LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

**Dipartimento di Impresa e Management**
**Cattedra di Diritto Pubblico dell'Economia**

# *Financial Cybercrime e rischi di mercato. Profili regolamentari.*

*Prof. Valerio Lemma*

Relatore

*Giovanni De Pietro, 268861*

Candidato

Anno Accademico 2023/24

*Nei tuoi occhi il mio riflesso,*
*nel mio cuore, il tuo.*
*A te che dall'alto mi rendi la corona,*
*ti sento oggi più vicino che mai.*

*A mio padre.*

# Indice

# Introduzione

Con il termine “innovazione” si intende il processo di creazione ed implementazione di nuove idee, prodotti, servizi o metodi che apportano miglioramenti significativi rispetto alle soluzioni esistenti.

Questo, il processo che include il miglioramento delle condizioni economiche, sociali, ambientali, attraverso il quale le società crescono e si evolvono, permettendo agli individui e alle comunità di prosperare.

Gli ultimi anni sono stati caratterizzati da un esponenziale e repentino processo innovativo, che ha coinvolto i più disparati settori, giungendo ad annoverare una totalità evolutiva guidata da un settore in particolare: quello della tecnologia e dell’informazione, di una risonanza tale da rivoluzionare diversi ambiti di applicazione, tra cui il settore bancario, i sistemi di pagamento, la gestione delle informazioni, e l’ampio settore delle comunicazioni.

Pur rappresentando l’innovazione e lo sviluppo, due delle più potenti forze che hanno inaugurato il mondo contemporaneo, apportando innumerevoli benefici e migliorando la qualità della vita delle persone tramite un efficientamento dei processi economici e sociali, è necessario considerare attentamente l’altra faccia della medaglia, macchiata dalle ingiustizie e dalle illiceità spesso perpetrate tra le file del progresso tecnologico.

Questo, il fertile terreno ove la criminalità ha avuto modo di prosperare ulteriormente, in modo subdolo e completamente distruttivo.

Il crimine digitale, noto anche come “*cybercrime*”, evolve in parallelo con la tecnologia, sfruttando le innovazioni per sviluppare tecniche sempre più sofisticate, adattandosi rapidamente alle nuove contromisure, spesso anticipandole e costituendo il motivo principale per l’adozione delle stesse.

Il primo capitolo del presente elaborato si propone di fornire una definizione approfondita di “*cybercrime*”, offrendo una panoramica generale del fenomeno e mettendo in evidenza gli aspetti storici ed etimologici che hanno portato all’attuale era criminale. Verrà esaminata la nascita del fenomeno sociale noto come “*Hacking*”, i primi risvolti criminali da esso derivanti, e le contromisure legislative adottate. Successivamente, il capitolo offrirà un’analisi dettagliata sull’infiltrazione illecita nel settore bancario, uno dei settori più colpiti dai cybercriminali a causa della sua natura estremamente sensibile e

profittevole. Verranno esplorati gli sviluppi e le tendenze emergenti di questo fenomeno criminale, tra cui l'uso dei nuovi strumenti valutari rappresentati dalle cripto-attività e la regolamentazione necessaria per gestirli.

Il secondo capitolo si propone di analizzare il connubio tra giurisprudenza e tecnologia, evidenziando come esse costituiscano due dimensioni reciprocamente e continuamente influenzate. Nello specifico, verranno trattati i temi della regolamentazione a livello internazionale e transfrontaliero, attraverso accordi e misure legislative come la *Convenzione di Budapest* e le *Direttive NIS* (*Network and Information Security*). Particolare attenzione sarà dedicata al ruolo delle autorità nella cooperazione transfrontaliera, mirata alla prevenzione e al contrasto della criminalità organizzata e, nello specifico, della criminalità informatica. Una concisa indagine circa il fenomeno della criminalità organizzata internazionale nell'epoca digitale precederà la seconda parte del capitolo, dedicata a un'approfondita analisi legislativa sul riciclaggio di denaro a livello domestico e internazionale. Verranno esaminati il reato di riciclaggio in Italia e in Europa attraverso misure legislative come l'*art. 648-bis* del Codice Penale e le *IV e V Direttive AML* (*Anti-Money Laundering*).

Caratterizzate da estremo dinamismo e complessità esecutiva, le tecniche di riciclaggio hanno vissuto un'evoluzione parallela a quelle tecnologiche. Quest'ultime, utilizzate, spesso, a tali illeciti scopi. Uno dei più lampanti esempi è costituito dal riciclaggio di denaro mediante le odierne, e non completamente regolamentate, tecniche basate sulle cripto-attività, che permettono l'esistenza del diramato e complesso mondo del "*cyberlaundering*".

Il terzo e ultimo capitolo di questo elaborato è dedicato allo studio di un caso di estrema attualità che, verificatosi meno di due mesi fa, ha generato rischi e preoccupazioni di ogni genere per l'azienda vittima (*Synlab*), le istituzioni, e soprattutto per le centinaia di migliaia di persone interessate dall'attacco hacker perpetrato dall'organizzazione criminale "*Black Basta*". In particolare, il capitolo analizzerà lo scenario con riferimento specifico agli attori coinvolti, per poi delineare le conseguenze già manifestate e quelle potenzialmente materializzabili. Saranno inoltre formulate previsioni su ciò che potrà accadere in ambito criminologico a partire da questo attacco, esaminando le misure di prevenzione e contrasto adottate in Italia e in Europa, con particolare attenzione al *Regolamento Generale sulla Protezione dei Dati* (*GDPR*), al *Decreto Legislativo n.*

*65/2018*, e al *Disegno di Legge "Cybersicurezza"*, attualmente in fase di approvazione in Senato.
Il caso, nello specifico, è simbolo di una criminalità che opera in silenzio, in completa autonomia, con una malvagità espressa esclusivamente attraverso strumenti digitali, rappresentando un punto di svolta persino nei meccanismi di azione criminale: questa, l'altra faccia della non sempre limpida medaglia evolutiva.

# 1. Panoramica sul cybercrime

## 1.1. Definizione di cybercrime

Divenuto un problema sempre più rilevante con l'avanzamento della tecnologia e l'ubiquità di internet, il fenomeno del *cybercrime* è causa di innumerevoli sfide per le forze dell'ordine, autorità giudiziarie, ma anche, e soprattutto, per gli individui comuni.
Prima di affrontare il dibattito circa i danni generati da questo fenomeno criminale, è bene sapere nel dettaglio di cosa si stia effettivamente parlando.
Secondo l'enciclopedia *Treccani*, la definizione di "*Cybercrime*" si articola come segue:

> "Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, perpetrato utilizzando un tale sistema o colpendolo. Nel primo caso ci si riferisce anche a reati informatici impropri, ossia ai reati comuni previsti dal Codice penale o dalla legislazione speciale, che solo incidentalmente vengono commessi mediante l'uso di un computer e della rete […]. Nel caso di un c. perpetrato per colpire un sistema informatico, si tratta invece di reati informatici propri, la maggior parte dei quali sono stati introdotti nell'ordinamento italiano dalla legge 547/1993 e dalla legge 48/2008 […]. La categoria concettuale dei c. non ha, tuttavia, un significato tecnico preciso dal punto di vista giuridico, poiché, fatta eccezione per la presenza di un sistema

informatico o telematico, vi rientrano una pluralità di condotte e beni giuridici protetti estremamente disomogenei."[1]

Il *Cybercrime*, o criminalità informatica, dunque, si riferisce a qualsiasi attività criminale che coinvolge l'uso di computer e reti informatiche.
Essendo uno tra i principali strumenti utilizzati dalle organizzazioni criminali a scopi lucrativi e non[2], il cybercrime costituisce una notevole piaga all'interno della tela rappresentata dalla società civile. Riuscire a ricucire questa piaga è il compito difficoltoso di molteplici autorità che, per quanto competenti, sono spesso costrette ad affrontare difficoltà di diverso genere, e mai affrontate prima.

### 1.1.1 Nascita del fenomeno "*Hacking*" e primi crimini informatici

L'*Hacking* è oggi un fenomeno ampiamente discusso e conosciuto, sebbene rimanga difficile da definire e identificare empiricamente, in quanto è arrivato a riferirsi a pratiche diverse, tra loro non sempre compatibili.[3] Nell'ultima metà di secolo, infatti, l'uso dei computer e di Internet è proliferato, rivoluzionando profondamente le dinamiche sociali e i comportamenti umani. Da questi cambiamenti, le risorse tecnologiche si evolvono, creando opportunità per commettere comportamenti criminali nel cyberspazio.[4] Ma è sempre stato così?
Per poter ottenere risposta a tale quesito, è bene analizzare la nascita del fenomeno che prende il nome di "*Hacking*", e la sua repentina evoluzione. Una prima definizione, infatti, della criminalità nel cyberspazio, è stata fornita da uno studio statunitense datato

[1] Cit. Enciclopedia Treccani: Cybercrime, Lessico del XXI Secolo (2012)

[2] Cfr. Gratteri, Nicola, and Antonio Nicaso. "Il grifone. Come la tecnologia sta cambiando il volto della 'Ndrangheta." Milano: Mondadori, 2024.

[3] Cfr. Jordan, Tim. "A Genealogy of Hacking." Sage Journals, Volume 23, no. 5.

[4] Cfr. "Hacking: Evolution, Conceptualization, and the Perpetrators." Contemporary Challenges for Cyber Security and Data Privacy. ResearchGate.

1979[5], secondo cui presupposto fondamentale, sia per eseguire che per perseguire l'illecito, vi sia la conoscenza della tecnologia informatica.

Nello specifico, la ricerca riporta un'interessante panoramica sulla nascita dello studio dell'informatica in America.

Nel corso dell'anno scolastico 1958-59, il *Massachusetts Institute of Technology (MIT)* di Boston lanciò i primi corsi universitari in Scienze Informatiche. Dopo quaranta ore di partecipazione attiva al *Tech Model Railroad Club (TMRC)*, veniva data agli studenti la possibilità di accedere a una stanza dove era installato un modello di ferrovia in miniatura, mosso da complessi circuiti elettronici e minuziose scenografie.

Mentre alcuni membri si dedicavano alla costruzione e al perfezionamento dei trenini, un gruppo più intraprendente e perspicace istituì il sottocomitato *Signal & Power (S&P)* per esplorare in dettaglio i meccanismi alla base del funzionamento del modello. All'interno dell'*S&P*, emerse rapidamente l'ambizioso progetto di automatizzare i trenini in miniatura collegandoli clandestinamente ai computer dell'università durante la notte, dando origine ai primi esempi di "scherzi informatici".

Questa iniziativa catturò l'interesse di alcuni insegnanti che, notando l'estesa competenza tecnica di questi pionieristici hacker, decisero di integrarli nei programmi di studi di informatica, ponendo fine al fenomeno delle incursioni notturne. In quegli anni, nel frattempo, andò consolidandosi il mito dell'hacker americano: un ragazzo brillante artefice del proprio successo, con l'ideale di espandere la cultura informatica nella totalità della società civile, e non solo negli ambienti universitari.[6]

Nonostante aver dunque evidenziato il nobile scopo di cui la comunità hacker divenne promotrice, è bene sapere che, parallelamente, vennero creati e raffinati metodi informatici atti al compimento di veri e propri crimini, come la diffusione di Malware, attacchi a server e reti, furto di identità e altri, estendendo la criminalità e l'immoralità al fenomeno *Hacking,* nato da una buona causa. Grazie proprio a quest'ultima spinta criminale è stato possibile osservare una classificazione della figura dell'hacker in tre

---

[5] Cfr. Baiguera Altieri, Dott. "La cultura Hacker negli Stati Uniti d'America." In La criminalità informatica in Svizzera e in Italia. Diritto.it.

[6] Cfr. Colombo, Cristina F. "Geodiritto, globalizzazione e nuovi canali per i reati d'impresa". Milano: Wolters Kluwer, 2021.

categorie, ad opera del *Dipartimento Informatico per la Sicurezza*, distinte in base alle loro intenzioni e metodologie:

1. *"Black hat"*: gruppi hacker che agiscono con intenti immorali, spesso composti da cyber-criminali che infrangono la sicurezza dei sistemi informatici principalmente per trarne profitto economico o per compiere atti illeciti.
2. *"Grey hat"*: categoria che include coloro che, pur non perseguendo obiettivi criminali, violano i sistemi informatici spinti dalla curiosità di esplorarne le potenzialità e i limiti.
3. *"White hat"*: professionisti etici che cooperano con enti, autorità di sicurezza e governi per proteggere i sistemi informatici. Essi conducono test per individuare e risolvere le vulnerabilità, contribuendo alla lotta contro il cybercrimine.[7]

Parallelamente a questa classificazione, si assiste all'emergere dei *"Cracker",* figure distinte dagli *hacker* per la loro propensione a introdursi in programmi altrui con l'obiettivo di danneggiarli, copiarli o utilizzarli illecitamente, eludendo le misure di sicurezza. La differenza tra *hacker* e *cracker* può anche essere tracciata dall'etimologia del termine *"Cracker"* stesso, coniato da *Richard Stallman*[8] proprio per indicare, con valore fortemente dispregiativo, una figura distinta che concentri le proprie capacità e abilità tecniche senza alcun principio etico, e con il solo fine di ricavarne vantaggi personali in termini economici o di visibilità.[9]

[7] Cit. Kaspersky. "Hacker Black Hat, White Hat e Gray Hat – Definizione e Spiegazione." Kaspersky IT Resource Center.

[8] Importante programmatore e attivista, conosciuto per la sua cruciale influenza nella comunità del software libero, avendo fondato il progetto GNU nel 1983.

[9] Cfr. Enciclopedia Treccani: "Cracker".

### 1.1.2. Profili regolamentari e vuoti di tutela

La criminalità informatica, nonostante possa sembrare un problema strettamente legato al recente avanzamento tecnologico, ha richiesto l'attenzione per una regolamentazione contro comportamenti dannosi o pericolosi nel settore digitale fin dagli anni '80. Durante questo periodo, sia gli esperti di legge che i tribunali hanno affrontato difficoltà nel concordare una definizione univoca che potesse abbracciare l'intera portata della criminalità digitale.[10]

Ci sono stati molti tentativi di inquadrare legalmente questa forma di criminalità, spaziando da teorie che sottolineavano la relazione tra il crimine e la competenza tecnologica a quelle che erroneamente associavano il reato alla tecnologia informatica, includendo anche il furto fisico di dispositivi. Allo stesso modo, le teorie che proponevano il computer come necessario oggetto o strumento del reato non hanno trovato molto sostegno, poiché ciò avrebbe ingiustamente ampliato la gamma di atti illeciti per includere il furto o la distruzione fisica di hardware, escludendo i danni ai dati o al software senza un uso diretto del computer.

Questo periodo così contrastato a livello teorico-giuridico apre la strada in numerosi paesi, sia in Europa (Francia, Austria, Norvegia, Danimarca) che al di fuori (Canada, Giappone, Australia, Stati Uniti), ad una specifica legislazione penale che possa arrivare a disciplinare il crimine informatico. Il legislatore italiano si muove, invece, solo nel 1993 con la formazione di una legge ad hoc, la Legge n. 547 del 23 dicembre, recependo di fatto la "Raccomandazione del Consiglio 13/09/1989 n. 9 sulla repressione della criminalità informatica" da parte dell'Unione Europea. Tale misura legislativa ha portato all'introduzione di nuovi tipi di crimini nel Codice Penale, optando per non classificare i crimini informatici come violazioni di nuovi diritti legali, ma piuttosto estendendo la protezione delle leggi penali già esistenti per coprire queste nuove forme di criminalità.[11]

La suddetta legge apportò diverse innovazioni all'interno del quadro normativo italiano, modificandolo così, nel tempo.

---

[10] Cfr. Colombo, Cristina F. *Geodiritto, globalizzazione e nuovi canali per i reati d'impresa*. Milano: Wolters Kluwer, 2021.

[11] Cfr. Università degli studi di Udine. Corso di informatica giuridica. "I reati commessi su internet: computer crimes e cybercrimes."

Alcune fra le più importanti innovazioni furono rappresentate da diverse condotte, inclusi reati di contraffazione relativi a documenti ufficiali e privati, elaborati mediante tecnologie informatiche: art. 491-bis c.p. e art. 617-sexies c.p.; azioni volte a danneggiare l'integrità dei dati e dei sistemi informatici, oggetti materiali soggetti all'innovazione tecnologica: art. 635-bis c.p., art. 615-quinquies c.p., art. 392 c.p., art. 420 c.p.;
frodi informatiche, dove non c'è inganno nei confronti di una persona: art. 640-ter c.p.; uso indebito di carte di credito magnetiche: art. 12, Legge n. 197 del 05/07/1991; azioni che violano la privacy di dati e software, art. 615 ter c.p. e 615 quater c.p., e le comunicazioni informatiche, art. 616 c.p., art. 617 quinquies e art. 623-bis c.p.
Tuttavia, tale ricostruzione non è convincente se si prende in considerazione che, riguardo la salvaguardia dei documenti digitali, è prioritaria, ancor prima dell'autenticità, la loro integrità, intesa come l'assenza di alterazioni o modifiche da parte di individui non autorizzati.[12] La necessità, dunque, di fornire una base normativa specifica per la gestione, l'archiviazione e l'utilizzo dei documenti informatici, nonché per garantire l'autenticità e l'integrità degli stessi, si materializzò con la Legge n. 48 del 18/03/2008: "Legge sulle disposizioni per la tutela dei documenti informatici e per l'autenticità del documento informatico.", come approvazione e attuazione della Convenzione del Consiglio d'Europa sulla cyber-criminalità, stipulata a Budapest il 23 novembre 2001[13], che costituisce il primo trattato internazionale che si occupa dei crimini perpetrati attraverso internet o altre reti di computer.[14] La legge in questione ha modificato vari articoli, introducendone altri, facendo in modo che il quadro legislativo risultasse più conforme alle esigenze punitive originate da una criminalità in continua evoluzione, che richiede il costante stato di allerta da parte del legislatore e le autorità dedite alla repressione della stessa, segnalando dunque come questi ultimi siano chiamati costantemente ad intervenire allo scopo di adeguare il nostro ordinamento giuridico alle novità sociali e tecnologiche, in continuo aumento.

---

[12] Cfr. Colombo, Cristina F. Economia criminale: geodiritto, globalizzazione e nuovi canali per i reati d'impresa. Milano: Wolters Kluwer, 2021.

[13] Cfr. Parlamento.it, Legge 18/03/2008

[14] Cfr. Dezzani, Giuseppe. "La criminalità informatica." Diritto.it.

## 1.2 Cybercrimini nel settore bancario

Il settore bancario, di cruciale importanza per l'economia globale e la crescente dipendenza dalla tecnologia digitale, si presenta come un bersaglio particolarmente attraente per i cybercriminali, essendo, di fatto, esposto ad una vasta gamma di attacchi, da parte di individui o gruppi che, sfruttando le vulnerabilità della rete e dei sistemi informativi delle banche, riescono nel compimento dei sopradetti, spaziando da furti di identità e frodi finanziarie, ad attacchi che paralizzano le operazioni quotidiane. La natura in evoluzione e sempre più sofisticata dei cybercrimini nel settore bancario richiede un'attenzione costante e la messa in atto di strategie di difesa all'avanguardia per proteggere dati sensibili e mantenere la fiducia nel sistema finanziario globale.[15]
Sfida che, come vedremo, è stata in grado di generare gravi perdite, e non solo finanziarie.

### 1.2.1. Tradizione e innovazione: Sistema bancario tradizionale e digitale

Per comprendere al meglio le operazioni illecite che costituiscono il fitto ed oscuro mondo del *financial cybercrime*, è necessario essere a conoscenza del contesto all'interno del quale operano i consumatori, istituzionali e non, cercando di capire quanti e quali siano i punti deboli che esso presenta, e che permettono a specifiche figure criminali di raggirare sistemi di sicurezza ed autenticazione, allo scopo di appropriarsi indebitamente di parte del patrimonio altrui.
Oggi, infatti, i consumatori hanno a disposizione una serie eterogenea di opzioni per le loro esigenze bancarie. Per molti anni, l'attività bancaria tradizionale è stata l'opzione predefinita, che va oggi affiancata, tuttavia, da un'avanzata tecnologia che consente ai clienti di accedere a servizi bancari che possono essere interamente online e mobili.
Ogni opzione, tuttavia, presenta delle differenze con le altre.
Parlando di *"traditional banking"*, cercando dunque di definire tale espressione, è bene sapere che con essa si fa riferimento all'ubicazione fisica della filiale della banca in

[15] Cfr. De Nederlandsche Bank. Eurosysteem: Innovation in Payments and Banking, Cybercrime.

esame. Il modello bancario tradizionale presenta delle caratteristiche che con il passare degli anni hanno contribuito ad instaurare e consolidare un senso di familiarità nella maggior parte delle persone che usufruiscono dei servizi bancari.

Parliamo dell'offerta di un'ampia gamma di servizi finanziari, talvolta non accessibili ai clienti delle banche digitali. Esempi di essi sono la possibilità di depositare contanti, usufruire della fitta rete di bancomat, varietà di opzioni per il servizio clienti, interazione umana con gli operatori bancari e via discorrendo.[16]

Il settore bancario sta subendo, tuttavia, una repentina evoluzione: le tendenze nell'innovazione tecnologica che coinvolgono tutte le industrie, le modifiche normative e la richiesta di maggiore flessibilità nel business, stanno influenzando significativamente il mercato dei servizi finanziari destinati al consumatore finale, che sulla base dei suoi bisogni, ricerca ciò che maggiormente li rispecchia.[17]

Non rappresenta certamente una coincidenza che, negli ultimi dieci anni, il profilo del consumatore italiano sia mutato significativamente, sia a causa di un'evoluzione continua determinata da fattori socioeconomici e demografici, sia a seguito delle influenze del progresso tecnologico e della pandemia di *COVID-19*. Le esigenze cui il *digital banking* risponde sono essenzialmente di duplice natura: la prima, quella dettata dalla ricerca della semplicità e della comodità, espletata tramite la possibilità di effettuare le operazioni desiderate ovunque, in qualsiasi momento e in pochi clic; la seconda, quella classica della ricerca alla convenienza, riscontrata di fatto nella tendenza delle banche digitali ad offrire vantaggi come: commissioni basse o assenti nei riguardi della manutenzione mensile, tassi di interesse competitivi sui conti deposito, requisiti di deposito bassi o nulli, e molteplici altri servizi, realizzati come indiretta conseguenza del grande vantaggio in termini di costi, generalmente inferiori rispetto a quelli sostenuti dalle banche tradizionali, che rendono di fatto possibile l'offerta delle numerose opzioni.[18]

Rispetto a dieci anni fa, c'è stato un aumento del 34% nell'uso di Internet tra gli italiani di età compresa tra i 45 ei 64 anni, rappresentando l'incremento più significativo tra le diverse fasce d'età della popolazione italiana, che varia comunque tra il +14,4% e il

---

[16] Cfr. Chase.com. "Online Banking vs. Traditional Banking: Exploring the Differences."

[17] Cfr. Il Sole 24 Ore. "La trasformazione digitale del banking parte dalla conoscenza del consumatore."

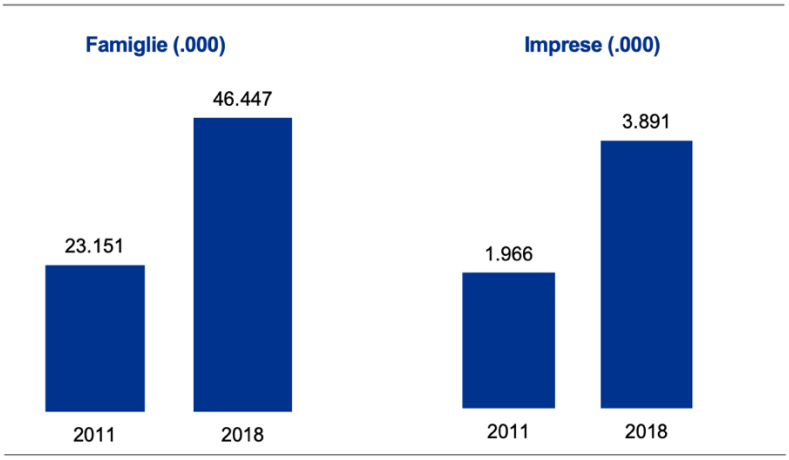
[18] Ibidem: Chase.com. "Online Banking vs. Traditional Banking: Exploring the Differences."

+21,5%. Tuttavia, tra gli italiani di età superiore ai 65 anni, il 71,2% afferma di non utilizzare Internet.[19]

L'evoluzione sociodemografica della popolazione italiana si manifesta nelle modalità di interazione con i fornitori di servizi bancari. Tra il 2011 e il 2019, si è confermato un aumento costante nell'uso del banking online da parte degli italiani, passando dal 20% al 36%. Tuttavia, questo livello corrisponde alla media europea del 2011, considerando che nel 2019 essa si attesta al 60%. Questi dati influenzano altresì le modalità con cui le famiglie e le aziende italiane utilizzano i servizi di *home banking* e *corporate banking*. Tra il 2011 e il 2018, come visibile dal *grafico 1*, si è assistito a un significativo aumento nell'uso del servizio di *home banking* da parte dei clienti privati, sia per reperire informazioni che per effettuare transazioni, con un incremento di 23,3 milioni di utenti, raddoppiando il numero iniziale. Parallelamente, l'utilizzo dei conti correnti aziendali per consultazioni e operazioni online ha registrato un forte aumento, raggiungendo 3,9 milioni di utenti nel 2019, quasi il doppio rispetto al 2011, con una crescita del 98%.[20]

**GRAFICO 1:**

**Internet banking: conti abilitati a servizi informativi e dispositivi online - Famiglie e Imprese (.000)**




*Fonte: elaborazione KPMG su dati Banca d'Italia*

[19] Cfr. Eurostat. "How Popular is Internet Use Among Older People?"

[20] Cfr. KPMG. Evoluzione dei modelli distributivi bancari: l'impatto del COVID-19 sui modelli di servizio delle banche italiane.

### 1.2.2. Cybersecurity nel settore bancario: strategie e complicazioni

Il settore bancario è un'area estremamente sensibile e cruciale per quanto riguarda la sicurezza informatica, richiedendo misure di difesa all'avanguardia e una strategia di sicurezza sistemica. Nell'era digitale, le istituzioni finanziarie sono diventate bersagli privilegiati per i criminali informatici, che utilizzano tecniche sempre più sofisticate per perpetrare frodi, furti e attacchi ai sistemi bancari. Le banche, infatti, gestiscono ampi volumi di transazioni finanziarie e custodiscono dati sensibili, rendendo di fatto imperativa l'adozione di tecnologie e robusti protocolli per la protezione contro intrusioni e attacchi informatici[21]. Questi attacchi non solo comportano significative perdite finanziarie dirette, ma possono anche infliggere danni duraturi alla reputazione delle istituzioni, erodendo la fiducia di clienti e investitori. Inoltre, le violazioni della sicurezza possono esporre le banche a severe penalità regolamentari, sottolineando l'importanza della conformità e della gestione proattiva dei rischi.[22]

Ma quali sono le forme attraverso cui questo tipo di criminalità viene manifestata?

Il cybercrime emerge con una varietà di tecniche, come il *phishing*, attacchi *malware*, attacchi *man-in-the-middle* e i *DDoS*, tutte accomunate dall'obiettivo di compromettere la sicurezza e l'integrità delle operazioni bancarie.

Pur condividendo la stessa volontà finalizzativa, tali misure criminali differiscono l'una dall'altra nei contenuti e nelle modalità di esecuzione.

Andando ad analizzarle nel dettaglio, è bene fornire delle definizioni che possano permetterci di comprendere pienamente le suddette[23]:

- Il *Phishing* è una tecnica di inganno che mira a truffare le vittime affinché condividano informazioni sensibili come password e dettagli delle carte di credito. Gli aggressori spesso inviano e-mail o messaggi che sembrano provenire da

[21] Cfr. PowerDmarc. "Sicurezza informatica nel settore bancario: Le principali minacce e i modi migliori per prevenirle."

[22] Cfr. S&P Global Ratings. "Cyber Risk Insights: European Banks' IT Complexity Amplifies Risk."

[23] Definizioni tratte da: OxfordLanguages

banche o istituti finanziari, inducendo le vittime a cliccare su link dannosi o a fornire dati personali.

- Parlando invece di quel che l'espressione "*attacchi malware*" indica, occorre soffermarsi sul termine "*malware*", che sintetizza la locuzione "*malicious software*" (software malevolo). Tale tecnica criminale implica vari tipi di software dannosi come *virus, worm, trojan e ransomware*, progettati per infiltrarsi, danneggiare o prendere il controllo di un sistema senza il consenso dell'utente.
- Tramite gli attacchi *Man-in-the-middle*, un esperto si inserisce nella comunicazione tra due parti, intercettando e potenzialmente alterando le informazioni trasmesse. In un contesto bancario, questo potrebbe significare l'intercettazione dei dati di un cliente mentre effettua un'operazione online.
- Infine, parlando degli attacchi *DDoS*, essi mirano a sovraccaricare le risorse di un sistema informatico, come i server di una banca, con una mole di traffico di dati eccessiva, così da renderlo indisponibile agli utenti legittimi. Spesso vengono utilizzate reti di computer infetti, chiamate *Botnet*[24], per generare questo traffico.

Il sistema di sicurezza informatica finanziaria è forte tanto quanto il suo anello più debole. È fondamentale disporre di una selezione di strumenti e approcci alla sicurezza informatica per proteggere dati e sistemi. Alcuni tra gli elementi essenziali per la sicurezza informatica sono: sorveglianza della sicurezza della rete, intesa come scansione continua di una rete alla ricerca di segnali di comportamento pericoloso o intrusivo; sicurezza del software, che consente l'elenco e la firma del codice ed ha un ruolo fondamentale per la sincronizzazione delle politiche di sicurezza con autorizzazioni di condivisione file e autenticazione a più fattori; gestione del rischio, che include la valutazione del rischio e la prevenzione dei danni derivanti da tali rischi, riguardando anche la sicurezza delle informazioni sensibili; protezione dei sistemi critici, per cui vengono sostenuti i rigidi standard di sicurezza stabiliti dal settore che gli utenti devono

[24] Computer Emergency Response Team AGID. "Con il termine Botnet, "rete di robot", si indica un insieme di computer o dispositivi che, precedentemente compromessi da parte di un malware, permette a un soggetto terzo di impartire istruzioni da remoto."

seguire quando adottano misure di sicurezza informatica per proteggere i propri dispositivi.[25]

Guardando al futuro, le banche devono continuare ad innovarsi al fine di gestire nel migliore dei modi le complessità poste dal cybercrimine, il quale molto spesso sottolinea ed agisce su nuove vulnerabilità dei sistemi, richiedendo dunque approcci di sicurezza rinnovati e adattivi.

### 1.2.3. Dall'erosione della fiducia ai danni reputazionali: Le conseguenze indirette del cybercrime nel settore bancario

Oltre alle perdite finanziarie dirette che potrebbero risultare da attacchi informatici, il settore bancario ne subisce di altre, diverse, che seppur indirette e spesso lasciate nell'ombra, necessitano di essere affrontate ed analizzate con occhio critico ed attento, in modo da render conto anche di quei risvolti non istantaneamente intuibili.

Tra essi, erosione della fiducia, danni reputazionali, ed implicazioni legali trovano un posto di estrema rilevanza.[26]

I consumatori, infatti, fanno affidamento sulle istituzioni finanziarie (banche, fondi, ecc.) per quanto riguarda la protezione dei loro dati personali e finanziari, per cui ogni violazione di tale fiducia è potenzialmente deleteria per la reputazione delle stesse. Per di più, la paura di essere vittime di crimini informatici nella propria sfera patrimoniale, può addirittura agire a monte, spingendo potenziali clienti a non utilizzare i servizi bancari, portando di conseguenza l'industria a generare meno profitti. Queste sono le motivazioni per cui lo sforzo impiegato per combattere il cybercrimine nel settore bancario debba prioritizzare la costruzione e il mantenimento della fiducia tra i consumatori, oltre che minimizzare la possibilità di subire attacchi informatici tramite una costante ottimizzazione e frequente attività di controllo dei propri sistemi informatici.

---

[25] Cfr. Knowledgehut. "La sicurezza informatica nel settore bancario: importanza, minacce, sfide."

[26] Sul punto si veda: Banca Centrale Europea. Vigilanza bancaria della BCE: Valutazione dei rischi e delle vulnerabilità per il 2021.

Fornendo un esempio circa i danni reputazionali cui gli attacchi informatici sono in grado di generare, osserviamo l'emblematico caso della violazione di dati subita, nel 2017, da *Equifax*, una delle più grandi agenzie statunitensi di valutazione del credito, che ha portato all'esposizione delle informazioni personali di oltre 150 milioni di clienti, provocando danni reputazionali e cause legali che hanno generato spese milionarie.[27] Le conseguenze di questa violazione sono state ampie. Numerose cause legali sono state intentate contro *Equifax*, e diverse indagini governative sono state avviate per esaminare la gestione dell'incidente da parte dell'azienda. Infine, *Equifax* ha raggiunto un accordo con la *Federal Trade Commission (FTC)* degli Stati Uniti e altri enti normativi, accettando di pagare fino a 700 milioni di dollari per compensare i consumatori colpiti e per migliorare le sue pratiche di sicurezza. Il danno reputazionale derivante da tale attacco è stato significativo e ha avuto implicazioni di lungo termine per l'azienda.[28] Le conseguenze, tuttavia, non si sono limitate alla perdita di fiducia da parte dei consumatori, coinvolgendo, infatti, ripercussioni anche sulla percezione del rischio da parte degli investitori e sulle valutazioni finanziarie dell'azienda. La gestione inadeguata della crisi, compreso il ritardo nella divulgazione dell'attacco e la mancanza di trasparenza, ha contribuito a rendere il danno reputazionale ancor più significativo. Quello di *Equifax*, un esempio che attesta l'importanza per le aziende del settore finanziario di dare priorità alla mitigazione dei rischi reputazionali legati alla governance e alla sicurezza dei dati.[29]

[27] Cfr. Mahawar, Sneha. "Cybercrime and Its Impact on the Banking Industry." IPleaders.

[28] Si veda: Federal Trade Commission. "Equifax, Inc.", July 31, 2019.

[29] Cfr. Hahn-Griffiths, Stephen. "The Equifax Breach Is a Reputational Crisis that Will Linger." RepTrack Company.

## 1.3 Sviluppi e tendenze emergenti del financial cybercrime

Il settore finanziario è frequentemente bersagliato da minacce ad opera di gruppi mossi da interessi economici, probabilmente a causa dell'evoluzione rapida dei servizi finanziari, stimolata dalla pandemia di *COVID-19*. Questo settore è vitale, fortemente interconnesso e dipendente da fornitori di servizi terzi essenziali.
Recentemente, le organizzazioni finanziarie si sono trovate a dover navigare in un ambiente sempre più sofisticato e specializzato, caratterizzato da un approccio prevalentemente opportunistico, dove le minacce di criminalità informatica sono estremamente redditizie. Tra queste minacce si annoverano attacchi come campagne di *Phishing*, furti di informazioni, violazioni di dati, ed utilizzo illecito di particolari e nuovi strumenti, come le cripto-attività e l'intelligenza artificiale.[30] Queste minacce, pur essendo solo poche delle molteplici che minacciano il settore economico-finanziario, colpiscono tanto le grandi istituzioni, che investono risorse economiche ed umane per contrastarle, quanto i portafogli dei comuni cittadini, che spesso finiscono per essere vittime di truffe e furti da parte di individui il cui unico scopo è arricchirsi a spese del prossimo.

### 1.3.1. Evoluzione strategica e tecnologia criminale

Durante l'esplorazione del vasto e complesso universo del cyberspazio, è necessaria la constatazione ed il riconoscimento di una realtà ove i criminali informatici non solo mantengono il passo con le innovazioni tecnologiche, ma spesso le anticipano, adattando con agilità le loro tattiche per sfruttare ogni nuova opportunità che emerge.
Nel 2023 abbiamo assistito ad una trasformazione radicale nel panorama della sicurezza informatica, segnando un'era di innovazioni guidate, in buona parte, dall'intelligenza artificiale. Da quando *OpenAI* ha lanciato *ChatGPT-3* nel novembre 2022, infatti, tali

[30] Cfr. Tibirna, Livia, Coline Chavane, and TDR (Threat Detection & Research). "Unmasking the Latest Trends of the Financial Cyber Threat Landscape." Io.Sekoia.blog.

strumenti tecnologici hanno giocato un ruolo cruciale sia nell'incremento delle difese di sicurezza, sia nell'elevazione della complessità degli attacchi cyber.

Questo avanzamento è accentuato dall'uso crescente dell'IA in scenari di cybercrime, complicato dall'incremento dell'*hacktivismo*[31] e di attacchi in contesti di crisi politica globale, e dall'espansione di campagne di disinformazione. L'utilizzo di *deepfakes* (video che mostrano corpi e volti raccolti online, trasformati e inseriti in un nuovo contesto attraverso un avanzato algoritmo di elaborazione)[32], e la clonazione vocale, hanno subito un incremento intimidatorio e minaccevole, andando di fatto a costituire sofisticati strumenti per la manipolazione sociale.[33] La *Federal Trade Commission* statunitense ha stimato che nel 2022, il danno economico risultante da queste attività illecite ammontava a 2,6 miliardi di dollari.[34]

La strategia adottata dai malintenzionati ha inizio con la raccolta, sulle piattaforme social, di dati sulle vittime e i loro familiari, comprese immagini e video. Utilizzando tecnologie avanzate, poi, vengono duplicate e riprodotte le voci delle persone con grande precisione. Questo processo, noto come *"clonazione vocale"*, viene applicato per realizzare frodi o estorsioni sfruttando la biometria vocale.[35] Nel 2023, l'intelligenza artificiale conta oltre 250 milioni di utenti e si prevede che raggiungerà i 700 milioni entro il 2030.[36]

Statistiche, le suddette, che sottolineano la repentina trasformazione di vari settori dell'economia globale ad opera dell'intelligenza artificiale, che nel 2024 contribuisce significativamente al successo di circa il 73% delle aziende americane.[37] Questa stessa tecnologia, tuttavia, non si limita a generare progresso economico; infatti, come abbiamo visto, svolge un ruolo cruciale anche nel settore della sicurezza informatica, dove funge sia da forza motrice per l'ottimizzazione dello stesso, sia da potenziale minaccia. Proseguendo il dibattito circa i pericoli insiti nell'evoluzione tecnologica, ad opera dei

---

[31] Cfr. Enciclopedia Treccani. "Hacktivism: Attivismo politico esercitato attraverso attacchi informatici."

[32] Cit: Enciclopedia Treccani. "Deepfake." Neologismi, 2018.

[33] Cfr. SoSafe. Cybercrime Trends 2024: The Latest Threats and Security Best Practices.

[34] Cit. Federal Trade Commission. "New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022."

[35] Si veda: Rainews.it. "Cybercrime, l'ultimo allarme dell'Intelligenza artificiale: clonare la voce delle vittime di truffa."

[36] Cfr. Statista. "Number of Artificial Intelligence (AI) Tool Users Globally from 2020 to 2030."

[37] Cfr: PwC. "2024 AI Business Predictions."

criminali informatici, è bene citare quello che, secondo i dati emersi da analisi ad opera dell'*FBI*, è il crimine digitale principale per numero di vittime nel 2022: il *Phishing*.[38]
Come già osservato nel paragrafo *1.2.1*, il *Phishing* è una tecnica che mira a truffare le vittime affinché condividano informazioni sensibili come password e dettagli delle carte di credito, con gli aggressori che raggiungono questo obiettivo inviando e-mail o messaggi che sembrano provenire da banche o istituti finanziari, inducendo le vittime a cliccare su link dannosi o a fornire dati personali.
Il settore bancario è il principale bersaglio delle campagne di *Phishing*. L'*Anti-Phishing Working Group (APWG)* rileva infatti che il 27,7% degli attacchi di questo genere, nel 2022, ha preso di mira proprio questo settore, colpendo importanti banche e servizi finanziari, tra cui nomi noti a livello globale come *PayPal*, *Crédit Agricole* e *La Banque Postale*.[39] Con il repentino sviluppo della tecnologia e dei servizi finanziari digitali, i cybercriminali hanno trovato terreno fertile per l'applicazione di furti e truffe digitali, tra cui il phishing si distingue come una tra le più pervasive ed insidiose.
Tale fenomeno incide negativamente anche nei confronti dell'innovazione tecnologica, generando scetticismo e minando la fiducia nei confronti di quegli strumenti digitali spesso annoverati come simbolo di un progresso finanziario sempre più indipendente dalle grandi istituzioni.
Fondamentale risulta, in tale contesto, il settore delle criptovalute, per nulla esente da questo tipo di attacchi, laddove è invece possibile osservare una relazione particolarmente preoccupante a causa della natura irreversibile delle transazioni *blockchain* e del valore spesso elevato associato a questi asset digitali.[40]

---

[38] Cfr: Federal Bureau of Investigation. Internet Crime Report, 2022, Internet Crime Complaint Center.

[39] Cfr. Tibirna, Livia, Coline Chavane, and TDR (Threat Detection & Research). "Unmasking the Latest Trends of the Financial Cyber Threat Landscape." Io.Sekoia.blog.

[40] Cit. United States Senate Committee on Homeland Security & Governmental Affairs. U.S. Senator Gary Peters, Chairman. "Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns."

### 1.3.2. Crypto-assets: rischi ed opportunità [41]

L'evoluzione tecnologica ha visto l'evolversi, negli ultimi anni, di nuove categorie di servizi, tra cui quella delle cripto-attività che, pur essendo destinati a svolgere molteplici funzioni, in particolare quella di pagamento, sono accumunati dalla caratteristica di essere emessi e scambiati utilizzando un nuovo meccanismo tecnologico, la c.d. *Distributed Ledger Technology* (*DLT*), o *Blockchain* ("catena di blocchi").

Si può parlare di tale tecnologia come un registro informativo che utilizza tecnica crittografica al fine di memorizzare informazioni e transazioni in modo certo, appurabile e permanente. Una rete Blockchain è composta da diversi nodi che svolgono il ruolo di punti di ingresso e di uscita per i dati, essendo poi ognuno responsabile della convalida delle transazioni e dei blocchi per assicurarne la validità.[42] Il settore delle criptovalute ha subito un'evoluzione tumultuosa: già nel 2019, un rapporto dell'*ESMA* (*European Securities and Market Authority* [43]) ne menzionava oltre 2050.[44]

Oggi, nonostante i problemi manifestati da un mercato ancora instabile, il numero è di gran lunga superiore.

In particolare, questo settore ha visto, dopo l'introduzione di *Bitcoin*, la diffusione di cripto-attività nel contesto di *Initial Coin Offerings* (*ICOs*), ossia di operazioni volte alla raccolta di capitali sul mercato, frequentemente in relazione con il debutto di nuove iniziative imprenditoriali, nuovi servizi, startup, correlati o meno al settore tecnologico, in competizione con le *Initial Public Offering (IPO)* e l'*equity crowdfunding.* Contrariamente a questi ultimi, però, una ICO comporta l'emissione di *coin* o *token digitali*, anziché strumenti finanziari convenzionali come, per esempio, le azioni. I *token* vengono offerti agli investitori che li acquistano contro denaro o, più comunemente, mediante criptovalute (in particolare *Bitcoin* ed *Ethereum*). La generazione, l'emissione e la circolazione dei *token* avvengono per mezzo della *blockchain*.

---

[41] Cfr. Annunziata, Filippo, et al. Cripto attività: antiriciclaggio e gestione dei rischi aziendali. Pisa: Pacini giuridica, 2024.

[42] Cit. Sharma, Pradip Kumar, Mu-Yen Chen, and Jong Hyuk Park. "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT."

[43] Trad: Autorità europea degli strumenti finanziari e dei mercati

[44] Cfr. ESMA50-157-1391. "Advice on Initial Coin Offerings and Crypto-Assets," January 9, 2019.

Nei primi anni del fenomeno, l'assenza di una normativa dettagliata per queste attività ha permesso una vasta diffusione delle ICOs a livello globale.[45]

Si sono poi affermate grandi piattaforme di scambio dei *token*, con la creazione di un vasto mercato secondario, per lo più non regolamentato e opaco.

I crypto-assets, in attesa di risposte regolatorie da parte di singoli Stati e comunità internazionali, hanno conosciuto anche un ampio fenomeno circolatorio. Le piattaforme di scambio tramite cui vengono acquistate e vendute le cripto-attività (*exchanges*) nacquero al di fuori di una specifica regolamentazione, ma, col passare del tempo, hanno posto problemi sempre più evidenti circa la loro natura, soprattutto legati all'incerta qualificazione di molti asset.

Nel 2021-2022 in un quadro regolatorio incerto e spesso carente, si sono verificati diversi fenomeni di crisi e frodi ai danni di grandi e piccoli operatori: si è parlato, a proposito, di un vero e proprio "*crypto-winter*" per riferirsi ad un periodo particolarmente opaco dello sviluppo di questi mercati, che urlava a gran voce la necessità di una risposta legislativa il più possibile decisa e coordinata a livello anche transnazionale.[46]

Lo sviluppo del mercato dei crypto-assets, nello specifico, coincide con la nascita di un settore che impiega tecnologia innovativa e offre nuovi servizi caratterizzati da un approccio *peer-to-peer* [47] e dall'uso della crittografia ai fini di tutela della privacy.

La comparsa di un "registro pubblico", all'interno del quale sono chiaramente visibili le transazioni che vi vengono registrate, e la inconoscibilità dei soggetti che le sottoscrivono in virtù del ricorso alla tecnica crittografica, se da un lato favorisce lo sviluppo dell'ecosistema, dall'altro lo rende attraente per attività illecite, che ne sfruttano le caratteristiche per l'occultamento e il riciclaggio di denaro.

Da un punto di vista generale, utilizzare la *DLT* e la *blockchain* per la realizzazione di attività illecite appare un vero e proprio controsenso, dal momento che il "registro pubblico" permette appunto di poter vedere e controllare i flussi dei crypto-assets tra i diversi portafogli. Questo, tuttavia, non sembra scoraggiare i criminali, che continuano ad utilizzare *blockchain* e criptovalute come mezzi di movimentazione dei loro guadagni illeciti. Le ragioni di tale atteggiamento sono ancora in buona parte da indagare ma, ad

---

[45] Cfr. Sandei, Claudia. L'offerta iniziale di cripto-attività. Torino: Giappichelli, 2022.

[46] Cfr. Forbes Advisor. "L'inverno delle criptovalute sta arrivando: tutto quello che devi sapere sul crypto winter."

[47] Trad. "Da pari a Pari"

una prima analisi, si è portati a ritenere che caratteristiche come la crittografia, la facilità di trasferimento dei fondi anche in ambito internazionale e la volatilità del valore di questi assets facilitino la gestione finanziaria delle attività illecite poste in essere dai criminali informatici. Pur rimanendo una quota relativamente piccola (0,24%) rispetto al volume totale delle transazioni in crypto-assets, il volume di attività illecite ha comunque registrato per la prima volta una crescita dal 2019.[48]

Secondo gli ultimi dati sui crimini commessi in questo mondo[49], il 2022 è stato un anno durante il quale il volume delle transazioni illecite osservabili sulla *blockchain* ha raggiunto i 20,6 miliardi di dollari, rappresentando, in valore assoluto, il dato più alto dal 2017, nonostante la flessione del volume delle transazioni totali legata alla crisi che ha attraversato il settore crypto nel 2022, generata dai gravi scandali che hanno coinvolto importanti operatori del mercato, dall'azione di controllo e repressione sulle attività illecite condotta da alcune autorità e dall'ondata ribassista che ha avuto inizio nel dicembre 2021 sulle principali criptovalute (*Bitcoin* ed *Ethereum*, entrambe determinanti nella capitalizzazione del settore).

### 1.3.3. Quadro normativo delle cripto-attività: MiFID II; Digital Finance Package; MiCA

Uno degli aspetti degli ultimi anni, che seppur fondamentale non ha saputo, in molte situazioni e aree geografiche, mostrare la reale esigenza di espletamento cui effettivamente avrebbe cambiato le sorti di tanti avvenuti eventi criminali, è rappresentato da un ben definito quadro normativo che vada a disciplinare il novello settore delle cripto-attività. L'assenza di un sistema di norme specifico per tali attività, ha creato un ambiente di incertezza riguardo alla possibilità di applicare, seppur per analogia, le varie normative esistenti, come quelle relative agli strumenti finanziari, all'offerta al pubblico e ai servizi di investimento. Questo ha favorito la nascita e l'evoluzione di fenomeni di

[48] Cfr. Collins, John. "Crypto, Crime and Control; Cryptocurrencies as an Enabler of Organized Crime." June 2022.

[49] Cit. Chainalysis. "Report sui Crimini Crypto." February 2023.

diversa natura, inclusi alcuni di natura criminale. Mentre gli organismi internazionali, inclusi il *Financial Stability Board (FSB)*, la *Banca per i Regolamenti Internazionali (BIS)* e il *Gruppo di Azione Finanziaria (FATF)*, procedono nell'elaborazione di linee guida universali per la regolamentazione del fenomeno della criptovaluta, anche per quanto riguarda la prevenzione del riciclaggio di denaro e del sostegno finanziario al terrorismo, l'Unione Europea ha anticipato tali movimenti.[50]

Nel settembre del 2020, infatti, l'Unione Europea ha concretamente intrapreso un percorso legislativo in quest'ambito, introducendo il *Digital Finance Package*, collocandosi in una posizione di avanguardia rispetto ad altri paesi e sistemi regolamentari, rappresentando per essi un punto di riferimento nella regolazione di questi fenomeni. Tale pacchetto legislativo si articola attraverso due direttrici strategiche principali: la *"Digital Finance Strategy"* e la *"Retail Payments Strategy"*.

Nell'ambito della *Digital Finance Strategy*, emerge in modo preponderante il regolamento sui crypto-assets, noto come *"Markets in Crypto Assets Regulation" (MiCA o MiCAR)*. Ad esso viene affiancato il regolamento *"Pilot Regime for DLT-based Market Infrastructures"*, destinato ai mercati di capitali che adottano tecnologie basate sulla *DLT*, e il *"Digital Operational Resilience Act" (DORA)*, che si occupa di resilienza operativa digitale nel settore finanziario.[51] Dopo un esteso dibattito, alimentato anche da recenti sviluppi del mercato in Europa e negli USA, il testo finale del *Regolamento MiCA* è stato pubblicato nella Gazzetta Ufficiale il 9 giugno 2023, entrando in vigore il 29 dello stesso mese, con applicabilità a partire dal 30 dicembre 2024.[52] Gli obiettivi del Regolamento coprono vari aspetti del mercato delle cripto-attività: la certezza del diritto, per favorire lo sviluppo di questi mercati all'interno dell'Unione Europea attraverso un quadro giuridico chiaro e robusto; il sostegno all'innovazione, essendo tale regolamento parte di un contesto più ampio volto a promuovere lo sviluppo degli strumenti basati su *DLT* per stimolare innovazione e concorrenza; ed infine la garanzia di adeguati livelli di protezione per consumatori e investitori, e di integrità del mercato, dato che gli asset crittografici non

---

[50] Cfr. Lifshits, I. "Cryptocurrencies in the Regulatory Field of International Organizations." In "Current Achievements, Challenges and Digital Chances of Knowledge-Based Economy", edited by S.I. Ashmarina and V.V. Mantulenko.

[51] Cfr. PwC Insights. "A Brief Run-Through of the European Union's Digital Finance Package."

[52] Cfr. Gazzetta ufficiale dell'Unione europea. "REGOLAMENTO (UE) 2023/1114." L 150/40.

regolamentati presentano rischi simili a quelli degli strumenti finanziari più tradizionali.[53]
In parallelo agli obiettivi del *MiCA*, la direttiva *MiFID II* continua a svolgere un ruolo fondamentale nel settore finanziario tradizionale, migliorando la trasparenza e la protezione degli investitori [54], principi ora estesi alle cripto-attività, dimostrando, nonostante le varie incompatibilità strutturali, l'adattabilità e la complementarità delle normative europee nell'ambito finanziario e tecnologico.
In tal senso, il *Regolamento MiCA* emerge come un ponte verso l'innovazione nel settore crypto, basandosi su solide basi derivanti dalla *MiFID II*. Infatti, mentre quest'ultima ha tracciato la strada per una maggiore trasparenza e affidabilità nei tradizionali mercati finanziari, il *Regolamento MiCA* estende tali principi al mondo digitale, con l'obiettivo di ispirare fiducia e sicurezza in un settore in precedenza esplorato solo marginalmente.[55]
Il connubio tra questi due regolamenti evidenzia l'impegno dell'Unione Europea nel plasmare un ambiente finanziario che possa essere al contempo innovativo e protetto, che favorisca il processo di ottenimento di fiducia da parte degli investitori persino verso quelle logiche di investimento legate a strumenti nuovi e poco conosciuti.[56]

# *2.* Giurisprudenza e tecnologia: influenze reciproche

## 2.1 Accordi e misure legislative comunitarie ed internazionali

Lo sviluppo tecnologico e la rivoluzione digitale, insieme all'intelligenza artificiale, sollecitano e impongono un aggiornamento continuo del diritto, essenziale affinché esso possa coprire, come suo campo, i fenomeni emergenti e mantenere il suo ruolo normativo e la sua efficacia, utilizzando l'intero arsenale di strumenti a sua disposizione:

---

[53] Cfr. European Commission. "Digital Finance Package." Directorate-General for Financial Stability, Financial Services and Capital Markets Union. September 24, 2020.

[54] Cit. Pellegrini, Mirella, ed. "Diritto Pubblico Dell'Economia."

[55] Cfr. Dirittobancario.it. "MiCAR: Le Prossime Misure di Attuazione per i Mercati delle Cripto-Attività."

[56] Cfr. Nicotra, Massimiliano, Fulvio Sarzana di S. Ippolito, and Massimo Simbula. "Micar - Guida al Regolamento Europeo sui Mercati dello Cripto". Milano: Giuffrè Francis Lefebvre, 2023.

dall'interpretazione evolutiva, dalla modifica o creazione di nuove leggi, alla formulazione di categorie concettuali e dottrinali innovative.

Per lungo tempo, e ancora oggi in certi contesti, è sopravvissuto l'ideale utopico secondo il quale la rete sia uno spazio esente dal diritto, un rifugio di anarchia e libertà assoluta, non soggetto al controllo degli Stati, legati alla materialità dei loro territori e confini geografici, dentro i quali si potrebbe esercitare la sovranità.[57] A conferma di ciò, vi è l'attuale e autorevole spinta condivisa per una "*Costituzione per Internet" (Bill of rights)*[58], ovvero un insieme di diritti fondamentali da riconoscere e proteggere su scala globale, a partire dalla reinterpretazione di quelli già esistenti nelle Carte e Convenzioni internazionali. Di fronte alla necessità di assicurare una protezione effettiva e possibilmente uniforme di questi diritti e interessi a livello globale, sorge la necessità di implementare sistemi "armonizzati" di incriminazioni e sanzioni, per condividere ed estendere buone ed efficienti pratiche di applicazione, rafforzando la sempre più indispensabile cooperazione internazionale, che deve coinvolgere, oltre ai singoli stati, anche il settore privato e le varie parti interessate, inclusi organismi e associazioni che rappresentano interessi diffusi e collettivi.

### 2.1.1. Accordi internazionali sulla criminalità informatica: Convenzione di Budapest e Direttive NIS

Nell'epoca digitale, lo sviluppo degli ambiti di operazione della criminalità informatica ha reso imperativa l'adozione di un approccio legislativo coordinato e comunitario, che potesse di fatto andare a sopperire alle lacune generate da un precedente sistema frammentario ed isolato, Stato per Stato. Al riguardo, infatti, si è assistito all'introduzione di strumenti giuridici multilaterali, essenziali per stabilire un fronte unito contro le sfide generate da atti criminosi nel cyberspazio. Gli strumenti legislativi, oggetto di quanto accennato, sono principalmente due: *la Convenzione di Budapest* e le *Direttive NIS (1 e*

[57] Cfr. Ziccardi. Hacker. Il Richiamo della Libertà. Milano, 2011.

[58] Sullo stesso ordine di idee si veda: Yilma, Kinfe. "Privacy and the Role of International Law in the Digital Age." In "Internet Bills of Rights." Chapter 4.

*2).* Dibattendo circa gli ambiti di applicazione e le effettive risoluzioni normative cui la Convenzione, sottoscritta a Budapest il 23/11/2001, è stata promotrice, è bene sottolineare che essa fu disposta e firmata in un periodo storico in cui ancora non poteva essere apprezzata la bontà sottostante a specifiche norme utili alla lotta al cybercrime, essendo essa, di fatto, stata ratificata solamente nel 2008 con la *L. 18.3.2008, n. 48*.[59] La suddetta, visse uno sviluppo caratterizzato da grande attenzione, dovuta dalle previsioni di quelle che sarebbero state le eventuali sfide della prospettiva investigativa e tecnologica.

L'obiettivo principale era formulare una politica penale unitaria per difendere la società contro il cybercrime, soprattutto attraverso una normazione appropriata di leggi e il potenziamento della cooperazione internazionale. Risultato di un impegno quadriennale da parte di un comitato di esperti creato specificamente dal Consiglio d'Europa, la Convenzione include regole generali per i reati informatici classici e, in particolare, dettagliate disposizioni riguardanti la raccolta, la conservazione e l'acquisizione delle c.d. "*digitalevidences"*.[60]

Nello specifico, essa si concentra su tre aree principali[61]: armonizzazione delle leggi nazionali; misure procedurali e tecniche; cooperazione internazionale.

Con riferimento alla prima area, la Convenzione prevede che gli stati aderenti adottino una legislazione comune per definire e perseguire i reati informatici, tramite norme che includono il trattamento di atti come l'accesso non autorizzato, l'interferenza nei sistemi e nei dati, e la frode informatica. Obiettivo di tale aspetto della Convenzione è eliminare le discrepanze legislative tra i paesi, migliorando così l'efficacia verso il contrasto al cybercrime su scala internazionale.

Relativamente alle misure procedurali e tecniche, seconda area trattata dalla Convenzione oggetto di analisi, è corretto sostenere che esse, indispensabili per abilitare i paesi membri a contrastare in modo efficace il cybercrime, delineano le modalità con cui le autorità hanno la facoltà di perquisire e confiscare apparati informatici, conservare i dati per prevenirne la distruzione, o eventuali modifiche, e raccogliere prove digitali (le

---

[59] Cfr. Cadoppi, Alberto. "Cybercrime." 2nd ed. Torino: UTET Giuridica, 2023.

[60] Cit. Cybercrime Convention Committee (T-CY). "The Budapest Convention on Cybercrime: Benefits and Impact in Practice."

[61] Si veda: Csigbologna. "Convenzione di Budapest sulla Criminalità Informatica a 20 Anni dall'Approvazione."

*digitalevidences* di cui sopra) in modo conforme alla legge e tecnicamente appropriato. Queste, risorse fondamentali per garantire che le indagini sui crimini informatici vengano effettuate rispettando le normative vigenti.[62]

In merito alla terza area esaminata dalla Convenzione di Budapest, dedicata alla cooperazione internazionale, è appropriato evidenziare che le disposizioni che la compongono descrivono come le autorità possano scambiarsi assistenza legale e informazioni rapidamente, nonché implementare procedure condivise per affrontare reati che superano i confini nazionali, in modo da assicurare indagini coordinate e conformi agli schemi globalizzati di un tipo di criminalità esente da fisici confini.[63]

Con esplicito riferimento alla cooperazione tra le autorità internazionali e facilitazione delle procedure di indagine, riveste un ruolo fondamentale quello che prende il nome di *"Second Additional Protocol"*[64] (secondo protocollo addizionale), che introduce specifiche disposizioni di trasparenza, come la possibilità per le autorità di richiedere direttamente ai fornitori di servizi digitali, anche esteri, ragguagli necessari per le indagini in fase di svolgimento, incluse informazioni sugli abbonati e dati di traffico, tramite strumenti di assistenza bilaterale. Il protocollo, d'altra parte, pone un forte accento sulla protezione dei dati personali e sulla necessità di trovare un equilibrio circa la sicurezza e la privacy degli individui, introducendo rigorose garanzie per la tutela delle informazioni sensibili. Misura legislativa che, per quanto condivida gli stessi obiettivi e propensioni della Convenzione di Budapest, risulta essere a sé stante, è costituita dalla *Direttiva NIS*, e come vedremo dopo, dalla *Direttiva NIS 2*.

*La Direttiva NIS 1 (Direttiva (UE) 2016/1148)*, nota come *"Network and Information Security",* è stata adottata il 6 luglio 2016, con recepimento fino al 9 maggio 2018 per gli Stati membri (in Italia tramite il *d.lgs. 65/2018, detto "Decreto NIS"*)[65]. Questa normativa distingue due principali categorie di entità alle quali si applicano specifiche

---

[62] Cfr. Parodi, Cesare, and Valentina Sellaroli, eds. "Diritto Penale dell'Informatica". Milano: Giuffrè, 2024.

[63] Cfr. The Budapest Convention on Cybercrime: benefits and impact in practice

[64] Cfr. Council of Europe. "Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224)."

[65] Cfr. European Union Agency For Cybersecurity: NIS Directive

disposizioni[66]: gli *Operatori di servizi essenziali (OSE)*, che comprendono enti pubblici e privati essenziali per il funzionamento della società e dell'economia, i quali devono essere individuati direttamente dai singoli Stati membri nei settori chiave in base alla criticità del servizio, e i *Fornitori di servizi digitali (FSD)*, che includono aziende che offrono servizi di e-commerce, cloud computing o motori di ricerca, a meno che non rientrino nella categoria delle PMI. Viene poi assegnata ai singoli Stati la facoltà di estendere la portata degli obblighi a ulteriori categorie.[67]

Le richieste specifiche della Direttiva includono la formulazione di una strategia nazionale per la sicurezza cibernetica che stabilisca obiettivi e priorità, l'assicurazione della cooperazione internazionale, la collaborazione con l'*ENISA (Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'Informazione)*, e la designazione di autorità nazionali competenti e del *CSIRT (Computer Security Incident Response Team)*, incaricati del monitoraggio degli incidenti a livello nazionale.

Per quanto riguarda *OSE* e *FSD*, la *Direttiva NIS 1* prevede l'adozione di misure di sicurezza proporzionate al rischio e volte a ridurre l'impatto degli incidenti, nonché la segnalazione tempestiva agli enti competenti di incidenti che influenzino significativamente la continuità dei servizi essenziali.[68]

Ciononostante, la *Direttiva NIS 1* presentava vari limiti, come, ad esempio, la vaghezza nei criteri di segnalazione e una insufficiente copertura delle minacce, che hanno portato alla sua abrogazione e alla conseguente *Direttiva NIS 2*. Adottata il 14 ottobre 2022, la nuova direttiva *(Direttiva (UE) 2022/2555)* mira a eliminare le discrepanze tra i vari ordinamenti nazionali, rafforzando le disposizioni di sicurezza cibernetica, espandendo i settori e le entità coinvolte e intensificando la cooperazione interstatale per una maggiore uniformità applicativa.[69]

---

[66] Cfr. Paracampo, Maria-Teresa. "FinTech: Introduzione ai Profili Giuridici di un Mercato Unico Tecnologico dei Servizi Finanziari". 2nd ed. Torino: Giappichelli, 2019.

[67] Sullo stesso ordine di idee si veda: CyberItalia. "Dalla Direttiva NIS 1 alla NIS 2 in Pillole."

[68] Cfr: "Gazzetta ufficiale dell'Unione europea". "DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO." December 14, 2022.

[69] Cfr. KPMG. "Network & Information Security Directive (NIS2)."

La *Direttiva NIS 2* elimina la distinzione tra *OSE* e *FSD*, sostituendoli con categorie basate su nuovi criteri, che identificano soggetti "essenziali" e "importanti", mantenendo fuori dall'ambito di applicazione le piccole e medie imprese, tranne alcune eccezioni.[70]
In definitiva, la *Direttiva NIS 2* amplia notevolmente gli obblighi della *Direttiva NIS 1*[71], enfatizzando un approccio multirischio, caratterizzato dall'adozione di misure di sicurezza adatte, riduzione dell'impatto degli incidenti, e definizione di uno schema preciso per la segnalazione e la notifica di incidenti rilevanti alle autorità competenti e al *CSIRT*, imponendo inoltre agli Stati di adottare misure di sorveglianza per i soggetti ritenuti essenziali e importanti, e di incrementare gli obblighi di condivisione delle informazioni relative alla sicurezza informatica.[72]

### 2.1.2. Analisi del fenomeno della criminalità organizzata internazionale nell'era digitale

Il fenomeno della criminalità organizzata su scala internazionale costituisce una minaccia rilevante per i sistemi economici e finanziari globali, rendendo imprescindibile una serie di interventi coordinati, volti a garantire che il processo di globalizzazione possa procedere senza ostacoli od infiltrazioni criminali nei suoi elementi strutturali.[73]
Dalla necessità di movimentare persone e merci attraverso i confini dell'Unione Europea, le organizzazioni criminali hanno istituito strutture e reti operative in ciascuno stato membro, sfruttando in alcuni casi le discrepanze legislative o la limitata efficacia delle misure di controllo da parte delle autorità locali.[74]

---

[70] Cfr. Dragomir, A. V. "What's New in the NIS 2 Directive Proposal Compared to the Old NIS Directive." SEA: Practical Application of Science, 2021.

[71] Sullo stesso ordine di idee si veda: CyberItalia. "Dalla Direttiva NIS 1 alla NIS 2 in Pillole."

[72] Cfr. Schmitz-Berndt, Sandra. "Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive." Journal of Cybersecurity.

[73] Cfr. Savona. "Processi di Globalizzazione e Criminalità Organizzata Transnazionale."

[74] Cfr. Laudati. "I Delitti Transnazionali, Nuovi Modelli di Incriminazione e di Procedimento all'interno dell'Unione Europea."

Di conseguenza, si è resa necessaria l'elaborazione di sistemi di perseguimento penale e strategie di contrasto coordinate tra i vari paesi, che possano rispondere collettivamente alla minaccia, indipendentemente dalla sua complessità. Riguardo alla criminalità informatica e al contesto virtuale, è lecito affermare che aspetti come la collaborazione e il coordinamento internazionale hanno subito l'impatto delle trasformazioni apportate dalla digitalizzazione, che ha modificato, parallelamente alla vita quotidiana dei cittadini, anche l'ambito investigativo. Oggi, dopo quasi vent'anni, l'investigatore moderno è inevitabilmente immerso in una dimensione parallela, impalpabile, costituita dal cyberspazio.[75]

La criminalità contemporanea ha saputo rapidamente sfruttare le possibilità offerte dall'evoluzione tecnologica, adottando innovativi canali di comunicazione nell'ambito criminale, e individuando contestualmente luoghi ideali per le proprie operazioni illecite. Un'analisi operativa condotta da *Eurojust*[76] mette in luce la presenza di entità criminali in continua evoluzione, dotate di una notevole capacità di adattamento alle innovazioni tecnologiche. Queste organizzazioni esibiscono una competenza digitale avanzata, segnale evidente della loro evoluzione e potenziamento operativo. L'incorporazione del digitale nelle loro operazioni ha marcato un cambiamento significativo, manifestando una considerevole destrezza nel bypassare i controlli attraverso l'utilizzo di tecnologie che ne assicurano l'indecifrabilità. Tali gruppi, infatti, fanno uso di piattaforme criptate e metodi di accesso al *dark web*[77] per comunicare, impiegando allo stesso tempo complessi sistemi di sorveglianza elettronica per monitorare le zone di interesse.

Parallelamente, è possibile notare una crescente inclinazione verso l'instaurazione di reti operative e l'adozione di economie di scala, che trasformano significativamente il modo

---

[75] Sullo stesso ordine di idee si veda: Sistema Penale. "Minaccia Cibernetica e Nuovi Paradigmi della Cooperazione Giudiziaria Internazionale: Il Ruolo di Eurojust." July 14, 2023.

[76] Cfr. "Gazzetta ufficiale dell'Unione Europea". "Conclusioni del Consiglio «Sinergie tra Eurojust e le Reti Istituite dal Consiglio nel Settore della Cooperazione Giudiziaria in Materia Penale» (2019/C 207/01)."

[77] Definizione tratta da Enciclopedia Treccani. "Il Dark Web, Accessibile Solo Tramite Software Specifici, è il Teatro di Attività Illecite come il Traffico di Armi e Droga, Influenzando Anche Rappresentazioni Artistiche e la Percezione Pubblica dei Media di Massa."

in cui le diverse organizzazioni fanno business, orientato sempre più verso un'ottica affaristica globale.[78]

Questa dinamica si manifesta anche nella fattispecie costituita dalla minaccia terroristica, ove l'impiego del digitale è particolarmente marcato. I gruppi terroristici utilizzano, infatti, siti web, social network, forum e altre piattaforme online per la diffusione di contenuti propagandistici e per il reclutamento di adepti, nonché per l'indottrinamento, il finanziamento, la promozione e l'incitamento a compiere atti terroristici. Questi strumenti digitali costituiscono alcune delle risorse più potenti a disposizione, ad esempio, dei *jihadisti* [79], paragonabili all'importanza di armi o esplosivi.[80]

### 2.1.3. Cooperazione transfrontaliera: Europol, Eurojust, Interpol, ENISA

Avendo dunque sottolineato l'importanza della cooperazione tra le varie autorità a livello internazionale, al fine di prevenire e minimizzare la criminalità organizzata, talvolta digitale, è bene porre maggiore attenzione sulle suddette autorità, delineandone il profilo e i tratti che le differenziano l'una dalle altre. *Europol*, *Eurojust*, *Interpol*, la "*FBI - Europol Cyber Task Force*", ed *ENISA* sono le principali autorità impegnate nella lotta alla criminalità, con attenzione specifica ai tratti più globalizzanti di essa.

Quando parliamo di *Europol*, facciamo riferimento al fulcro della lotta alla criminalità grave e organizzata a livello internazionale. In qualità di agenzia di polizia criminale dell'Unione Europea, essa ha un ruolo fondamentale negli aspetti gestionali di quelle questioni criminali legate soprattutto ai reati perpetrati nel cyberspazio. Sotto tale aspetto, l'*Europol* ha fondato il *Centro Europeo per la Lotta al Cybercrime (EC3)*, che si dedica

---

[78] Cit. Risk & Compliance: Platform Europe. "L'infiltrazione della Criminalità Organizzata nell'Economia Italiana: dalla Prevenzione al Contrasto."

[79] Definizione tratta da - Enciclopedia Treccani. "Fenomeno Terroristico Armato che Invoca il Principio-Dovere Islamico del Jihād, alla Luce del Pensiero più Radicale del Cosiddetto "Fondamentalismo Islamico"."

[80] Cfr. InsideOver. "Così Terrorismo e Criminalità Sfruttano il Lato Oscuro dei Social Media."

a numerosi aspetti della prevenzione e del contrasto di diverse forme di criminalità informatica.[81]

Per quanto riguarda i reati finanziari, nello specifico, *Europol* ha istituito il *Centro Europeo per i Reati Economici e Finanziari (EFECC)*, che incentiva il coerente utilizzo delle indagini finanziarie e la confisca di beni, collaborando con organizzazioni pubbliche e private.[82] L'*EFECC* si impegna, in particolare, a fornire assistenza operativa e analitica nelle indagini concernenti i reati economici e finanziari, tra cui corruzione, contraffazione, falsificazione di denaro, frode fiscale e riciclaggio, frequentemente perpetrati tramite l'utilizzo di tecnologie digitali.

Dunque, mentre l' *Europol*, come abbiamo visto, costituisce l'agenzia di polizia dell'UE che si concentra sull'aspetto investigativo e di intelligence, fornendo analisi e facilitando lo scambio di informazioni tra le forze di polizia nazionali, *Eurojust*, che rappresenta l'agenzia dell'Unione Europea per la cooperazione giudiziaria penale, offre supporto alle autorità nazionali in indagini penali transnazionali, affrontando le problematiche dettate da quella tipologia di organizzazioni criminali che rende internazionale il suo operato, agendo al di fuori dei confini di un determinato paese. *Eurojust*, nello specifico, ha come obiettivo primario il rafforzamento del coordinamento e della collaborazione tra le autorità giudiziarie dei paesi membri.[83]

Essa supporta dal punto di vista operativo e strategico le indagini e le azioni penali su vasta scala, compresa la gestione di complessi casi di cybercrime che possono includere frodi, attacchi *ransomware* e l'uso illecito di piattaforme di comunicazione crittografata, occupando dunque un ruolo fondamentale nella lotta al cybercrime e i reati finanziari spesso tra loro correlati.

Nel contesto del cybercrime, *Eurojust* supporta gli Stati membri fornendo assistenza nelle indagini relative alle piattaforme di comunicazione cifrata, gestendo migliaia di casi

---

[81] Cfr. Europol.europa.eu. "Cybercrime."

[82] Cfr. Europol.europa.eu. "European Financial and Economic Crime Centre – EFECC."

[83] Cfr. EuropeanUnion.Europa.eu. "European Union Agency for Criminal Justice Cooperation: 3.8 Cybercrime."

derivanti dalle indagini su piattaforme come *EncroChat* e *Sky ECC* dal 2020, ospitando anche la *Rete Giudiziaria Europea per il Cybercrime* presso la propria sede.[84]

*Eurojust* è impegnata anche sul fronte di quelle sfide significative strettamente legate al financial cybercrime, che colpisce istituzioni finanziarie e infrastrutture nazionali sotto forma di una vasta gamma di attività criminali, come il furto di dati sensibili o attacchi informatici su larga scala, che possono avere ripercussioni profonde sulla sicurezza finanziaria nazionale[85], cui l'*Eurojust* si prefigge di salvaguardare tramite l'uso di strumenti come l'*Ordine di Indagine Europeo* e il *Mandato d'Arresto Europeo*, fondamentali nella lotta al cybercrime nella sua natura transnazionale.

Diversamente dall'*Europol* per quanto riguarda struttura, ambito operativo e modalità d'intervento, l'*Interpol* è la più vasta organizzazione di polizia internazionale con 194 paesi membri[86], dedita a coordinare operazioni riguardo vari aspetti del mondo criminale, che vanno dal sostegno in termini di cattura ed estradizione, alla ricerca di persone scomparse, identificazione di cadaveri e contrasto al crescente fenomeno della criminalità organizzata transnazionale, incluse quelle operazioni legate al traffico di droga, traffico di esseri umani ed armi, riciclaggio di denaro e criminalità informatica. Attraverso il suo *Centro per i Crimini Finanziari e Anti-Corruzione (IFCACC)*, l'*Interpol* svolge attivamente il proprio ruolo di supporto per quanto riguarda il tracciamento di sospetti che attraversano i confini internazionali, e nell'emissione dei cosiddetti "*Notices*", ovvero avvisi di ricerca internazionali.[87] L'*Interpol*, tuttavia, non possiede agenti con poteri di arresto diretti, fungendo piuttosto da facilitatore per la cooperazione tra le forze di polizia nazionali.

Sottolineando l'importanza della collaborazione internazionale nel contrasto al cybercrime, occorre porre lo sguardo sulla "*FBI-Europol Cyber Task Force*", un'iniziativa congiunta tra il *Centro Europeo per la Criminalità Informatica (EC3)* di

---

[84] Ivi. European Union Agency for Criminal Justice Cooperation: 3.8 Cybercrime; Operational support to cybercrime cases

[85] Sullo stesso ordine di idee si veda: Rusi.org: Financial Institutions and Cybercrime: Threats, Challenges and Opportunities

[86] Cit. Interpol.int - What is Interpol?

[87] Cfr. Interpol.int: Our role in fighting financial crime

*Europol* precitato, e l'*FBI*, creata appositamente per contrastare il cybercrime e i reati finanziari tramite strumenti digitali.[88]

Tale intesa unisce risorse e competenze allo scopo di combattere importanti minacce cibernetiche, avendo il rilevante e complesso ruolo di coordinare le indagini su scala internazionale. Essa, inoltre, agisce da piattaforma di scambio delle informazioni e attuazione delle strategie operative tra i paesi membri dell'UE e gli Stati Uniti.

L'*ENISA*, l'agenzia dell'Unione Europea per la cybersecurity, svolge un ruolo chiave nella lotta contro il cybercrime e i reati finanziari tramite strumenti digitali.[89]

*ENISA* supporta la cooperazione tra i team di risposta agli incidenti di sicurezza informatica (*CSIRTs*), le agenzie di applicazione della legge (*LEAs*) e il sistema giudiziario, ottimizzando, inoltre, la gestione delle indagini sui crimini informatici.[90] Obiettivo di tale collaborazione è rendere maggiormente efficiente la raccolta e l'analisi delle prove necessarie nel coordinare le azioni legali contro i crimini informatici, compresi quelli finanziari. Ulteriore attività svolta dall'*ENISA* consiste nella pubblicazione di report annuali sul panorama delle minacce informatiche, offrendo analisi approfondite riguardo le principali minacce, attori coinvolti e delle diverse tecniche di attacco, nonché delle misure di mitigazione pertinenti.[91]

## 2.2 Riciclaggio di denaro, strumenti digitali e disciplina AML

La repressione del fenomeno del riciclaggio di denaro proveniente da origine illecita costituisce un rilevante aspetto nella battaglia contro le diverse forme di criminalità, dato che, oltre alle ripercussioni sociali da esso generate, è bene notare l'importanza delle conseguenze che vanno ad affliggere direttamente l'intero sistema economico e legale, sia sul piano nazionale che su quello internazionale.

---

[88] Cfr. Joint Cybercrime Action Taskforce (J-CAT): Fighting cybercrime around the world

[89] Cfr. Enisa.europa.eu "About ENISA - The European Union Agency for Cybersecurity"

[90] Id./Ead. Enisa.europa.eu. "Incidents Handling and Cybercrime Investigations."

[91] Cfr. SpringerLink. "ENISA's Contribution to National Cyber Security Strategies."

La crescente consapevolezza della comunità internazionale sugli effetti dannosi del riciclaggio ha stimolato l'adozione di numerose misure, sia a livello sovranazionale che domestico.

A partire dagli anni '80, si è assistito alla prima fase di sviluppo di proposte legislative aventi l'obiettivo comune di regolamentazione e prevenzione, cercando in particolare di impedire l'infiltrazione delle risorse finanziarie della criminalità organizzata nella cosiddetta "economia legale", sfruttando soprattutto i canali dell'intermediazione finanziaria.[92]

In una seconda fase, la legislazione è stata vista principalmente come uno strumento per prevenire il consolidamento delle organizzazioni criminali, mirando alla protezione dell'interesse generale circa il mantenimento dell'integrità dell'economia e dei mercati bancari e finanziari, liberi dall'interferenza del capitale illecito.

Nell'analizzare la disciplina antiriciclaggio, tuttavia, non si può ignorare un elemento fondamentale: essa non è caratterizzata da staticità, quanto piuttosto da una continua e repentina evoluzione, influenzata da fattori che mutano nel tempo, legati ai cambiamenti strutturali della criminalità organizzata, all'evoluzione delle tecniche criminali e le innovazioni finanziarie che, inconsapevolmente, offrono nuovi mezzi per il reinvestimento di ricchezze accumulate e generate illegalmente.

È dunque erroneo considerare che ci possa essere una disciplina stabile in materia, tuttavia, un monitoraggio costante può contribuire all'efficacia, nel tempo, delle misure antiriciclaggio.[93]

La totalità dei documenti di matrice regolamentare adottati in sede internazionale pongono in evidenza alcuni principi cardine ai quali gli ordinamenti nazionali devono ispirarsi per garantire l'efficacia delle misure preventive e repressive contro il riciclaggio.

Nell'analisi circa il contesto internazionale, non si può tuttavia trascurare l'impegno dell'Unione Europea allo scopo di proteggere il sistema finanziario dall'abuso per fini di riciclaggio di denaro.

Tale impegno ha avuto una prima manifestazione con la *Raccomandazione n. 80/10* del Comitato dei ministri del Consiglio d'Europa nel 1980, avente l'intenzione principale di

---

[92] Cit. Gratteri, Nicola, and Antonio Nicaso. Fiumi d'oro. Milano: Mondadori, 2018.

[93] Sullo stesso ordine di idee si veda: Banca d'Italia Eurosistema. "Supervisione e Normativa Antiriciclaggio."

sensibilizzare gli Stati membri sul problema crescente del riciclaggio di denaro, ed in particolare quello derivante dal traffico di droga e altre attività criminali, incoraggiando la cooperazione internazionale per combattere questo fenomeno.[94] L'iniziativa maggiormente significativa, tuttavia, è costituita dall'emanazione di cinque Direttive comunitarie, adottate in Italia nel 1991, 2001, 2005, 2015 e 2018, aventi l'obiettivo primario di prevenire i sistemi economici e finanziari dall'utilizzo a fini di riciclaggio, regolamentando, e allo stesso tempo innovando, ognuna a modo proprio, la normativa antiriciclaggio.

Discutendo di quella che effettivamente costituisce la piaga cui il percorso normativo appena citato mira a contrastare, ovvero il riciclaggio di denaro, è bene delinearne alcuni aspetti fondamentali, per comprenderne struttura e metodologie di funzionamento.

Il riciclaggio di denaro, infatti, si sviluppa in una serie di fasi specifiche e coordinate, che conferiscono alla sua struttura una precisione finalizzata a rendere difficile il tracciamento dei proventi ottenuti in modo illecito, e l'attività criminale da cui derivano. Le fasi, nello specifico, sono 3, e sono[95]: *Placement* (collocamento); *Layering* (stratificazione); *Integration* (integrazione).

Vediamole nel dettaglio.

1. *Placement* (collocamento): questa prima fase consiste nel collocamento materiale dei proventi di reato presso istituzioni o intermediari bancari e finanziari direttamente nel mercato. Tipico di quest'inizio di operazioni è il frazionamento delle operazioni effettuate su denaro contante allo scopo di sfuggire agli obblighi di segnalazione. Tipicamente la fase più rischiosa per chi ricicla denaro, data la possibilità delle autorità di individuare l'illegale origine, la fase di placement è spesso eseguita tramite depositi frazionati in diverse banche, acquisto di beni costosi, come gioielli e automobili, che possono essere rivenduti, e uso di attività commerciali legittime per coprire l'origine del denaro.
2. *Layering* (stratificazione): la seconda fase che costituisce il tipico schema per il riciclaggio di denaro consiste nel compimento di una serie di operazioni

[94] Cfr. Banca d'Italia Eurosistema: Quaderni dell'antiriciclaggio; Analisi e studi: Il riciclaggio nella prospettiva penale ed in quella amministrativa; Definizioni di riciclaggio

[95] Cfr. Fisicaro, Marco, and Luigi Ciampoli. La criminalità economica organizzata: analisi comparata con la conspiracy statunitense. Milano: UTET giuridica, 2022.

finanziarie dirette a separare il capitale dalla sua origine illecita. Qui si fa generalmente riferimento a grandi circuiti internazionali di riciclaggio di denaro, ove presenti professionisti capaci di gestire il flusso di denaro sporco. Tali trasferimenti avvengono tramite un dirottamento ramificato tra scambi di valute, acquisto di beni immobili, società fantasma e immissione presso istituzioni finanziarie di diversi Stati, preferibilmente *off shore*. Tale fase è fondamentale nel processo di riciclaggio di denaro tramite piattaforme digitali, il c.d. *cyberlaundering*, come vedremo dopo.

3. *Integration* (integrazione): ultima fase che consiste nell'integrare i fondi illeciti all'interno dell'economia legittima. È la fase in cui i capitali di origine criminale vengono mescolati con quelli di provenienza lecita, completando di fatto il processo di riciclaggio. L'obiettivo di tale fase è far sembrare che il denaro provenga da fonti legittime, per cui investimenti finanziari, acquisti immobiliari e beni di lusso costituiscono comuni mezzi per il compimento dell'integrazione.

Il riciclaggio di denaro, come abbiamo visto, è un fenomeno complesso che genera significativi impatti negativi sul sistema economico-legale e sulla società stessa.
L'armonizzazione normativa e la cooperazione tra autorità e Stati sono fondamentali, ma ancor più essenziale è il monitoraggio continuo del fenomeno e un approccio integrato che coinvolga istituzioni finanziarie, autorità di vigilanza e professionisti del settore, in modo da proteggere nel migliore dei modi l'integrità dei mercati finanziari, contribuendo inoltre alla lotta contro la criminalità organizzata.[96]

[96] Cfr. Galmarini, Sabrina. Antiriciclaggio. Milano: Wolters Kluwer, 2019.

### 2.2.1. Reato di riciclaggio: analisi legislativa

All'interno del quadro giuridico italiano, il reato di riciclaggio è disciplinato dall'*articolo 648 bis del Codice penale*, misura legislativa che prevede pene severe per chiunque sostituisca o trasferisca denaro, secondo specifiche metodologie e requisiti. Nello specifico, l'articolo recita:

*"Fuori dai casi di concorso nel reato, chiunque, sostituendo o trasferendo denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compiendo in relazione ad essi altre operazioni, ne ostacola l'identificazione della provenienza delittuosa è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale."*[97]

Il reato di riciclaggio, dunque, presenta diversi elementi costitutivi: condotta, provenienza illecita, dolo. La condotta incriminata può essere rappresentata dalla sostituzione o trasferimento di denaro, beni o altre utilità provenienti da delitti non colposi, o da qualsiasi operazione che possa ostacolare l'identificazione della loro provenienza delittuosa. Perché si configuri il reato, è necessario che i beni oggetto del riciclaggio provengano da un delitto commesso con dolo, escludendo così i reati commessi per negligenza, imprudenza o imperizia. Il dolo, un elemento imprescindibile: il reato è punibile solo se commesso con la consapevolezza e la volontà di ostacolare l'identificazione della provenienza delittuosa dei beni.[98]

Come è possibile notare dalla parte finale del testo dell'articolo, il legislatore ha previsto un aggravamento della pena nella fattispecie in cui il reato sia commesso nell'esercizio di un'attività professionale, riconoscendo una maggiore pericolosità del comportamento da parte di chi sfrutta la propria posizione professionale per porlo in atto. Il reato di riciclaggio può essere considerato "istantaneo" in quanto si consuma con il compimento

[97] Cfr. Codice Penale, art. 648-bis." Gazzetta Ufficiale della Repubblica Italiana, 26 ottobre 1930

[98] Cfr. Fisicaro, Marco, and Luigi Ciampoli. La criminalità economica organizzata: analisi comparata con la conspiracy statunitense. Milano: UTET giuridica, 2022.

di una delle condotte previste, ma può anche proseguire con ulteriori azioni atte a nascondere l'origine delittuosa del bene.[99]

Nonostante la rigida definizione, la normativa prevede riduzioni di pena per chi collabora efficacemente con le autorità, ad esempio nel caso di furto semplice, che ha una pena massima inferiore rispetto a reati come la rapina aggravata.[100]

Volendo poi confrontare il reato di riciclaggio e altri reati ad esso affini, è bene distinguerlo dal reato di ricettazione e reimpiego, rispettivamente disciplinati *dall'articolo 648 c.p. e 648-ter c.p.* La ricettazione, infatti, richiede solo il dolo di profitto, mentre il riciclaggio la specifica finalità di far perdere le tracce dell'origine illecita. Il reimpiego, invece, prevede l'utilizzo delle risorse di origine illecita in attività economiche o finanziarie. Da un punto di vista maggiormente esteso, la normativa italiana in materia di riciclaggio si inserisce in un quadro più ampio di disposizioni normative volte a prevenire e contrastare il crimine organizzato e il finanziamento del terrorismo, integrandosi con le direttive dell'Unione Europea e con gli standard internazionali stabiliti dal *Gruppo di Azione Finanziaria Internazionale* (*GAFI*), riflettendo così la necessità di una cooperazione internazionale per affrontare un fenomeno criminale che spesso assume caratteri transnazionali.[101]

Anche in quella che costituisce la dimensione regolamentare nazionale, sono coinvolte diverse autorità nella prevenzione e repressione del riciclaggio, tra cui la *UIF* (*Unità di Informazione Finanziaria*), il *Ministero dell'Economia e delle Finanze*, e varie autorità di vigilanza settoriali come la *Banca d'Italia,* l'*IVASS* e la *CONSOB*.[102]

Rappresentando una delle principali misure legislative volte a contrastare il flusso di denaro e beni di provenienza illecita, impedendo il reinserimento di essi nel circuito economico legale, il reato di riciclaggio si caratterizza per le rigide pene previste e per l'impegno, sia nazionale che comunitario, in esso profuso. La realtà, tuttavia, in termini statistici, risulta essere da quanto appena affermato discordante: Nel 2022, si è raggiunto

---

[99] Cfr. De Simone, Maria Vittoria. "Reato di riciclaggio: elementi costitutivi, pena e procedibilità." DeQuo, 29 ottobre 2021

[100] Cfr. Tringali, Giovanni. "Il reato di riciclaggio." Studio Cataldi, 14 novembre 2021.

[101] Cfr. Galmarini, Sabrina. Antiriciclaggio. Milano: Wolters Kluwer, 2019.

[102] Cfr. Aucone, Giovanna, e Valentina Groccia. "Il reato di riciclaggio nella normativa italiana." Allianz Darta, 24 maggio 2022

un record di 155.426 segnalazioni di operazioni sospette ricevute dall'Unità di Informazione Finanziaria (UIF) della Banca d'Italia, con un incremento significativo rispetto agli anni precedenti. Di esse, Circa il 99,8% è riconducibile a ipotesi di riciclaggio.[103]

### 2.2.2. Cyberlaundering: tecniche di Peel Chain, Mixing-Tumbling e Crypto-based loans

Il tema del *cyberlaundering* è oggi più rilevante che mai. Possiamo definire tale fenomeno come l'insieme di tutte quelle attività illecite che sono finalizzate a "ripulire" non solo denaro, ma anche altri beni, attraverso sistemi o mezzi informatici.
Nonostante le sue uniche caratteristiche, la struttura e l'organizzazione del *cyberlaundering* non si discostano molto dai metodi tradizionali. Si può infatti affermare che la tipica struttura "tripartita" del reato di riciclaggio (collocamento, stratificazione e integrazione) sia applicabile anche al *cyberlaundering*. In teoria, queste attività possono essere incluse nelle definizioni normative dell'art. 648-bis del Codice penale[104], che comprende anche il "reinvestimento di capitali di provenienza illecita" (art. 648-ter c.p.) e il reato di autoriciclaggio (art. 648-ter.1 c.p.), coinvolgendo inoltre altri reati connessi a operazioni che realizzano le fasi sopra menzionate e che mirano ad "occultare" l'origine criminale e a "convertire" denaro, beni e valori attraverso l'acquisto e la vendita di crypto-assets, così come la conversione in valuta fiat o in altre criptovalute. Il principale motivo per cui la tecnologia *blockchain* è cuore pulsante dei processi di *cyberlaundering* è che sembra offrire un maggiore grado di anonimato, permettendo di condurre operazioni di riciclaggio, anche di grandi somme, senza lasciare tracce che possano collegare le transazioni a un individuo specifico.[105]
Questa tecnologia cerca di combinare le caratteristiche sia della moneta fisica che di quella elettronica, creando un sistema che goda dei benefici ottenibili mediante l'utilizzo

[103] Cfr. Redazione ANSA. "Nel 2022 riciclaggio denaro da record per la Cgia." ANSA, 9 settembre 2023

[104] Cfr. Gazzetta Ufficiale: Art. 648-bis. (Riciclaggio)

[105] Sul punto si veda: Governo Italiano: Ministero della Giustizia: "cyberlaundering"

combinato dei due meccanismi, e che dunque dia la possibilità di effettuare pagamenti a distanza, tipicamente offerta dalla moneta elettronica, garantendo allo stesso tempo un certo grado di anonimato, di cui generalmente si gode tramite l'uso dei contanti. Il *wallet*, cioè il portafoglio dell'utente (persona fisica o entità giuridica) che ha inviato o ricevuto il pagamento o il crypto-asset, è identificabile attraverso l'indirizzo pubblico della transazione, ma il possessore di esso non viene automaticamente rivelato, proprio come accade con il contante. Non c'è dunque modo per identificare le persone coinvolte nelle diverse transazioni. Tuttavia, una delle problematiche che essi potrebbero affrontare è il rischio di essere collegati al mondo reale e quindi identificati durante la conversione delle criptovalute in valuta fiat e il successivo prelievo per l'utilizzo nell'economia reale. Dunque, anche se il riciclaggio di denaro all'interno della *blockchain* è considerato "sicuro", è alquanto complesso il processo di conversione dei crypto-assets in *valuta fiat* senza essere scoperti.[106] Nel 2021, i criminali informatici hanno riciclato complessivamente 8,6 miliardi di dollari in criptovalute, con un aumento del 30% rispetto al 2020. Questa crescita non sorprende, dato l'aumento significativo dell'attività legata alle criptovalute, sia legittima che illecita, nello stesso anno. Dal 2017, i cybercriminali hanno riciclato oltre 33 miliardi di dollari in criptovalute, la maggior parte dei quali trasferiti verso *exchange*s centralizzati.[107]

Le principali tecniche di riciclaggio tramite *blockchain* e *DLT* includono operazioni come il frazionamento e l'offuscamento dell'identità dei proprietari degli asset coinvolti. Rispettando la struttura tipica del riciclaggio di denaro, consistente dunque, in ordine, nelle fasi di: *placement*, *layering* e *integration*, analizziamo una specifica tecnica utilizzata per ogni fase di essa.

Partendo con il delineare quella che costituisce uno degli stratagemmi impiegati dai criminali per il collocamento dei fondi illeciti sul mercato, e dunque l'attività principale eseguita nella fase di *placement*, è bene fare riferimento alla cosiddetta tecnica *"peel chain"*[108].

---

[106] Cfr. Rea, Alessandra. 'Criptovalute: a che punto siamo?'. Diritto Penale e Uomo. Pubblicato il 22/07/2020.

[107] Cfr. Chainalysis. "The Chainalysis 2022 Crypto Crime Report."

[108] Cfr. Hudson Intelligence. "Peel Chain | Cryptocurrency Investigation." Hudson Intelligence.

Nel dettaglio, essa è impiegata per riciclare una grande quantità di criptovaluta attraverso lunghe serie di operazioni frazionate, in modo da evitare il rilevamento dei sistemi di sicurezza. Immaginiamo di trasferire acqua da un grande secchio a molte piccole tazze, una alla volta. Tale strategia criminale ha inizio con la presenza di una grande quantità di criptovaluta, contenuta in un unico indirizzo o portafoglio digitale. Dal suddetto, vengono effettuati trasferimenti di piccole quantità di criptovaluta verso altri indirizzi, spesso tramite *exchanges*, dove la criptovaluta può essere scambiata per valuta reale o altri asset digitali. Il valore dei singoli trasferimenti è volutamente piccolo, proprio per evitare di attirare l'attenzione dei sistemi di monitoraggio antiriciclaggio. In parallelo, la porzione maggiore dei fondi viene trasferita ad un nuovo indirizzo, che diventa il nuovo punto di partenza per ulteriori transazioni frazionate, e il medesimo processo si ripete fino a quando l'intero ammontare di crypto-assets viene convertito in *valuta fiat* e completamente riciclata, rendendo estremamente complessa la ricostruzione del percorso originale dei fondi illeciti. Utilizzando la *peel chain*, dunque, i criminali possono efficacemente mascherare l'ingresso dei fondi illeciti nel sistema economico formale, rendendo complessa la loro individuazione durante la prima fase (*placement*) del processo di riciclaggio. Una volta immessi i fondi illeciti all'interno del legittimo circuito economico, e dunque una volta terminata la fase di placement, ha inizio il secondo passo del processo di riciclaggio, costituito dalla fase di *Layering*, ossia di stratificazione, avente obiettivo primario la separazione dei fondi dalla loro origine criminale. In tal senso, una delle strategie maggiormente utilizzate, e che genera non pochi problemi a livello legislativo, è la cosiddetta tecnica *Mixing-Tumbling.*[109]

In questo contesto, un ruolo fondamentale è svolto dai "*mixer*" di criptovalute, servizi che uniscono le criptovalute di vari utenti per offuscare le loro origini e l'identità dei possessori. Dato che le *blockchain* pubbliche come *Bitcoin* ed *Ethereum* sono trasparenti, il livello di privacy richiesto da alcuni utenti (non necessariamente per scopi illeciti) è difficile da ottenere senza utilizzare servizi di questo tipo.

Un certo numero di utenti che si avvale dei *mixer* è composto da cybercriminali, che li utilizzano allo scopo di nascondere la connessione tra i portafogli di criptovalute ove

[109] Cfr. Merkle Science. (2022). Mixers and Tumblers: Regulatory Overview and Use in Illicit Activities. 18/02/2022:

accumulano i profitti illeciti e quelli dai quali trasferiscono i fondi, con l'intento di evitare pattern sospetti di riciclaggio.

I *mixer* raggruppano e mescolano in modo "pseudo-casuale" le criptovalute depositate da diversi utenti. I fondi vengono poi prelevati da nuovi indirizzi controllati da ciascun utente, meno una piccola commissione trattenuta dal gestore del servizio di *mixing*. La maggior parte dei *mixer* rende difficile tracciare i fondi depositati, permettendo agli utenti di prelevare importi casuali a intervalli casuali. Alcuni cercano di oscurare ulteriormente l'uso del *mixer* variando le commissioni per le transazioni e i tipi di indirizzi di prelievo. Nonostante l'utilizzo da parte dei criminali, i *mixer* di criptovalute non sono propriamente illegali nella maggior parte delle giurisdizioni. Tuttavia, la conformità alle normative antiriciclaggio è una questione diversa: secondo *Chainalysis*[110], nessun *mixer* attualmente adempie alla normativa antiriciclaggio. Dato che la tutela della privacy è il principale motivo per cui gli utenti utilizzano i *mixer*, è improbabile che questi servizi possano rispettare le norme contro il riciclaggio e il finanziamento del terrorismo mantenendo il loro bacino di utenti.

A questo punto ha inizio la terza fase che compone il processo di riciclaggio di denaro tramite la *blockchain*, la fase di *integration* (integrazione), spesso portata a termine con la cosiddetta tecnica dei "*Crypto-backed loans*".[111] Nello specifico, tale stratagemma permette ai riciclatori di denaro di trasformare la criptovaluta in liquidità legale senza necessariamente vendere le criptovalute in modo diretto, facilitando l'integrazione di fondi illeciti all'interno del sistema economico formale in maniera apparentemente legittima, finalità della fase di integrazione.

Il processo ha inizio con la messa in pegno di una quantità di criptovalute su una dedicata piattaforma che offre tali servizi di prestito, ricevendo in cambio un prestito in *valuta fiat*, il cui ammontare è generalmente proporzionale al valore del collaterale crypto depositato. Tale approccio permette all'individuo di mantenere l'esposizione agli asset digitali mentre utilizza la valuta fiat ottenuta per transazioni nel mercato reale. In questo modo, la liquidità così acquisita può essere impiegata per acquisti o investimenti che sono difficilmente riconducibili direttamente alla vendita di criptovaluta, grazie al fatto che il

[110] Cit. The Chainalysis 2022 Crypto Crime Report

[111] Cfr. Investopedia. "Crypto Lending: What It Is, How It Works, Types." August 16, 2023.

denaro in circolazione appare come il prodotto di un accordo di finanziamento. Infine, il rimborso del prestito e il recupero del collaterale completano il ciclo di integrazione, che permette al riciclatore non solo di recuperare l'investimento iniziale in criptovalute, ma chiude anche il ciclo finanziario in maniera che preservi la continuità e il valore del collaterale digitale. Pertanto, i *Crypto-Backed Loans* costituiscono una tecnologia all'avanguardia per il compimento di attività di riciclaggio di denaro, andando di fatto a chiudere un cerchio articolato in diverse fasi.

### 2.2.3. Normativa europea: IV Direttiva AML

La *Direttiva 2015/849/UE*, emanata dal Parlamento europeo e dal Consiglio il 20 maggio 2015 [112], riguarda la prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo. Questa direttiva modifica il *regolamento (UE) n. 648/2012* del Parlamento europeo e del Consiglio, che aveva ad oggetto gli strumenti derivati *OTC* (*Over The Counter*), le controparti centrali e i repertori di dati sulle negoziazioni[113], e abroga la *Direttiva 2005/60/CE* (la *III Direttiva*). Conosciuta come "*IV Direttiva Antiriciclaggio*", essa potenzia il sistema di prevenzione degli Stati membri, in coerenza con le linee tracciate dalle Raccomandazioni del *GAFI* del 2012.[114]

La nuova disciplina europea valorizza l'approccio basato sul rischio, criterio fondamentale per graduare le misure preventive e i controlli. Inoltre, accresce la trasparenza delle informazioni relative alla titolarità effettiva di società e trust, conferma il regime di assoluta riservatezza dei dati relativi alle operazioni sospette, e delinea criteri sanzionatori specifici per le violazioni degli obblighi in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

---

[112] Cfr. DLA Piper. "Anti Money Laundering Directive in Italy." June 26, 2017.

[113] Cfr. EUR-Lex. "Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories."

[114] Def. Financial Action Task Force (FATF). "Le Raccomandazioni del GAFI del 2012 Sono Standard Internazionali per Contrastare il Riciclaggio di Denaro, il Finanziamento del Terrorismo e la Proliferazione delle Armi di Distruzione di Massa."

In aggiunta, la direttiva attribuisce un ruolo centrale alle *Financial Intelligence Unit* (*FIU*)[115], agenzie governative specializzate che si occupano di raccogliere, analizzare e trasmettere le segnalazioni di operazioni sospette relative al riciclaggio di denaro, finanziamento del terrorismo, e ad altre minacce alla stabilità finanziaria di uno stato. Nello specifico, essa delinea una disciplina più articolata che ne rafforza le prerogative istituzionali, ampliandone le funzioni.

Le disposizioni sottolineano l'importanza dei requisiti fondamentali di autonomia e indipendenza, ridefinendo la stessa nozione di *FIU* e chiarendone i compiti principali, che includono: la ricezione; l'analisi; e la disseminazione delle informazioni.

Anche le norme sulla collaborazione internazionale tra *FIU* sono state riviste e ampliate. È previsto, tra l'altro, che le risposte alle richieste provenienti da *FIU* estere debbano essere fornite utilizzando gli stessi poteri disponibili per le analisi interne, indipendentemente dalle eventuali differenze nelle legislazioni degli Stati membri e nella definizione dei reati presupposto.

La direttiva introduce un sistema di "scambio automatico" di segnalazioni sospette a carattere transfrontaliero, assicurando che le *FIU* condividano rapidamente con le controparti europee le segnalazioni che riguardano altri Stati membri.

Inoltre, l'approccio basato sul rischio richiede valutazioni a diversi livelli: nazionale, sovranazionale e individuale. La Commissione europea coordina l'analisi sovranazionale per identificare le minacce comuni tra gli Stati membri, mentre ogni Stato conduce una propria valutazione nazionale.

Nel giugno 2017, la Commissione ha pubblicato la prima relazione sovranazionale, identificando i principali rischi per settore e i metodi utilizzati dai criminali per il riciclaggio di denaro, insieme a specifiche raccomandazioni per gli Stati membri.

La direttiva prevede 68 Considerando e 69 articoli, includendo:

- L'abbassamento delle soglie per i pagamenti in contanti a 10.000 euro sia per le persone fisiche che giuridiche che negoziano beni, sia in un'unica operazione che in più transazioni collegate.
- L'inclusione dei prestatori di servizi di gioco d'azzardo tra i soggetti obbligati, intendendosi, il gioco d'azzardo, «servizio che implica una posta pecuniaria in giochi di

[115] Trad. Unità di Informazione Finanziaria

sorte, compresi quelli che comportano elementi di abilità, quali le lotterie, i giochi da casinò, il poker e le scommesse, prestati in locali fisici o, a prescindere dal modo, a distanza, mediante mezzi elettronici».

- La previsione, nell'area dell'attività criminosa, dei reati fiscali «relativi a imposte dirette e indirette, quali specificati nel diritto nazionale, punibili con una pena privativa della libertà di durata massima superiore ad un anno […]».
- La valutazione dei rischi di riciclaggio e di finanziamento del terrorismo a livello europeo, a livello nazionale e per i singoli soggetti obbligati.
- L'introduzione di nuove misure allo scopo di conferire maggiore chiarezza e accessibilità alle notizie sulla titolarità effettiva, prescrivendo che le società o gli enti giuridici stabilite nel territorio dell'Unione europea ottengano e mantengano informazioni adeguate, accurate e aggiornate sui propri titolari effettivi e che le autorità competenti, gli enti obbligati e qualunque persona od organizzazione che possa dimostrare un legittimo interesse, ne abbiano accesso.
- L'estensione delle misure alle Persone Politicamente Esposte.
- L'eliminazione dell'equivalenza positiva nei confronti dei Paesi terzi, favorendo l'adeguata verifica basata sul rischio.
- Un sistema di sanzioni amministrative per le violazioni gravi o sistematiche degli obblighi di verifica, conservazione dei documenti e segnalazione delle operazioni sospette.
- L'applicazione di sanzioni amministrative che siano effettive, proporzionate e dissuasive.
- Il rafforzamento, coordinamento e scambio di informazioni tra le Financial Intelligence Unit.

Nel 2018 è stata promulgata la *Direttiva 2018/843* (*V Direttiva Antiriciclaggio*), la quale, come vedremo nel paragrafo successivo, costituisce un ulteriore passo verso la lotta al riciclaggio di denaro e al finanziamento del terrorismo. Tale atto normativo rappresenta anche la prima regolamentazione a livello dell'Unione Europea che affronta il fenomeno delle "valute virtuali", fino a quel momento non regolamentato, conferendo loro una disciplina ufficiale e, necessariamente, anche una definizione.[116]

[116] Cfr. Dirittobancario.it: Antiriciclaggio e criptovalute: le anticipazioni alla V Direttiva AML. 26/04/2018

### 2.2.4. V Direttiva Anti Money Laundering

La normativa antiriciclaggio, sia a livello comunitario che nazionale, si è evoluta nel tempo in modo da allinearsi ai principi internazionali e alle nascenti esigenze dettate dal propagarsi di nuovi strumenti tecnologici, con l'obiettivo di creare un quadro normativo armonizzato tra gli Stati membri.

Una delle principali evoluzioni in questo contesto è rappresentata dalla *Direttiva n.2018/843*[117] del Parlamento europeo e del Consiglio, del 30 maggio 2018 (nota come *V direttiva antiriciclaggio*), che modifica la *Direttiva 2015/849* (*IV direttiva antiriciclaggio*), di cui l'esposizione nel precedente paragrafo. Il recepimento di questa nuova direttiva è disciplinato dall'art. 4 della direttiva stessa, secondo il quale gli Stati membri devono mettere in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla direttiva, entro il 10 gennaio 2020.

Nel contesto del diritto dell'Unione europea, infatti, la direttiva vincola lo Stato membro cui è rivolta con riferimento al "risultato da raggiungere", lasciando, invece, libero il medesimo Stato in merito alla forma e ai mezzi da adottare ai fini della modificazione dell'ordinamento interno in senso conforme alla direttiva, stabilendo inoltre il termine entro il quale lo Stato membro deve dare alla stessa attuazione (*art. 288 par. 3 TFUE*).[118]

Gli attentati terroristici avvenuti nel periodo immediatamente antecedente l'approvazione della direttiva, come quelli a Parigi nel 2015 e a Bruxelles nel 2016, hanno rivelato nuove tendenze, in particolare riguardo le modalità di finanziamento e operatività dei gruppi terroristici. Alcuni servizi basati sulle tecnologie moderne, come descritto nel paragrafo *2.2.2*, stanno assumendo sempre più popolarità come sistemi finanziari alternativi e privi di regolamentazione specifica. Per affrontare prudentemente le sfide da tali nuove tendenze derivanti, sono state introdotte misure volte a garantire una maggiore trasparenza nelle operazioni finanziarie, nelle società e altri soggetti giuridici, nonché dei trust e degli istituti giuridici aventi assetto affine a questi ultimi.

---

[117] Cfr. EUR-Lex. "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018."

[118] Cit. Pellegrini, Mirella. "Il Sistema delle Fonti." In *Diritto Pubblico dell'Economia*, 85. Padova: Cedam, 2023.

La riforma copre diversi ambiti e affronta vari aspetti, includendo, tra essi, i fornitori di servizi di cambio tra valute virtuali e valute aventi corso legale, e i fornitori di servizi di portafoglio digitale, ai quali sono stati estesi gli obblighi antiriciclaggio, quali: segnalazione di operazioni sospette, conservazione dei documenti e altre misure preventive previste per altri soggetti già precedentemente obbligati, come le banche e le istituzioni finanziarie.[119] Questa, la risposta ad una falla di sistema che ha permesso ai gruppi terroristici di trasferire ingenti somme di denaro in totale anonimato, dissimulando i trasferimenti tramite scambi di cryptovalute. Da qui l'esigenza di modificare e ampliare l'ambito di applicazione della *Direttiva 2015/849*, includendo i fornitori di tali servizi tra i soggetti tenuti agli obblighi antiriciclaggio.

Anche strumenti come le carte di pagamento prepagate sono stati oggetto di analisi e regolamentazione da parte della *V Direttiva*. Pur rappresentando, infatti, un importante strumento di inclusione sociale, le carte prepagate anonime possono facilmente essere utilizzate per finanziare atti terroristici e compiere altri illeciti digitali.

Esse, tipicamente ricaricabili con piccoli importi, non sono soggette a tracciabilità. Risulta dunque necessario ridurre ulteriormente i limiti e gli importi massimi al di sotto dei quali i soggetti obbligati possono non applicare determinate misure di adeguata verifica della clientela, tenendo comunque conto delle esigenze dei consumatori riguardo l'utilizzo generale di tali strumenti, senza porre freno ad un processo di inclusione sociale e finanziaria in forte sviluppo.[120]

Nei riguardi delle *FIU* (*Financial Intelligence Unit*), di cui si parla ampiamente nel paragrafo precedente, la *V Direttiva* ne ha ampliato poteri e competenze, potenziando il loro ruolo e facilitando, ad esempio, l'identificazione dei beneficiari effettivi delle transazioni, la cooperazione nei rapporti con gli Stati membri, e la collaborazione con le entità private, nonché l'adozione di nuove tecnologie per l'analisi e il monitoraggio delle

---

[119] Cfr. Masi, Serena. "V Direttiva Antiriciclaggio: Obiettivi, Ambito di Riforma, Modifiche." Altalex, May 28, 2019.

[120] Cfr. Financial Action Task Force (FATF). "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services."

transazioni finanziarie. Tali cambiamenti, di fatto, rafforzano le capacità analitiche delle *FIU*, incoraggiate, inoltre, nell'adozione di un approccio *risk-based*.[121]

Considerevoli modifiche sono inoltre state apportate allo scopo di migliorare la trasparenza e il controllo sui *trust* e sugli istituti giuridici affini. Secondo quanto riportato dalla *Convenzione dell'Aja del 1° luglio 1985*, per "*trust*" si intendono i rapporti giuridici istituiti da una persona (il disponente), mediante un atto tra vivi o mortis causa, quando dei beni sono posti sotto il controllo di un trustee nell'interesse di un beneficiario o per un fine determinato.

La direttiva, nello specifico, ha cercato di affrontare le difficoltà legate alla disomogeneità tra i sistemi giuridici degli Stati membri, stabilendo che le norme applicabili a questi istituti riguardo l'accesso alle informazioni sulla loro titolarità effettiva devono essere comparabili a quelle applicate alle società e agli altri soggetti giuridici. Viene data agli Stati membri la responsabilità di decidere se un trust o un istituto giuridico analogo sia comparabile a una società o ad altri soggetti giuridici, con il categorico dovere di impedire l'utilizzo di essi per il compimento di attività di riciclaggio o finanziamento del terrorismo, imponendo che le informazioni sulla titolarità effettiva dei trust siano registrate nei paesi dove i fiduciari o i soggetti equivalenti risiedono o sono stabiliti.

In un analogo contesto, il legislatore europeo ha apportato modifiche significative alla *IV direttiva antiriciclaggio*.

Essa ha infatti esteso l'elenco dei soggetti tenuti a conformarsi agli obblighi antiriciclaggio, includendo, oltre ai precitati prestatori di servizi di cambio tra valute virtuali e valute legali, e prestatori di servizi di portafoglio digitale, i galleristi, i gestori di case d'asta e gli antiquari.

A livello europeo, con la *V Direttiva* sono stati inclusi anche le persone che commerciano opere d'arte o che agiscono come intermediari nel commercio delle stesse, anche quando tale attività è svolta da gallerie d'arte e case d'aste, nel caso in cui il valore dell'operazione o di una serie di operazioni legate tra loro sia pari o superiore a 10.000 euro.

La motivazione alla base di queste regolamentazioni, nello specifico, è riconducibile ad un frequente utilizzo di tali asset in processi dediti al riciclaggio di denaro, dato il loro

---

[121] Cfr. European Commission. "Communication from the Commission to the European Parliament and the Council Towards Better Implementation of the EU's Anti-Money Laundering and Countering the Financing of Terrorism Framework." July 24, 2019.

potenziale impiego nel trasferimento di grandi somme di denaro in modo relativamente anonimo. Le opere d'arte possono essere infatti acquistate con denaro illecito e poi rivendute, spesso a prezzi gonfiati, per creare un'apparenza di legittimità ai proventi.
Le gallerie d'arte e le case d'aste, se non regolamentate adeguatamente, possono fungere da intermediari che facilitano la movimentazione di fondi illeciti senza attirare troppo l'attenzione delle autorità.
Il valore elevato e spesso soggettivo delle opere d'arte rende difficile valutare se una transazione sia giustificata o giustificabile, rendendo questo settore attraente per chi vuole ripulire denaro sporco.[122]
In conclusione, la *V Direttiva Antiriciclaggio* rappresenta un importante avanzamento nel contrasto al riciclaggio di denaro e al finanziamento del terrorismo nell'Unione Europea, rendendo maggiormente efficace la cooperazione tra Stati membri e adattando le normative alle sfide tecnologiche emergenti, in modo da contribuire alla costruzione e alla salvaguardia di un sistema finanziario che possa essere sicuro e trasparente.

### 2.2.5. Considerazioni personali

In conclusione, la messa in luce dell'intrinseco legame tra sviluppo tecnologico e adattabilità delle organizzazioni criminali, che sanno agilmente sfruttare le innovazioni digitali per perpetrare atti illeciti, spesso anticipando le regolamentazioni che potrebbero contrastarli, risulta fondamentale per avere un esteso quadro di comprensione del tema e delle sfide da esso generate. Questa tendenza solleva questioni etiche significative e riflette un ciclo quasi parassitario in cui la tecnologia, pur essendo una forza progressiva per il bene economico e sociale, costituisce al contempo uno strumento facilitante per la criminalità organizzata.
Oggetto di tali considerazioni sarà l'etica, profondamente problematica, di tale meccanismo. L'innovazione tecnologica, infatti, pur indubbiamente apportando numerosi aspetti positivi nelle quotidiane operazioni di ognuno, è caratterizzata da una neutralità

[122] Cfr. Financial Action Task Force (FATF). "Money Laundering and Terrorist Financing in the Art and Antiquities Market." February 27, 2023.

morale che le permette di essere sfruttata tanto per il bene quanto per il male, materializzandosi in una dualità che pone sfide continue per i legislatori e le autorità di regolamentazione, costretti a dover correre al fine di tenere il passo con l'evoluzione delle strategie azionate da criminali di diverso genere. Spontaneamente si solleva la questione secondo cui le tecnologie dovrebbero essere progettate fin dall'inizio per impedire l'abuso, incorporando principi di "security by design", approccio che pone la sicurezza come una priorità fin dalle prime fasi del processo di sviluppo di tali strumenti, ed "ethics by design", metodo che integra considerazioni etiche in ogni fase del medesimo.

Il successo nell'espletamento di processi atti al riciclaggio di denaro tramite tecnologie avanzate, come la blockchain e le criptovalute, illustra un pattern ricorrente, che vede l'uso malintenzionato precedere e spesso stimolare la regolamentazione, sottolineando una realtà in cui le misure preventive sono formulate in risposta, piuttosto che in prevenzione. Tale ritardo nella regolamentazione offre alle organizzazioni criminali una preziosa finestra temporale al fine di sfruttare nuove tecnologie a loro vantaggio, complicando, di conseguenza, gli sforzi per il loro contrasto.

Un'ulteriore messa alla prova circa l'efficacia delle politiche antiriciclaggio è da ricondurre alla rapidità con cui avviene l'adozione globale di tali strumenti, che supera la velocità di azione delle singole giurisdizioni, richiedendo dunque un approccio coordinato a livello internazionale. Analisi empiriche mostrano, di fatto, che la cooperazione internazionale risulta essere essenziale, e ciononostante, spesso ostacolata da discrepanze normative, interessi nazionali e capacità di enforcement.

Di fronte allo scenario in analisi, è evidente che il ruolo dei regolatori non è solo di reagire, ma anche di anticipare. Ciò, tuttavia, richiede un cambiamento paradigmatico verso una vigilanza caratterizzata da proattività e impegno nei confronti di un'innovazione responsabile. La posta in gioco, infatti, è alta: la stabilità dell'ordine economico e sociale globale dipende dalla capacità di governare l'uso delle tecnologie emergenti in modo che favoriscano il progresso senza alimentare l'illegalità.

In ultima analisi, sottolineo dunque l'urgente necessità di un continuo dialogo tra i diversi attori nei seppur vari, complementari, ambiti di operatività: sviluppatori tecnologici, legislatori, enti di regolamentazione e comunità internazionale. È proprio attraverso un impegno congiunto e una visione condivisa proiettata verso un futuro eticamente guidato e sicuro, infatti, che si può sperare di rimanere un passo avanti rispetto a coloro che

cercano costantemente di sfruttare e boicottare i propri concorrenti, nella gara caratterizzata dallo sviluppo tecnologico che vede come traguardo la tutela dell'umanità e della sua dignità.

# 3. Caso studio "attacco Hacker Synlab"

## 3.1 Attacco Hacker a Synlab Italia: introduzione

In uno scenario di aggressione, si è soliti immaginare, per facilità di pensiero, il coinvolgimento di soli due attori: un aggressore e una vittima. Il caso che verrà analizzato nelle seguenti righe, tuttavia, costituisce l'eccezione che non conferma la regola, coinvolgendo, esso, un aggressore e centinaia di migliaia di vittime.
Ma come è possibile tutto ciò? Come è possibile che una singola organizzazione, composta da pochi individui, situati in tutt'altra parte del mondo, possa colpire un numero così elevato di persone, talvolta senza neanche uscire dal proprio nucleo abitativo?
La risposta, purtroppo, è più semplice di quanto si pensi, e tale semplicità sottolinea la spiccata indifferenza e superficialità con cui ci interfacciamo a temi che, volenti o nolenti, costituiscono una parte fondamentale, sia diretta che indiretta, della nostra quotidianità: la tecnologia e il ramificato mondo dei big data. Questi offrono molte opportunità, persino per i criminali, che riescono a sfruttarli a proprio vantaggio per perpetrare illiceità di ogni genere. Ma nello specifico, dunque, cosa è accaduto?

### 3.1.1. Scenario e attori coinvolti: cos'è accaduto?

Il 13 maggio 2024, *Synlab Italia*, azienda sanitaria privata, parte della multinazionale *Synlab*, nonché uno dei principali fornitori di servizi di diagnosi medica, ha annunciato di aver subito un devastante attacco hacker di tipo *ransomware* il 18 aprile 2024 da parte

dell'organizzazione di criminali informatici *Black Basta*, pubblicando sull'ufficiale sito web di loro appartenenza la seguente nota[123]:

*"Nel pomeriggio del 13 maggio 2024, come da nostro comunicato pubblicato lo stesso giorno, l'organizzazione cybercriminale "Black Basta", responsabile dell'attacco informatico, ha pubblicato in aree del dark web informazioni sottratte illecitamente a SYNLAB, compresi documenti e dati personali. A seguito della pubblicazione dei dati da parte dell'organizzazione cybercriminale, SYNLAB si è attivata per l'analisi e l'identificazione dei dati oggetto di pubblicazione avvalendosi anche di fornitori specializzati del settore: considerate le complessità nella acquisizione dell'intero dataset attraverso il dark web, l'attività potrà richiedere diverso tempo. SYNLAB è al lavoro per l'individuazione di differenti strategie che permettano di accelerare tali operazioni. Dalle prime analisi condotte internamente, abbiamo potuto rilevare che tra i dati pubblicati vi sono anche dati personali relativi a certi nostri pazienti. All'esito dell'attività di analisi seguirà la classificazione dei dati pubblicati al fine di individuare i soggetti interessati, alla data attuale non singolarmente identificabili. Parallelamente, SYNLAB continua a collaborare con le Pubbliche Autorità investigative competenti e si è attivata per integrare ulteriormente le notifiche preliminari all'Autorità Garante per la Protezione dei Dati personali."*

Proseguiamo passo dopo passo, andando ad analizzare dettagliatamente quanto comunicato.

L'attacco informatico cui si fa riferimento, avvenuto circa 25 giorni prima della comunicazione, ha costretto l'azienda a sospendere le attività diagnostiche, mettendo a serio rischio la privacy di migliaia di pazienti, e rallentando drasticamente il sistema sanitario nazionale. L'organizzazione cybercriminale *Black Basta*, che ha rivendicato la riuscita dell'attacco hacker settimane dopo la sua manifestazione, ha sottratto documenti e dati personali dei clienti di *Synlab*, chiedendo un ingente riscatto in criptovalute, ed in seguito al conseguente rifiuto da parte dell'azienda di pagare il riscatto, pubblicato 1,5

[123] Cfr. SYNLAB Italia: "Aggiornamenti sui Sistemi."

terabyte di dati sensibili, tra cui documenti d'identità, analisi mediche e referti, all'interno del *dark web*, rendendoli facilmente accessibili a malintenzionati.

Le conseguenze di tale attacco sono devastanti e si manifestano ancora oggi, poiché i dati sottratti possono essere utilizzati da criminali anche anni dopo l'incidente, permettendo loro di agire quando ritengono più opportuno. Appena informata dell'attacco, *Synlab Italia* ha immediatamente attivato una *task force* dedicata per bloccare l'intrusione e ripristinare i propri servizi. Sono stati disattivati i sistemi informatici per poi metterli in sicurezza, identificare e isolare il *malware* responsabile e successivamente riattivare i servizi. Nonostante l'ingente furto di dati, *Synlab Italia* disponeva di backup adeguati che hanno permesso di recuperare i dati, limitando così gli effetti del furto al di fuori dell'azienda e garantendo la continuità operativa, fondamentale per il sistema sanitario e la salute dei cittadini.[124]

Tuttavia, gli effetti complessivi dell'attacco continuano a essere caratterizzati da un considerevole potere distruttivo, dannoso sia per l'azienda stessa che per tutti i soggetti indirettamente coinvolti.

### 3.1.2. Contesto Criminale: Black Basta e modus operandi

Secondo la *Cybersecurity and Infrastructure Security Agency* (*CISA*), agenzia statunitense che si occupa di proteggere l'infrastruttura critica del paese da minacce informatiche, "*Black Basta*" è un'organizzazione criminale informatica che si è distinta per la sua abilità e organizzazione nel condurre attacchi ransomware.[125] Rapidamente acquisita una reputazione temibile, specialmente per i danni causati a settori critici come l'amministrazione pubblica e le infrastrutture essenziali, il gruppo criminale si fonda su un modello di business noto come "*crime-as-a-service*" (crimine come servizio) o "*ransomware-as-a-service*" (ransomware come servizio), secondo il quale vi sono diversi programmi di affiliazione che permettono ai cybercriminali di partecipare a diverse fasi

[124] Cfr. "Synlab Italia Attack Admitted by Black Basta." SC Media

[125] Cfr. Cybersecurity and Infrastructure Security Agency. "CISA and Partners Release Advisory on Black Basta Ransomware." May 10, 2024.

dell'attacco in cambio di una parte dei profitti ottenuti tramite i conseguenti riscatti.[126] Il modus operandi dell'organizzazione criminale (nello specifico *Black Basta*, ma altrettanto applicabile alle organizzazioni affini) è chiaro, e segue lo schema seguente[127]:

1. *Fase di ricognizione*, ove ha luogo la raccolta di informazioni da parte degli hacker circa la vittima, dati tecnici ed organizzativi, e l'identificazione delle vulnerabilità sfruttabili per perpetrare l'attacco ideato, tramite l'attento compimento di analisi che riguardano i sistemi della vittima.

2. *Fase di intrusione*, caratterizzata da un accesso iniziale che avviene tramite tecniche di *phishing*, *malware* o sfruttamento delle vulnerabilità al fine di ottenere accesso ai sistemi identificati, e l'escalation dei privilegi per cui, conseguentemente, si cerca di ottenere privilegi amministrativi con lo scopo di avere un completo controllo sui sistemi.

3. *Fase di esecuzione*, che comprende l'installazione del ransomware sui sistemi compromessi e la crittografia dei dati per bloccare l'accesso ai sistemi, che avviene al termine del processo di esfiltrazione, ove grandi quantità di informazioni sensibili e riservate vengono estratte dai database.

4. *Fase di riscatto*, che prevede un'iniziale formale richiesta, seguita dalla fase di trattativa. Viene contattata la vittima, informandola dell'attacco e chiedendo un ingente riscatto in criptovalute per decrittare i dati e non pubblicare le informazioni sottratte, per poi dare inizio alla fase di trattativa con la vittima stessa, dove si cerca di ottenere il pagamento del riscatto, anche scendendo a compromessi estorsivi.
   Le criptovalute sono utilizzate, in scenari simili, per la loro spiccata capacità nel garantire anonimato, decentralizzazione, globalità ed irreversibilità, tramite il corretto utilizzo delle tecniche analizzate nel punto 2.2.2.

---

[126] Cfr. U.S. Department of Health and Human Services. "Black Basta Threat Profile.".

[127] Cfr. Agence nationale de la sécurité des systèmes d'information (ANSSI). "Ransomware Attacks: All Concerned.".

5. *Fase di pubblicazione*: se la vittima si rifiuta di pagare il riscatto, si procede con la pubblicazione (gratuita o tramite vendita) dei dati sottratti su forum presenti all'interno del *dark web*, rendendoli in tal modo accessibili a malintenzionati. Avviene poi la ripetizione della minaccia, secondo cui i criminali possono continuare a minacciare la vittima, magari pubblicando gradualmente i dati in modo da esercitare maggiore pressione.

6. *Fase di dissoluzione*, che avviene tipicamente dopo aver completato l'attacco, al fine di cancellare le tracce dello stesso, in modo da evitare il rintracciamento da parte delle autorità. Vi è poi l'ipotetica preparazione per il prossimo attacco: le organizzazioni coinvolte si preparano cercando nuove vittime e ripetendo il ciclo appena concluso.

L'attacco a *Synlab* è solo l'ultimo. *Black Basta* è monitorato dall'aprile del 2022, da quando ha cominciato a firmare i primi attacchi, tuttavia, la carriera criminale dei componenti del gruppo hacker non ha avuto inizio nel 2022. Secondo varie indagini ad opera di ricercatori di *Sentinel Labs*, infatti, emergerebbero vari legami tra *Black Basta* e un altro gruppo cybercriminale tracciato dal 2020, denominato *FIN7*.[128] Durante le indagini è stato notato come alcuni campioni di un malware denominato *WindefCheck.exe.*, che mostra una falsa interfaccia di sicurezza di *Windows* che indica che il sistema è "sano" anche quando *Windows Defender* e altre funzionalità sono disabilitate[129], era collegato al *backdoor BIRDDOG*, che, noto anche come *SocksBot*, è frequentemente utilizzato dal gruppo *FIN7*.
Le somiglianze tra i campioni suggeriscono che lo stesso attore delle minacce potrebbe essere coinvolto sia nei casi di *Black Basta* che in quelli di *FIN7*, poiché sembrano condividere lo stesso codice per l'impacchettamento del malware.
Oltre ai collegamenti con *FIN7* c'è un altro nome che ritorna nelle poche biografie che si trovano sui siti specializzati. *Black Basta* infatti sarebbe sorta dalle ceneri del *Gruppo*

[128] Cfr. Cocomazzi, Antonio, and Antonio Pirozzi. "Black Basta Ransomware Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor." SentinelOne, November 3, 2022.
[129] Cfr. CyberProof Blog. "How Ransomware Actors Use EDR Bypassing to Run Cybercrime Campaigns."

*Conti*, uno dei gruppi hacker che ha collezionato più attacchi al mondo, riuscendo a guadagnare, secondo alcune stime, oltre 150 milioni di dollari.[130]

Al netto delle sue origini, in due anni *Black Basta* è diventato uno dei gruppi criminali più attivi nel panorama mondiale. Secondo un report di *Kaspersky*, esso è il 12° gruppo più attivo al mondo. Solo nell'aprile del 2024, *Black Basta* è stato coinvolto in 28 dei 372 attacchi ransomware registrati in tutto il mondo. Questi, registrati negli Stati Uniti, Canada, Regno Unito e Italia.[131]

Secondo la piattaforma *The Hacker News*, i dati sanitari sono tra i bottini più ricercati da *Black Basta*, essendo, le organizzazioni sanitarie, caratterizzate da grandi dimensioni, infrastrutture tecnologiche delicate e dall'estrema sensibilità delle informazioni sanitarie, il cui malfunzionamento dei relativi database comporterebbe impatti diretti persino sulla salute dei pazienti.

### 3.1.3. Rischi e conseguenze dell'attacco

Le conseguenze di un attacco di tale portata sono caratterizzate da una rilevanza facilmente intuibile, tuttavia, è opportuno valutarle nella loro totalità, tenendo in considerazione i rischi e le ripercussioni dirette ed indirette, senza che nulla sia esente da un'analisi che ha come obiettivo la verifica oggettiva di tale avvenimento.

Compiamo, innanzitutto, una prima classificazione cronologica di tali conseguenze.

Nonostante *Synlab Italia* abbia attivato una task force specifica per porre fine all'intrusione criminale e procedere all'isolamento del malware, e nonostante abbia adottato le necessarie misure di contrasto, l'azienda è stata costretta a sospendere temporaneamente tutte le attività presso i punti di prelievo, inclusi i servizi di download e ritiro dei referti, in modo da garantire la sicurezza dei dati.[132]

---

[130] Cfr. Berra, Valerio. "Cos'è Black Basta, la Cybergang dell'attacco Hacker a Synlab che ha Rubato i Dati ai Pazienti." Fanpage.it, May 17, 2024.

[131] Cfr. Rivero, Marc, Jornt van der Wiel, Dmitry Galov, and Sergey Lozhkin. "Luna and Black Basta — New Ransomware for Windows, Linux and ESXi." Securelist by Kaspersky, July 20, 2022.

[132] Cfr. SYNLAB Italia. Aggiornamenti sui Sistemi.

Questa situazione ha causato un drastico rallentamento nella macchina sanitaria italiana[133], dato che *Synlab Italia* è presente in ben otto regioni, tra cui quelle a più alta densità abitativa[134]: Lombardia, Veneto, Friuli-Venezia Giulia, Emilia-Romagna, Lazio, Liguria, Campania e Toscana. Con circa 380 laboratori propri e svolgendo il ruolo di principale fornitrice per oltre 800 strutture sanitarie in tutta Italia, *Synlab* garantisce la realizzazione di circa 35 milioni di esami, tra prelievi del sangue, check-up e test prenatali.[135] È evidente, dunque, il sovraccarico ed il malfunzionamento di una macchina che richiederebbe un'attenzione tale da poter essere oleata alla perfezione, e che invece vive una situazione pressoché drammatica nel suo funzionamento ordinario, generando lunghissime liste d'attesa e favorendo la predominanza del settore sanitario privato rispetto a quello pubblico. È chiaro, quindi, che tale avvenimento criminale non costituisce altro che l'ennesimo problema che grava su istituzioni, strutture sanitarie e, soprattutto, sui cittadini. Sebbene il processo di isolamento del malware abbia causato un temporaneo malfunzionamento generale, è vero anche che nel giro di poco tempo è stata possibile una ripresa del sistema, che di fatto ha permesso il recupero delle condizioni precedentemente caratterizzanti. Tale situazione, dunque, rappresenta una minaccia indiretta e temporanea, che, tuttavia, presenta costi molto elevati, soprattutto in termini di manodopera specializzata e tecnologie di sicurezza avanzate, oltre che costi di downtime (perdita di entrate dovuta all'inattività dei sistemi), costi legali ed operativi.[136]

Se da un lato, dunque, abbiamo avuto modo di notare gli effetti che l'attacco ha generato in termini di interferenze con l'intero sistema, dall'altro lato troviamo la conseguenza maggiormente impattante, e che implica rischi maggiori: *1,5 terabyte* di dati sensibili di milioni di persone sono ora in mano a criminali che hanno tutta l'intenzione di utilizzarli al fine di perpetrare truffe, furti di identità e campagne di *phishing*.

---

[133] Cfr. Serena, Giulia. "Synlab Italia, Scoperti Finalmente gli Autori dell'Attacco Hacker." "Tom's Hardware", May 6, 2024.

[134] Cfr. Istituto Nazionale di Statistica (Istat). Annuario Statistico Italiano 2023. Roma: Istituto Nazionale di Statistica, 2023.

[135] Cfr. SYNLAB Italia. "Chi Siamo: Il Nostro Network."

[136] Cfr. SYNLAB: Pubblicati i Dati Sanitari dei Pazienti, Cosa Impariamo da Questo Grave Data Breach." CyberSecurity360.

Purtroppo, ad oggi, *Synlab* e le autorità competenti non hanno ancora fornito indicazioni precise sul numero esatto, o una stima affidabile, delle persone coinvolte come vittime, comunicando sul proprio sito web ufficiale che:

"*All'esito dell'attività di analisi seguirà la classificazione dei dati pubblicati al fine di individuare i soggetti interessati, alla data attuale non singolarmente identificabili."* [137]

In assenza di dati precisi, è opportuno, per comprendere la reale portata di questa minaccia, capire a quanto effettivamente corrispondano 1,5 terabyte di dati. Per attribuire a tale concetto una praticità che permetta, di fatto, di percepire le dimensioni indicate, prendiamo come punto di riferimento un film in alta risoluzione (1080p): affinché possa essere occupato uno spazio corrispondente a 1,5 terabyte, è necessario che, su tale disco di memoria, siano scaricati all'incirca 375 film da 2 ore ciascuno, occupando essi, in media, 4 gigabyte. 1,5 TB di dati, corrispondenti a 375 film da 2 ore, per un totale complessivo di 750 ore, equivalgono a 31,25 giorni passati a vedere film.

Secondo esempio: per riempire 1,5 terabyte di dati, sarebbe necessario immagazzinare circa 37.500 canzoni. In media, infatti, un brano musicale in formato MP3 a 320 kbps (alta qualità) occupa circa 10 megabyte per ogni minuto di musica, e se consideriamo che una canzone dura in media 4 minuti, ciascuna canzone occupa circa 40 megabyte.

Tutto ciò corrisponde ad oltre 3 anni di musica ininterrotta, ascoltata 24 ore su 24, senza che venga mai ripetuta una canzone. Una volta dunque aver dato un'idea dell'immensità dimensionale dell'attacco in questione, risulta più facile analizzare da un punto di vista oggettivo il malcontento e lo spiccato timore di centinaia di migliaia di individui, preoccupati che i loro dati possano essere utilizzati dai cybercriminali per scopi illeciti.

L'attacco hacker ha avuto un profondo impatto sull'immagine aziendale e sulla fiducia dei clienti, esponendo *Synlab* a una significativa perdita di credibilità circa le misure di sicurezza intraprese e, di riflesso, all'attenzione che essa ripone verso la sicurezza e la privacy dei clienti.[138] Essendo uno degli effetti più immediati, il danno alla reputazione dell'azienda risulta anche uno tra i più devastanti, che viene alimentato persino dalle misure intraprese successivamente a fini di contrasto. In particolare, la decisione di *Synlab* di non pagare il riscatto richiesto dagli hacker, pur riflettendo un impegno etico

---

[137] Cfr. SYNLAB Italia. Aggiornamenti sui Sistemi.

[138] Cfr. Cyberattack Shuts Down 380 Labs in Italy: SYNLAB Scrambles to Protect Patient Data." CloudSEK News, April 2024.

per non finanziare attività criminali, ha portato alla pubblicazione dei dati rubati sul *dark web*, accentuando ulteriormente il danno reputazionale. In risposta agli effetti descritti, *Synlab* ha intrapreso diverse misure per contenere il danno e rassicurare i clienti, dando vita ad una stretta collaborazione con le autorità competenti per investigare sulla vicenda, comunicando pubblicamente il proprio impegno a informare le persone coinvolte. Queste azioni, tuttavia, sebbene necessarie, potrebbero non essere sufficienti a riparare rapidamente il danno reputazionale subito, in quanto la fiducia dei clienti è stata più che scossa, e il processo di riconquista si presenta in prospettiva lungo e complesso.

### 3.1.4. Cosa può accadere in ottica criminosa: possibili risvolti criminali

In seguito al rifiuto da parte di *Synlab* di soddisfare la richiesta estorsiva, come ribadito diverse volte nel testo, l'organizzazione criminale *Black Basta* ha proceduto alla pubblicazione, sul *dark web*, dei dati oggetto del furto.
Questa, la promessa mantenuta dai criminali, che porta alla formazione di conseguenti nuovi scenari, di diversa entità. I seguenti, caratterizzati quasi principalmente, in ottica criminosa, dall'utilizzo dei dati ora facilmente accessibili ai malintenzionati, che possono sfruttarli in diverso modo. Dibattendo riguardo alcune delle modalità tramite le quali tali utilizzi possono essere concretizzati, risulta di fondamentale importanza menzionare quelle rappresentate da: furti di identità, minacce estorsive e attacchi mirati, truffe e frodi mediche, e ultime ma non per importanza, meccanismi di *phishing*.
Riguardo i furti di identità, occorre in prima istanza sapere perché essi avvengono, e quale sia il potenziale utilizzo da parte dei criminali. Secondo Claudio Telmon, esperto del *Clusit* (associazione cyber security italiana), e come anche riportato da *Ilsole24Ore*[139], il furto di identità avviene principalmente in due casi: il primo, quando qualcuno utilizza l'identità di un'altra persona al fine di svolgere attività le cui conseguenze si vogliono addossare a un altro individuo, come nel caso di un finanziamento al consumo. In questa situazione, un malintenzionato potrebbe usare le informazioni personali di una vittima,

[139] Cfr. Longo, Alessandro. "Furto di identità: ecco quali informazioni e (dati) tenere protetti." Il Sole 24 ORE.

ad esempio, per ottenere un prestito personale o una carta di credito a suo nome, facendo poi acquisti e lasciando alla vittima l'onere di ripagare il debito. In questo caso, al criminale non interessa chi sia la vittima. Diverso negli scopi è il secondo caso, ove il criminale agisce per compiere operazioni a nome della specifica persona cui appartengono i dati, come un'impersonificazione su un social network al fine di attribuirle dichiarazioni che non le appartengono. Da un punto di vista giuridico, il furto d'identità è disciplinato ai sensi dell'*articolo 494 del Codice penale* che prevede il reato di sostituzione di persona, al fine di tutelare tanto la fede pubblica quanto gli interessi del privato, recitando:

"*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno".*[140]

Nei riguardi di quelle che indichiamo con l'espressione "minacce estorsive", l'articolo del Codice penale italiano che le disciplina è il 629. Tale articolo definisce le condotte che configurano il reato e stabilisce le relative sanzioni.

Nello specifico: *"Chiunque, mediante violenza o minaccia, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000."*[141]

Questa categoria di minaccia si basa su attacchi mirati nei confronti della vittima, con l'obiettivo di spingerla a compiere una determinata azione per ottenere un ingiusto profitto a suo discapito. Attacchi di questo tipo, nel contesto dell'analisi in corso, possono essere particolarmente pericolosi a seconda del grado di sensibilità dei dati coinvolti, poiché ciò aumenta il potere coercitivo dei malintenzionati.

Le conseguenze di tali attacchi possono essere gravi e di vasta portata. Una delle principali rappresentata dalla perdita economica che le vittime possono subire a causa della pressione subita ad opera degli aggressori, derivante sia dai pagamenti richiesti sia

---

[140] Cfr. Codice Penale: art. 494. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

[141] Cfr. Codice Penale: art. 629. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

dai costi associati alla protezione dei propri dati e alla riparazione dei danni.[142] Vanno osservati con molta attenzione, poi, quelle che sono le conseguenze psicologiche potenzialmente causate da tali minacce. La costante pressione e il timore di ulteriori minacce sono in grado di generare stress e ansia di varia intensità, causando problemi come il *disturbo da stress post-traumatico* (*PTSD*), o traumi duraturi, che influenzano negativamente la qualità della vita e la salute mentale delle persone coinvolte.[143]

Un'altra grave conseguenza è la compromissione della reputazione. Se le informazioni sensibili delle persone minacciate includono dati personali o relativi alla loro sfera più intima, è possibile che ne derivino danni reputazionali significativi. Un esempio specifico è rappresentato dalle *sextorsion* finanziarie, che sono aumentate di circa il 150% dal 2022 (10.731 segnalazioni) al 2023 (26.718 segnalazioni), secondo i dati del *National Center for Missing & Exploited Children* (*NCMEC*).[144] Ulteriore modalità di sfruttamento criminale dei dati oggetto del furto, consiste nel compiere truffe e frodi mediche, che pur rappresentando un aspetto meno noto, rispetto alle minacce estorsive e il furto di dati, risulta altrettanto rischiosa e preoccupante. Esse possono essere eseguite per vari scopi, generalmente accomunati dalla natura profittevole dello sfruttamento, e attuate tramite diverse modalità di utilizzo.

Una delle frodi mediche più comuni e rilevanti è la presentazione di falsi reclami assicurativi. I criminali, utilizzando i dati rubati, sono in grado di inventare diagnosi o trattamenti medici mai effettivamente ricevuti dalle vittime, presentando richieste di rimborso alle compagnie assicurative. La riuscita di queste procedure si basa sull'utilizzo estremamente dettagliato dei dati dei pazienti, che rende difficile per le compagnie assicurative distinguere tra richieste legittime e fraudolente.

I truffatori, inoltre, possono combinare informazioni di più persone al fine di dar vita a identità fittizie, presentando così richieste di rimborso multiple, massimizzando il loro profitto illegale. A tal proposito, un'azione coordinata del *Dipartimento di Giustizia degli Stati Uniti* ha portato all'accusa di 36 imputati per schemi fraudolenti che coinvolgevano

---

[142] Cfr. Higgins, Malcolm. "Cyber extortion: What is it and how to protect yourself." NordVPN.

[143] Cfr. Quali sono i diversi tipi di molestie? E quali le conseguenze psicologiche?" GuidaPsicologi, June 3, 2021.

[144] Cfr. NCMEC Releases New Sextortion Data." National Center for Missing & Exploited Children, April 15, 2024.

oltre 1,2 miliardi di dollari in richieste relative alla telemedicina e a test medici di svariato tipo.[145] La frode medica attraverso la presentazione di false richieste di risarcimento assicurativo è un problema significativo che colpisce sia i programmi sanitari nazionali (o federali, nel caso degli Stati Uniti), che gli assicuratori privati.

Un altro modo in cui le informazioni sanitarie possono essere sfruttate per ottenere un illecito profitto è la creazione di false prescrizioni mediche. Ciò consente ai criminali di ottenere costosi farmaci, come quelli utilizzati per trattamenti antitumorali o malattie croniche, senza pagarli, rivendendoli poi sul mercato nero, generando ingenti profitti.

In Italia, da un punto di vista giuridico, tali fenomeni sono disciplinati da due specifici articoli del Codice penale: l'*Art. 640*[146], che prevede il reato di truffa, particolarmente applicabile al fenomeno dei risarcimenti assicurativi, e l'*Art. 640 bis*[147], che riguarda la truffa aggravata per il conseguimento di erogazioni pubbliche.

I meccanismi di *phishing*, in ultima istanza, si manifestano attraverso l'utilizzo di e-mail e messaggi falsi creati con l'intento di ingannare le vittime inducendole a rivelare, nel nostro contesto di analisi, informazioni finanziarie o di accesso. Questo fenomeno rappresenta una tra le minacce più gravi e complesse in tale contesto, dato che i dati sanitari sono altamente preziosi, contenendo essi informazioni specifiche circa: nomi, indirizzi, numeri di telefono, codice fiscale, e altri dettagli medici. Sono infatti diverse le ragioni e le tecniche attraverso cui si manifesta il particolare interesse dei criminali riguardo i dati sanitari. Innanzitutto, è opportuno menzionare una delle tecniche più comuni, quale l'invio di e-mail e SMS personalizzati, all'interno dei quali i truffatori si immedesimano in fornitori di servizi sanitari, cliniche o assicurazioni nel modo più accurato possibile, utilizzando le informazioni rubate per personalizzare le comunicazioni inviate, rendendole più credibili. Questi messaggi possono contenere link a siti web falsi che imitano quelli legittimi, dove le vittime sono indotte a inserire ulteriori informazioni personali o credenziali di accesso, nonché dati finanziari. Un'altra tecnica fraudolenta, tramite *phishing*, è rappresentata dalle telefonate ingannevoli. Utilizzando le informazioni rubate, i truffatori chiamano le vittime fingendosi rappresentanti di istituti medici o

---

[145] Cfr. False Claims Act Settlements and Judgments Exceed $2.68 Billion in Fiscal Year 2023. United States Department of Justice, February 22, 2024.

[146] Cfr. Codice Penale: art. 640. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

[147] Cfr. Codice Penale: art. 640 bis. Gazzetta Ufficiale della Repubblica Italiana

assicurativi. Queste telefonate sfruttano il contatto diretto e la pressione psicologica per indurre la vittima a compiere azioni di diversa natura. I truffatori creano scenari credibili, come la necessità di aggiornare le informazioni dell'assicurazione sanitaria, confermare appuntamenti medici o discutere di risultati di esami urgenti, facendo spesso riferimento, durante e queste telefonate, a dettagli personali e medici della vittima per dimostrare autenticità e ottenere fiducia. Un alternativo metodo, altrettanto subdolo, è rappresentato dall'invio di fatture false per prestazioni sanitarie mai ricevute. Compito di chi attua questa strategia criminale è di rendere le fatture ben dettagliate e professionalmente curate, in modo che siano più autentiche possibile. Al fine di aumentare la pressione, i truffatori possono includere minacce di azioni legali o di segnalazioni negative agli uffici di credito se la fattura non viene pagata entro un certo termine. Le vittime sono poi invitate a pagare tramite metodi che rendono difficile il recupero del denaro.[148]
Alla luce di ciò, risultano chiari e tangibili i rischi legati ad un potenziale utilizzo, pressoché certo, dei sensibili dati pubblicati sul *dark web*, da parte di malintenzionati che, con una certa cura nella ricerca delle vittime adatte, tenteranno di trarre ingenti profitti economici.

## 3.2. Controlli, prevenzione e contrasto

### 3.2.1. Regolamento Generale sulla Protezione dei Dati: GDPR

*Synlab*, essendo un'impresa operante in un delicato settore come quello medico-diagnostico, è tenuta a rispettare svariate norme e regolamenti, di diversa natura.
In tal senso, risulta fondamentale approfondire la questione legata al *GDPR: Regolamento Generale sulla Protezione dei Dati*, anche conosciuto come Regolamento UE 2016/679, attuato in Italia attraverso il Decreto Legislativo n. 101 del 10 agosto 2018. Tale regolamento, entrato in vigore il 25 maggio 2018, ha introdotto una serie di norme volte alla tutela dei dati personali per tutte le aziende operanti all'interno dell'Unione

[148] Cfr. National Health Care Fraud Enforcement Action Results in Charges Involving over $1.4 Billion in Alleged Losses," United States Department of Justice.

Europea.[149] Le organizzazioni che trattano questi dati devono adottare adeguate misure tecniche e organizzative al fine di proteggerli, tutelando in tal modo i consumatori, e garantendo una maggiore sicurezza e riservatezza. Quando si verifica un furto di dati, come quello subito da *Synlab*, le disposizioni del *GDPR* offrono un limpido quadro tramite il quale è possibile gestire l'incidente e le conseguenze da esso generate. Innanzitutto, è obbligo dell'azienda attivare in modo tempestivo un piano di risposta che includa la valutazione dell'estensione della violazione, l'identificazione delle vulnerabilità sfruttate, e la messa in atto di misure correttive per impedire ulteriori accessi non autorizzati. Secondo le disposizioni del *GDPR*, *Synlab* deve notificare le violazioni subite alle autorità di controllo competenti entro 72 ore dalla scoperta delle stesse, come è infatti avvenuto il 20 aprile 2024, a distanza di circa 48 ore dall'attacco. La notifica deve includere una descrizione della natura della violazione dei dati personali, il numero approssimativo degli individui coinvolti, le categorie di dati compromessi, e le ipotizzabili conseguenze della violazione. Se la violazione dei dati comporta un rischio elevato per i diritti e le libertà delle persone fisiche, *Synlab* ha l'obbligo di informare anche gli interessati senza ritardo, comunicando loro in modo chiaro tutte le informazioni pertinenti, affinché essi abbiano la facoltà di adottare le misure necessarie per proteggersi, entro i limiti di autonomia.

Un elemento fondamentale del *GDPR* è rappresentato dalla responsabilità proattiva, secondo cui le aziende devono adottare misure preventive per la protezione dei dati. Ciò, applicato a *Synlab*, significa assicurarsi che tutti i dati personali siano adeguatamente crittografati e pseudonimizzati, riducendo così il rischio di esposizione in caso di furto.

Oltre che alla risposta a possibili incidenti e violazioni, particolarmente rilevanti sono le disposizioni del *GDPR* relative alla gestione dei dati personali nelle aziende sanitarie. Queste organizzazioni, come già detto, trattano dati sensibili, e pertanto sono soggette a obblighi ancora più stringenti. Prima di tutto, le aziende sanitarie devono condurre una valutazione d'impatto sulla protezione dei dati (*DPIA*), come previsto dall' *art. 35* e dai *considerando n. 90 e 93* del regolamento[150], quando il trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche.

---

[149] Cfr. Garante per la Protezione dei Dati Personali. 'Il testo del Regolamento (UE) 2016/679

[150] Cfr. Articolo 35 GDPR: Valutazione di Impatto sulla Protezione dei Dati." Altalex, April 12, 2018.

Un secondo aspetto dalla medesima importanza è la nomina di un *Responsabile della Protezione dei Dati* (*DPO*), il quale ha il compito di monitorare la conformità dell'azienda al *GDPR*, fungere da punto di contatto per le autorità di controllo e gli interessati, e fornire consulenza sulle attività di trattamento dei dati.
Infine, il *GDPR* richiede che le aziende mantengano un registro delle attività di trattamento dei dati, documentando dettagliatamente ogni operazione di trattamento, inclusi i fini di esso, le categorie dei dati personali trattati, i soggetti interessati, e le misure di sicurezza adottate. Questo registro deve essere aggiornato regolarmente e messo a disposizione delle autorità di controllo su richiesta.

### 3.2.2. Contesto normativo italiano: DL n. 65/2018; DDL Cybersicurezza

Avendo analizzato la situazione normativa circa la sicurezza relativa alla raccolta e alla gestione dei dati a livello europeo, soffermandoci sul *GDPR*, risulta opportuno restringere il campo visivo, andando a descrivere quelli che sono stati i risvolti normativi in Italia in seguito al *Decreto Legislativo n. 65/2018*, analizzando al contempo le prospettive future con il *DDL Cybersicurezza*, attualmente in fase di revisione parlamentare.
Il Decreto legislativo n. 65 del 2018 [151], noto anche come "*Decreto per la sicurezza delle reti e dei sistemi informativi*", è stato adottato dall'Italia al fine di recepire la *Direttiva (UE) 2016/1148*, conosciuta come *Direttiva NIS* (*Network and Information Security*), precedentemente trattata al punto 2.1.1. L'obiettivo di questo decreto è di rafforzare la sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura di servizi essenziali in settori critici come energia, trasporti, banche, fornitura e distribuzione di acqua potabile e infrastrutture digitali.
Riguardo la cooperazione tra gli Stati membri dell'Unione Europea in materia di cybersecurity, occorre sottolineare che tale misura legislativa ha proceduto all'identificazione degli *Operatori di Servizi Essenziali* (*OSE*), ovvero le entità che forniscono servizi essenziali la cui interruzione avrebbe un impatto significativo sulla

[151] Cfr. Gazzetta Ufficiale: DECRETO LEGISLATIVO 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016

società e sull'economia. Il decreto, nello specifico, stabilisce criteri per identificare questi operatori, richiedendo loro di adottare misure di sicurezza adeguate e di notificare tempestivamente gli incidenti rilevanti. Rimanendo nell'ambito della cooperazione internazionale, è stato istituito un quadro per la cooperazione tra diverse autorità competenti e il *Computer Security Incident Response Team* (*CSIRT*), che funge da punto di contatto unico per la gestione degli incidenti di sicurezza informatica sia a livello nazionale che transfrontaliero.

Il furto di dati subito da *SynLab* sottolinea la rilevanza delle misure di sicurezza informatica previste dal *Decreto legislativo n. 65/2018*, ed in particolare la necessità di implementare rigorosi protocolli per proteggere i dati sensibili e garantire la continuità dei servizi essenziali. *Synlab Italia* ha infatti comunicato prontamente alle autorità incaricate, potendo così rispondere nel modo maggiormente adatto, volto a limitare i danni e a prevenire ulteriori violazioni e minacce da parte del gruppo criminale.

Volendo compiere un'analisi orientata verso le prospettive future in tema di cybersicurezza, occorre menzionare il *DDL Cybersicurezza*[152], il quale rappresenta un passo necessario al fine di rafforzare la protezione delle infrastrutture critiche in Italia, comprese le aziende sanitarie.

Approvato dal *Consiglio dei ministri* il 25 gennaio 2024, il *DDL Cybersicurezza* ha come obiettivo l'invigorimento della sicurezza informatica in Italia, mediante l'introduzione di norme volte alla protezione delle infrastrutture critiche e alla gestione efficace degli incidenti informatici, promuovendo al contempo la collaborazione tra enti pubblici e privati. Attualmente in fase di revisione in Senato, il *DDL cybersicurezza* prevede, nello specifico, un inasprimento delle pene per i reati informatici, al fine di dissuadere i cybercriminali e ridurre la frequenza degli attacchi. Esso introduce nuove figure di reato come l'estorsione cibernetica, che abbiamo analizzato precedentemente al fine di sottolineare l'enorme potere che, talvolta, i criminali posseggono. Il *DDL cybersicurezza* è caratterizzato da un ulteriore elemento chiave, quale il rafforzamento delle capacità *dell'Agenzia per la Cybersicurezza Nazionale* (*ACN*), la quale vedrà ampliati i propri compiti, includendo tra essi la promozione dell'intelligenza artificiale come strumento per la cybersicurezza. Esprimendosi anche riguardo la pubblica amministrazione, il

[152] Cfr. Comunicato stampa del Consiglio dei ministri n. 78." Governo Italiano.

disegno di legge introduce nuovi obblighi, tra cui la notifica all'*ACN* di eventuali incidenti informatici che abbiano un impatto su reti, sistemi informativi e servizi entro 24 ore dalla loro conoscenza. Sarà inoltre introdotta una figura dedicata alla cybersecurity in ogni amministrazione pubblica, responsabile della gestione e del coordinamento delle misure di sicurezza informatica.
In conclusione, è possibile affermare che se le novità previste dal *DDL cybersicurezza* fossero state già implementate alla data di esecuzione dell'attacco hacker, *Synlab* avrebbe potuto limitarne l'impatto, riducendo inoltre la diffusione delle informazioni.

# Conclusioni

Volendo trarre le fila dell'analisi sin qui condotta, appare evidente e tangibile il rischio cui la modernizzazione tecnologica ci sottopone.
Fin dall'antichità, infatti, ad ogni genuina evoluzione in grado di apportare significativi positivi cambiamenti alla vita delle persone, è corrisposto un parallelo sviluppo caratterizzato dalla ricerca di profitto di qualunque genere, da parte di una minoritaria fetta di popolazione alla ricerca di fortuna mediante meccanismi elusivi, capaci di lesionare gli schemi della società civile, generando domanda circa soluzioni regolatrici atte alla soppressione dei predetti metodi criminali. Emerge dunque chiaro lo storico compito civile di repressione e contrasto, nonché di previsione e regolamentazione.
Quella che dunque può essere definita fascia grigia del processo evolutivo sociale, è stata in grado di cambiare e adattarsi in risposta ai costanti tentativi di repressione, aggiornandosi sempre più in fretta, e stanziando le proprie radici all'interno del circuito economico e sociale "legale", ad oggi osservabile tramite i meccanismi di una criminalità sempre più organizzata e intelligente.
Al giorno d'oggi, scontrarsi con la criminalità organizzata, andando dunque ad interagire coi cosiddetti "sistemi", e di riflesso con quella criminalità che sfrutta la realtà digitale per perpetrare illiceità di ogni tipo, risulta essere un fenomeno alquanto complicato, e talvolta rischioso, che richiede una spinta predittiva, strategica e regolatrice da parte delle autorità dedite alla soppressione criminale, e ai diversi legislatori di tutto il mondo.
Tirando le somme di quanto descritto all'interno del presente elaborato, ritroviamo la messa in evidenza circa la scelta delle vittime, modalità e scopi di aggressione da parte di

una criminalità che sfrutta a proprio vantaggio il digitale e gli strumenti che da esso dipendono.

Il primo capitolo ha avuto l'obiettivo di definire storicamente il fenomeno del cybercrime, andando a comprenderne le origini, i ricorrenti schemi di pensiero e di operatività, nonché l'impegno da parte delle istituzioni e delle autorità nella soppressione di esso.

Nei riguardi della scelta delle vittime ad opera di tali soggetti criminali, è importante sottolineare la sensibilità dei settori maggiormente colpiti, evidenziando come, nella maggior parte dei casi, sensibilità e profittabilità risultano in un rapporto di preziosità direttamente proporzionale. Ciò è alquanto evidente nei casi riportati, che riguardano il settore bancario e sanitario, spesso bersagli di attacchi informatici da parte di individui o organizzazioni, generando in tal modo l'esigenza di ingenti investimenti in cybersecurity, nonché i costanti rischi reputazionali cui si va in contro, se esposti a questo tipo di criminalità.

Caratterizzato da estrema resilienza e rapida capacità di adattamento alle circostanze regolatrici, il cybercrime annovera, spesso, eccellenti abilità nell'utilizzo delle nuove tecnologie, riuscendo talvolta a costituire motore di innovazioni cui può giovare la totalità della popolazione, non relegando la stessa alla zona grigia in precedenza oggetto di riferimento.

Il secondo capitolo dell'elaborato esplora il rapporto tra giurisprudenza e tecnologia, analizzando come l'una sia costantemente influenzata dall'altra, e come la forte presenza della criminalità organizzata a livello transfrontaliero renda urgente un intervento coordinato atto alla prevenzione e al contrasto da parte delle autorità internazionali, tenute a collaborare strettamente al fine di contenere e minimizzare i rischi derivanti da operazioni criminale di diverso genere ed entità. L'attenzione riposta al fenomeno del riciclaggio di denaro ed altri beni di valore sottolinea la complessità e la ramificazione di un sistema all'interno del quale, nel corso del tempo, è stato possibile eludere leggi, corrompere i meccanismi giudiziari e legislativi, sfruttando cavilli legali al fine di trarre vantaggio in termini di realizzazione di circuiti di riciclaggio.

Rappresentando, le risorse utilizzate, una grande fetta della ricchezza globale totale, intercettarle e scoprirne le illecite modalità di sfruttamento costituirebbe un atto capace di generare effetti positivi per la totalità dei cittadini, disincentivando al contempo i criminali dal compimento di reati realizzati al fine di trarre profitto economico.

Il caso d'indagine del terzo capitolo rappresenta una lente d'ingrandimento pratica di quanto descritto in linea teorica, mostrando esso l'effettivo potenziale distruttivo dei crimini perpetrati sul digitale, e nello specifico del furto di dati personali e conseguenti richieste estorsive. Tale analisi risulta utile al fine di comprendere il modus operandi e gli schemi di pensiero delle organizzazioni criminali, osservando da un punto di vista pratico i risvolti preventivi e di contrasto posti in atto da *Synlab*, l'azienda vittima dell'attacco, e dalle istituzioni in generale, giungendo, in questo caso, a porre maggiore pressione circa l'approvazione del *DDL Cybersicurezza*, che rappresenta un punto di svolta fondamentale all'interno del panorama legislativo italiano in materia di criminalità informatica.

Considerando l'approfondita analisi condotta, è con decisa chiarezza che emergono gli effettivi rischi di mercato e i vuoti regolamentari causati dalla criminalità informatica, la quale gode, grazie alle sue caratteristiche principali, dell'assenza di confini fisici al di fuori dei quali non è possibile operare, e che va, di fatto, a donare aspetti globalizzanti persino a quella costante ricerca di illegittime soluzioni in grado di fornire ricchezza, eludendo i meccanismi che costituiscono le fondamenta della società civile all'interno della quale viviamo.

In conclusione, risulta evidente, in tale contesto, un approccio multidimensionale atto alla repressione e al contrasto della criminalità, che comprenda non solo la rigida applicazione della legge, ma anche una cooperazione più intensa e un continuo impegno nel promuovere l'educazione alla sicurezza digitale tra i cittadini e le organizzazioni. Infatti, mentre la tecnologia continua a evolvere a un ritmo senza precedenti, anche il campo del cybercrime si trasforma con essa, rappresentando un formidabile banco di prova per l'efficacia e la resilienza dei sistemi legislativi e di sicurezza globali, continuamente impegnati nelle sfide poste dalla pervasività e sofisticazione insite in tale fenomeno criminale, e dalle organizzazioni in esso coinvolte.

# Bibliografia


Agence nationale de la sécurité des systèmes d'information (ANSSI). "Ransomware Attacks: All Concerned."

Annunziata, Filippo, et al. Cripto attività: antiriciclaggio e gestione dei rischi aziendali. Pisa: Pacini giuridica, 2024.

Banca d'Italia Eurosistema. "Supervisione e Normativa Antiriciclaggio."

Banca d'Italia Eurosistema. Quaderni dell'antiriciclaggio; Analisi e Studi: Il Riciclaggio nella Prospettiva Penale ed in Quella Amministrativa; Definizioni di Riciclaggio.

Chainalysis. "Report sui Crimini Crypto." February 2023.

Chainalysis. "The Chainalysis 2022 Crypto Crime Report."

Codice Penale, art. 494. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

Codice Penale, art. 629. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

Codice Penale, art. 640 bis. Gazzetta Ufficiale della Repubblica Italiana.

Codice Penale, art. 640. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

Codice Penale, art. 648-bis. Gazzetta Ufficiale della Repubblica Italiana, October 26, 1930.

Collins, John. "Crypto, Crime and Control; Cryptocurrencies as an Enabler of Organized Crime." June 2022.

Colombo, Cristina F. Geodiritto, globalizzazione e nuovi canali per i reati d'impresa. Milano: Wolters Kluwer, 2021.

Comunicato stampa del Consiglio dei ministri n. 78. Governo Italiano.

Council of Europe. "Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224)."

Csigbologna. "Convenzione di Budapest sulla Criminalità Informatica a 20 Anni dall'Approvazione."

Cybercrime Convention Committee (T-CY). "The Budapest Convention on Cybercrime: Benefits and Impact in Practice."

De Simone, Maria Vittoria. "Reato di riciclaggio: elementi costitutivi, pena e procedibilità." DeQuo, October 29, 2021.

Dirittoaldigitale.com: CyberItalia. "Dalla Direttiva NIS 1 alla NIS 2 in Pillole."

Dragomir, A. V. "What's New in the NIS 2 Directive Proposal Compared to the Old NIS Directive." SEA: Practical Application of Science, 2021.

ESMA50-157-1391. "Advice on Initial Coin Offerings and Crypto-Assets," January 9, 2019.

EUR-Lex. "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018." May 30, 2018.

EUR-Lex. “Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories
European Commission. “Communication from the Commission to the European Parliament and the Council Towards Better Implementation of the EU’s Anti-Money Laundering and Countering the Financing of Terrorism Framework.” July 24, 2019.

European Commission. “Digital Finance Package.” Directorate-General for Financial Stability, Financial Services and Capital Markets Union. September 24, 2020

Federal Trade Commission. “Equifax, Inc.”, July 31, 2019.

Financial Action Task Force (FATF). “Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services.”

Financial Action Task Force (FATF). “Le Raccomandazioni del GAFI del 2012 Sono Standard Internazionali per Contrastare il Riciclaggio di Denaro, il Finanziamento del Terrorismo e la Proliferazione delle Armi di Distruzione di Massa.”

Financial Action Task Force (FATF). “Money Laundering and Terrorist Financing in the Art and Antiquities Market.” February 27, 2023.

Fisicaro, Marco, and Luigi Ciampoli. La criminalità economica organizzata: analisi comparata con la conspiracy statunitense. Milano: UTETgiuridica, 2022.

Galmarini, Sabrina. Antiriciclaggio. Milano: Wolters Kluwer, 2019.

Gazzetta ufficiale dell’Unione Europea. “Conclusioni del Consiglio «Sinergie tra Eurojust e le Reti Istituite dal Consiglio nel Settore della Cooperazione Giudiziaria in Materia Penale» (2019/C 207/01).”

Gazzetta ufficiale dell’Unione europea. “DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.” December 14, 2022

Gazzetta ufficiale dell’Unione europea. “REGOLAMENTO (UE) 2023/1114.” L 150/40.

Gazzetta Ufficiale. “Art. 648-bis. (Riciclaggio).”

Gazzetta Ufficiale. “DECRETO LEGISLATIVO 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016.”

Gratteri, Nicola, and Antonio Nicaso. Fiumi d’oro. Milano: Mondadori, 2018.

Gratteri, Nicola, and Antonio Nicaso. Il grifone. Come la tecnologia sta cambiando il volto della ‘Ndrangheta. Milano: Mondadori, 2024.

Hacking: Evolution, Conceptualization, and the Perpetrators. Contemporary Challenges for Cyber Security and Data Privacy. ResearchGate.

InsideOver. “Così Terrorismo e Criminalità Sfruttano il Lato Oscuro dei Social Media.”

Investopedia. “Crypto Lending: What It Is, How It Works, Types.” August 16, 2023.

Istituto Nazionale di Statistica (Istat). Annuario Statistico Italiano 2023. Roma: Istituto Nazionale di Statistica, 2023.

Jordan, Tim. “A Genealogy of Hacking.” Sage Journals, Volume 23, no. 5.

Knowledgehut. “La sicurezza informatica nel settore bancario: importanza, minacce, sfide.”

KPMG. “Network & Information Security Directive (NIS2).”

LAUDATI, “I delitti transnazionali, nuovi modelli di incriminazione e di procedimento all’interno dell’Unione Europea”, in Dir. Pen. Proc. 2006, p. 401

Laudati. “I delitti transnazionali, nuovi modelli di incriminazione e di procedimento all’interno dell’Unione Europea.”

Lifshits, I. “Cryptocurrencies in the Regulatory Field of International Organizations.” In *Current Achievements, Challenges and Digital Chances of Knowledge-Based Economy*, edited by S.I. Ashmarina and V.V. Mantulenko.

Longo, Alessandro. “Furto di identità: ecco quali informazioni e (dati) tenere protetti.” Il Sole 24 ORE.

Mahawar, Sneha. “Cybercrime and its impact on the banking industry.” IPleaders.

Mahawar, Sneha. “Cybercrime and Its Impact on the Banking Industry.” IPleaders.

Nicotra, Massimiliano, Fulvio Sarzana di S. Ippolito, and Massimo Simbula. Micar - Guida al Regolamento Europeo sui Mercati dello Cripto. Milano: Giuffrè Francis Lefebvre, 2023.

Paracampo, Maria-Teresa. FinTech: introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari. 2nd ed. Torino: Giappichelli, 2019.

Parlamento.it. Legge 18/03/2008.

Parodi, Cesare, and Valentina Sellaroli, eds. Diritto Penale dell’Informatica. Milano: Giuffrè, 2024.

Pellegrini, Mirella. “Il sistema delle fonti.” In Diritto pubblico dell’economia, 85. Padova: Cedam, 2023.

Rea, Alessandra. “Criptovalute: a Che Punto Siamo?” Diritto Penale e Uomo. Published July 22, 2020.

Risk & Compliance: Platform Europe. “L’infiltrazione della Criminalità Organizzata nell’Economia Italiana: dalla Prevenzione al Contrasto.”

Rivero, Marc, Jornt van der Wiel, Dmitry Galov, and Sergey Lozhkin. “Luna and Black Basta — New Ransomware for Windows, Linux and ESXi.” Securelist by Kaspersky, July 20, 2022.

Rusi.org. “Financial Institutions and Cybercrime: Threats, Challenges and Opportunities.”

S&P Global Ratings. “Cyber Risk Insights: European Banks’ IT Complexity Amplifies Risk.”

Sandei, Claudia. L’offerta iniziale di cripto-attività. Torino: Giappichelli, 2022.

Savona. “Processi di globalizzazione e criminalità organizzata transnazionale.”

Schmitz-Berndt, Sandra. “Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive.” Journal of Cybersecurity.

Sharma, Pradip Kumar, Mu-Yen Chen, and Jong Hyuk Park. “A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT.”

Sistema Penale. “Minaccia Cibernetica e Nuovi Paradigmi della Cooperazione Giudiziaria Internazionale: Il Ruolo di Eurojust.” July 14, 2023

SoSafe. Cybercrime Trends 2024: The Latest Threats and Security Best Practices.

SpringerLink. “ENISA’s Contribution to National Cyber Security Strategies.”

U.S. Department of Health and Human Services. “Black Basta Threat Profile.”
United States Senate Committee on Homeland Security & Governmental Affairs. U.S. Senator Gary Peters, Chairman. “Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns.”

Yilma, Kinfe. “Privacy and the Role of International Law in the Digital Age.” In Internet Bills of Rights. Chapter 4.

Ziccardi. Hacker. Il Richiamo della Libertà. Milano, 2011.

# Sitografia

Articolo 35 GDPR: Valutazione di Impatto sulla Protezione dei Dati. Altalex, April 12, 2018. https://www.altalex.com/documents/news/2019/06/06/valutazione-impatto-sulla-protezione-dei-dati-istruzioni-operative-e-modulistica

Aucone, Giovanna, and Valentina Groccia. “Il Reato di Riciclaggio nella Normativa Italiana.” Allianz Darta, May 24, 2022. https://news.allianzdarta.ie/esperto-risponde/il-reato-di-riciclaggio-nella-normativa-italiana/

Autorità europea degli strumenti finanziari e dei mercati. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-securities-and-markets-authority-esma_it

Baiguera Altieri, Dott. “La cultura Hacker negli Stati Uniti d’America.” In La criminalità informatica in Svizzera e in Italia. Diritto.it. https://www.diritto.it/la-criminalita-informatica-in-svizzera-ed-in-italia/

Banca Centrale Europea. Vigilanza bancaria della BCE: Valutazione dei rischi e delle vulnerabilità per il 2021. https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2021~edbbea1f8f.it.html

Berra, Valerio. “Cos’è Black Basta, la Cybergang dell’attacco Hacker a Synlab che ha Rubato i Dati ai Pazienti.” Fanpage.it, May 17, 2024. https://www.fanpage.it/innovazione/tecnologia/cose-black-basta-la-cybergang-dellattacco-hacker-a-synlab-che-ha-rubato-i-dati-ai-pazienti/

Chase.com. “Online Banking vs. Traditional Banking: Exploring the Differences.” https://www.chase.com/personal/banking/education/basics/banking-traditional-vs-online-banking

Cocomazzi, Antonio, and Antonio Pirozzi. “Black Basta Ransomware Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor.” SentinelOne, November 3, 2022. https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

Computer Emergency Response Team AGID. “Con il termine Botnet, “rete di robot”, si indica un insieme di computer o dispositivi che, precedentemente compromessi da parte di un malware, permette a un soggetto terzo di impartire istruzioni da remoto.” https://cert-agid.gov.it/glossario/botnet/

Cyberattack Shuts Down 380 Labs in Italy: SYNLAB Scrambles to Protect Patient Data. CloudSEK News, April 2024. https://news.cloudsek.com/2024/04/cyberattack-shuts-down-380-labs-in-italy-synlab-scrambles-to-protect-patient-data/

CyberProof Blog. “How Ransomware Actors Use EDR Bypassing to Run Cybercrime Campaigns.” https://www.cyberproof.com/blog/how-ransomware-actors-use-edr-bypassing-to-run-cybercrime-campaigns

Cybersecurity and Infrastructure Security Agency. “CISA and Partners Release Advisory on Black Basta Ransomware.” May 10, 2024. https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware

De Nederlandsche Bank. Eurosysteem: Innovation in Payments and Banking, Cybercrime. https://www.dnb.nl/en/innovations-in-payments-and-banking/

Dezzani, Giuseppe. “La criminalità informatica.” Diritto.it. https://www.diritto.it/la-criminalita-informatica/

Dirittobancario.it. “MiCAR: Le Prossime Misure di Attuazione per i Mercati delle Cripto-Attività.” https://www.dirittobancario.it/art/micar-le-prossime-misure-di-attuazione-per-i-mercati-delle-cripto-attivita/

DLA Piper. “Anti Money Laundering Directive in Italy.” June 26, 2017. https://www.dlapiper.com/it-it/insights/publications/2017/06/anti-money-laundering-directive-in-italy

Enciclopedia Treccani. “Cracker.” https://www.treccani.it/vocabolario/cracker/

Enciclopedia Treccani. “Cybercrime.” Lessico del XXI Secolo, 2012. https://www.treccani.it/enciclopedia/cybercrime_(Lessico-del-XXI-Secolo)/

Enciclopedia Treccani. “Deepfake.” Neologismi, 2018. https://www.treccani.it/vocabolario/deepfake_(Neologismi)/

Enciclopedia Treccani. “Fenomeno Terroristico Armato che Invoca il Principio-Dovere Islamico del Jihād, alla Luce del Pensiero più Radicale del Cosiddetto “Fondamentalismo Islamico”.” https://www.treccani.it/enciclopedia/jihadismo/

Enciclopedia Treccani. “Hacktivism: Attivismo politico esercitato attraverso attacchi informatici.” https://www.treccani.it/enciclopedia/hacktivism_(Lessico-del-XXI-Secolo)/

Enciclopedia Treccani. “Il Dark Web, Accessibile Solo Tramite Software Specifici, è il Teatro di Attività Illecite come il Traffico di Armi e Droga, Influenzando Anche Rappresentazioni Artistiche e la Percezione Pubblica dei Media di Massa.” https://www.treccani.it/enciclopedia/darkweb_(altro)/

Enisa.europa.eu. “About ENISA - The European Union Agency for Cybersecurity.” https://www.enisa.europa.eu/about-enisa

Enisa.europa.eu. “Incidents Handling and Cybercrime Investigations.” https://www.enisa.europa.eu/news/enisa-news/incidents-handling-and-cybercrime-investigations

European Union Agency for Cybersecurity. “NIS Directive.” https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool

EuropeanUnion.Europa.eu. “European Union Agency for Criminal Justice Cooperation: 3.8 Cybercrime.” https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurojust_en

Europol.europa.eu. “Cybercrime.” https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Europol.europa.eu. “European Financial and Economic Crime Centre – EFECC.” https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc

Eurostat. “How Popular is Internet Use Among Older People?” https://ec.europa.eu/eurostat/statistics-explained/index.php?title=How_popular_is_internet_use_among_older_people

False Claims Act Settlements and Judgments Exceed $2.68 Billion in Fiscal Year 2023. United States Department of Justice, February 22, 2024. https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023

Federal Bureau of Investigation. Internet Crime Report, 2022, Internet Crime Complaint Center. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report

Federal Trade Commission. "New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022." https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

Forbes Advisor. "L'inverno delle criptovalute sta arrivando: tutto quello che devi sapere sul crypto winter." https://www.forbes.com/advisor/it/investire/criptovalute/crypto-winter/#:~:text=Secondo%20il%20parere%20degli%20esperti,di%20cominciare%20una%20lunga%20discesa.

Garante per la Protezione dei Dati Personali. "Il testo del Regolamento (UE) 2016/679." https://www.garanteprivacy.it/il-testo-del-regolamento

Governo Italiano: Ministero della Giustizia. "Cyberlaundering." https://www.giustizia.it/giustizia/it/mg_2_5_12_1.page?contentId=GLM1144138

Hahn-Griffiths, Stephen. "The Equifax Breach Is a Reputational Crisis that Will Linger." RepTrack Company. https://www.reptrak.com/blog/the-equifax-breach-is-a-reputational-crisis-that-will-linger/

Higgins, Malcolm. "Cyber Extortion: What Is It and How to Protect Yourself." NordVPN. https://nordvpn.com/it/blog/cyberextortion/

Hudson Intelligence. "Peel Chain | Cryptocurrency Investigation." Hudson Intelligence. https://www.hudsonintelligence.com/peel-chain-cryptocurrency-investigation

Il Sole 24 Ore. "La trasformazione digitale del banking parte dalla conoscenza del consumatore." https://www.ilsole24ore.com/art/la-trasformazione-digitale-banking-parte-conoscenza-consumatore-ADt2671

Interpol.int. "Our Role in Fighting Financial Crime." https://www.interpol.int/Crimes/Financial-crime/Our-role-in-fighting-financial-crime

Interpol.int. "What is Interpol?" https://www.interpol.int/Who-we-are/What-is-INTERPOL#:~:text=Our%20full%20name%20is%20the,the%20world%20a%20safer%20place.

Joint Cybercrime Action Taskforce (J-CAT). "Fighting Cybercrime around the World." https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce

Kaspersky. "Hacker Black Hat, White Hat e Gray Hat – Definizione e Spiegazione." Kaspersky IT Resource Center. https://www.kaspersky.it/resource-center/definitions/hacker-hat-types

KPMG. Evoluzione dei modelli distributivi bancari: l'impatto del COVID-19 sui modelli di servizio delle banche italiane. https://kpmg.com/it/it/home/insights/2021/03/modelli-distributivi-bancari-post-covid.html

Masi, Serena. "V Direttiva Antiriciclaggio: Obiettivi, Ambito di Riforma, Modifiche." Altalex, May 28, 2019. https://www.altalex.com/documents/news/2019/05/28/v-direttiva-antiriciclaggio

Merkle Science. "Mixers and Tumblers: Regulatory Overview and Use in Illicit Activities." February 18, 2022. https://knowledgebase.merklescience.com/technologies/mixers-and-tumblers

National Health Care Fraud Enforcement Action Results in Charges Involving over $1.4 Billion in Alleged Losses. United States Department of Justice. https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

NCMEC Releases New Sextortion Data. National Center for Missing & Exploited Children, April 15, 2024. https://www.missingkids.org/blog/2024/ncmec-releases-new-sextortion-data#:~:text=For%20the%20first%20time%2C%20the,from%2010%2C731%20reports%20in%202022.

Oxford Languages. https://languages.oup.com/google-dictionary-en/

PowerDmarc. "Sicurezza informatica nel settore bancario: Le principali minacce e i modi migliori per prevenirle." https://powerdmarc.com/it/cyber-security-in-banking/

PwC Insights. "A Brief Run-Through of the European Union's Digital Finance Package." https://www.pwc.com/mt/en/publications/asset-management/a-brief-run-through-of-the-european-union-digital-finance-package.html

PwC. "2024 AI Business Predictions." https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html

Quali sono i diversi tipi di molestie? E quali le conseguenze psicologiche? GuidaPsicologi, June 3, 2021. https://www.guidapsicologi.it/articoli/quali-sono-i-diversi-tipi-di-molestie-e-quali-le-conseguenze-psicologiche

Rainews.it. "Cybercrime, l'ultimo allarme dell'Intelligenza artificiale: clonare la voce delle vittime di truffa." https://www.rainews.it/articoli/2023/09/cybercrime-lultima-frontiera-dallintelligenza-artificiale-clonare-la-voce-delle-vittime-f29283b6-2c65-4dd8-8979-f45c364745ff.html

Redazione ANSA. "Nel 2022 Riciclaggio Denaro da Record per la Cgia." ANSA, September 9, 2023. https://www.ansa.it/veneto/notizie/2023/09/09/nel-2022-riciclaggio-denaro-da-record-per-la-cgia_fccf08e1-fedf-490e-a058-53b2e78cc1fd.html

Serena, Giulia. "Synlab Italia, Scoperti Finalmente gli Autori dell'Attacco Hacker." Tom's Hardware, May 6, 2024. https://www.tomshw.it/hardware/synlab-italia-scoperti-finalmente-gli-autori-dellattacco-hacker-2024-05-06

Statista. "Number of Artificial Intelligence (AI) Tool Users Globally from 2020 to 2030." https://www.statista.com/forecasts/1449844/ai-tool-users-worldwide#:~:text=AI%20tool%20user%20numbers%20worldwide%20from%202020%2D2030&text=People%20using%20AI%20tools%20globally,the%20end%20of%20the%20decade.

Synlab Italia Attack Admitted by Black Basta. SC Media. https://www.scmagazine.com/brief/synlab-italia-attack-admitted-by-black-basta

SYNLAB Italia. "Aggiornamenti sui Sistemi." https://synlab.it/news/novit%C3%A0/sistemi-18aprile.html

SYNLAB Italia. "Chi Siamo: Il Nostro Network." https://synlab.it/chi-siamo/network.html

SYNLAB: Pubblicati i Dati Sanitari dei Pazienti, Cosa Impariamo da Questo Grave Data Breach. CyberSecurity360. https://www.cybersecurity360.it/news/synlab-pubblicati-i-dati-sanitari-dei-pazienti-cosa-impariamo-da-questo-grave-data-breach/

Tibirna, Livia, Coline Chavane, and TDR (Threat Detection & Research). "Unmasking the Latest Trends of the Financial Cyber Threat Landscape." Io.Sekoia.blog. https://blog.sekoia.io/unmasking-the-latest-trends-of-the-financial-cyber-threat-landscape

Tringali, Giovanni. "Il Reato di Riciclaggio." Studio Cataldi, November 14, 2021 https://www.studiocataldi.it/articoli/22334-il-reato-di-riciclaggio.asp

Università degli studi di Udine. Corso di informatica giuridica. "I reati commessi su internet: computer crimes e cybercrimes." https://www.fog.it/corsoinformatica/reati.html