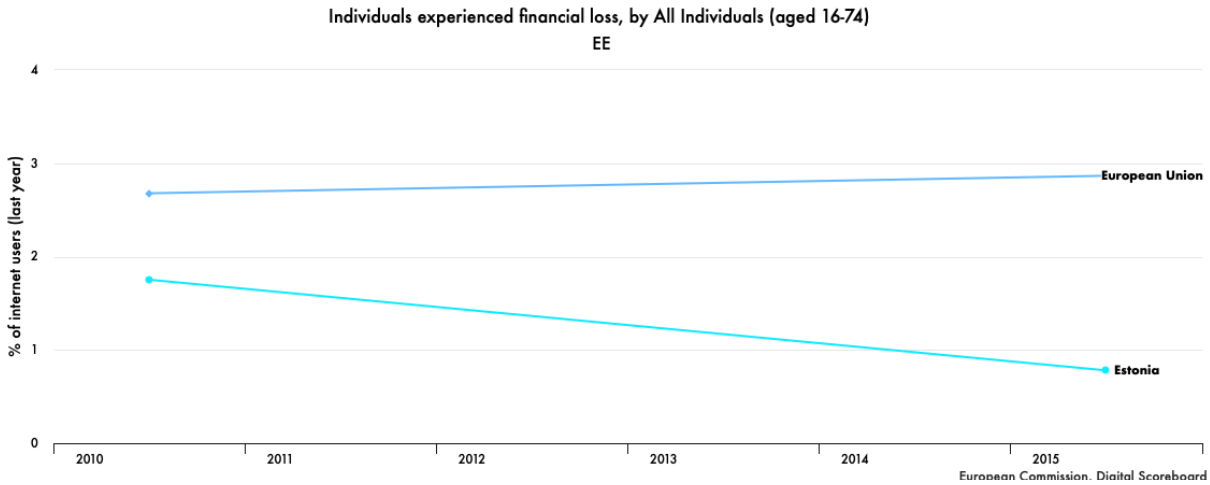

Figura 7: % di individui che hanno subito perdite finanziarie (16-74 anni).

Fonte: Commissione Europea.

A partire dal 2014, Commissione Europea ha predisposto il *Digital Economy and Society Index* (DESI), al fine di monitorare lo sviluppo e la competitività nel settore digitale dei singoli Stati Membri[129]. L'indice prende in considerazione cinque differenti dimensioni della società e dell'economia digitale europea: la connettività, il capitale umano, l'uso di servizi di Internet, l'integrazione della tecnologia digitale e i servizi pubblici digitali[130]. Sulla base degli indicatori individuati per ciascuna dimensione, è possibile ricavare un profilo valutativo per ciascun paese e di conseguenza una classifica europea. Nel 2020, l'Estonia ha ottenuto un punteggio DESI di 61.1, posizionandosi al settimo posto su 28 paesi membri, ed un punteggio di 89.3 nel settore dei servizi pubblici digitali, all'interno del quale vengono inserite anche le spese per la *cybersecurity*, posizionandosi al primo posto in tutta l'Unione Europea[131] (Figura 8).

[129] https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi?etrans=it.
[130] *Ibidem*.
[131] European Commission. (2020). *Digital Economy and Society Index (DESI) 2020. Estonia*.

	Estonia		EU
	rank	score	score
DESI 2020	**7**	**61.1**	**52.6**
DESI 2019	5	58.3	49.4
DESI 2018	5	55.7	46.5

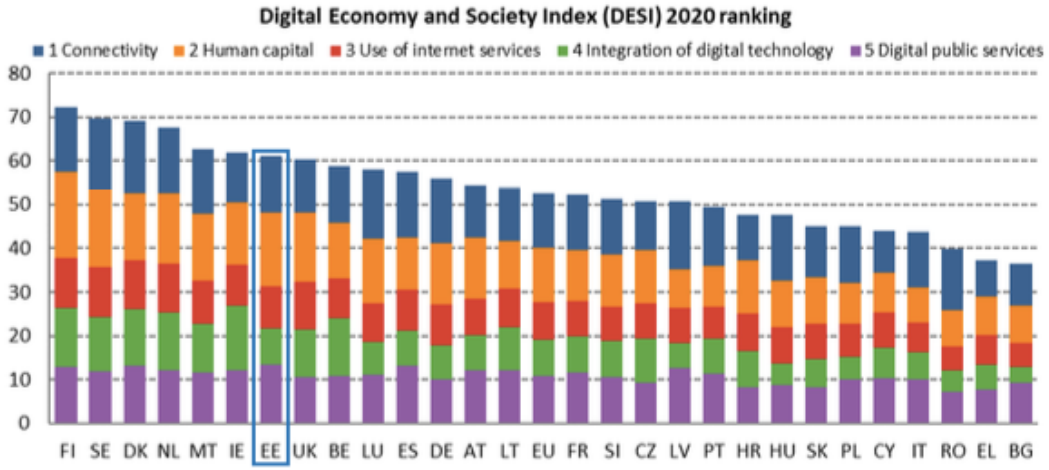

Figura 8: Indice DESI, classifica 2020.

Fonte: European Commission, *Digital Economy and Society Index (DESI) 2020. Estonia*, 2020.

Nel'attuale contesto della pandemia da COVID-19, la connettività, la sicurezza informatica, l'intelligenza artificiale e la digitalizzazione sono diventati settori prioritari, al fine di proteggere la salute economica mondiale[132]. "*Digital will also play a key role in the economic recovery as the European Council and the Commission have undertaken to frame the support to the recovery along the twin transition to a climate neutral and resilient digital transformation*[133]". L'Estonia, grazie all'elevato grado di organizzazione e di gestione dei servizi digitali nazionali e grazie agli sforzi messi in atto nel campo della cibersicurezza, ha saputo affrontare la crisi pandemica al meglio, ponendosi al di sopra della media europea nel processo di transizione digitale e risentendo di meno degli effetti negativi della pandemia.

[132] *Ibidem*.
[133] *Ibidem*.

CONCLUSIONI

Il presente elaborato si è posto l'obiettivo di analizzare il contesto normativo ed economico dell'Unione Europea, al fine di dimostrare la validità del settore della sicurezza informatica come strumento di crescita economica. Le ricerche e gli studi effettuati hanno innanzitutto rilevato una correlazione tra gli strumenti di digitalizzazione ed il funzionamento dell'economia europea. L'espansione dei processi digitali innovativi all'interno dell'Unione Europea ha permesso lo sviluppo sia del tessuto industriale che di quello finanziario, i quali rappresentano due degli ambiti più rilevanti, e allo stesso tempo più vulnerabili, del sistema economico europeo.

Con la nascita e l'espansione del *Single Digital Market*, resa possibile dalla crescente possibilità di accesso dei cittadini europei ai servizi informatici, le economie digitali dei singoli paesi membri dell'Unione hanno raggiunto un grado di interconnessione elevato, richiedendo di conseguenza un costante aggiornamento del quadro normativo europeo in campo digitale, e soprattutto in ambito *cyber*. La protezione dei dati e dei diritti digitali dei cittadini dell'UE, esercitata sulla base di un *framework* legislativo affidabile ed efficacie, è necessaria affinché possa essere garantito l'esercizio delle singole attività economiche presenti sul territorio comunitario e, più in generale, del mercato interno europeo. Questa analisi ha difatti rilevato come la riduzione delle conseguenze negative dei crimini informatici, attraverso la creazione di un approccio strategico che punti sul perfezionamento e sull'incremento degli investimenti nella *cybersecurity*, sia indispensabile per il sostentamento di tutte quelle strutture fondamentali del sistema economico dell'UE, in particolare le banche e le piccole-medie imprese. Il sistema di finanziamento messo in piedi dalle istituzioni europee con lo scopo di sostenere lo sviluppo del settore della sicurezza informatica è particolarmente articolato e in fase di espansione. Gli strumenti finanziari e i progetti di investimento previsti posseggono una notevole capacità economica, rilevando la volontà dell'Unione Europea di elevare il settore *cyber* a strumento di ripresa e crescita economica, soprattutto nel contesto dell'attuale crisi pandemica.

Sulla base dell'analisi delle diverse strategie europee di transizione digitale, l'elaborato ha messo in luce i meccanismi interni al Mercato Unico Digitale europeo in grado di garantire la stabilità finanziaria dell'UE, evidenziando l'importanza strategica della sicurezza informatica. Per evitare futuri danni al sistema economico le istituzioni europee, ed in particolare la Commissione Europea, si sono concentrate sulla creazione di un piano

strategico digitale che prevedesse tra le azioni prioritarie una protezione adeguata del settore finanziario dai crescenti attacchi informatici. Nel contesto europeo, molti istituti finanziari e bancari, ma anche un numero ingente di attori privati, si sono ritrovati vittime di perdite finanziarie durante la navigazione *online*, rilevando la necessità di sviluppare una finanza digitale più sicura e dotata di una *governance* più efficiente. Focalizzandosi sull'impatto della criminalità informatica sul sistema economico mondiale, il presente studio ha evidenziato che l'aumento costante dei costi del *cybercrime*, correlato al processo di digitalizzazione, ha provocato e continuerà a provocare danni economici di elevata portata nell'Unione Europea e nel resto del mondo. Nonostante sia stato rilevato un aumento della spesa per la sicurezza informatica, soprattutto a seguito della diffusione della pandemia da Covid-19, è stato dimostrato come a livello europeo vi siano ancora alcune cause strutturali che impediscono un calcolo esaustivo dei costi per la *cybersecurity*, e che pertanto devono essere rimosse al fine di non intaccare il funzionamento del sistema economico digitale dell'Unione Europea.

Nonostante il quadro legislativo europeo sia abbastanza consolidato, vi sono ancora molte problematiche e sfide che l'Unione Europea deve affrontare in materia di sicurezza informatica. In assenza di obiettivi misurabili e di sufficienti dati attendibili, realizzare nel contesto pratico le ampie finalità definite all'interno della strategia europea per la *cybersecurity* diventa complicato, e di conseguenza il processo di trasformazione del sistema digitale europeo nell'ambiente più sicuro al mondo viene rallentato. Un'altra problematica riguarda l'incompletezza del quadro normativo europeo nell'ambito preso in questione. Le lacune presenti nel diritto europeo, unitamente ad una sua trasposizione non uniforme, possono far sì che la normativa europea in materia di sicurezza informatica non esplichi appieno le sue potenzialità, come nel caso delle norme per la formazione, la certificazione o le valutazioni dei rischi informatici, attualmente limitate. Per sapere quali lacune colmare è essenziale che l'UE e gli Stati membri abbiano una chiara visione d'insieme del problema rappresentato dalla criminalità informatica, possibilità ancora troppo lontana, dato il carattere disomogeneo del processo di digitalizzazione all'interno dell'Unione Europea. Il caso dell'Estonia, analizzato nell'ultima parte dell'elaborato, rileva proprio come non tutti gli Stati Membri abbiano riconosciuto la *cybersecurity* come una pratica di elevata priorità strategica. Una terza sfida è più in generale rappresentata dalla debolezza del sistema di *governance* della sicurezza informatica, la quale abbonda sia a livello europeo che internazionale, compromettendo la capacità della comunità mondiale di sviluppare una

resilienza informatica in grado di contenere e prevenire gli attacchi informatici. Partire da un'opera di sensibilizzazione alla sicurezza informatica in tutti i settori e i livelli della società è dunque indispensabile, data l'assenza di personale esperto e data la carenza generale di competenze in materia di cibersicurezza.

Le sfide evidenziate, poste dalle minacce informatiche con cui si confrontano l'UE e il più ampio contesto mondiale, rischiano di mettere a rischio il sistema economico comunitario e dei singoli Stati Membri, e necessitano pertanto di un impegno indefesso e di un'adesione piena e costante ai valori dell'Unione Europea.

BIBLIOGRAFIA

Agenzia per l'Italia Digitale. (2020). *Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali*. Reperibile su: https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/modelli-di-finanziamento.html.

Atlantic Council. (2015). *Risk Nexus - Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*.

Barbieri, C. (2020). *La difesa cibernetica in Europa. Una panoramica degli ultimi sviluppi e le opportunità per l'Italia*. A cura dell'Istituto Affari Internazionali (IAI). Parlamento italiano.

Bhattacharyya, K., Frinking, E., Kertysova, K., Maričić, A., van den Dool, K. (2018). *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*. European Economic and Social Committee (EESC): "Visits and Publications" Unit. doi:10.2864/98090.

Björck F., Henkel M., Stirna J., Zdravkovic J. (2015). *Cyber Resilience – Fundamentals for a Definition*. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol 353. Springer, Cham.

Brauchle, J., Krüger, P. S. (2021*) The European Union, Cybersecurity, and the Financial Sector: A Primer*. Cyber Policy Initiative Working Paper Series "Cybersecurity and the Financial System" No. 9. Reperibile su: https://carnegieendowment.org/files/Krueger_Brauchle_Cybersecurity_legislation.pdf.

Cencetti, C. (2014). *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Nuova Cultura.

Center for Strategic and International Studies. (2013). *The Economic Impact of Cybercrime And Cyber Espionage*. McAfee. Reperibile su: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf.

Commissione Europea. (2013). *Strategia dell'Unione Europea per la cybersicurezza.* Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione europea. (2001). *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002.* (COM/2000/890). Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

Commissione Europea. (2001). *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni -*

Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo (COM/2001/0298). Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

Commissione europea. (2001). *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002* (COM/2000/890). Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

Commissione Europea. (2010). *EUROPA 2020 Una strategia per una crescita intelligente, sostenibile e inclusiva,* (COM/2010/2020). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2010). *Un'Agenda digitale europea*, (COM/2010/245). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2012). *Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica*, COM (2012) 140 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2015). *Strategia per il mercato unico digitale in Europa*, (COM/2015/192 final). Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2017). *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE*. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2018). *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, COM (2018) 109 final. Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

Commissione Europea. (2020). *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE*, COM (2020) 591 final. Bruxelles: Ufficio delle Pubblicazioni dell'Unione Europea.

Commissione Europea. (2020). *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN (2020) 18 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2020). *La strategia dell'UE per l'Unione della sicurezza 2020-2025*, COM (2020) 605 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2020). *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, COM (2020) 825 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Commissione Europea. (2020). *Proposta di regolamento del parlamento europeo e del consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*, COM (2020) 842 final. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

Consiglio d'Europa, *Convenzione sulla criminalità informatica*, aperta alla firma a Budapest il 23 novembre 2001, entrata in vigore il 1° luglio 2004, STE n. 185.

Consiglio dell'Unione Europea. (2003). *Strategia Europea in materia di sicurezza*. Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea.

Corte dei Conti Europea. (2019). *Analisi n. 02/2019: Le sfide insite in un'efficace politica dell'UE in materia di cybersicurezza (Documento di riflessione)*. Reperibile su: https://www.eca.europa.eu/it/Pages/DocItem.aspx?did=49416.

Council of the EU. (2008). *Report on the Implementation of the European Security Strategy*. (S407/08). Reperibile su: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf.

Council of the EU. (2018). Joint *declaration on EU-NATO cooperation by President of the European Council Donald Tusk, President of the European Commission Jean-Claude Juncker, and Secretary General of NATO Jens Stoltenberg*. Reperibile su: https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/.

CSIS, McAfee. (2018). *Economic Impact of Cybercrime - No Slowing Down*. Reperibile su: https://www.mcafee.com/enterprise/en-us/forms/gated-form-thanks.html?docID=5fee1c652573999d75e4388122bf72f5&tag=ec&eid=18TL_ECGLQ1_CT_WW#form-download.

Cybersecurity Strategy Committee. (2008). *Cybersecurity Strategy*. Tallin: Ministry of Defence.

Di Biagio, S. (2019). *Cybersecurity Act, da oggi in vigore il nuovo regolamento UE sulla sicurezza informatica*. Il Sole 24 ORE. Reperibile su: https://www.ilsole24ore.com/art/cybersecurity-act-oggi-vigore-nuovo-regolamento-ue-sicurezza-informatica-ACDp1zU.
Directorate-General for Research & Innovation (European Commission). (2017*). The economic rationale for public R&I funding and its impact*. Luxembourg: Publications Office of the European Union.

Directorate-General for Research and Innovation (European Commission). (2021). *Horizon Europe Strategic Plan 2021-2024*. Luxembourg: Publications Office of the European Union.

Direttiva (UE) 2016/1148, 6 luglio 2016.

ECS. (2016). *European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP)*. Reperibile su: https://www.ecs-org.eu/documents/uploads/sria.pdf.

ECS. (2019). *European Cyber Security Organisation - ECS cPPP Progress Monitoring Report 2018*. Reperibile su: https://www.ecs-org.eu/documents/uploads/cppp-progress-monitoring-report-2018.pdf.

EIOPA. (2020). *EIOPA strategy on cyber underwriting*. doi: 10.2854/793935.

ENISA. (2021). *EU cybersecurity initiatives in the finance sector*. Reperibile su: https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector.

Eurojust e Europol. (2019). *Common challenges in combating cybercrime, as identified by Eurojust and Europol*, joint report Europol and Eurojust Public Information.

European Banking Authority. (2017). *Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2*. EBA/GL/2017/17.

European Banking Authority. (2019). *Final report on guidelines on ICT and security risk management*, EBA/GL/2019/04.

European Commission. (2019). *Consultation Document - Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*. Bruxelles: Ufficio delle pubblicazioni dell'Unione europea.

European Commission. (2017). *EU cybersecurity initiatives working towards a more secure online environment – Factsheet*. Reperibile su: https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment. (Ultimo accesso 10 aprile 2021).

European Commission. (2020). *Digital Economy and Society Index (DESI) 2020. Estonia*.

Government of the Republic of Estonia. (2018). *Digital Agenda 2020 for Estonia*.

Herzog, S. (2011). *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. Journal of Strategic Security 4, no. 2.

Holzleitner MT., Reichl J. (2017). *European provisions for cyber security in the smart grid – an overview of the NIS-directive.* In *Elektrotech. Inftech.* 134.

Juncker, JC. (2017). *Discorso sullo stato dell'Unione 2017*. Commissione Europea [Discorso].

Kohler, K. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture*, pag. 4. Doi: 10.3929/ethz-b000438276.

Mcguinness, D. (2017). *How A Cyber Attack Transformed Estonia*. BBC News. Reperibile su: https://www.bbc.com/news/39655415.

Meccanismo Per Collegare L'Europa. (2021). Il Sole 24 ORE. Reperibile su: https://st.ilsole24ore.com/art/osservatorio-finanziamenti-ue/2014-02-21/meccanismo-collegare-europa-113016.shtml?uuid=ABPMO9x.

Mensi, M. (2017). *Cybersecurity and the European digital market*, ISPI. Reperibile su: https://www.ispionline.it/it/pubblicazione/cybersecurity-and-european-digital-market-18234.

Paganini, P. (2020). *Lagarde (Bce): «Un attacco informatico alle principali banche potrebbe innescare una crisi di liquidità»*. Il manifesto. Reperibile su: https://ilmanifesto.it/lagarde-bce-un-attacco-informatico-alle-principali-banche-potrebbe-innescare-una-crisi-di-liquidita/.

Parenti, R. (2020). Sistema europeo di vigilanza finanziaria (SEVIF). Parlamento Europeo. Reperibile su: https://www.europarl.europa.eu/ftu/pdf/it/FTU_2.6.14.pdf.

Parlamento Europeo e Consiglio. (2016). Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio.

Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global*.

Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, 17 aprile 2019.

Republic of Estonia. Ministry of Economic Affairs and Communication. (2019). *Cybersecurity Strategy Republic of Estonia*.

RFC 2350 CERT-EU, versione 5.1, settembre 2019.

Samartsev, D. (2020). *Cybercrime is maturing. Here's how organizations can keep up*. World Economic Forum. Reperibile su: https://www.weforum.org/agenda/2020/11/how-to-protect-companies-from-cybercrime/.

Schmidt, A. (2013). *The Estonian Cyberattacks*, pag. 14. Capitolo preparato per il libro "The fierce domain – conflicts in cyberspace 1986-2012", modificato da Jason Healey, Washington, D.C.: Atlantic Council, 2013.

Trimintzios, P., et al. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU*. EPRS/STOA/SER/16/214N.

SITOGRAFIA

Agenzia per la Promozione della Ricerca Europea. *Verso Horizon Europe*. Reperibile su: https://www.versohorizoneurope.it/articoli/95-miliardi-horizon-europe/.

Commissione Europea. *Cosa significa protezione dei dati «fin dalla progettazione» e «di default»?*. Reperibile su: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_it.

Commissione Europea. *Un'Europa pronta per l'era digitale*. Reperibile su: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_it.

Consiglio Europeo. (2020). *Lettera d'invito del presidente Charles Michel ai membri del Consiglio europeo prima della videoconferenza del 23 aprile 2020* [Comunicato stampa]. Reperibile su: https://www.consilium.europa.eu/it/press/press-

releases/2020/04/21/invitation-letter-by-president-charles-michel-to-the-members-of-the-european-council-ahead-of-their-video-conference-on-23-april-2020-2020/.

Consiglio Europeo. (2020). *Lettera d'invito del presidente Charles Michel ai membri del Consiglio europeo prima della videoconferenza del 23 aprile 2020* [Comunicato stampa]. Reperibile su: https://www.consilium.europa.eu/it/press/press-releases/2020/04/21/invitation-letter-by-president-charles-michel-to-the-members-of-the-european-council-ahead-of-their-video-conference-on-23-april-2020-2020/.

Consiglio Europeo. (2021). *Meccanismo Per Collegare L'Europa: Accordo Informale Con Il Parlamento Europeo Sul Programma Dopo Il 2020*. [Comunicato stampa]. Reperibile su: https://www.consilium.europa.eu/it/press/press-releases/2021/03/11/connecting-europe-facility-informal-agreement-with-european-parliament-on-the-post-2020-programme/.

Consiglio Europeo. *Una nuova agenda strategica 2019–2024*. (2019). [Comunicato stampa]. Reperibile su: https://www.consilium.europa.eu/it/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/.

Consiglio Europeo. (2021). *Programma Europa Digitale – Accordo Informale Con Il Parlamento Europeo*. [Comunicato stampa]. Reperibile su: https://www.consilium.europa.eu/it/press/press-releases/2020/12/14/digital-europe-programme-informal-agreement-with-european-parliament/.

Consiglio Europeo. (2020*). Programma Europa digitale – Accordo informale con il Parlamento europeo* [Comunicato stampa]. Reperibile su: https://www.consilium.europa.eu/it/press/press-releases/2020/12/14/digital-europe-programme-informal-agreement-with-european-parliament/.

Consiglio Europeo*. Un piano per la ripresa dell'Europa*. (2021). Reperibile su: https://www.consilium.europa.eu/it/policies/eu-recovery-plan/.

E-Estonia. Reperibile su: https://e-estonia.com.

ECS. *Contractual Public-Private Partnership (cPPP) with the European Commission*. Reperibile su: https://ecs-org.eu/cppp.

ENISA. *CSIRT Services*. Reperibile su: https://www.enisa.europa.eu/topics/csirt-cert-services.

ENISA. *European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership*. Reperibile su: https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership.

European Banking Authority*. The Single Rulebook*. (2021). Reperibile su: https://www.eba.europa.eu/regulation-and-policy/single-rulebook.

Eurojust. *Cybercrime*. Reperibile su: https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime.

European Central Bank. *Euro Cyber Resilience Board for pan-European Financial Infrastructures*. Reperibile su: https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html.
European Commission. *Digital Economy and Society Index*. Reperibile su: https://digital-strategy.ec.europa.eu/en/policies/desi.

European Commission. *EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems.* Reperibile su*:* https://digitalstrategy.ec.europa.eu/en/node/925/printable/pdf.

European Commission*. European Structural and Investment Funds Data*. Reperibile su: https://cohesiondata.ec.europa.eu/2014-2020/Planned-ERDF-Investments-to-make-Europe-fit-for-th/vmmp-peu6.

European Commission. *Key indicators of the European information society*. Reperibile su: https://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-countries#chart={"indicator-group":"security-privacy","indicator":"i_secfl","breakdown":"ind_total","unit-measure":"pc_ind_ilt12","ref-area":["EE","EU"]}.

Eurostat. *Internet access of households, 2014 and 2019 (% of all households).* Reperibile su: explained/index.php?title=File:Internet_access_of_households,_2014_and_2019_(%25_of_all_households).png&oldid=502733.

Eurostat. *Security related problems experienced when using the internet*. Reperibile su: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb$DV_538/default/line?lang=en.

FS-ISAC. Reperibile su: https://www.fsisac.com.

National Cyber Security Index. Reperibile su: https://ncsi.ega.ee/methodology/. https://ncsi.ega.ee/ncsi-index/?order=-ncsi.

Statista. *Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted)*. Reperibile su: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

The International Telecommunication Union (ITU). *Global Cybersecurity Index*. Reperibile su: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

The World Bank Data. Reperibile su: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2019&locations=EE&start=2019&view=bar. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=EE.

ABSTRACT

With the onset of the Digital Age the issue of cyber security has extended to almost all areas of present-day society, affecting every aspect of international economic and political governance systems. Following the arrival of digitisation in the European Union, cybercrime and lawlessness have evolved considerably, and as a result, European institutions and Member States have become increasingly aware of cyber security as an emergency that needs to be tackled on several fronts. Currently, the European system for monitoring and responding to cyber-attacks is based on multidimensional and transversal actions, aimed at training and awareness-raising on cyber security, at developing a common cyber language, and at establishing a certification regime, involving both public and private actors.

Over the last twenty years, the European Union's role in the field of cyber security has undergone a considerable transformation. It was not until the 2000s that the topic of cyber security was first included in European political and economic discussions. An important step was taken in 2004, when the European Union Agency for Network and Information Security (ENISA) was established. ENISA is as an advisory body, which contributes to policy development and awareness-raising in the field of cyber security. In addition to ENISA, several European agencies are involved in the cyber security sector. Firstly, the European Cybercrime Centre (EC3), which was set up to strengthen EU actions against cybercrime. Another body is the Computer Emergency Response Team (CERT-EU), which assists all EU institutions, bodies and agencies in combating and preventing cyber-attacks. The European External Action Service (EEAS), on the other hand, is in charge of cyber defence, cyber diplomacy and strategic communication, as well as hosting analysis and intelligence centres. Finally, the European Defence Agency (EDA), which is in charge of developing European cyber defence capabilities.

The first step towards the creation of a legislative framework for cyber security was taken in 2013, when the European institutions approved the '*European Union Strategy for Cybersecurity*', which is the first European action plan entirely aimed at cyber security. This major strategic plan was followed by the 2016 Network and Information System Directive (NIS), the first cyber security legislation introduced at European level, and by the General Data Protection Regulation (GDPR), which imposes a common model for the processing and defence of personal data across the EU. The NIS Directive established a common strategic line between the various EU states against the risk of cyber incidents, while the

GDPR established a system of rules, including obligations relating to data protection management, storage and confidentiality.

In 2017, the European Commission presented to the European Parliament and the Council a package entitled *'Resilience, Deterrence and Defence: towards strong cyber security for the EU*'. The aim of this communication was to reform and strengthen the European regulatory framework on cyber security, especially the 2013 Cyber security Strategy and the 2016 NIS Directive. However, this objective set out in the Commission's package was only achieved in April 2019, with the approval of the regulation on the European Union Cybersecurity Agency (ENISA) and on cyber security certification for information and communication technologies, also known as the *'Cybersecurity Act'*. This regulation was envisaged with the aim of enhancing the Union's cyber resilience, creating a single market for cyber security in terms of products, services and processes, and strengthening the role of ENISA. In December 2020, on the other hand, the Commission presented a new cyber-security strategy to implement 'three main instruments - regulatory, investment and policy - for three areas of EU action: (1) resilience, technological sovereignty and leadership; (2) developing operational capabilities for prevention, deterrence and response; and (3) promoting a global and open cyberspace[134]'. The new cyber security strategy is designed to improve the quality of Europe's digitisation process, which requires an even higher level of security, defence and reliability than a few decades ago.

Faced with the growing expansion and evolution of cyberspace and the consequent increase in cybercrime, the European Union felt the need to increase funding and financing in the field of cyber security and to focus on a more active collaboration between research, businesses and governments in order to make Europe's digital system among the most secure and efficient in the world. The financing system set up by the European institutions is particularly well organised and is currently expanding. The financial instruments and investment projects envisaged have a considerable economic capacity, underlining the European Union's desire to elevate the cyber sector as a tool for economic recovery and growth, especially in the context of the current pandemic crisis. Numerous funds have been allocated by the European Union to the cyber security sector. A first group of funds is aimed at the research and innovation sector and represents the largest item of expenditure for cyber security programmes. Through the Horizon 2020 programme, the European Union has

[134] European Commission (2020). *The EU cybersecurity strategy for the digital decade*, JOIN (2020) 18 final, pg. 5.

financed investments to develop all the technologies needed to ensure proper protection of European citizens' digital rights. Horizon 2020's contribution to the development of innovative cyber security projects and policies was strengthened in 2016, with the creation of a contractual Public-Private Partnership (cPPP) between the European Commission and the European Cyber Security Organization (ECSO), aimed at strengthening the European cyber security industry. The vastness and complexity of issues related to cyber security require cooperative forms between actors that, albeit with different roles, operate in this strategic sector for the security and economy of the EU. The work undertaken by the European Union in the field of research and innovation with Horizon 2020 will continue in the period 2021-2017, in view of the development of a new framework programme called "Horizon Europe", with which the EU aims to strengthen the fight against cybercrime and to defend the integrity of the Digital Single Market. The second major group of cyber security funds is aimed at digital infrastructures. Through the European Structural and Investment Funds (EIS Funds), the Digital Europe programme and the Connecting Europe Facility, large sums of money have been allocated to ensure an adequate level of security of digital frameworks. The main beneficiaries of these funds are European small and medium-sized enterprises (SMEs), which represent some of the categories most affected by cybercrime.

Despite the fact that the European legislative and financial framework on cyber security is fairly well established, there are still systemic gaps that allow cybercrime to expand, negatively impacting two sectors in particular: the financial sector and the industrial sector. The vulnerability of these sectors, especially the financial one, to cyber-attacks has forced the European Union to pursue a number of cyber initiatives, in line with the European cyber security legislative framework. In 2018, the European Commission unveiled the FinTech Action Plan with the aim of increasing the level of security of new fintech products, which have revolutionised the way the financial sector operates, but at the same time have exposed it to risks related to cyber security. According to the Commission, an adequate cyber security in the financial sector can be ensured through cooperation between financial institutions that make use of new fintech technologies, and in particular through the exchange of information on possible cyber-attacks and through coordination of prevention and response to attacks. In addition to the European Commission, there are other agencies that are specialized in the implementation of the European cyber policy within the financial, banking and insurance sectors. These include the European Banking Agency (EBA) and the

European Insurance and Occupational Pensions Authority (EIOPA), which are an integral part of the European System of Financial Supervision (ESFS). EBA provides guidance, recommendations and opinions to banking and financial institutions on issues related to the use of new digital technologies and helps them improve their cyber resilience capabilities. For example, under the Payment Services Directive (EU) 2015/2366 (PSD2)[135], the EBA and the ECB assist payment service providers, by advising them on how to prevent and respond to most operational and security incidents, including cyber incidents, following the issuance of (*online*) payment services in the European market. Regarding the role of the EIOPA, this agency is in charge of protecting consumers and promoting the training of financial institutions in sound cyber security practices and cyber underwriting, which corresponds to risk management measures in digital finance.

As highlighted above, the industrial sector is the other area particularly affected by cybercrime, especially in the context of the European Union. As a result of the digitisation process undertaken by European companies, which have invested heavily in new information and communication technologies, thus exposing themselves to greater cyber risks, cyber security has been included by European institutions within the EU industrial policy. In spite of the strong growth in productivity and competitiveness of European companies in both European and non-EU markets, due to these investments in digital technology, the European industrial fabric, and in particular SMEs, have not been able to prepare themselves as well as possible for the fight against cyber-attacks, thus falling among the main victims of cybercrime. In contrast to large multinational companies, which are aware of the importance of proper risk management and observation of cyber security procedures, a large part of European SMEs does not have adequate 'cyber maturity', which means that they are not aware of the threat posed by the rise and expansion of cybercrime. This backwardness of SMEs in the field of cyber security is primarily linked to the inefficient allocation of financial resources for cyber security by the European institutions, which leads to a deterioration in the state of health of a good amount of European companies. Increasing financial support to European companies and enhancing cooperation with national cyber investigation and response institutes (national CERTs) are two necessary objectives in order to develop SMEs' capacity building in cyber security.

[135] European Banking Authority. (2017). *Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2*.

The fulfilment of the Digital Single Market requires, first of all, an appropriate level of harmonisation of the digitisation process among the different European Union Member States. As shown by the Digital Economy and Society Index (DESI), prepared by the European Commission, the digital transformation has been and continues to be uneven within the European context, where there are both highly digitised countries and countries with a low level of investment in the digital sector and cyber security. Among the most digitally advanced European countries is Estonia, a country which, despite its small size, is known throughout Europe and the rest of the world for the efficiency of its national cyber security strategy, representing a reference point for the fight against cybercrime and for the development of cyber security and cyber defence policies. The experience of the cyber-attack that Estonian government institutions suffered in 2007 completely overturned the cyber security needs of Estonia and the entire European Union, contributing to the definition of the European Union's strategic cyber path. Estonia was one of the first European countries to focus on the full digitisation of state services and the promotion of digital security, as these were perceived as two necessary goals in order to support the country's socio-economic growth. Indeed, the basis for the proper functioning of the Estonian economy in the context of the European Digital Single Market includes the extensive promotion of cyber security measures, demonstrating that an adequate cyber strategy is necessary for the sustenance and development of a country's economic activities and processes. The case of Estonia shows that not all European Union Member States perceive network and digital rights security as an indispensable element of economic safeguards, despite the fact that the current context shows an increasing dependence of national economies on new digital technologies and a consequent increase in cybercrime.

There are several actions that the European Union and its Member States can take in the field of cyber security in order to protect the integrity of the EU economic system. Strengthening governance and investment programmes in cyber security both in the public and private sectors is essential to stimulate a homogeneous advancement of the digitisation process throughout the Union, but it is more important to start by raising awareness of cyber security in order to ensure the development of cyber maturity on all economic and social levels.