Modelli di Cybersecurity e Prevenzione dei Cyber Crimes

Aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo

a cura di Giacomo Di Gennaro

Federico II University Press

fedOA Press

Università degli studi di Napoli Federico II
Studi e ricerche Criminologiche, Giuridiche e Sociali
5

Modelli di cybersecurity e prevenzione dei cyber crimes

Aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo

a cura di Giacomo Di Gennaro

Federico II University Press

fedOA Press

Modelli di cybersecurity e prevenzione dei cyber crimes : aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo / a cura di Giacomo Di Gennaro. – Napoli : FedOAPress, 2025. – 182 p. : ill. ; 24 cm. – (Studi e ricerche Criminologiche, Giuridiche e Sociali ; 5)

Accesso alla versione elettronica: http://www.fedoabooks.unina.it

ISBN: 978-88-6887-404-9
DOI: 10.6093/ 978-88-6887-404-9

Volume pubblicato con i fondi del Progetto PNRR Hard Disc, Spoke 1: Law and Regulation for a Better-Safe Cyberspace (Cyber rights). Sotto progetto: *Human-Centered Approach and Regulatory Dimension in Developing an Interoperable and Secure Cyberspace*, acronimo Hard Disc, Spoke 4, Cybersecurity. Università degli Studi di Napoli Federico II, Università di Trento e Università di Verona. Coordinamento Università di Napoli Federico II.

Università degli Studi di Napoli Federico II
Centro di Ateneo per le Biblioteche "Roberto Pettorino"
Piazza Bellini 59-60
80138 Napoli, Italy
http://www.fedoapress.unina.it/
Published in Italy
Prima edizione: dicembre 2025

Indice

Introduzione

Le sfide poste dalla società digitale al riconoscimento dei diritti tra normatività e garanzie di sicurezza

Giacomo Di Gennaro

È con vivo apprezzamento e gratitudine che ringrazio quanti hanno accettato di essere presenti oggi a questo incontro che costituisce – nell'ambito delle iniziative promosse dal *Partenariato Esteso (PE 7 Serics), Security and Rights in the CyberSpace*[1] – una prima tappa di un cammino di analisi e riflessione più ampie cui l'Unità di Ricerca della Federico II aderisce, circa le sfide che la società digitale, il nuovo orizzonte artificiale, la svolta dell'IA pongono a chi osserva e intende comprendere gli indirizzi che sta prendendo il nuovo millennio.

Nel dare conto di qual è il recinto dentro il quale ci muoveremo nel corso di questa giornata, questo convegno rappresenta un secondo appuntamento che fa seguito a quello che già c'è stato a Roma nella presentazione del partenariato il 19 luglio 2024 presso il Dipartimento di Giurisprudenza dell'Università di Roma Tre. L'appuntamento di oggi[2] è sostanzialmente incentrato su un aspetto che ritengo veramente centrale per i tempi che stiamo vivendo e per quelli che vivremo nell'immediato futuro: il tema della regolazione, che non è solo la regolazione normativa del *CyberSpace* ma il tema, innanzitutto, del riconoscimento dei diritti fondamentali che all'interno del *CyberSpace* si determinano. E quindi, l'indicazione che noi intercettiamo dal progetto ci invita ad affrontare ed esaminare quali sono le connessioni *con* e in che misura è oggi efficace *la* normativa che abbiamo a disposizione a garanzia della cyber security e a garanzia della stessa investigazione, delle stesse indagini in ambiente digitale, poiché la sicurezza è il

[1] Project PNRR Hard Disc, Spoke 1: Law and Regulation for a Better-Safe Cyberspace (Cyber rights). Sotto progetto: *Human-Centered Approach and Regulatory Dimension in Developing an Interoperable and Secure Cyberspace*, acronimo **Hard Disc**, Spoke 4, Cybersecurity. Università degli Studi di Napoli, Federico II°, Università di Trento e Università di Verona. Coordinamento Università di Napoli, Federico II°.

[2] Il convegno "Modelli di Cybersecurity e prevenzione dei cyber crimes. Aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo", si è svolto il 24 gennaio 2025 presso il Dipartimento di Scienze Politiche, Aula Spinelli, dell'Università degli Studi di Napoli, Federico II°.

diritto basilare che consente di vivere *in* libertà, di esperire *la* libertà, essendo il tempo presente scandito dall'*online* permanente, da un corpo fisico e mentale che si sviluppa talmente nell'ambiente digitale al punto da assumerne i caratteri di velocità, contemporaneità, istantaneità. Ad esito di questi caratteri, la sicurezza si sbriciola facilmente in un mondo digitale che ci rende tutti vulnerabili. Essa non riguarda più solo lo spazio interattivo reale ma anche quello digitale. Il funzionamento della mente cambia; mutano il pensiero umano, i meccanismi cognitivi e il modo in cui percepiamo la realtà e con essi, cambia, inoltre, la grammatica relazionale con lo spazio fisico e i corpi degli altri. L'impatto del digitale sulla mente (specie dell'AI generativa) partecipa attivamente alla costruzione della realtà, modifica i comportamenti sociali e la struttura stessa della percezione al punto che la mediazione digitale diventa essa stessa un ambiente cognitivo.

La condizione culturale dell'epoca contemporanea è segnata da volatilità, frammentazione e sovraccarico informativo. Questa condizione produce conseguenze rilevanti sui processi cognitivi: la ricerca di informazioni avviene in ecosistemi governati da algoritmi, sistemi di clusterizzazione e logiche di personalizzazione che restringono il campo delle fonti e favoriscono la costruzione di "bolle informative"[3]. La grande rivoluzione tecnologica che stiamo vivendo è così rapida e pervasiva che impedisce di produrre discussioni o lenti aggiustamenti. Il problema, infatti, non è la tecnologia in sé, ma la capacità della società di ripensare se stessa mentre il cambiamento è in corso. La capacità di costruire nuove categorie concettuali, istituzioni e regole per qualcosa che non ha precedenti. D'altra parte, come tutte le realtà che viviamo anche l'ambiente digitale è caratterizzato da ambivalenza: da un lato, il mondo di Internet ci ha avvicinati in tempo reale. Scambiamo informazioni, comunichiamo con persone lontane, interagiamo con i parenti, gli amici e con persone anche che non conosciamo, lavoriamo da casa e commerciamo da lontano.

Come si sottolinea nel Rapporto dell'AGID "Strategia italiana per l'intelligenza artificiale 2024-2026" (https://www.agid.gov.it/sites/agid/files/2024-07/Strategiaitaliana_per_l_Intelligenza_artificiale_2024-2026.pdf), «*le tecnologie basate sull'Intelligenza Artificiale (IA) hanno ampiamente rivelato, ormai già da alcuni anni a questa parte, il proprio impatto pervasivo e il proprio potenziale tra-*

[3] D. de Kerckhove, "*Il tempo del XXI secolo smette di essere lineare e ridisegna comunicazione, politica e intelligence*", lezione al Master in Intelligence dell'Università della Calabria", 2025, in https://news.socint.org/intelligence-derrick-de-kerckhove.

sformativo delle dinamiche sociali e produttive. L'Intelligenza Artificiale sta rivoluzionando il mondo in cui viviamo e le modalità con cui produciamo valore in tutti i settori, sta impattando profondamente sul sistema dell'educazione, sulle attività professionali e sull'industria» (Ivi, p. 4).

I sistemi di IA sono sempre più diffusi e sono parte integrante della nostra vita. Assistenti digitali, commercio online, navigatori, playlist personalizzate, filtri sulle caselle email, lotta alle frodi bancarie, elettrodomestici intelligenti, smartphone: sono solo alcuni degli strumenti di uso quotidiano nei quali l'IA gioca un ruolo essenziale. Lo stesso uso di ChatGPT (un modello linguistico di grandi dimensioni LLM)[4] è diventato patrimonio comune, al punto che il dialogo con esso si sviluppa anche chiedendo all'algoritmo pareri su questioni personali. Tutta la tecnologia digitale e l'IA si va sviluppando in un modo che prospetta una diffusione forse in tutti gli ambiti ai quali, tuttavia, non sono esenti interrogativi sui rischi insiti al modo in cui funziona.

Dall'altro, infatti, la diffusione e acquisizione delle informazioni, quelle che immettiamo in rete, l'apparente nascondimento della nostra identità, l'uso strategico di false identità, l'agire in totale anonimato e il potenziale abbassamento di inibizione comportamentale, rappresentano aspetti che rendono conto di nuove dinamiche foriere della crescita di nuovi comportamenti antisociali, devianti, legati alla ricerca compulsiva del piacere e del desiderio, di attenzioni indesiderate che possono comportare gravi rischi per il benessere psicologico di una persona. Basti pensare al *grooming online*, al *cyberbullismo*, al *bodyshaming*, al *sextortion*, alla *cyber-pedopornografia*, al *phishing*, al *cyberstalking*, alle frodi informatiche, al *cyberlaundering*, al *revenge porn*, agli attacchi *ransomware*, a tutte le forme di intrusione mediante *malware* e agli accessi abusivi in altre forme o al danneggiamento di informazioni e dati, fino al *cyberterrorismo*. Insomma, quel corollario di reati che a partire dal lontano 1993 vengono indicati dalla legge n. 547 che modifica e integra le norme del codice penale e del codice di procedura penale, nonché, a seguito delle modifiche ulteriori apportate per effetto della ratifica della Convenzione del Consiglio D'Europa sulla criminalità informatica, la legge 18 marzo 2008, n. 48 e la successiva legge 15 febbraio 2012, n. 12 recante «norme in materia di misure per il contrasto ai fenomeni di criminalità informatica».

Questa architettura normativa si è poi arricchita del D.lgs. 231/2001 dell'8 giugno, recante la "Disciplina della responsabilità amministrativa delle persone

[4] Nel glossario dell'IA si definiscono tali modelli linguistici *Large Language Model* (LLM).

giuridiche, delle società e delle associazioni anche prive di personalità giuridica", che, come noto, ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per reati commessi nel loro interesse o vantaggio da persone legate al soggetto giuridico da specifici rapporti normativamente previsti, e della legge 90/2024 recante "Disposizioni per il rafforzamento di cybersicurezza nazionale e reati informatici" prevedendo l'aggiornamento del catalogo dei reati 231, in particolare dell'art. 24-bis *Delitti informatici e trattamento illecito di dati*, che ha modificato il reato di «truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee». Infine, la recente legge 23 settembre 2025, n. 132 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" ed entrata in vigore il 10 ottobre dello stesso anno, integrando l'*AI Act* europeo con norme nazionali su settori come lavoro, giustizia, sanità e fornendo deleghe al Governo per definire discipline dettagliate, tutela dei diritti e governance del settore[5].

Se il quadro normativo si è reso via via urgente e necessario di costanti aggiornamenti e modifiche, è perché vi è presupposta una tensione criminologica tra la necessità del controllo, l'esercizio del potere e il riconoscimento dei diritti. Ma qui il problema è: di quali diritti parliamo?

Innanzitutto, potremmo dire, il diritto ad essere informati per essere maggiormente consapevoli in quanto utenti. L'Unione Europea è intervenuta ripetutamente su questo aspetto adottando un Regolamento conosciuto come *AI Act* che ha un duplice obiettivo: promuovere l'innovazione e proteggere dagli effetti nocivi dell'IA[6]. Il cammino legislativo dell'AI Act è stato lungo e complesso, a

[5] Il Governo avrà 12 mesi di tempo per produrre i decreti attuativi. In realtà, come si vedrà, la legge 132/2025 recepisce il Regolamento europeo entrando ufficialmente nell'era dell'intelligenza artificiale ma generando una legge che – giustamente – è stata definita "un vuoto pneumatico": «nessuna comprensione reale della specificità dell'intelligenza artificiale generativa, nessuna definizione operativa dei modelli, nessuna disciplina concreta delle tecnologie oggi effettivamente in uso, nessuna copertura finanziaria", così A. Scarano, *L'Italia e l'intelligenza artificiale: la legge che va bene per il frigo*, in «Il Fatto quotidiano», lunedì, 5 gennaio 2026.

[6] *Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*; https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it. L'AI Act è composto da un lungo preambolo (180 articoli) e da 103 articoli distinti in 13 capi cui fanno seguito 13 allegati. Il Regolamento sarà applicato dal 2 agosto 2026, ma i capi I e II sono stati applicati a decorrere dal 2 febbraio 2025; il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo

partire dal 2018 quando venne istituito dalla Commissione europea un gruppo di esperti cui fu affidato il compito di elaborare alcune linee guida etiche per una IA affidabile[7].

1. *Non può esserci sviluppo di IA senza il rispetto di alcuni diritti*

Se c'è un contenuto forte che emerge dal lavoro del gruppo indipendente di esperti è che occorre seguire una serie di principi nello sviluppo dell'IA e in particolare il rispetto dei diritti fondamentali, della sicurezza, trasparenza, responsabilità e garantire la supervisione umana[8]. Sulla scia di tale lavoro il 21 aprile 2021 inizia l'iter legislativo europeo sintetizzato dalla Commissione europea con una proposta di regolamento dell'AI. Il testo verrà sottoposto all'esame del Parlamento europeo e del Consiglio e il dibattito intenso che ne è scaturito ha reso possibile l'inserimento di alcune norme dedicate all'AI generativa (capo V), inizialmente non considerata perché tecnologia non ancora diffusa. Occorrerà arrivare al dicembre del 2023 per registrare un accordo tra i rappresentanti delle istituzioni europee su ciò che è l'AI Act[9].

All'art. 1 dell'AI Act sono esplicitate le finalità della nuova legislazione: «*migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo*

101; l'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al regolamento si applicano a decorrere dal 2 agosto 2027.

[7] Gruppo Indipendente di Esperti ad Alto Livello Sull'Intelligenza Artificiale (2019), *Orientamenti etici per un'IA affidabile*, 8 aprile, in https://digital-strategy.ec.europa.eu.

[8] Questi principi sono presenti anche nelle linee guida del *Rome Call for AI Ethics* del 2020; https://www.vatican.va/roman_curia/pontifical_academies/acdlife/documents/rcpont-acd_life_doc_20202228_rome-call-for-ai-ethics_en.pdf. Il documento è frutto di una iniziativa promossa dalla Pontificia accademia per la vita al quale vi hanno collaborato Microsoft, IBM e diverse istituzioni, tra cui la FAO e il Governo italiano.

[9] Il testo definitivo, infatti, sarà approvato dal Parlamento europeo il 13 marzo 2024 e dal Consiglio dell'Unione Europea il 21 maggio 2024.

Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione».

Quindi due fondamentali obiettivi: protezione contro gli effetti nocivi dell'AI; miglioramento del funzionamento del mercato interno promuovendo l'innovazione. Ovvero, «costruire un ecosistema che permetta a consumatori e imprese di fidarsi dei modelli di AI che risultano conformi al Regolamento, sapendo che non arrecano danni e non discriminano»[10].

Il sistema di fiducia dovrebbe essere garantito e prodotto da un quadro di certezza giuridica relativo alle imprese circa le loro responsabilità e obblighi. L'AI Act rappresenta per l'UE un riferimento globale per l'ambito dell'intelligenza artificiale che costituisce aspetto di rilievo sia sul piano strategico che geopolitico per l'Unione, replicando quanto già fatto con il Regolamento generale sulla protezione dei dati (GDPR). L'approccio adottato fa perno sul livello di rischio che i sistemi di AI comportano. Tali livelli sono suddivisi in quattro categorie: sistemi proibiti, ad alto rischio, a rischio limitato, a rischio minimo. I diversi articoli determinano l'ambito di applicazione della normativa e indica le definizioni chiave, le pratiche proibite, i requisiti per i sistemi di AI ad alto rischio, gli obblighi di trasparenza per i sistemi a rischi limitato, gli obblighi specifici per i sistemi a rischio minimo, la governance, la sorveglianza del mercato e le sanzioni. L'approccio scelto è funzionale alla promozione dell'AI. «Non si specifica ciò che è permesso, ma si sottolinea ciò che non si deve realizzare e ciò che invece si può attuare, ma con attenzione»[11].

L'art. 5 dà conto di alcune pratiche proibite (es. l'uso di tecniche subliminali o manipolative) che alterano il comportamento delle persone, nonché i sistemi che sfruttano le vulnerabilità di segmenti di popolazione (es. gli anziani affetti da particolari disabilità) e che possono causare danni (es. pubblicità ingannevoli che spingono a comprare farmaci inutili, polizze assicurative fraudolente, ecc.). Tra i modelli vietati vi sono anche i sistemi di *social scoring* che valutano o classificano le persone aggregando dati che profilano il loro comportamento sociale, civico e finanziario, nonché l'orientamento sessuale[12]. Sono vietati anche modelli predittivi o prognostici relativi alla probabilità di commissione di un reato, così

[10] A. Carobene, *Regolare l'intelligenza artificiale. La scelta europea dell'AI Act*, «Aggiornamenti sociali», 11, 2025, pp. 638-645, cit. p. 640.

[11] A. Carobene, *Regolare l'intelligenza artificiale*, op. cit. p. 641.

[12] Y. Wang e M. Kosinski, *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*, «Journal of Personality and Social Psychology», 114, 2, 2018, pp. 246-257.

come l'uso indiscriminato di dati biometrici per il riconoscimento facciale, delle emozioni nei luoghi di lavoro o negli istituti di istruzione[13]. Le sanzioni previste per le imprese (art. 99) sono molto severe.

Come detto, oltre ai modelli vietati vi sono i sistemi classificati ad alto rischio (capo III e allegato III) e quelli a rischio limitato e minimo. Tra i primi rientrano i rischi per la salute, la sicurezza o i diritti fondamentali delle persone[14]. L'AI Act prevede in tali casi diversi obblighi stringenti che vanno dalla realizzazione di un sistema di gestione dei rischi, alla predisposizione di una documentazione tecnica prima della messa in commercio; dall'analisi della qualità dei dati usati per addestrare il sistema, ad una adeguata sorveglianza umana, un elevato livello di robustezza, sicurezza e accuratezza informatica. Ono previsti, infine, obblighi di comunicazione alle autorità nazionali le quali devono monitorare l'attuazione dell'AI Act (l'AGID e l'ACN per l'Italia).

I sistemi classificati a rischio limitato assolvono alla funzione di attenzionare la manipolazione o la mancanza di trasparenza per evitare usi distorti dei modelli di AI. Da qui l'esigenza di assicurare maggiore consapevolezza negli utenti circa la modalità di interazione con i sistemi di AI (es. una chatbot) e comprendere che si ha a che fare con contenuti generati dall'intelligenza artificiale ed evitare quindi casi di deep fake. Quelli, invece, classificati a rischio minimo o nullo non intaccano i diritti fondamentali delle persone o la sicurezza (es. i filtri antispam dei servizi di posta elettronica) e per essi non sono previsti obblighi.

Obblighi specifici, invece, sono previsti dall'AI Act per chi produce e usa modelli per finalità generali (capo V). I produttori (fornitori) sono tenuti ad aggiornare la documentazione tecnica; garantire il rispetto del diritto di autore nella fase di addestramento dei modelli; specificare su quali dati hanno effettuato l'addestramento dell'AI; cooperare con le autorità per il rispetto del Regolamento e fornire informazioni sufficienti per comprendere capacità e limiti a chi vuole integrare i loro modelli.

[13] L'art. 2 dell'AI Act prevede che per scopi di sicurezza pubblica o di ambito militare molte delle patiche indicate non si applichino.

[14] Si pensi ai modelli di AI utilizzati nei trasporti e agli effetti delle interruzioni sulle vite umane, o quelli che attengono l'accesso all'istruzione e alla carriera professionale. Si pensi all'AI applicata nella chirurgia assistita da robot, oppure ai software di *credit scoring* per la determinazione della solvibilità di una persona o azienda utilizzati per l'accesso a prestiti; quelli usati nella gestione dell'emigrazione, dell'asilo e controllo alle frontiere per l'esame automatizzato delle domande di visto, ecc.

Gli obblighi diventano più stringenti per i modelli che l'AI Act definisce a rischio sistemico, ovvero quelli che per le loro dimensioni e la loro diffusione possono arrecare danni significativi, impattando su un grandissimo numero di utenti e mettendo in crisi alcuni aspetti fondamentali della società (es, crisi sanitaria; truffe finanziarie; proliferazione di armi chimiche. Nel caso di rischio sistemico il Regolamento europeo prevede una valutazione dei rischi propri del modello, l'obbligo della segnalazione degli incidenti (es. perdita di dati), l'adesione a codici di condotta redatti su base volontaria.

Occorre sottolineare che l'AI Act non offre risposte a tutte le questioni legate all'uso dell'AI sia perché è in continua evoluzione la tecnologia sia perché l'oggetto stesso della normativa è di difficile definizione. Il campo di applicazione dell'AI Act non potrà mai essere definito con precisione una volta per tutte. Tant'è che l'allegato III contiene l'elenco dei sistemi ad alto rischio e sarà oggetto di revisioni periodiche atteso che non è possibile oggi prevedere quali saranno in futuro gli ambiti "sensibili" nell'uso dell'AI.

Che il Regolamento europeo – di attuazione progressiva – rischi di imbrigliare l'attività delle imprese e l'innovazione europea appare a non pochi possibile, specie in quei campi (es. la salute) ove lo sviluppo tecnologico è ad alto rischio. Certo la ricerca potrebbe risentirne atteso che la competizione in questi e altri campi in altri Paesi è resa difficile da una normativa meno restrittiva. Per non parlare dell'AI generativa che vede colossi come Meta che hanno annunciato di non voler firmare lo specifico Codice di condotta europeo. Inoltre, altra questione delicata attiene il diritto d'autore. Il Regolamento chiede agli sviluppatori di modelli di AI generativa l'obbligo di dichiarare i dati di addestramento utilizzati (specie quelli protetti da copyright). Il contrasto tra lavoro intellettuale degli autori e segreto industriale nonché necessità di preservare la proprietà intellettuale degli stessi sviluppatori è evidente, atteso il rischio di svelare le tecniche di training utilizzate. E poi chi detiene i diritti d'autore sulle opere generate dall'AI? Infine, la solita incognita: chi controlla e con quali strumenti? Le autorità nazionali e l'Ufficio europeo per l'AI (European AI Office) saranno in grado di far rispettare le regole?

Vi è poi, un secondo diritto da non sottovalutare: conciliare sicurezza e, in qualche modo, salvaguardia permanente. Ovvero, non lasciare che il rapido progresso tecnologico – foriero indubbiamente di risultati entusiasmanti, ma anche di altrettante contemporanee preoccupazioni sulla sicurezza e sull'etica dell'intelligenza artificiale, niente affatto tecnologia immateriale e neutrale – soppianti quell'allineamento con i valori e con le intenzioni umane che garantiscono la libertà, la giustizia, la trasparenza, la solidarietà, la minore disuguaglianza.

Questo perché è sotto gli occhi di tutti una operatività della rete globale, dei sistemi e delle informazioni troppo incentrata nelle mani di pochi che hanno ridisegnato, e continuano a farlo, il panorama geopolitico, orientandosi per strade diverse all'utilizzo dei sistemi informatici, dell'intelligenza artificiale, all'uso della stessa *machine learning* in funzione del mantenimento o della conquista di posizioni nella gerarchia del potere globale. Non può destare preoccupazioni per la sicurezza pubblica, l'adesione ad un orientamento di gestione e controllo, di fatto privatizzato, di tutte le comunicazioni e informazioni in materia militare, giudiziaria, relativo alle relazioni diplomatiche, ai servizi segreti, alla protezione civile, alla sanità, alla ricerca scientifica.

Insomma, una sorta di monopolio dello spazio extra-atmosferico garantito dalla messa in orbita di migliaia di satelliti intorno al nostro pianeta, tutti targati Starlink. Per questa strada, credo, che andremo incontro a un aumento della dipendenza esterna in settori strategici che garantiscono la sicurezza economica, già resa vulnerabile dal crescente contesto d'instabilità globale, dove le catene di approvvigionamento, le relazioni commerciali sono soggette a tensioni e interruzioni. Settori particolarmente critici includono le materie prime essenziali e le tecnologie avanzate, dove l'Europa mostra vulnerabilità significative.

Un recente rapporto del 2023 della Commissione europea riporta che l'Unione europea dipende dai paesi terzi per oltre il 90% del suo fabbisogno di terre rare e per il 98% del suo approvvigionamento di magnesio, che sono elementi cruciali per molte industrie dell'hi-tech.

Nelle linee di indirizzo presenti nelle cartelline di oggi sui contenuti del convegno, abbiamo sottolineato che, se da un lato gli sviluppi della tecnologia digitale si pongono in linea funzionale con gli sviluppi dell'economia nazionale – nei cui settori nevralgici dell'imprenditoria nostrana e in quelli delle istituzioni pubbliche è in atto una digitalizzazione integrale dei propri apparati operativi, indirizzati ovviamente anche ad un risparmio di spesa con la dematerializzazione dei processi – dall'altro esiste una precisa istanza di tutela intorno alle attività richiamate. Per ragioni di asincronia, però, non si riesce a far fronte in maniera soddisfacente. L'aggressione portata alla funzionalità dei sistemi informatici e i progetti di predare informazioni sensibili che fanno capo a strutture critiche di apparati di sicurezza dello Stato e di soggetti economici operanti nei mercati, assume quindi un livello di rischio imponderabile che impone interventi di difesa efficaci, di natura tecnologica e normativa.

Quindi ci troviamo di fronte a problemi di tipicità delle singole fattispecie nell'assetto normativo e di coerenza legislativa relativa agli interessi di tutela nel

settore della cyber sicurezza, oltretutto – e qui ce lo può confermare il capo gabinetto dell'Agenzia per la Cybersicurezza Nazionale – spesso carente di mezzi, di risorse umane, di personale, di risorse finanziarie adeguate, e per il quale si richiede costantemente di equilibrare il campo normativo, legislativo, giurisprudenziale che ogni giorno si allarga in maniera anche, a volte, come dire in modo poco chiaro.

Cresce il bisogno di protezione rispetto a fatti predatori dotati di incontrollabile aggressività, commessi con i mezzi informatici e, con essi, cresce l'attenzione e il livello di intervento disordinato, a volte, del legislatore nazionale, in carenza di un disegno razionale e organico dell'intervento regolativo. Da un lato, quindi, si pongono problemi di tipicità delle singole fattispecie nell'assetto normativo e di carenza legislativa relativa agli interessi di tutela di riferimento; dall'altro, le questioni investono la competenza del settore giustizia per adeguare i propri strumenti d'indagine a vicende che richiedono un alto tasso di conoscenza e di applicazione delle tecnologie informatiche.

Occorre quindi una puntuale definizione dei mezzi informatici, dispositivi telematici, dispositivi di comunicazione e dati informatici che dovrebbero costituire il discrimine tra diverse categorie di reato. Così come gli ambiti di tipicità dei diversi settori normativi presidiati da fattispecie di reato che intrecciano contenuti identitari diversi.

Da qui, allora, la difficoltà delle scelte interpretative per l'applicazione della fattispecie di reato più precisa e adeguata al caso da perseguire. Quindi, restano ripartite, e occorre che siano più efficaci, le competenze in capo a presidi istituzionali in cui si rilevano poteri di vigilanza, di intervento, profondamente interconnessi tra loro. Penso, in questo caso, alla Direzione nazionale antimafia, all'Autorità per la cyber security, al garante per la privacy.

Le esigenze poste, quindi, alla base dell'importanza della ricerca che si sta svolgendo e di questo convegno, si possono sintetizzare in 2 punti di analisi:

1) le direttrici giuridiche per rendere razionale e coerente in misura maggiore il settore dei reati da perseguire (tenuto conto del fatto che si presenta all'interprete una duplice categoria: reati commessi *con* i mezzi informatici e reati commessi *sui* mezzi informatici);
2) in secondo luogo, quali sono le risorse tecniche cui possono fare ricorso gli inquirenti per l'accertamento dei reati, quali le regole processuali che presidiano i singoli atti di indagine alla ricerca della prova, quali le normative poste a tutela e garanzia dei diritti fondamentali (anche degli indagati, degli imputati e delle parti offese).

Ecco. Il convegno si propone di indagare anche la prassiologia e di fornire i primi esiti sulla ricognizione giurisprudenziale (di cui si darà conto nel corso della mattinata) per verificare se l'attuale numero delle fattispecie punitive è stato in grado sinora di assolvere alle aspettative riposte nella magmatica legislazione di settore negli ultimi anni.

Un ultimo aspetto che voglio richiamare è che abbiamo la piena consapevolezza che nell'ambiente digitale c'è una influenza forte sulle strutture e sulle dinamiche del crimine e della vittimizzazione, il che impone di riflettere analiticamente e approfondire non solo concentrandosi sugli autori di reato ma, dal lato della vittima, mappare le nuove vulnerabilità socio-giuridiche determinate dalle caratteristiche del *cyber space* e identificando e valutando le nuove minacce informatiche. Qui vale il principio che sta maturando di fronte all'asincronia temporale tra l'azione delle agenzie di contrasto e quanti ogni giorno sono vittimizzati: quali sono le garanzie alle quali siamo disposti a rinunciare per contrastare crimini gravi che colpiscono la mente, la psiche, il portafoglio, la serenità delle persone?

Ringrazio tutti per l'attenzione e dichiaro che si dia inizio all'apertura dei lavori.

Sezione Prima

Capitolo Primo

Cybersicurezza e alfabetizzazione digitale: elementi cardine della tutela dei diritti fondamentali nell'ecosistema digitale

Carlo Colapietro

Premessa

Il cyberspazio, inteso come l'insieme delle infrastrutture digitali e delle reti di comunicazione che permettono l'interazione tra individui, imprese e Istituzioni, si configura oggi come una dimensione imprescindibile dell'esperienza umana. Non si tratta più di un ambito separato dalla realtà quotidiana, ma di uno spazio integrato nella vita sociale, politica, economica e culturale. In questo contesto, l'accesso al cyberspazio assume un valore strategico e costituisce una condizione necessaria per il pieno esercizio di una vasta gamma di diritti fondamentali, tra cui la libertà di espressione, il diritto all'informazione, la partecipazione democratica, il diritto all'istruzione e alla salute. Garantire un accesso equo e sicuro a tale ambiente significa, quindi, promuovere l'inclusione digitale e rafforzare la cittadinanza attiva.

Quanto più il digitale pervade l'esistenza quotidiana degli individui e delle amministrazioni, tanto più emerge il tema di come gli Stati debbano regolare il cyberspazio e garantire all'interno di esso i diritti degli individui: non assicurare a questi ultimi il godimento dei diritti in Internet significa determinarne l'esclusione dal contesto sociale (digitale), nonché dal godimento dei diritti fondamentali e dall'esercizio dei doveri costituzionali. È stato, infatti, sottolineato come la cittadinanza oggi abbia acquisito una dimensione (anche) digitale: «l'innovazione tecnologica ha infatti aperto la strada a una nuova fase della vicenda di questa istituzione. Da *materiale*, essa si è fatta, in un certo senso *virtuale*»[1].

[1] F. Amoretti, E. Gargiulo, *Dall'appartenenza materiale all'appartenenza virtuale. La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione*, in «*Pol. dir.*», 3, 2010, 354, secondo cui «l'esercizio di molti diritti fondamentali è stato svincolato dal rapporto diretto tra il cittadino e gli apparati istituzionali, divenendo mediato da strumenti informatici che, per la loro stessa natura, si collocano al di fuori degli spazi fisici entro cui il rapporto tra il primo e i secondi ha comunemente luogo. La cittadinanza elettronica, in virtù della sua natura immateriale – in quanto tale adatta ad aggirare gli ostacoli di natura materiale

Quindi, considerata la rilevanza del digitale nella vita dei singoli individui, garantire la cybersicurezza – per questa intendendosi «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»[2] – significa garantire i diritti fondamentali che vengono esercitati nella "realtà *online*"[3].

A sua volta, garantire la cybersicurezza richiede un'organizzazione istituzionale in cui l'Unione europea è chiamata a svolgere un ruolo da protagonista, che implichi non solo una rivendicazione della *leadership* normativa, ma l'utilizzo di strumenti normativi funzionali alla difesa dei diritti fondamentali dell'individuo[4]. In questo senso, l'Unione europea è spesso accusata di regolare troppo, a differenza delle altre grandi superpotenze – come soprattutto gli USA – che invece lasciano più liberi i colossi del digitale. Tuttavia, contro le degenerazioni anti-libertarie che potrebbero emergere nel cyberspazio[5], il rimedio non può essere costituito dall'assenza di regole o dal lasciare in mano a pochi soggetti privati[6] il dominio del cyberspazio e la sua regolazione. La risposta dell'Unione europea – e, a valle, degli Stati membri – è stata salda, negli ultimi anni, nel trasportare anche nello spazio cibernetico il pieno rispetto dei principi dello Stato di diritto. Ciò è necessario in quanto il «malfunzionamento deliberato di un sistema», dovuto ad attacchi informatici, «[impedisce] lo svolgimento di funzioni pubbliche o l'erogazione di servizi essenziali, cagionando importanti disservizi in grado

che spesso si frappongono tra il cittadino e i suoi bisogni formalmente tutelati – sembrerebbe offrire inedite opportunità di esercitare diritti civili e politici fino a ora rimasti sulla carta e, nondimeno, di rivendicare nuovi tipi di diritti».

[2] Art. 2 ("Definizioni"), punto 1), del Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[3] C. Lotta, G*overnance della Rete, accesso a Internet e cybersicurezza*, Editoriale Scientifica, Napoli 2024, 181 ss.

[4] G. Finocchiaro, *Sovranità digitale*, in «*Dir. Pubbl.*», 3, 2022, 827.

[5] Tra l'altro, anacronistiche, oggi, si rivelano le dichiarazioni di indipendenza del cyberspazio che, nel secolo scorso, propugnavano un modello di Internet senza la presenza degli Stati: si veda, in particolare, J.P. Barlow, *Dichiarazione d'indipendenza del Cyberspazio*, in «*Duke Law & Technology Review*», 5-7, 2019.

[6] … comunque, chiamati a rispettare il contenuto essenziale dei diritti fondamentali (C. Caruso, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, in Aa.Vv., *Liber Amicorum per Pasquale Costanzo*, Vol. I, in *Consulta Online*, 2020, 166).

addirittura di ledere diritti costituzionalmente riconosciuti ai cittadini (salute, istruzione, assistenza, lavoro, sicurezza ecc.)»[7].

In questo senso, cybersicurezza e alfabetizzazione digitale diventano entrambi elementi cardine della tutela dei diritti fondamentali nell'ecosistema digitale, posto che il legame tra loro è strutturale. La cybersicurezza si basa sull'adozione di tecnologie, protocolli e pratiche volte a proteggere dati, reti e sistemi digitali da accessi non autorizzati, attacchi informatici e manipolazioni malevole. Tuttavia, anche i sistemi più avanzati diventano vulnerabili se gli utenti non sono adeguatamente formati e consapevoli dei rischi connessi all'uso delle tecnologie digitali.

L'Italia registra un significativo ritardo rispetto alla media UE in materia di competenze digitali: nel 2023 solo il 46% degli adulti possedeva competenze digitali almeno di base. Il quadro è aggravato da divari generazionali e territoriali: tra i giovani (16-24 anni) la quota sale al 59%, mentre tra gli *over* 65 crolla al 19%, con le regioni del Sud ampiamente sotto la media UE (34%).

L'alfabetizzazione digitale – intesa come la capacità non solo tecnica ma anche critica di interagire in modo consapevole con gli strumenti digitali – rappresenta quindi una componente essenziale della sicurezza informatica. In altre parole, la cybersicurezza è tanto una questione tecnologica quanto culturale, dato che senza cittadini digitalmente alfabetizzati, le strategie di sicurezza rischiano di essere inefficaci o incomplete.

Nel presente contributo, dopo aver esaminato – quantomeno per cenni – la normativa europea in materia di cybersicurezza (e aver richiamato alcune disposizioni significative in materia di alfabetizzazione digitale), si intende quindi esplorare il legame tra cybersicurezza e alfabetizzazione digitale, non solo con lo scopo di evidenziare la necessità di sviluppare competenze digitali solide e trasversali per la prevenzione e la gestione degli attacchi informatici, ma anche per dimostrare come la *cybersecurity* assurga oggi a vero e proprio "metainteresse" nella tutela dei diritti fondamentali.

[7] E. Longo, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, 207.

1. *Cenni sulla normativa europea e nazionale in materia di cybersicurezza (e di alfabetizzazione digitale)*

Il tema della cybersicurezza riguarda da vicino l'Italia, che risulta particolarmente colpita: a partire dal 2022, l'Italia è stata bersaglio di attacchi informatici in misura sempre crescente. In particolare, nel 2024 si è registrata una crescita degli incidenti informatici del 27% rispetto al 2023; inoltre, sempre nel 2024, gli incidenti "critici" o "gravi" hanno costituito l'80% del totale[8]. Nel 2024, l'ACN ha gestito 756 eventi cyber ai danni di istituzioni pubbliche nazionali, in sensibile aumento rispetto ai 383 del 2023: ascrivibile almeno in parte alle modifiche all'impianto normativo, oltre che alla più ampia capacità del CSIRT Italia di rilevare eventi, incidenti e criticità[9]. Si è, pertanto, dinanzi ad una "guerra cibernetica diffusa".

Da qui la necessità di coordinamento tra Istituzioni europee, Istituzioni nazionali e Autorità di settore per una gestione sinergica della cybersicurezza, il cui prodotto è costituito dalla normativa europea volta a garantire la sicurezza delle reti, dei sistemi informativi e dei dati che circolano in Internet.

A tal proposito, occorre far preliminarmente riferimento alla Direttiva NIS 2[10] che, abrogando la Direttiva NIS 1[11], stabilisce un livello comune elevato di cybersicurezza nell'Unione. Si consideri anzitutto che la fonte europea della direttiva richiede un approccio sinergico degli Stati europei, che devono tutti cooperare per raggiungere gli scopi individuati dalla direttiva stessa[12], ovvero

[8] Associazione Italiana Per La Sicurezza Informatica, *Rapporto Clusit sulla sicurezza ICT in Italia*, 2025*,* 7, reperibile al sito internet https://clusit.it/rapporto-clusit/.

[9] Agenzia per la cybersicurezza nazionale, *Relazione annuale al Parlamento 2024*, p. 46. Nel 2024 tutte le attività operative dell'ACN hanno subito un notevole incremento rispetto all'anno precedente, indice di un generale aumento della minaccia cyber: in particolare, 1.979 sono stati gli eventi cyber gestiti (165 al mese) e 573 incidenti con impatto confermato (48 al mese).

[10] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva UE 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 1).

[11] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita dal decreto legislativo 18 maggio 2018, n. 65.

[12] Per una critica all'utilizzo dello strumento della direttiva in materia di regolazione della cybersicurezza v. M Buffa, *La Direttiva NIS II Cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in *Democrazie e Diritti Sociali*, 1, 2023, 48, secondo cui «[…] l'obiettivo dell'uniformità delle legislazioni nazionali avrebbe certamente potuto essere perseguito con

rafforzare la sicurezza cibernetica a livello europeo aumentando la sicurezza delle infrastrutture tecnologiche e combattendo in maniera efficace i rischi causati dal cybercrime. La Direttiva NIS 2, quindi, è stata varata al fine di rendere uniforme, nello spazio europeo, un elevato livello di cibersicurezza per gli operatori di rete "essenziali e importanti"[13], a carico dei quali sono previsti specifici obblighi in materia di protezione della rete e dei sistemi informativi. Tale direttiva è stata recepita nel nostro Paese con il decreto legislativo n. 138 del 2024[14].

Ancora a livello europeo, il Regolamento (UE) 2019/881 (*Cybersecurity Act*)[15], "allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, cyber-resilienza e fiducia nell'ambito dell'Unione", definisce gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA («Agenzia dell'Unione europea per la cibersicurezza»)[16] e un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza.

Più di recente, si pensi al *Cyber Resilience Act*[17], che garantisce la sicurezza di prodotti e servizi, e al *Cyber Solidarity Act*[18], che migliora la capacità dell'Unione

migliore e maggiore efficacia grazie all'adozione di un regolamento (direttamente applicabile senza la necessità di una normativa nazionale di recepimento). Ciò a partire dalla necessità di considerare le ricadute importanti della cybersecurity in materia di diritti fondamentali dei cittadini dell'UE, nonché in relazione alla evidente e sempre maggiore interconnessione tra le infrastrutture critiche dei diversi Stati membri».

[13] Direttiva (Ue) 2022/2555, art. 3 ("Soggetti essenziali e importanti"). Sul punto v. F. Bavetta, *Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo,* in «*Media Laws*», 3, 2023, 408 e F. Casarosa, *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2*, in «*Rivista italiana di informatica e diritto*», 1, 2024, 13.

[14] Decreto legislativo 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

[15] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[16] Sul ruolo dell'ENISA v. L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi.it*, 25, 2022, 73 ss. e S. Calzolaio, *Autorità indipendenti e di governo nella società digitale*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino (a cura di), *La regolazione europea della società digitale*, cit., 90 ss.

[17] Regolamento (UE) 2024/2487 del Parlamento europeo e del Consiglio del 23 ottobre 2024, relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla cyber-resilienza).

[18] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio del 19 dicembre 2024,

di reagire agli attacchi informatici. Come è stato evidenziato, il diritto europeo della cybersicurezza a volte identifica la resilienza con la cybersicurezza; altre volte qualifica la prima come dimensione della seconda. In ogni caso, a prescindere dal *nomen*, il diritto dell'UE intende garantire sistemi che siano in grado di resistere agli attacchi informatici, di adattarsi nel caso in cui siano stati attaccati e di ripristinare le proprie capacità operative nel minor tempo possibile[19].

Al livello nazionale si consideri il decreto-legge n. 105 del 2019[20], che ha istituito il perimetro nazionale di sicurezza cibernetica (PNSC), "al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale" (art. 1)[21].

Successivamente, è stato adottato dapprima il DPCM n. 131 del 2020[22], con il quale sono stati individuati i soggetti pubblici e privati rientranti nel perimetro cibernetico nazionale e definiti i criteri per la predisposizione delle reti, dei sistemi informativi e dei sistemi informatici, e poi il DPCM n. 81 del 2021[23], relativo, in particolare, alle notifiche degli incidenti[24].

che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione e di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cyber-solidarietà).

[19] Cfr. P.G. Chiara, R. Brighi, *La dimensione della "resilienza" nel diritto Ue della cybersicurezza,* in «*Ragion pratica*», 2, 2024, 422 s.

[20] Decreto-legge 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*", convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[21] Sul tema v. S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica,* in «*Media Laws*», 2, 2023, 404 ss.

[22] Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'art. 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*".

[23] Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante "*Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'art. 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*".

[24] Art. 1, comma 1, lett. h).

Quindi, con il decreto-legge n. 82 del 2021[25], si è "ritenuto […] di dover intervenire con urgenza al fine di ridefinire l'architettura italiana di cybersicurezza, prevedendo anche l'istituzione di un'apposita Agenzia per la cybersicurezza nazionale, per adeguarla all'evoluzione tecnologica, al contesto di minaccia proveniente dallo spazio cibernetico, nonché al quadro normativo europeo, e di dover raccordare, altresì, pure a tutela dell'unità giuridica dell'ordinamento, le disposizioni in materia di sicurezza delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche"[26].

Con il decreto-legge in esame è stata attribuita in via esclusiva al Presidente del Consiglio dei ministri un cospicuo numero di funzioni nell'ambito della cybersicurezza[27]. In particolare, egli ha la competenza dell'alta direzione e della responsabilità generale delle politiche di cybersicurezza; dell'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC); della nomina e della revoca del direttore generale e del vicedirettore generale dell'Agenzia per la cybersicurezza nazionale, previa deliberazione del Consiglio dei ministri"[28].

Nell'ambito del decreto-legge n. 82 del 2021 assume primaria importanza l'art. 5 con il quale viene istituita – colmando «una grave lacuna nell'architettura istituzionale nazionale in materia di cybersicurezza»[29] – l'Agenzia per la cybersicurezza nazionale (ACN) "a tutela degli interessi nazionali nel campo nella

[25] Decreto-legge 14 giugno 2021, n. 82, recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", convertito con modificazioni dalla legge 4 agosto 2021, n. 109. Sul decreto-legge in esame si veda F. Serini, L*a nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 12, 2022, 241 ss.

[26] Così il Preambolo del decreto-legge 14 giugno 2021, n. 82. Sulle diverse connotazioni della minaccia cibernetica, v. M. Mensi, L*a sicurezza cibernetica*, in M. Mensi, P. Falletta (a cura di), *Il diritto nel web*, Cedam, Padova 2018, 282 ss., che distingue le minacce cibernetiche nelle seguenti tipologie: *cyber-crime*, *cyber-espionage*, *cyber-terrorism*, *cyber-warfare*.

[27] Sul tema v. L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 14, 2024, 192 ss. ed O. Caramaschi, L*a cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in *Osservatorio AIC*, 4, 2022, 76 ss.

[28] Art. 2 ("Competenze del Presidente del Consiglio dei ministri"). Sul ruolo della Presidenza del Consiglio dei ministri nell'ambito della *cybersecurity* v. T. F. Giupponi, *Il governo nazionale della cybersicurezza*, in «*Quad. Cost.*», 2, 2024, 295 ss.

[29] L. Parona, L'*istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di diritto amministrativo*, 6, 2021, 711.

cybersicurezza". Le funzioni dell'ACN includono, oltre la tutela degli interessi nazionali in ambito di cybersicurezza, la predisposizione della strategia nazionale e la qualificazione dei servizi *cloud* per la Pubblica amministrazione. L'Agenzia rappresenta, inoltre, il punto di contatto unico per le finalità del decreto NIS, potendo irrogare sanzioni agli operatori di servizi essenziali o ai fornitori di servizi digitali; assume le funzioni in materia di cybersicurezza del Ministero dello Sviluppo Economico, del Dipartimento delle Informazioni per la Sicurezza e della stessa AgId. L'istituzione dell'ACN è strumentale all'esercizio delle competenze che il d.l. n. 82/2021 assegna al Presidente del Consiglio dei ministri – l'autorità al vertice dell'architettura della sicurezza cibernetica – al quale è attribuita l'alta direzione e la responsabilità generale delle "politiche di cybersicurezza", ed a cui spetta l'adozione della relativa strategia nazionale, nonché, come si ricordava poc'anzi, la nomina (e la revoca) dei vertici dell'Agenzia (Direttore e Vicedirettore)[30].

Successivamente è stata approvata, più di recente, la legge n. 90 del 2024[31] che, come è stato acutamente osservato, non costituisce diretta attuazione della Direttiva NIS 2, piuttosto «ne anticipa alcune misure, senza tuttavia prevedere forme di raccordo con essa. L'intervento proposto risulta quindi asincrono, e rischia di produrre ulteriore incertezza»[32].

La legge n. 90 del 2024 si presenta eterogenea, quanto ai contenuti, atteso che al Capo I prevede "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici*". Il Capo II, invece, raccoglie le "*Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamenti degli interventi*

[30] Sul punto v. A. Venanzoni, *L'ordine costituzionale della* cybersecurity, in «*Forum Quad. Cost.*», 4, 2024, 62.

[31] Legge 28 giugno 2024, n. 90, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*".

[32] Così M. Pietrangelo, *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, in *Rivista italiana di informatica e diritto*, 1, 2024, 25. V. anche E. Longo, *Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)*, in «*Rivista italiana di informatica e diritto*», 1, 2024, 68.

in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche dati in uso presso gli uffici giudiziari".

È stato rilevato che all'eterogeneità delle disposizioni si affianca un'altra criticità, dovuta alla presenza della consueta clausola di invarianza finanziaria, per cui «l'intero progetto non è credibile se non si individuano risorse adeguate»[33]. Ciò contrasta con la fondamentale esigenza di formazione sulla cibersicurezza, che, «parte di un deficit di conoscenze digitali dei cittadini italiani, deve essere assunta come un'emergenza democratica ed una questione costituzionalmente rilevante»[34]. Non solo: la legge n. 90 del 2024 pone l'accento sugli aspetti sanzionatori, ma non si occupa del profilo inerente all'aggiornamento delle competenze del personale della Pubblica amministrazione che quegli attacchi dovrebbe essere in grado di riconoscere e reprimere[35].

Pur non essendo possibile, in questa sede, richiamare tutte le disposizioni e le iniziative dedicate allo sviluppo delle competenze digitali, appare comunque utile menzionare le principali, per testimoniare lo sforzo delle Istituzioni europee e nazionali in materia di alfabetizzazione digitale. È opportuno partire dall'art. 8 del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82. La disposizione (rubricata proprio "*Alfabetizzazione informatica dei cittadini*") è stata peraltro modificata e ampliata con il decreto legislativo 26 agosto 2016, n. 179[36] e ora stabilisce che "lo Stato e i soggetti di cui all'articolo 2, comma 2[37], promuovono iniziative volte a favorire la diffusione della cultura

[33] Cfr. ancora M. Pietrangelo, *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, cit., 26 s., che quindi, propone di ancorare le misure di cui alla legge n. 90 del 2024 ai fondi destinati alla cybersicurezza istituiti con la legge n. 197 del 2022 (il "*Fondo per l'attuazione della Strategia nazionale di cybersicurezza*" e il "*Fondo per la gestione della cybersicurezza*").

[34] A. Iannuzzi, *Considerazioni sul disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati» (AC 1717)*, in «*Rivista italiana di informatica e diritto*», 1, 2024, 60.

[35] E. Longo, *Audizione informale*, cit., 68.

[36] Recante "*Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*".

[37] L'art. 2, comma 2 del CAD recita che: "Le disposizioni del presente Codice si applicano:

a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;

digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo"[38].

Anche a livello di Unione europea è stata riservata una certa attenzione al tema, a partire almeno dall'art. 33-*bis*, paragrafo 3, della direttiva (UE) 2018/1808, in base al quale "gli Stati membri promuovono lo sviluppo dell'alfabetizzazione mediatica e adottano misure a tal fine". L'impegno è proseguito, a livello europeo, con il piano d'azione per l'istruzione digitale (2021-2027), un'iniziativa politica rinnovata dell'Unione europea che definisce una visione comune di un'istruzione digitale di alta qualità, inclusiva e accessibile in Europa e che punta a sostenere l'adeguamento dei sistemi di istruzione e formazione degli Stati membri all'era digitale. Lo sviluppo delle competenze digitali è uno degli obiettivi strategici dell'Unione, che mira a dotare almeno l'80% dei cittadini tra i 16 e i 74 anni di competenze digitali di base entro il 2030. A guidare questo processo è il quadro europeo DigComp 2.2, che individua cinque aree chiave – dalla sicurezza informatica, alla creazione di contenuti – ritenute essenziali per una piena partecipazione alla vita sociale e professionale.

Tornando al versante nazionale, nel 2020 si è adottata la Strategia Nazionale per le Competenze Digitali con l'obiettivo di eliminare il *gap* con gli altri Paesi europei, in termini generali di digitalizzazione e rispetto ai singoli assi di intervento, e di abbattere il *digital divide* tra varie aree del territorio nazionale. Il Piano nazionale di ripresa e resilienza ha poi, da ultimo, dedicato particolare attenzione al tema, attivando anche la misura "Rete dei servizi di facilitazione digitale", con l'obiettivo di formare 2 milioni di cittadini entro il 2026 attraverso 3000 Punti Digitale Facile.

b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)".

[38] La disposizione, prima della modifica del 2016, si limitava invece a stabilire che "Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni".

La rapida panoramica sulle fonti che disciplinano la cybersicurezza mostra come le normative hanno posto un forte accento sulla protezione delle infrastrutture critiche, sulla tutela dei dati personali e sulla repressione degli attacchi informatici. Come si è visto, anche l'alfabetizzazione digitale ha ricevuto una certa attenzione dal legislatore europeo e da quello nazionale, che tuttavia non appare ancora del tutto sufficiente ad affrontare le nuove sfide emergenti. Eppure, l'alfabetizzazione digitale rappresenta un elemento chiave per la costruzione di una società resiliente e consapevole, in grado di riconoscere, prevenire e reagire efficacemente alle minacce informatiche. Queste lacune rischiano di indebolire la capacità del Paese di affrontare le sfide poste dalla digitalizzazione crescente, lasciando ampi spazi di vulnerabilità non tanto nelle tecnologie, ma nelle competenze degli utenti stessi.

Peraltro, sapersi muovere nel cyberspazio in sicurezza e in modo consapevole è ormai una necessità imprescindibile. È fondamentale, infatti, che ogni cittadino sia in grado di padroneggiare le nuove tecnologie per muoversi con competenza e tutela nel mondo digitale. In questo contesto, la scuola può e deve assumere un ruolo centrale, rappresentando il principale veicolo per diffondere conoscenze e competenze digitali fin dalla giovane età.

È incoraggiante, a tal proposito, il recente Protocollo d'intesa stipulato tra il Dipartimento per la trasformazione digitale (DTD) e l'Agenzia per la cybersicurezza nazionale (ACN), col quale si è dato vita a una nuova sinergia volta a potenziare le attività di sensibilizzazione e accrescimento delle competenze digitali sulla cybersicurezza e rafforzare la consapevolezza dei cittadini sulla materia[39]. L'accordo testimonia quantomeno della raggiunta consapevolezza, da parte delle Istituzioni italiane, sull'importanza del legame sempre più stretto che occorre instaurare tra cybersicurezza e competenze digitali.

[39] L'iniziativa, che si inserisce nel contesto del PNRR, coinvolge gli oltre 3.300 "Punti Digitale Facile", attivati nell'ambito della misura 1.7.2 del PNRR e gli Operatori volontari del Servizio Civile Digitale (misura 1.7.1), insieme alle oltre 280 organizzazioni della Coalizione Nazionale per le competenze digitali, parte integrante del programma strategico "Repubblica Digitale". Le attività di formazione prevedono anche materiali formativi di supporto ai Facilitatori, Operatori Volontari e organizzazioni della Coalizione nell'erogazione di corsi di formazione, workshop, ed eventi di sensibilizzazione sull'uso sicuro e consapevole degli strumenti digitali. La campagna di sensibilizzazione coinvolgerà anche i canali social del DTD e di ACN, con l'obiettivo di promuovere le attività svolte sul territorio e di diffondere strumenti e buone pratiche.

2. *Necessità di sviluppare competenze digitali per la prevenzione e la gestione degli attacchi informatici*

Dall'analisi normativa appare evidente come l'Unione europea e il legislatore statale abbiano inteso dar vita ad un vasto *corpus* normativo volto alla tutela delle infrastrutture di rete e dei dati che circolano in Internet, considerato che la cybersicurezza è funzionale all'esercizio dei diritti fondamentali: in assenza di dispostivi tecnologicamente avanzati atti a tutelare le reti e senza un idoneo strumentario normativo non può esistere la cybersicurezza. Tuttavia, si deve subito aggiungere che la creazione di un apparato – anzitutto normativo – volto a disciplinare la cybersicurezza è condizione necessaria, ma non sufficiente per assicurare la tutela dei diritti fondamentali dell'individuo nell'ecosistema digitale. Infatti, sia le direttive ed i regolamenti europei che le leggi necessitano di soggetti che siano in grado di avvalersi delle tecnologie sulla cybersicurezza. In altre parole, è necessario che pubbliche istituzioni e soggetti privati siano supportati nell'acquisizione (o nel miglioramento) delle competenze digitali.

Pertanto, la cybersicurezza richiede non solo adeguamenti normativi, ma anche un profondo cambio di impostazione culturale. Così come, nel corso degli ultimi dieci anni, si è assistito all'affermarsi di una cultura della protezione dei dati personali, incentivata anche da strumenti normativi come il GDPR, oggi è necessario che vi sia uno slancio per favorire la cultura della cybersicurezza.

Il tema in esame, invero, ha molto a che fare con l'alfabetizzazione digitale volta a ridurre il c.d. divario digitale (*digital divide*), inteso quale discrimine tra coloro che sono in grado di utilizzare gli strumenti informatici e coloro che, per ragioni economiche, culturali, generazionali, non sono in grado di avvalersene[40]. Il tema della alfabetizzazione digitale – preso in considerazione nel PNRR[41] – ha

[40] L. Nannipieri, *Costituzione e nuove tecnologie: profili costituzionali dell'accesso a Internet*, in *Rivista dell'Associazione "Gruppo di Pisa"*, Secondo seminario annuale del "Gruppo di Pisa" con i dottorandi delle discipline giuspubblicistiche su *"Lo studio delle fonti del diritto e dei diritti fondamentali in alcune ricerche dottorali"*, Università degli Studi Roma Tre, 20 settembre 2013, 3.

[41] Il Piano Nazionale di Ripresa e Resilienza (PNRR) alla Missione 1 ("Digitalizzazione, innovazione, competitività, cultura e turismo"), componente 1 ("Digitalizzazione, innovazione e sicurezza nella PA"), investimento 1.7 ("Competenze digitali di base") prevede interventi miranti a supportare le fasce della popolazione che, più delle altre, potrebbero subire le conseguenze negative del *digital divide*. In particolare, la missione in esame mira a rafforzare il «network territoriale di supporto digitale» e il «Servizio Civile Digitale, attraverso il reclutamento di diverse migliaia di giovani che aiutino circa un milione di utenti ad acquisire competenze digitali

infatti a che vedere con il concetto di "cittadinanza digitale" perché, come visto, essa oggi si sviluppa anche (forse, soprattutto) in una dimensione digitale. Non essere in grado di utilizzare gli strumenti informatici può comportare – e di fatto comporta – il rischio di una emarginazione dalla società e nell'esclusione dall'esercizio di molti diritti fondamentali.

Ebbene, è necessario operare una differenziazione tra alfabetizzazione digitale in senso stretto (rientrante, cioè, sotto la tutela dell'art. 34 della Costituzione e rivolta a coloro che sono in età scolastica[42]) e diritto all'"inclusione sociale digitale". Quest'ultimo trova, infatti, il suo fondamento costituzionale nell'art. 3, comma 2, Cost. ed è stato configurato dal legislatore come un diritto sociale per il cui inveramento sono state stanziate risorse economiche volte a garantirne l'attuazione[43].

Quindi, sia l'alfabetizzazione digitale che il diritto all'inclusione sociale digitale devono essere orientati alla implementazione di conoscenze digitali in materia di cybersicurezza, soprattutto se si considera che la normativa in materia di cybersecurity riguarda quasi esclusivamente le Pubbliche Amministrazioni e le imprese (soprattutto le piccole e medie imprese). Della cybersecurity, tuttavia, deve aver cognizione anche il singolo cittadino, perché possa tutelarsi dai rischi che quotidianamente si corrono nella navigazione in Internet. Solo in tal modo si formano individui in grado di riconoscere e gestire minacce informatiche che possono minare i loro diritti e costituire un impedimento all'adempimento dei propri doveri.

In un contesto digitale sempre più interconnesso e vulnerabile, la diffusione di competenze digitali si impone, quindi, come una priorità strategica per garantire la sicurezza dei sistemi informativi e la protezione dei dati personali e istituzionali. Gli attacchi informatici, per loro natura mutevoli e sofisticati, richiedono risposte che vadano oltre le sole misure tecnologiche: è necessario che i cittadini siano in grado di comprendere, anticipare e gestire le minacce informatiche in modo consapevole e proattivo.

di base». Il programma "Servizio Civile Digitale", sub investimento 1.7.1., per il quale sono stanziati 60 milioni di euro, si inserisce nel quadro della "Strategia nazionale per le competenze digitali" e del connesso Piano Operativo, entrambi sviluppati nell'ambito del progetto "Repubblica digitale".

[42] Sul punto si consideri il Piano nazionale per la scuola digitale, istituito dall'art. 1, comma 56, della legge 13 luglio 2015, n. 107.

[43] Come rileva C. Lotta, *Governance della Rete*, cit., 157 ss.

Lo sviluppo di tali competenze non deve essere limitato agli specialisti, ma deve riguardare l'intera popolazione, attraverso percorsi di alfabetizzazione digitale diffusa e continua, integrati nei sistemi educativi, nella formazione professionale e nelle politiche pubbliche. In questo quadro, le competenze digitali rappresentano non solo una leva di innovazione, ma anche un presidio essenziale di sicurezza e di esercizio dei diritti nella sfera digitale.

Infine, sul versante dell'alfabetizzazione digitale in senso stretto – rientrante, come si è detto, nel diritto all'istruzione di cui all'art. 34 Cost.[44] – è auspicabile che il legislatore implementi un percorso strutturato di educazione digitale che comprenda in modo esplicito e approfondito anche la formazione alla cybersicurezza. Incorporare, infatti, l'educazione alla cybersicurezza nel percorso scolastico significa fornire ai giovani non solo gli strumenti tecnici di base, ma anche farli giungere a comportamenti responsabili, fondamentali per prevenire i rischi più diffusi.

La percentuale di persone prive di competenze digitali adeguate resta ancora troppo elevata, rappresentando un ostacolo significativo all'inclusione piena nella società digitale[45].

Per colmare queste carenze, un primo significativo passo è rappresentato dalla legge 20 agosto 2019, n. 92 "*Introduzione dell'insegnamento scolastico dell'educazione civica*", che all'art. 5 ha appunto introdotto l'educazione digitale nell'ambito dell'insegnamento trasversale dell'educazione civica, le cui modalità di attuazione sono state definite con le Linee guida ministeriali emanate con il recente D.M. 7 settembre 2024, n. 183.

Ma non basta; parallelamente si tratta anche di garantire agli istituti scolastici dotazioni tecnologiche moderne e spazi adeguati, come aule informatiche dedicate, fondamentali per un apprendimento efficace delle competenze digitali. Purtroppo, tali strutture sono spesso assenti o insufficienti in molte scuole italiane, limitando così le possibilità di formazione pratica e l'accesso a un'educazione digitale di qualità. Tuttavia, solo investendo in infrastrutture

[44] Cfr. sul punto L. Palazzani, *Digital Divide* (voce), in A.C. Amato Mangiameli, G. Saraceni (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli, Torino 2023, 161; E. D'Orlando, *Profili costituzionali dell'Amministrazione digitale*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2011, 220; E. De Marco, *Introduzione alla eguaglianza digitale*, in *Federalismi.it*, 12, 2008, 4 s.

[45] Il livello di competenze digitali in Italia è tra i più bassi d'Europa: cfr. Openpolis, *La sfida dell'alfabetizzazione digitale per contrastare le disuguaglianze*, 28 gennaio 2025.

scolastiche adeguate sarà possibile creare un ambiente formativo che favorisca lo sviluppo delle competenze digitali indispensabili per affrontare le sfide del presente e del futuro.

3. *Considerazioni conclusive: la cybersecurity "metainteresse" nella tutela dei diritti fondamentali*

È oggi attraverso il digitale che si assicura la fornitura di servizi essenziali per la collettività e che si consente alle aziende l'esercizio di gran parte delle attività imprenditoriali. La sicurezza delle reti è, quindi, il presupposto per l'erogazione di attività pubbliche e private su cui si basa non solo la nostra economia (come trapela spesso dalle normative europee di armonizzazione delle previsioni nazionali), ma anche il nostro Stato sociale.

Così come la sicurezza è stata già vista in passato come valore super-primario[46], la cybersicurezza costituisce un "metainteresse" rispetto all'esercizio di taluni diritti fondamentali da parte dei singoli, che saranno tanto più restii al loro esercizio, quanto più è debole la loro *fiducia* nella sicurezza delle informazioni che li riguardano. In proposito, si deve riflettere sul fatto che la rinuncia all'accesso a determinate piattaforme equivale alla rinuncia all'accesso ai diritti e ai servizi.

Si può poi discutere sulla configurabilità di un "diritto fondamentale alla cybersicurezza"[47], cioè di una qualificazione della cybersicurezza come di un "diritto al diritto di essere protetti", proprio in quanto la disponibilità e integrità dei sistemi digitali sono condizioni preminenti per poter esercitare i propri diritti online.

[46] G. Cerrina Feroni, G. Morbidelli, *La sicurezza: un valore superprimario,* in «*Percorsi costituzionali*», 2008, 31 ss. Cfr., più di recente G. Pistorio, *La sicurezza giuridica. Profili attuali di un problema antico,* Editoriale Scientifica, Napoli, 2021, 216, secondo cui, invece, "la sicurezza non è, né può essere al di sopra di tutto. Tutt'altro. La garanzia costituzionale della sicurezza è assicurata solo tramite la tutela complessiva, contestuale, armonica dei diversi 'beni' costituzionali che si intersecano …".

[47] Ritiene che non sia possibile parlare di un "diritto fondamentale alla cybersicurezza" E. Longo, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in «*Rassegna parlamentare*», n. 2, 2024, 313 s. *Contra* P.G. Chiara, *Towards a Right to Cybersecurity in EU Law? The Challenges Ahead*, in «*Computer Law & Security Review*», 2023, online, 1 s.; G. Cerrina Feroni, G. Morbidelli, *La sicurezza: un valore superprimario*, cit., 31 s.

Senza giungere necessariamente a tali conclusioni, è indubbio tuttavia che la cybersicurezza si configura come un vero e proprio "metainteresse", ossia un interesse che sostiene l'attuazione di altri interessi: un prerequisito strutturale per il godimento dei diritti fondamentali. Senza sicurezza digitale, si minano libertà civili, accesso ai servizi, *privacy*, partecipazione democratica e fiducia nelle Istituzioni. Si può allora ben intuire quanto sia imprescindibile una preparazione sulle tematiche connesse alla garanzia dei sistemi di informazione e di rete, ma anche di base, rivolta a chi quotidianamente tratta dati, personali e non, nel contesto digitale.

La digitalizzazione, infatti, non è solo una questione tecnologica, ma incide profondamente sui diritti e sulle libertà fondamentali dei cittadini. Come è stato osservato in dottrina, infatti, «nella società digitale, […] accade che ciascun diritto fondamentale finisca per assumere una dimensione bifronte, mostrando accanto al volto tradizionale, il suo doppio digitale, così che si possa parlare di identità personale e di identità digitale, di sicurezza e di sicurezza informatica o cybersicurezza, di uguaglianza e di disuguaglianza digitale o *digital divide*, di doveri costituzionali di solidarietà e di solidarietà digitale e via dicendo»[48].

Risulta dunque evidente che la cybersicurezza non può essere considerata un ambito esclusivamente tecnico o riservato agli operatori del settore informatico, ma si configura come una questione trasversale, che coinvolge direttamente la sfera dei diritti fondamentali e della cittadinanza digitale. In tale prospettiva, l'alfabetizzazione digitale rappresenta non solo uno strumento abilitante per la partecipazione consapevole alla vita digitale, ma anche un fattore determinante per la prevenzione e la mitigazione delle minacce informatiche. Una *cybersecurity* efficace non può prescindere, quindi, da una società digitalmente consapevole. Investire in programmi di alfabetizzazione digitale rappresenta oggi una condizione necessaria per garantire la resilienza del sistema digitale e la tutela sostanziale dei diritti nell'ambiente cibernetico.

È quindi urgente un ripensamento normativo che, integrando le misure di sicurezza tecnica con investimenti concreti in formazione e alfabetizzazione digitale, rafforzi la cultura della sicurezza informatica a tutti i livelli della società. Un'adeguata formazione non solo favorisce l'accesso e l'utilizzo consapevole degli strumenti digitali, ma riveste anche un ruolo cruciale nel rafforzare la consapevo-

[48] Così A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in «*Dir. cost.*», 1, 2023, 12.

lezza riguardo ai rischi connessi alla condivisione di informazioni *online,* come la tutela della *privacy* e la sicurezza informatica. Solo attraverso l'educazione digitale sarà possibile formare cittadini preparati, capaci di navigare in modo sicuro e responsabile nell'ambiente digitale, contribuendo così a una società più inclusiva e resiliente.

Capitolo Secondo

La ricerca di un nuovo assetto teleologico in materia di sicurezza nel settore informatico

Pasquale Troncone

1. *La nuova dimensione disciplinare*

Questo Convegno si propone di aprire uno sguardo sul futuro in una prospettiva giuridica forse visionaria, forse incauta, forse temeraria, come tutta la tecnologia moderna ci induce a ritenere, nella piena consapevolezza che le decisioni e le elaborazioni del diritto, in particolare del settore penale, guardano sempre al passato, a ciò che è accaduto, al fatto allarmante, a ciò che ormai non può non essere impedito e mai verso il futuro a ciò che occorre progettare e controllare in termini di disciplina e di coerenza sistematica delle determinazioni giuridiche.

Il primo problema da affrontare è certamente quello delle fonti di questo diritto che non investe soltanto la materia penale, ma che vede intersecarsi il diritto civile e il diritto amministrativo che proprio nelle figure di reato del settore informatico realizzano la funzione di incriminazione integratrice.

Si tratta di una nuova forma di diritto, un diritto in divenire che vede il decisore politico collocato su diversi livelli normativi, dal diritto interno al diritto continentale e poi ancora quello internazionale, sovrastatuale, anche se è assente un testo condiviso dei principi validi per tutti a rendere omogeneo il sostrato giuridico[1]. Non mancano, tuttavia, norme autoprodotte dai gestori degli ambienti digitali, quali le autonome discipline di regolazione dei comportamenti in Rete adottate dai grandi motori di ricerca e normative e prescrizioni che provengono dalla Autorità autonome di garanzia – oltre la giurisdizione statuale – che, allo stesso tempo e a determinate condizioni, giustiziano diritti e sanzionano i contravventori (Zeno-Zencovich, 2003: 89).

[1] Il tentativo di progettare un testo costituzionale *ad hoc* è rinvenibile in Rodotà S., *Una costituzione per internet?* in «*Pol. del dir.*», 2010, p. 337. Allegri M. R., *Riflessioni e ipotesi di costituzionalizzazione del diritto di accesso a Internet*, in «*Rivista AIC*», 1/2016, p. 8.

Dunque, un modello regolativo del tutto nuovo e largamente inedito nel panorama delle fonti penalistiche che finisce per condizionare la singola norma penale punitiva e le scelte in sede applicativa operate dal giudice.

In questo nuovo orizzonte normativo mutano anche i soggetti che tradizionalmente sono all'attenzione del diritto penale, per cui non esiste più il soggetto agente che commette reati, ma il soggetto utente che lede diritti e interessi giuridicamente protetti di altro utente, con una forma di spersonalizzazione sconosciuta al diritto punitivo di matrice classica.

Questo nuovo scenario induce a progettare una politica criminale a base tecnologica, il cui paradigma, pur iscrivendosi nel solco dei principi regolatori della materia penale, deve affrontare il confronto con saperi diversi per la necessaria opera di prevenzione e poi di repressione nel contrasto al crimine tecnologico che fa parte del suo modello identitario. I nuovi "strumenti" da adoperare rispetto agli attori sulla scena non sono più il criminale, il giudice, la prigione, ma accanto a questi si ritrovano oggi nuovi attori istituzionali e professionalità del tutto nuove nel campo penale.

Il vecchio paradigma, infatti, guardava alla relazione tra persone e poi tra persone e soggetti, oggi occorre guardare a una relazione tra soggetti fondata su un diaframma, un legame intermedio, uno strumentario di natura tecnologica, la cui portata deve essere valutata in termini di relazione complessa, dove non esiste un autore del crimine bensì un apparato immerso nella immaterialità di una condotta; una platea di soggetti offendibili di natura vulnerabile per essere anche sotto-dotati tecnologicamente; una giustizia penale che oltre ai codici è chiamata a utilizzare mezzi altamente sofisticati per accertare i fatti; un processo penale la cui lunghezza può lasciare insoddisfatti i danneggiati se non si dota di un contesto tecnologico oltre che tecnico-giuridico che offra tempestività ed effettività alla decisione (Sisto, 1985: 28).

Il tema ha raggiunto una tale dimensione che il penalista tradizionale perde di vista il "fatto reato", la sua articolazione costitutiva, la sua rilevanza sociale, e prende atto che la sua analisi deve affrontare fenomeni di massa, danni a interessi giuridicamente qualificati che riguardano un numero indefinibile di individui – i c.d. reati a soggetto passivo diffuso –; illeciti commessi su un territorio senza confini; identificazione dei responsabili le cui tracce si disperdono in un universo immateriale.

La stessa indagine probatoria per l'accertamento del reato sembra essere stata depotenziata se è necessario attraversare itinerari che non sono più di semplice rilevazione di una circostanza concreta, ma di un apprezzamento e un giudizio

che passa per le maglie di discipline tecniche e tecnologiche, diverse da quella giuridica.

Anche la categoria della c.d. "*quarta rivoluzione industriale*" appartiene al lessico di un modello tradizionale, superato, di considerare il rapporto uomo-macchina. Oggi è necessario guardare a un rapporto rovesciato macchina-uomo, non solo perché la macchina si sostituisce all'uomo seguendo il progetto di massima dell'uomo, perché la macchina tende a divenire indipendente dall'uomo e l'uomo è destinato a intervenire solo per correggere o arginare l'azione dei meccanismi tecnologici che compongono la nuova macchina: dal Web 2.0 con interazione tra gli utenti al Web 4.0 con la prevalente operatività dell'Intelligenza Artificiale.

La nuova e imprevedibile frontiera è un diritto penale difensivo, vale a dire il rovescio della medaglia dell'attuale, perché alla base è sempre necessaria la difesa dell'uomo e delle sue libertà anche rispetto alle iniziative della macchina pensante.

È inutile negare che il vasto panorama dei regimi regolativi che si svela al gius-penalista è talmente ampio, variegato e diverso dal solito che la sola esegesi svolta sull'attuale assetto normativo rischia di perdere razionalità. La legislazione del settore informatico è talmente caotica e confusa anche per le scelte normative che non sono armonizzate con le numerose e disseminate norme penali vigenti, per cui occorre ricercare un razionale ordine sistematico dotato di intrinseca coerenza attraverso un'opera svolta con rigore ed equilibrio.

2. *Verso un nuovo paradigma di tutela. I nuovi interessi giuridici che emergono dal mondo digitale*

Le istanze di tutela dei beni e degli interessi personali e collettivi nel diritto penale impongono che siano elaborate norme punitiva in grado di apprestare una puntuale protezione in questo nuovo settore della materia penale destinato a una decisa e cospicua evoluzione (Amato Mangiameli – Saraceni, 2019).

Originariamente il nuovo assetto normativo passava sotto la definizione di diritto penale dell'informatica, dove le diverse figure di reato presidiavano i dati digitali e i sistemi di elaborazione degli stessi (Picotti et alii, 2020: 5). L'evoluzione tecnologica ha sviluppato, tuttavia, e rapidamente un nuovo indirizzo disciplinare, per cui il quadro complessivo oggi appare a struttura funzionale composita: da un lato la *Cybersecurity*, vista come difesa del complesso tecnologico, vale a

dire dei sistemi e delle strutture informatiche critiche dagli attacchi ostili provenienti dall'esterno; dall'altro la *Sicurezza informatica*, vale a dire la protezione delle informazioni, dei dati e dei programmi per il loro trattamento. Entrambi capaci di cagionare danni irreversibili o temporanei, come tipiche espressioni operative di una contesa armata combattuta con armi diverse e che si distinguono per essere una moderna *Cyberware*.

Per queste ragioni e per tenere nel debito conto il principio di sicurezza che governa questo nuovo ambito normativo appare più congruente ridefinire la materia come quella della "Sicurezza informatica e dei dati", per fare in modo da compendiare il duplice assetto di tutela che merita una sinergica regolazione giuridica in termini di prevenzione e repressione.

Questa è la ragione per cui, diversamente dal mondo reale, c'è bisogno di forme di tutela differenziata per la difesa dalle ostilità informatiche, una tutela tecnologica e una tutela giuridica che svolgano, dunque, simultaneamente quella necessaria funzione preventiva e punitiva.

La realtà insegna che nella finalità degli attacchi è insita la sottrazione o rendere temporaneamente indisponibili le informazioni di archivio e le operatività delle risorse informatiche in settori nevralgici della società, quali quello commerciale, strategico, militare, sanitario, per ottenere un profitto illecito e non solo. Sul piano del danno si stima, infatti, che queste pratiche illegali sempre più diffuse hanno registrato negli ultimi anni un peso economico su scala mondiale di oltre 2000 miliardi di dollari.

A proposito della tutela penale non si può prescindere dal fatto che le originarie fattispecie di reato in questa materia erano finalizzate a tutelare prevalentemente il patrimonio individuale della vittima, come primo avamposto di tutela che ha finito per condizionare la prima stagione della legislazione penale che gravita intorno al settore dell'informatica (Pecorella, 2006).

Il primo atto sovranazionale non è lontano nel tempo, vale a dire la *Convenzione Cybercrime di Budapest del 2001*, chiamata per la prima volta a regolare in maniera omogenea alcuni fatti cui assegnare rilevanza penale negli ordinamenti dei Paesi sottoscrittori[2].

Da questa primo progetto di regolazione a livello internazionale e poi con gli interventi successivi, sia sovranazionali che interni, sono emerse due distinte categorie normative: a) I sistemi informatici quali beni o oggetti di tutela penale;

[2] Che ha trovato attuazione in Italia con la legge n. 48 del 18 marzo 2008.

b) I sistemi informatici quali strumenti di commissione dei reati che compaiono come elementi costitutivi della fattispecie incriminatrice[3].

In questo modo si imprime una svolta alla materia informatica che progressivamente scivola dalla categoria dei servizi a quella dei beni, imponendo interventi progettuali destinati a riconoscere una autonoma e indipendente collocazione sistematica alla relativa disciplina penale.

Questa è la ragione per cui l'attuale ampia piattaforma legislativa invoca l'individuazione di un bene giuridico di categoria di nuovo conio, del tutto diverso e onnicomprensivo rispetto alle categorie tradizionali che la dottrina ha utilizzato finora, come ad es. il patrimonio, la riservatezza (*la privacy*) desumendola dalle norme di valore dall'art. 14 Cost. – sulla segretezza della corrispondenza – e dall'art. 15 Cost. – sul domicilio informatico –, e, a livello di regolazione sovranazionale continentale dal principio di democrazia.

Se un bene ideale di riferimento appariva ancora del tutto incerto, di contro un denominatore comune risultava l'oggetto materiale del reato che assumeva connotazione di elemento costitutivo del fatto in ogni fattispecie incriminatrice. Per cui, a nostro avviso, va delineandosi un quadro normativo in cui compaiono in maniera ricorrente i sistemi informatici da una parte e i dati informatici dall'altra.

Esaminando la prospettiva teleologica della nuova materia, come già si è detto, ad emergere non è un singolo bene bensì un "luogo di tutela", un arcipelago di interessi rilevanti, così come per assimilazione si definisce il concetto di pubblica economia, anch'esso ampio campo di tutela con interessi differenziati che lo compongono.

Lo sfondo ideale di questo assetto di tutela chiamato alla protezione della sicurezza del settore informatico è del tutto corrispondente alla tutela dei beni comuni, come avviene per l'acqua, le matrici ambientali. Si tratta di una gestione svolta in maniera non egoistica di un macro-bene, un diritto di uso in forma collettiva, dove appunto quella gestione comunitaria va a coincidere con la forma di protezione.

In questo modo si assiste alla variazione identitaria dell'utente, che non è più tale, ma si trasforma in consumatore che assume i profili identificativi e quali-

[3] Si veda a tale proposito il Disegno di legge 2773 Ministro di Grazia e Giustizia, XI legislatura Camera dei deputati, secondo il quale le nuove fattispecie criminose rappresentano semplicemente "…*nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, ecc.), già oggetto di tutela nelle diverse parti del corpo del codice*".

ficativi della categoria e del tipo di vittima, per cui si procede alla profilazione anagrafica, la profilazione professionale, la profilazione sanitaria, la profilazione etnica, la profilazione politica, etc.

Da qui la considerazione della posizione di vulnerabilità implicita del soggetto, il quale si trova nella posizione, per il solo fatto di navigare in Rete, di chi agisce sulla base di un suo consenso presunto, di un consenso non espresso esplicitamente e formalmente, ma indirettamente sussistente per il solo fatto di trovarsi in Rete. Sulla base di questa qualificazione che viene riconosciuto dagli altri utenti e profilato in modo da essere identificato, seppure non abbia ceduto espressamente con il suo consenso il proprio profilo identificativo.

3. *Le premesse teoriche per una svolta dommatica in una nuova materia penale*

Porre le basi della sicurezza del settore informatico vuol dire prima di tutto riesaminare tutta la disseminata materia legislativa dedicata all'informatica alla luce della dommatica penale tradizionale, per regolare e cogliere le peculiarità del nuovo e del tutto inedito ambito normativo.

Occorre partire dal concetto di *Cyberspazio* che non ha un territorio di riferimento dove si consumano reati e, dunque, non consente con certezza di individuare il giudice competente a decidere, perché diventa difficile stabilire le coordinate di consumazione del fatto reato a seconda dell'evento o della condotta (Fumo, 2013: 771). Il concetto di libertà di agire che è alla base della fisiologia dell'ecosistema della Rete vede come suo corrispettivo l'autodeterminazione ad agire in ambiti territoriali sempre diversi (Perusia, 2001: 1835).

Occorre allora, nel pieno rispetto dei principi di orientamento della materia penale, fare ricorso alle "buone pratiche" legislative per adattare quelle vigenti e allestire nuove ipotesi di reato, puntuali, precise, definite, effettive, pronte ad essere utilizzate. Un nucleo di reati che si caratterizzi per le particolari modalità di realizzazione della condotta e per lo strumentario tecnologico in uso nel mondo dematerializzato della Rete.

Sul piano della struttura del fatto-reato la prima considerazione investe la natura della condotta. Si tratterà di descrivere, sembrerebbe, solo reati di azione, dando rilievo al caso dell'omissione colpevole attraverso la regola degli obblighi giuridici e le relative posizioni di garanzia dell'art. 40 cpv c.p. Con l'inevitabile carico di qualificare la causa rilevante in riferimento alla posizione di colui che non ha impedito il verificarsi dell'evento che aveva l'obbligo di impedire.

Come valutare e individuare, poi, la causa determinante o la contemporanea esistenza di altre cause che hanno dato vita all'evento facendo ricorso a una disciplina datata al 1930 che già con il banco di prova del disastro innominato non ha fornito adeguate risposte? E in questo caso come può giocare l'incidenza della causa individualizzante sul piano statistico di probabilità e possibilità nell'ottica fornita dalla sentenza Franzese? In questo ambito la relazione causa-effetto come va intesa, dal momento che, se è vero che nella realtà concreta si può raggiungere un ragionevole grado di certezza, nel caso della Rete diventa invece difficile sceverare tra le tante cause che intervengono e si affiancano a quella iniziale e forse perdono vigore per effetto di quelle sopravvenute: saranno da reputare sempre eccezionali?

L'evento. Sarà da intendere in senso naturalistico o in senso giuridico come sembra suggerire il contesto dematerializzato da cui prende ragione? Tra le pieghe della valutazione del fatto non può mancare il riferimento all'elemento soggettivo e da qui il dilemma se, ai fini risarcitori, va considerato il rischio sociale della navigazione in Rete che qualunque utente dovrà considerare nel momento in cui ne fa accesso, e la rilevanza della colpevolezza a chiudere il cerchio dell'accertamento della responsabilità penale. L'importanza del contributo con-causale della vittima quando i reati vengono realizzati con il contributo fattivo inconsapevole o con la collaborazione inerte della vittima a questo punto non può essere sottovalutato.

Sul piano della risposta punitiva occorre tenere nella debita considerazione anche la responsabilità amministrativa degli Enti del D.lgs. n. 231/2001 (Aa.Vv., 2022). Soprattutto armonizzando le cause estintive del reato di natura premiale o deflattiva con la legislazione di settore, valorizzando la riabilitazione dell'Ente alla luce degli interventi correttivi conformi alle leggi, alla luce della *compliance*.

Il vero problema però resta quello di valorizzare gli scudi protettivi per le vittime come ci indirizzano le fonti europee, bersagli di danni che non sempre è possibile qualificare con parametri econometrici, perché gli indici di danno in larga parte ricadono sui diritti della personalità.

Esiste inoltre lo scottante problema della permanenza degli eventi dannosi in Rete e, per questo, ipotizzare reati a consumazione prolungata? Come nella corruzione?

Possono permanere in Rete senza soluzione di continuità i patrimoni informativi di persona decedute, i cui eredi non sempre hanno competenza e capacità tecnologiche per gestire la correttezza di quelle informazioni.

E poi come è possibile trattare la punibilità di una fonte infettiva, di un *malware* che si propaga nel *device* e si diffonde in Rete? In questo caso occorrono

gli ingegneri ad accompagnare il legislatore e prevedere in maniera inequivocabile, con appropriata terminologia, forse con una tabella integrativa della legge come è avvenuto con DPR n. 309/90 in materia di stupefacenti.

Il punto più oscuro resta però quello della effettività della pena, quale può essere la risposta punitiva in termini di rieducazione aderente a quel tipo, alla natura di quel reato? Quali possono essere ipotizzate come pene tecnologiche?

E le misure cautelari reali come vanno congegnate? E le pene o le misure tecnologiche inabilitative, come spesso si è sentito dell'ergastolo informatico, come vanno irrogate e controllate? L'esperienza del braccialetto elettronico per le misure alternative ci fornisce spunti di esperienza importanti per comprendere la fallibilità di un sistema tecnologico che non si mostra ancora all'altezza.

Infine, quale risposta indennitaria per la vittima in permanente minorata difesa?

4. *La disseminazione delle fonti. La necessità di un testo di legge autonomo*

Riteniamo sia giunto il momento di dare vita a un'esperienza legislativa destinata a sciogliere tutti i nodi di questa complessa materia che acquista progressivamente una sempre maggiore ampiezza introducendo un corpo normativo unico, che potrebbe essere denominato: "Codice per la sicurezza informatica e dei dati".

Da alcuni mesi si registrano le prime crepe interpretative che spingono i giudici a una giurisprudenza creativa oltre la norma. In questo modo si evidenziano i limiti di una legislazione improvvisata e mai organizzata secondo un criterio sistematico: «*Forse anche per questo – muovendosi in un'ottica di stampo contenutistico – il legislatore ha ritenuto di non varare un corpus unitario di (nuove) norme repressive, ma ha scelto di prevedere le "nuove condotte criminali" (se non tutte, almeno le più rilevanti), collocandole "topograficamente" negli habitat normativi che sembravano – di volta in volta – più opportuni. Non sempre si è trattato però di scelte felici*» (Fumo, 2013: 775).

Occorrerebbe invece richiamare l'impegno deontologico del legislatore nella cura della legge, verso una formulazione anche lessicale che non possa lasciare margini al dubbio nei destinatari, in termini di prevedibilità della condanna, e nel giudice chiamato ad applicarla con sufficiente precisione.

Diversamente dal recente passato oggi esiste un vincolo normativo per il legislatore dettato dall'art. 3-*bis* c.p., vale a dire l'obbligo di disciplinare in modo organico fattispecie incriminatrici appartenenti a una stessa materia. Una materia

che va individuata sulla base del comune denominatore intorno al quale strutturare il precetto e che trova il suo punto di qualificazione giuridica, il suo comune denominatore di principio nella "Sicurezza informatica e dei dati" che altro non è se non la cybersicurezza declinata attraverso i suoi strumenti operativi.

D'altro canto, per le scelte di tecnica normativa occorre fare leva sull'art. 15 del codice penale "*Materia regolata da più leggi penali o da più disposizioni della medesima legge penale*" ed elaborare figure di reato, seppure nel *genus* già esistenti nella legislazione, nella *species* distinte per elementi specializzanti, come si è proceduto con il delitto di danneggiamento dell'art. 635-*bis* c.p., anche se le varie ipotesi di danneggiamento andrebbero ridotte a una sola figura di reato, e non come avvenuto con l'introduzione del terzo comma dell'art. 629 c.p. che punisce l'estorsione informatica come semplice aggravante.

Un Testo Unico con un autonomo catalogo di reati eviterebbe i continui rinvii sistematici che gli attuali testi contengono, sottraendo omogeneità e coerenza alla normativa di settore.

Peraltro, seguendo l'esempio delle Direttive dell'Unione Europea, sarebbe addirittura auspicabile una sinossi normativa in apertura del provvedimento, contenente la esatta definizione dei vari requisiti e dei concetti che sono contemplati come elementi di tipicità del fatto di reato.

Ad esempio, non è sempre chiaro in quale modo il legislatore declina il concetto di vantaggio, cosa diversa dal profitto, eppure utilizzato indifferentemente (es. la finalità ulteriore nel furto). Così come il concetto di danno è cosa diversa dal nocumento e la nozione di appropriazione, figlia di una concezione proprietaria, in materia informatica si traduce in una copiatura di file, in una forma di clonazione e non di sottrazione definitiva.

Attualmente, invece, assistiamo a degli innesti normativi di nuove fattispecie nelle classi di reato tradizionali e di parti di norme nei precetti preesistenti che non sempre mostrano una decisiva coerenza, collocate nelle classi dei delitti contro la libertà morale, contro l'inviolabilità del domicilio, contro l'inviolabilità dei segreti, contro il patrimonio.

Ad esempio, il c.d. *revenge porn* o, meglio, la "*Diffusione illecita di immagini o video sessualmente espliciti*" dell'art. 612-*ter* c.p. è una forma di trattamento illecito di dati personali, è violazione della riservatezza, e tuttavia non si trova nel Codice del trattamento dei dati personali, perché l'art. 167 CdP si apre con una clausola di sussidiarietà espressa che lo esclude. Ma si tratta del medesimo "tipo" di illecito, sebbene con un diverso disvalore qualificato dal genere di danno cagionato alla vittima.

Allo stesso modo la tutela degli archivi dei dati informatici, si trova rubricata sia nel Codice penale artt. 615-*ter* "*Accesso abusivo ad un sistema informatico*" del Codice penale (Casale, 2021) e quello previsto nel Codice del trattamento dei dati all'art. 167-*bis* "*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*" CdP. Si tratta dello stesso fatto, commesso con le stesse modalità di condotta.

Ad esempio, nel campo patrimoniale circoscritto alle criptovalute si individua nei meccanismi di funzionalità della *blockchain* un trattamento di *dati non personali*, dati contenuti nelle due chiavi informatiche che ne regolano anche la titolarità. Non c'è uno scambio di valuta bensì uno scambio di dati che coincide con uno scambio di valori economici. Andrebbe, dunque, ipotizzata una disciplina specifica nel settore informatico, per assicurare la stessa tutela che il Codice penale riserva alla moneta ufficiale in corso, prima la lira oggi l'euro.

Su questo tema si agita senza sicuri approdi la giurisprudenza degli ultimi anni, non avendo il legislatore regolato il regime giuridico della circolazione delle criptovalute e il suo valore condiviso dal mercato, marcandola soltanto a fini fiscali, rendendo anche ardua l'applicazione di tutte le ipotesi di sequestro penale finalizzati alla confisca degli artt. 240 e ss. c.p. (Corasaniti, 2012: 819).

Come si vede l'orizzonte è ampio e il cammino, a mio avviso, è ancora lungo per superare steccati culturali che sanno di antico e che non apportano armonia alle moderne esigenze legislative. Le condotte di sopraffazione di una criminalità che agisce in uno spazio indistinto si scontra con i nostri strumenti di tutela che regolano spazi finiti, confini certi, elementi identificativi concreti e incontrovertibili.

Bibliografia

Aa.Vv., *Cybercrime e responsabilità da reato degli enti. Prevenzione e modello organizzativo e indagini preliminari*, in Monti A. (a cura di), Giuffrè, Milano, 2022.

Aa.Vv., *Diritto penale dell'informatica. Reati della rete e sulla rete*, in Parodi C., Sellaroli V. (a cura di), Giuffrè, Milano, 2020.

Allegri M. R., *Riflessioni e ipotesi di costituzionalizzazione del diritto di accesso a Internet*, in «*Rivista AIC*», 1/2016

Amato Mangiameli A.C., Saraceni G., *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2019.

Berghella F., Blaiotta R., *Diritto penale dell'informatica e beni giuridici*, in «Cass.pen.», Fasc. 9, 1995.

Casale P. P., *Prima "legge" della sicurezza informatica: "un computer sicuro è un computer spento"*, in www.archiviopenale.it, n. 2, 2021.

Corasaniti G., *Brevi note in tema di confisca obbligatoria di beni e strumenti di commissione dei reati informatici alla luce della legge 15 febbraio 2002 n. 12*, in «Il dir. dell'inf. e dell'inform.», 2012.

Fumo M., *La condotta nei reati informatici*, in «Arch.pen.», 2013.

Giannantonio E., *L'oggetto giuridico dei reati in-formatici*, in «Cass.pen.», Fasc. 7-8, 2001.

Pecorella C., *Diritto penale dell'informatica*, Cedam, Padova, 2006.

Perusia E., *Giurisdizione italiana anche per le offese on line su un sito straniero*, in «Cass.pen.», 2001.

Picotti L., Salvadori I., Flor R., *Reati informatici, riservatezza, identità digitale*, in www.aipdp.it.

Rodotà S., *Una costituzione per internet?* in «*Pol. del dir.*», 2010.

Sisto F.P., *Diritto penale dell'informatica e recupero dei modelli tradizionali*, in «Crit.pen.», 1985, fasc. 3.

Zeno-Zencovich V., *Informatica ed evoluzione del diritto*, in «Il dir. dell'inf. e dell'inform.», 2003.

Capitolo Terzo

Il delitto di accesso abusivo a sistema informatico, tra limiti di stretta legalità e adattamenti giurisprudenziali

Andrea Alberico

Il mio intervento è in linea di continuità con quelli che stamattina sono stati tenuti dai colleghi Flor e Troncone, e in particolar modo si concentrerà sull'art. 615 *ter* c.p. – cioè, sulla fattispecie di accesso abusivo a sistema informatico – che costituisce in qualche misura il fulcro del micro-sistema penale nella materia dei reati informatici, ammesso che di sistema si possa davvero parlare.

La trattazione coinvolgerà necessariamente ed in primo luogo le criticità strutturali della disposizione incriminatrice, concentrandosi poi su quelle applicative.

Cominciamo però col dire che la fattispecie di accesso abusivo a sistema informatico, in questo momento storico, si trova ad essere – si direbbe suo malgrado, ma forse neanche troppo – al centro della riflessione dottrinale intorno a quello che è forse il più significativo problema della penalistica contemporanea, e cioè il rapporto tra legge e giudice, in uno con le ricadute che questo rapporto determina sui consociati[1].

Questa scomoda posizione ha inevitabilmente condizionato le capacità prestazionali dell'art. 615 *ter* c.p., stimolando dunque il giurista teorico a provare a mettere ordine nella congerie di questioni che si pongono sul tavolo. Tutto, occorre dirlo, nel colpevole silenzio del legislatore che non ha colto la dimensione dei problemi esistenti ed anzi, quando è intervenuto nella materia – da ultimo con la legge n. 90 del 2024 –, lo ha fatto in maniera non convincente, e forse dando la stura a problemi ulteriori rispetto a quelli già esistenti.

Naturalmente il mio punto di vista è quello del penalista: stamattina se vogliamo avete ascoltato una difesa della l. 90/2024 su altri aspetti, in merito ai quali lungi da me prendere posizione; però rispetto alla morfologia complessiva dell'incriminazione dovremo necessariamente segnalare talune nuove criticità generate proprio dall'ultimo intervento legislativo.

[1] Cfr. Cass., Sez. 6, Sentenza n. 28594 del 26/03/2024 Ud. (dep. 16/07/2024) Rv. 286770, con nota di Maiello (2025, 406 ss).

Quindi idealmente possiamo dividere questo intervento in due parti: la prima sarà dedicata allo stato dell'arte sull'interpretazione dell'art. 615 *ter* c.p., ed in questo contesto toccheremo anche il tema del rapporto tra legge e giudice; la seconda parte, invece, affronterà i problemi applicativi che potrebbero presentarsi all'indomani della riforma del 2024.

Possiamo prendere le mosse da una considerazione che a mio sommesso avviso contribuisce a illuminare le coordinate di complessità del delitto di accesso abusivo: la formulazione dell'art. 615 *ter* c.p., ed in particolare il testo del primo comma, resiste in questa versione sin dal momento della sua introduzione, che risale al 1993, ad opera della legge n. 547.

La fattispecie è rubricata "*accesso abusivo ad un sistema informatico o telematico*", ma già analizzando la descrizione della condotta tipica ci si avvede che la scelta semantica risulta infelice: si punisce colui che *si introduce* nel sistema. L'opzione in favore del verbo "introdurre", nella variante "introdursi", si spiega in ragione del fatto che il legislatore del 1993, in maniera più che comprensibile per l'epoca, ha disciplinato l'accesso abusivo per analogia rispetto alla limitrofa fattispecie di cui all'art. 614 c.p., che punisce la violazione di domicilio. Il legislatore, in altri termini, ha considerato il sistema informatico alla stregua di un luogo chiuso, ad accesso regolamentato dal titolare, come è appunto il domicilio privato. Ma mentre nel domicilio è possibile l'ingresso, l'introduzione fisica, evidentemente questa condotta risulta incoerente al cospetto di un sistema informatico nel quale di certo l'individuo non può penetrare fisicamente. La scelta verbale risulta ancor più deficitaria se si considera che la rubrica parla di "accesso", termine invero più elastico e capace di inquadrare meglio il fatto penalmente rilevante.

In altri termini, nella condotta tipica non c'è, né può esserci, una componente fisica. Piuttosto, si intende punire il dialogo logico 'non autorizzato' che il colpevole instaura con il sistema bersaglio (Salvadori, 2023: 561), preceduto dal superamento delle 'misure di sicurezza' (Di Florio, Zarra, 2022: 11) (altra scelta semantica non particolarmente felice, come diceva il Professore Flor stamattina; per semplificare, il concetto di misura di sicurezza rimanda alla eventuale presenza di password o verifiche biometriche richieste per accedere al contenuto del sistema).

La condotta, infine, deve qualificarsi per il connotato della abusività: il legislatore ricorre ad una caratterizzazione modale che di primo acchito sembrerebbe scolpire una clausola di antigiuridicità espressa, con la quale sostanzialmente vuole limitare lo spazio di rilevanza penale alle sole condotte che non siano accompagnate dall'adesione, dal consenso, del soggetto titolare del sistema.

Anche siffatta scelta risulta discutibile, atteso che – mutuando proprio il lessico e la struttura della limitrofa fattispecie di violazione di domicilio – si sarebbe potuto ricorrere al concetto di *violazione* ivi presente nella rubrica – che rimanda immediatamente al superamento illecito della *voluntas excludendi* – e di *clandestinità* dell'accesso, ivi impiegato nella descrizione del tipo criminoso.

Ora, l'opzione in favore della clausola in esame ha inevitabilmente creato problemi rispetto a cosa debba intendersi per accesso abusivo. È abbastanza agevole affermare che l'accesso sia abusivo (e clandestino) quando colui che lo effettua non sia stato dotato delle 'chiavi' necessarie per superare le misure di sicurezza. Allo stesso tempo, è agevole affermare che l'accesso non può essere abusivo (né clandestino) dal punto di vista penale se il titolare del sistema non vi oppone barriere *excludendi alios*.

Il discorso diviene già più articolato qualora, invece, taluno acceda al sistema avendone titolarità e possedendone altresì le chiavi – e la prassi purtroppo ci restituisce una significativa evidenza di come siano spesso gli stessi appartenenti alle forze dell'ordine o alla pubblica amministrazione a tenere questo tipo di condotte –, ma per perseguire finalità diverse da quelle per le quali le password stesse gli erano state fornite.

Questa esemplificazione contribuisce a segnare in maniera puntuale il campo elettivo della fattispecie: come può notarsi, essa non appare destinata a reprimere esclusivamente il fenomeno degli attacchi informatici gravi, posti in essere da persone qualificate che comunemente chiamiamo "hacker", ma si candida ad essere applicabile ogni qual volta si possa apprezzare la violazione del rapporto di esclusività che esiste (e che va tutelato) tra il titolare e il sistema informatico o telematico.

L'interprete, dunque, deve impegnarsi per ricostruire una dimensione operativa della fattispecie che consenta di impiegarla tanto di fronte a fenomeni particolarmente allarmanti, perché coinvolgono come bersagli soggetti istituzionali piuttosto che aziende di dimensioni rilevanti e che custodiscono dati o programmi cruciali per gli individui o per il funzionamento di servizi essenziali, quanto nella difesa dell'inviolabilità dello spazio informatico "privato", nel quale ciascun essere umano colloca (o può collocare) dei dati ritenuti fondamentali per la propria esistenza.

La criticità delle scelte semantiche prese dal legislatore nel 1993 ha tardato ad emergere, nel senso che è venuta in rilievo solo dopo la rivoluzione che, a cavaliere del nuovo millennio, ha attraversato la società sul piano informatico e cibernetico. Il legislatore del 1993 forse non poteva neanche immaginare il tipo

di rapporto che si è progressivamente delineato tra l'essere umano e gli strumenti informatici, e la pervasività dell'impiego di questi nella vita quotidiana.

Se per curiosità si passa in rassegna la relazione illustrativa della legge n. 547 del 1993, si comprende come il legislatore pensasse all'uso dei sistemi informatici prevalentemente da parte dei soggetti pubblici – sono nominati espressamente l'Inps, il sistema bancario, quello dei trasporti, le assicurazioni –, ed in specie in quei contesti nei quali prima e meglio di tanti altri c'era già stata una transizione dalla carta al digitale.

I problemi ermeneutici più complessi sono emersi a partire dalla seconda decade del nuovo millennio, quando la fattispecie di accesso abusivo è approdata alle Sezioni Unite della Corte di cassazione in ben tre occasioni: 2012, 2015, 2017. Già questo dato dovrebbe in qualche modo preoccupare, perché, come è noto, si ricorre alle Sezioni unite nell'interpretazione di una norma incriminatrice quando di questa vengono offerte diverse ricostruzioni, diverse calibrature applicative da parte delle Sezioni semplici. La circostanza che la disposizione sia pervenuta in tre occasioni al vaglio del massimo organo della nomofilachia costituisce dunque già di per sé un campanello di allarme.

La decisione intermedia, quella del 2015[2], afferiva prevalentemente alla determinazione del luogo del commesso reato, questione molto delicata sul piano processuale, ma non strettamente connessa alla morfologia del tipo, sicché è possibile escluderla dal presente vaglio.

Nel 2012 e nel 2017, invece, la questione rimessa alle Sezioni unite investiva proprio la necessità di chiarire a quali condizioni un accesso potesse dirsi abusivo. Si trattava di due vicende, esemplificative di moltissime altre analoghe, nelle quali l'imputato era dotato legittimamente delle chiavi per accedere al sistema: nella sentenza del 2012 il ricorrente era un carabiniere che aveva consultato il sistema SDI per finalità, diciamo così, privatistiche, e quindi non per ragioni investigative o di servizio; nella sentenza del 2017 l'imputata era invece una dipendente della Procura della Repubblica che aveva interrogato il registro di cui all'art. 335 c.p.p. per far sapere ad un conoscente se fosse o meno indagato.

Nella decisione del 2012[3] la Suprema Corte affermò che l'accesso compiuto da quel carabiniere doveva considerarsi abusivo, nonostante fosse dotato delle

[2] Cass., Sez. un., Sentenza n. 17325 del 26/03/2015 Cc. (dep. 24/04/2015) Rv. 263020.

[3] Cass., Sez. un., Sentenza n. 4694 del 27/10/2011 Ud. (dep. 07/02/2012) Rv. 251269, con nota di Pecorella (2012, 3692 ss.).

chiavi di accesso, perché era tenuto *per ragioni ontologicamente incompatibili* con quelle per le quali era stato dotato della password per consultare la banca dati in questione. In estrema sintesi, gli appartenenti alle forze dell'ordine possono interrogare il sistema di indagine esclusivamente per ragioni connesse al servizio, non certo in forza di un privilegio di categoria. In mancanza di una delega di indagine, o della necessità di compiere accertamenti di iniziativa, evidentemente quell'accesso risultava privo di giustificazioni, e dunque secondo la giurisprudenza abusivo.

Bisogna però fare una precisazione, perché nonostante la sentenza non lo ponga in risalto, in realtà questa pronuncia – come quella del 2017 – verteva sull'ipotesi aggravata del 615 *ter* c.p., riferita appunto all'accesso compiuto dai pubblici ufficiali. In questi termini, la Cassazione ha avuto buon gioco nel rassegnare una simile interpretazione del predicato della abusività, atteso che gli imputati erano soggetti qualificati, giocoforza tenuti a rispettare delle direttive esplicite e note proprio per il fatto di appartenere ad una determinata amministrazione. Il dato è dunque dirimente perché si risolve in una ricostruzione dell'abusività che potrebbe non essere spendibile, tal quale, in contesti ove manchi la qualifica pubblicistica del soggetto agente.

Ad ogni modo, dal 2012 si è stabilizzata un'interpretazione secondo la quale l'accesso è abusivo non solo se chi lo effettua non ha la disponibilità delle chiavi di ingresso, ma altresì quando, pur possedendole, esso è indirizzato verso obiettivi ontologicamente incompatibili con i motivi per i quali quelle stesse chiavi gli erano state fornite.

Questa soluzione ermeneutica va in crisi quando – nei cinque anni successivi – si sedimenta un nuovo conflitto di giurisprudenza, rispetto alla casistica di chi possegga legittimamente le chiavi di accesso, non versi in una condizione di ontologica incompatibilità, e agisca altresì in mancanza di prescrizioni da parte del titolare del sistema.

Questa classe di fatti è ben esemplificata dalla vicenda che ha portato all'ultimo intervento delle Sezioni unite nel 2017[4]. L'imputata, come detto, funzionaria della Procura della Repubblica che aveva consultato il registro delle notizie di reato per far sapere ad un conoscente se fosse indagato, si difendeva in giudizio sostenendo di avere piena disponibilità delle chiavi di accesso ed aggiungendo come non vi fosse alcuna direttiva interna all'Ufficio che le precludesse quel tipo

[4] Cass., Sez. un., Sentenza n. 41210 del 18/05/2017 Ud. (dep. 08/09/2017) Rv. 271061.

di accesso. Secondo le Sezioni Unite, però, anche in questo caso l'accesso doveva essere giudicato abusivo perché, se è vero che mancassero direttive di segno contrario, l'accesso compiuto si presentava in *eccesso di potere* o, meglio ancora, in *sviamento di potere*, nel senso che la funzionaria aveva esercitato un potere pubblico per finalità diverse da quelle di pubblico interesse; aveva, quindi, piegato al proprio tornaconto privato il *munus publicum* di cui era dotata.

Merita notare come, ancora una volta, siamo al cospetto di un'interpretazione spendibile solo a patto che il soggetto presumibilmente autore del reato sia dotato di un potere pubblico, sicché risulterà molto difficile mutuare questo principio di diritto a cospetto di un privato cittadino.

Successivamente, e precisamente nel luglio del 2024, è accaduto qualcosa di difficilmente preconizzabile, che in principio di questa analisi ha portato a dire che l'art. 615 *ter* c.p. si trova nel pieno della *querelle* sul rapporto tra legge e giudice. È accaduto, infatti, la Sesta sezione della Cassazione è stata chiamata a vagliare la posizione di un soggetto che nel 2016 aveva tenuto una condotta conforme alle indicazioni offerte dalle Sezioni Unite nel 2012, ma difforme all'interpretazione praticata invece dalle stesse Sezioni Unite nel 2017, che ovviamente costui non poteva conoscere perché intervenuta successivamente. Ebbene la Corte di cassazione ha affermato la non punibilità di questo individuo, sul presupposto che egli non potesse conformare la propria condotta all'interpretazione tassativizzante, ma modificativa, rilasciata dalle Sezioni Unite nel 2017. Quindi la Cassazione nel 2024 ha sostanzialmente concluso che il panorama interpretativo in tema di accesso abusivo a sistema informatico, tra il 2012 e il 2017, era così controverso, frastagliato, indecifrabile per il consociato, quandanche qualificato dal ruolo pubblico rivestito, che è stato legittimo che costui abbia fatto affidamento sulla pronuncia del 2012, anche se poi questa è stata messa in soffitta da quella del 2017.

Ora, le vicende appena ricostruite testimoniano anche una certa cattiva sorte della nostra materia, e per essa del legislatore, nel senso che questa sentenza del luglio del 2024 è stata depositata quasi in concomitanza con l'approvazione della legge n. 90, e forse, fosse accaduto prima, poteva essere una buona occasione per il legislatore per riflettere sulla opportunità di intervenire sulla trama semantica del 615 *ter* c.p., per adeguarla alle mutate esigenze del tempo presente.

Vengo rapidamente alla seconda parte dell'intervento.

L'accesso abusivo tutela, in chiave chiaramente anticipatoria, la possibilità che qualcuno, entrando nel sistema informatico bersaglio, maneggi o prenda contezza di dati dei quali non avrebbe titolo ad ottenere la conoscenza o, peggio, li sottragga al titolare.

È allora opportuno interrogarsi su cosa accada, dal punto di vista penale, nel caso in cui all'esito dell'accesso abusivo ci sia anche una condotta che impropriamente possiamo definire di "sottrazione di dati".

Questa ipotesi non era contemplata nell'art. 615 *ter* c.p. fino alla l. 90 del 2024, al punto che la giurisprudenza della Cassazione[5], secondo un percorso che potrebbe dirsi non in linea con i principi fondamentali del diritto penale (su tutti il divieto di analogia *in malam partem*) per come riconosciuti dal nostro Stato di diritto, aveva applicato a queste ipotesi le fattispecie di appropriazione indebita ovvero furto: il colpevole aveva realizzato un accesso abusivo nel sistema, aveva scaricato i dati ivi contenuti e li aveva anche cancellati, rendendoli non più fruibili da parte del titolare. Secondo la Cassazione il segmento di condotta riferito alla copia e alla cancellazione andava qualificato come furto ovvero (a seconda dei casi) appropriazione indebita di dati. Nell'offrire questa interpretazione, la Suprema Corte, come qualcuno ha anche anticipato stamattina, ha sostenuto che i dati sono cose mobili[6]. È il caso di riportare pedissequamente il principio di diritto: "*integra il delitto di appropriazione indebita la sottrazione definitiva di dati informatici o file mediante copiatura da un personal computer, in quanto i dati informatici per fisicità strutturale, possibilità di misurarne le dimensioni e trasferibilità da un luogo all'altro, sono qualificabili come cose mobili ai sensi della legge penale*".

[5] Cass., Sez. 2, Sentenza n. 11959 del 07/11/2019 Ud. (dep. 10/04/2020) Rv. 278571, (Pisani, 2020).

[6] La vicenda processuale riguardava un soggetto che, nel dare dimissioni senza preavviso da un'azienda, aveva restituito il computer portatile aziendale con l'*hard disk* formattato, dopo aver copiato i *file* relativi all'attività lavorativa sul nuovo computer che gli era stato messo a disposizione dal nuovo ente privato presso il quale era stato assunto, operante nel medesimo settore del precedente. Attraverso la formattazione del disco rigido, quei dati erano stati così cancellati dal computer di origine. Dopo aver individuato i caratteri della cosa mobile nella "materialità e fisicità dell'oggetto" che deve risultare definibile nello spazio e suscettibile di essere sposato da luogo all'altro, la Cassazione ritiene e ravvisa la fisicità dei *file* e la loro definitezza spaziale nel fatto che essi occupano fisicamente una porzione di memoria qualificabile, la dimensione della quale dipende dalla quantità di dati che in essa possono essere contenuti. La Cassazione, quindi, riteneva che il *file*, pur non essendo essere materialmente percepito dal punto di vista sensoriale, avrebbe una dimensione fisica, costituita dalla grandezza dei dati che lo compongono; ciò troverebbe conferma nell'esistenza di un'unità di misurazione della capacità di un *file* di contenere i dati e nella differente grandezza dei supporti fisici in cui *file* possono essere conservate ed elaborati. Il *file* è un elemento che ha la capacità di essere trasferito da un supporto informatico ad un altro, mantenendo le proprie caratteristiche strutturali e quindi è suscettibile di sottrazione.

Ma a mio sommesso avviso, è legittimo dubitare che i dati informatici siano effettivamente trasferibili da un luogo ad un altro.

Ecco, questa situazione dà corpo a quello che diceva Flor stamattina: i limiti di conoscenza della materia informatica si trasformano in limiti nella sua applicazione giudiziaria.

Ed infatti, l'idea stessa della trasferibilità spaziale dei dati risulta impropria se declinata secondo parametri di ordine tecnico informatico: se, per semplificare, si invia un allegato tramite posta elettronica, non si stanno trasferendo i dati che giacciono sul sistema informatico di partenza, ma se ne sta fornendo al destinatario solo una copia. E ciò vale anche in un trasferimento mediante una "chiavetta" usb. Chi invia non può estrapolare un dato dal sistema e spostarlo in un altro: per inviarlo ne genera una copia e, se lo ritiene, deve semmai cancellarlo dal sistema originario per 'privarsene', e dunque perderne il 'possesso'. Questo procedimento che non rende "mobile" quel dato, che infatti non si sposta dal sistema (Gentile, 2022: 89).

Ora, al netto delle indicate perplessità, ciò che interessa notare è che la Cassazione ha patrocinato l'interpretazione qui in esame per sopperire ad una pretesa lacuna normativa. Mancando una figura tipizzata di 'copia illecita di dati' ha chiamato in soccorso, come si diceva anche stamattina, le fattispecie tradizionali a tutela del patrimonio, ma lo ha fatto in una prospettiva evidentemente analogica che non dovrebbe essere consentita nel nostro sistema.

Occorre rimarcare, peraltro, come la tensione giurisprudenziale in questa materia non sia altro che una conferma di come la legislazione abbia faticato a stare al passo con l'evoluzione nell'impiego delle tecnologie informatiche e con la pervasività che queste hanno raggiunto nella vita quotidiana. La 'sottrazione' di dati, la presa di conoscenza indebita degli stessi, sono fenomeni purtroppo all'ordine del giorno che non sono stati adeguatamente vagliati neanche nell'ambito della disciplina in materia di *privacy*, mal attagliandosi tanto alla figura base del trattamento illecito, quanto a quella di nuovo conio dell'acquisizione fraudolenta di un archivio di dati (artt. 167 e 167 *ter* del Codice della privacy).

In questo contesto, come si anticipava, la legge n. 90 del 2024 ha mostrato se non altro maggiore consapevolezza dei problemi, perché il legislatore ha modificato la circostanza aggravante di cui al comma 2, numero 3, dell'art. 615 *ter* c.p., dando specifico rilievo alle condotte prima considerate.

È interessante, però, riportare il testo della nuova circostanza, per verificare se, ancora una volta, le scelte semantiche possano considerarsi in linea con gli scopi che si intendeva perseguire. La disposizione recita: *"la pena è aumentata se*

dal fatto deriva, (…) la distruzione o il danneggiamento – come già era previsto – *ovvero la sottrazione, anche mediante la riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati"* contenuti nel sistema. Mi pare di poter dire che la locuzione "*se dal fatto deriva la sottrazione"* sia distonica rispetto alla prospettiva di punire chi *sottrae* i dati.

Per analizzare meglio la questione è necessario svolgere alcune premesse. In primo luogo, si tratta di una disposizione a più circostanze, o se si preferisce una circostanza a fattispecie alternative, potendo integrarsi in presenza di eventi oggettivamente diversi tra loro, ma equiparati sul piano del disvalore penale.

Va poi sottolineato che questa circostanza è, in linea di principio, compatibile con il regime di imputazione colposa: l'evento aggravatore che essa stigmatizza può infatti verificarsi in assenza di una diretta volontà del colpevole.

Prima della riforma del 2024, l'ipotesi di più frequente riscontro pratico dell'aggravante in esame era quella del danneggiamento dei dati dopo l'accesso abusivo. In giurisprudenza si è posto il problema del concorso tra la figura in esame e la fattispecie di cui all'art. 635 *bis* c.p., che punisce autonomamente proprio il danneggiamento di dati, comunque cagionato.

Secondo la Corte regolatrice, il conflitto andava risolto in questo modo: qualora il danneggiamento fosse conseguenza dolosa dell'accesso abusivo, doveva applicarsi il concorso di reati; quando invece fosse epilogo non voluto da parte di chi aveva realizzato l'accesso abusivo, si sarebbe applicata solamente l'aggravante dell'art. 615 *ter* c.p.[7].

Proviamo ad esemplificare: se il colpevole entra nel sistema e danneggia volontariamente i dati, per esempio cancellandoli, non si applicherebbe la circostanza, ma verrebbe a configurarsi il concorso di reati tra l'accesso abusivo e il danneggiamento di cui all'art. 635 *bis* c.p., perché sono entrambe fattispecie dolose. La circostanza, invece, grazie al criterio di imputazione dell'art. 59 c.p., si è sempre applicata alle ipotesi nelle quali il danneggiamento dei dati fosse l'evento aggravatore non voluto da parte del soggetto agente, intervenuto per sua mera colpa.

Ciò premesso, è legittimo chiedersi se si possa mai verificare per colpa la condotta di sottrazione dei dati anche mediante, come recita la disposizione, la *riproduzione o la relativa copiatura*. Mi pare di poter affermare che è impossibile

[7] Cass., Sez. 5, Sentenza n. 18284 del 25/03/2019 Ud. (dep. 02/05/2019) Rv. 275914.

che la copiatura o la riproduzione avvengano per colpa: la locuzione "se dal fatto deriva" rimanda a qualcosa di non voluto, di puramente causale.

Ma soprattutto occorre considerare il contrasto tra *sottrazione* e *riproduzione*: se il dato è riprodotto vuol dire che non è stato sottratto ma solo copiato, il che significa che il relativo originale è rimasto all'interno del sistema. La sottrazione, di contro, richiama necessariamente la perdita del dato, e dunque il suo danneggiamento.

Emerge allora che anche gli sforzi profusi dal legislatore con la legge n. 90 del 2024, nella direzione di adeguare il sistema normativo a questa nuova istanza di tutela rappresentata appunto dai "furti di dati", non siano all'altezza della esigenza di politica criminale cui sopperire, perché, in attesa chiaramente di vedere cosa ci dirà la giurisprudenza, mi pare che si sia licenziato un testo, seppur di una fattispecie aggravante, che sarà di elevata criticità applicativa, sia per quanto detto a proposito di una impossibile sottrazione di dati mediante riproduzione dopo un accesso abusivo a sistema informatico che non sia sorretta dal dolo di fattispecie, sia perché il punto di riferimento nelle ipotesi di 'sottrazione' del dato rimarrà pur sempre la fattispecie di danneggiamento di cui all'art. 635 *bis* c.p. Ora, è ovvio che la circostanza potrà applicarsi nelle ipotesi di "copiatura" dolosa dei dati – e su questo il sistema è stato di certo innovato positivamente – ma il dolo deve essere coerente con la struttura della fattispecie circostanziata, e dunque la stessa andava formulata diversamente. Ricorrere alla locuzione "*se dal fatto deriva*" non è lo stesso che dire "*se dal fatto il soggetto sottrae o comunque ottiene il materiale informatico contenuto nel sistema bersaglio*".

Infine, occorre ribadire e tener conto che la latitudine applicativa della fattispecie di accesso abusivo non si limita ai fenomeni gravi di aggressione a sistemi informatici condotta in maniera professionale da soggetti altamente qualificati, ma si estende – doverosamente – anche a condotte più rudimentali e limitate, che esprimono però un significativo disvalore se inquadrate nella prospettiva del titolare del sistema.

Bisognerebbe riflettere, allora, su un ripensamento complessivo della struttura del tipo criminoso, anche magari prevedendo autonome condotte da dedicare ai diversi fenomeni qui considerati. Ciò renderebbe lo statuto applicativo di questo reato certamente più conforme alle esigenze della prassi.

Concludo facendo un passo indietro: in quella stessa sentenza prima citata in cui la Cassazione ha applicato la fattispecie di appropriazione indebita per punire colui che aveva sottratto i dati, in realtà sarebbe bastato applicare l'art. 635 *bis* c.p.: il fatto era già tipico, perché formattando il sistema l'autore dell'accesso

abusivo aveva commesso pacificamente un danneggiamento di dati, rendendoli inservibili in capo al titolare del sistema medesimo. Quindi, senza bisogno di acrobazie interpretative a favore delle fattispecie a tutela del patrimonio, bastava utilizzare la normativa esistente per ottenere il medesimo esito punitivo ma rimanendo nei confini del principio di legalità.

Bibliografia

Di Florio M., Zarra P., *L'accesso abusivo ad un sistema informatico o telematico*, in Sicignano G. J., Di Maio A. (a cura di), *I nuovi reati informatici,* 2022, p. 1 ss.

Gentile G., *Il furto di dati informatici*, in Sicignano G. J., Di Maio A. (a cura di), *I nuovi reati informatici,* 2022, p. 1 ss.

Maiello V., *L'overruling sfavorevole tra tipo e colpevolezza*, in *Giur. it.,* 2025, p. 406 ss.

Pecorella C., *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen.,* 2012, p. 3692 ss.

Pisani N., *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica*, in *Dir. pen. proc.*, 2020, p. 651.

Salvadori I., *I reati contro la riservatezza informatica*, in Cadoppi A., Canestrari S., Manna A., Papa M. (a cura di), *Cybercrime,* 2023, p. 552 ss.

Capitolo Quarto

Governare il rischio digitale: cybersicurezza, intelligenza artificiale e obblighi della P. A.

Giovanni Cocozza

Premessa

Il tema della *cybersecurity* si propone nell'attualità con particolare rilevanza nel dibattito politico e giuridico. Si tratta, infatti, come è noto, di uno dei settori più in rapida evoluzione nell'ambito delle tecnologie dell'informazione e della comunicazione. Con l'incremento della digitalizzazione e la crescente interconnessione tra dispositivi, la protezione dei dati, delle informazioni sensibili e delle infrastrutture critiche è diventata una priorità per individui, aziende e governi.

Come è stato anche recentemente riconosciuto a livello governativo[1], «la cybersecurity non è più questione di resilienza ma di sicurezza nazionale».

L'intreccio sempre più stretto tra trasformazione digitale, sicurezza dei sistemi informatici e tutela degli interessi nazionali si riflette sugli strumenti giuridici e amministrativi tradizionali. Di qui l'interesse a indagarne gli aspetti, con particolare riferimento alla possibilità di impiegare l'intelligenza artificiale come strumento a supporto della cybersicurezza, verificandone l'impatto sulla capacità delle pubbliche amministrazioni di prevenire, rilevare e rispondere a minacce informatiche complesse. In questa prospettiva, come si vedrà, l'analisi si sviluppa osservando il modo in cui le tecnologie intelligenti stiano già contribuendo a ridefinire le funzioni amministrative – dalla gestione degli incidenti alla selezione dei fornitori ICT – e quali garanzie giuridiche debbano essere assicurate per coniugare innovazione e legalità.

Con lo spostamento dal luogo "reale" a quello "virtuale" le minacce informatiche tendono ad assumere forme molteplici e in continuo mutamento, adattandosi alle nuove tecnologie e tecniche di difesa. È un processo non facile da affrontare con i soliti livelli previsionali ed è assolutamente necessario adottare tecniche in

[1] Così il sottosegretario Alfredo Mantovano, Autorità delegata per la sicurezza della Repubblica, al convegno "*La nuova direttiva NIS per un più alto livello di cybersicurezza del sistema Paese*", Università La Sapienza di Roma, 27 novembre 2024.

grado di offrire risposte, anche considerando che nella stragrande maggioranza dei casi è proprio il fattore umano responsabile di molti attacchi cibernetici.

Da più parti si sottolinea la necessità di un approccio fondato sulla cooperazione e sul coordinamento tra diversi attori, anche se nella relazione fra soggetti pubblici e privati in quest'ambito si percepisce ancora la presenza di un approccio autoritativo, che si mostra non coerente con uno dei pilastri concettuali fondanti della strategia di *cybersecurity*.

Come si vedrà a breve osservando il quadro normativo in materia, è un approccio che sembra venire in rilievo tanto nella disciplina generale predisposta in materia di *cybersecurity*, quanto in quella degli appalti di beni e servizi *cyber*, con un esercizio *top down* che può essere criticabile. In tal senso, si mostrano interessanti le formule "democrazia digitale" o "sovranità digitale cooperativa"[2], per esprimere in modo sintetico l'importanza di un reale coordinamento tra gli attori coinvolti (De Minico, 2022; Casonato, 2020; Losano, 2021).

1. *Il composito quadro normativo in materia di cybersicurezza*

Occorre partire da un'osservazione che ben rappresenta le difficoltà, e cioè che il quadro normativo in materia di cybersicurezza si presenta piuttosto complesso da ricostruire e non particolarmente organico, anche per l'intreccio tra norme nazionali ed europee. Gli interventi del legislatore italiano restituiscono, infatti, un sistema normativo stratificato, all'interno del quale la disciplina NIS 2 ("*Network and Information Systems*"), recepita nel d.lgs. n. 138 del 2024 e la c.d. "Legge perimetro" (d.l. 21 settembre 2019, n. 105, conv. con mod. dalla l. 18 novembre 2019, n. 133) costituiscono i capisaldi della cybersicurezza (Bavetta, 2022; Salvaggio- Gonzalez, 2023).

A livello nazionale, va aggiunto poi che il recente intervento normativo con la legge n. 90 del 2024 (rubricata "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"), ha offerto ulteriori elementi da valutare e di cui si parlerà a breve.

Naturalmente, la proliferazione di fonti normative rende difficile un effettivo coordinamento, e ciò è ancora più vero quando quest'ultimo si mostra elemento

[2] Espressione, quella di "democrazia digitale", adoperata anche da Bruno Frattasi, direttore dell'Agenzia per la Cybersicurezza nazionale.

indispensabile per affrontare in modo efficace le sfide che il tema pone. Una tale esigenza emerge anche leggendo la direttiva NIS, dove si afferma che gli Stati devono garantire che anche i soggetti esclusi dalla NIS debbano raggiungere un livello elevato di cybersicurezza e gli Stati membri devono sostenere l'attuazione di misure equivalenti di gestione dei rischi. Inoltre, ai sensi dell'art. 14 del decreto di recepimento ("*Cooperazione tra Autorità nazionali*"), vi è una previsione volta ad assicurare la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS con Autorità nazionali, tra le quali il Garante per la protezione dei dati personali, l'Agenzia per l'Italia digitale (AgID) quale organismo di vigilanza ai sensi del regolamento (UE) n. 910/2014, il Ministero della difesa, quale responsabile in materia di difesa dello Stato, nonché con altre autorità nazionali competenti anche ai sensi di altri atti giuridici settoriali dell'Unione europea, ivi incluso lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti[3].

L'obiettivo di costruire un'architettura multilivello si traduce poi anche nella previsione di molteplici sedi di raccordo, come il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza, che intende sviluppare le risorse e le competenze dell'Unione e ridurre la sua dipendenza da Paesi terzi; l'Unità congiunta per il cyberspazio (*Joint Cyber Unit*), quale piattaforma finalizzata a promuovere lo scambio di informazioni, buone pratiche e conoscenze, nonché la cooperazione tra forze dell'ordine e della difesa, autorità civili e diplomatiche, soggetti privati in caso di gravi attacchi o incidenti di natura transfrontaliera; la Rete dei Centri operativi di sicurezza (*c.d. SOC, Security Operations Center*), quale *network* finalizzato ad assicurare un monitoraggio costante, diffuso e in tempo reale delle intrusioni e delle anomalie informatiche nelle reti e nei sistemi di diversi portatori di interesse.

Come si anticipava, la recente legge 28 giugno 2024, n. 90 ("*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*") si pone l'obiettivo di introdurre e armonizzare un ventaglio molto ampio e varie-

[3] L'esigenza di coordinamento istituzionale nella governance della cybersicurezza trova riscontro anche nella giurisprudenza costituzionale. In particolare, la Corte costituzionale, con sentenza n. 8 del 2022, ha affermato che la tutela della sicurezza nazionale – anche nella sua declinazione cibernetica – deve essere esercitata in modo coerente con il principio di proporzionalità e con il rispetto dei diritti fondamentali. Questo bilanciamento assume rilevanza primaria nei contesti tecnologici, nei quali l'espansione dell'intervento pubblico deve essere sostenuta da adeguate garanzie di legalità e trasparenza (Violini, 2022).

gato di temi legati al mondo della *cybersecurity*: dalla *governance* agli obblighi di notifica degli incidenti, dai requisiti di cybersicurezza nei contratti pubblici alle preclusioni per l'assunzione di alcune tipologie di professionalità provenienti dal mondo della *cybersecurity* pubblica e della sicurezza nazionale, fino all'ampia novella sui reati informatici.

I due Capi distinti in cui si articola sono in tal modo finalizzati a offrire un quadro sufficientemente strutturato.

Il Capo I individua le misure di rafforzamento della cybersicurezza nazionale, la resilienza delle pubbliche amministrazioni e i contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici. Si interviene, in particolare, sulle misure in caso di incidenti informatici; sull'architettura della sicurezza cibernetica e sui rapporti tra i diversi attori; sui criteri nella disciplina dei contratti pubblici; sulle preclusioni all'assunzione di personale che abbia ricoperto specifici ruoli presso alcune pubbliche amministrazioni centrali, sanzionando i contratti stipulati con la nullità.

Il Capo II apporta modifiche al Codice penale e, in particolare, alle previgenti norme in materia di prevenzione e contrasto dei reati informatici, e individua disposizioni in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici, prevedendo inasprimenti di pene e introducendo nuove fattispecie delittuose.

Colpisce, tuttavia, il limitato richiamo alle previsioni della NIS 2. Anche il decreto di recepimento non sembra operare un ottimale coordinamento tra discipline.

La legge italiana si caratterizza, in tal modo, per l'intento di offrire un ambito di applicazione molto ampio, che ricomprende le pubbliche amministrazioni individuate puntualmente dalla norma; i soggetti ricompresi nel Perimetro di Sicurezza Nazionale Cibernetica; i soggetti sottoposti al dettato della Direttiva NIS (poi NIS 2); gli organi dello Stato considerati ormai come centrali nel settore della cybersicurezza come il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), gli Organismi di Informazione per la Sicurezza, l'Agenzia per la Cybersicurezza Nazionale (ACN) e il suo Nucleo per la Cybersicurezza.

Con specifico riferimento alle pubbliche amministrazioni, che sono poste al centro della prima parte dell'atto legislativo, si individuano i principali attori pubblici che dovranno applicare quanto previsto dal legislatore[4]. Il provvedimen-

[4] Essi sono le pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT; le Regioni

to legislativo indica, poi, tra i principali obblighi, quello di rafforzare la resilienza in materia di cybersicurezza. E ciò attraverso la enunciazione di quattro specifici adempimenti.

Innanzitutto, la predisposizione di una struttura per la cybersicurezza di cui è necessario dotarsi, anche nell'ambito delle già esistenti risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Con l'ulteriore precisazione che tale struttura può essere individuata anche in quella dell'ufficio del responsabile per la transizione al digitale.

Poi, l'istituzione della figura del referente per la cybersicurezza, da individuare in ragione delle sue specifiche professionalità e competenze nella materia. A tale soggetto, il cui nominativo deve essere obbligatoriamente comunicato all'Agenzia per la Cybersicurezza Nazionale, viene affidata anzitutto la funzione di punto di contatto unico dell'amministrazione con tale autorità in merito a quanto previsto dalla legge e dalle normative settoriali in materia di cybersicurezza. Oltre alla possibilità di individuare tale figura nell'ambito di quella del responsabile per la transizione al digitale, con la possibilità, nel caso in cui la pubblica amministrazione non abbia al proprio interno un dipendente con tali requisiti, di incaricare il dipendente di un'altra pubblica amministrazione.

Ancora, l'obbligo di segnalare gli incidenti che si verificano. In particolare, il legislatore italiano prevede che le pubbliche amministrazioni debbano notificare tali incidenti utilizzando le procedure disponibili sul sito internet dell'Agenzia per la Cybersicurezza Nazionale, osservando i termini previsti. La mancata osservanza potrà provocare l'applicazione di una sanzione amministrativa pecuniaria da un minimo di 25.000 euro a un massimo di 125.000 euro. Tale violazione, inoltre, può anche costituire causa di responsabilità disciplinare e amministrativo-contabile dei funzionari e dei dirigenti.

Infine, l'adozione tempestiva degli interventi risolutivi indicati dall'Agenzia per la Cybersicurezza Nazionale, nel caso in cui essa segnali specifiche vulnerabilità cui le pubbliche amministrazioni interessate dalla legge risultino potenzialmente esposte. I destinatari delle segnalazioni devono intervenire senza ritardo, e comun-

e le province autonome di Trento e di Bolzano; le Città metropolitane; i Comuni con popolazione superiore a 100.000 abitanti; i Comuni capoluoghi di regione; le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; le aziende sanitarie locali; le società in house di tali enti, qualora siano fornitrici di servizi informatici, dei servizi di trasporto, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, ovvero servizi di gestione dei rifiuti.

que non oltre quindici giorni dalla ricezione della comunicazione. Anche in questo caso, la mancata o ritardata adozione determina l'intervento dell'Agenzia per la Cybersicurezza Nazionale, che invierà una comunicazione alla pubblica amministrazione inadempiente, avvisandola che la reiterazione di tale omissione nell'arco di 5 anni comporterà l'applicazione di una sanzione amministrativa pecuniaria da un minimo di 25.000 euro a un massimo di 125.000 euro. Tuttavia, il legislatore specifica che la sanzione può non essere applicata nel caso in cui vengano tempestivamente comunicate all'Agenzia per la Cybersicurezza Nazionale le motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione degli interventi risolutivi indicati o ne comportino il differimento oltre il termine di 15 giorni.

Già da questa breve e limitata osservazione di alcuni contenuti delle previsioni legislative si percepisce come le pubbliche amministrazioni siano al centro dell'intervento del legislatore, che richiede un ampio ventaglio di adempimenti in materia di *cybersecurity*, legati alla loro *governance* interna, ma anche in materia di obblighi di notifica degli incidenti e di verifica e correzione di vulnerabilità in alcune tipologie di *software*.

C'è, in particolare, un aspetto che merita attenzione, e cioè il possibile criterio sostanziale da utilizzare proprio per individuare i soggetti essenziali della pubblica amministrazione.

Nel complesso, la legge sulla cybersicurezza si è mostrata tesa ad anticipare alcuni adempimenti previsti dalla Direttiva NIS 2, determinando un criterio di selezione delle pubbliche amministrazioni particolarmente adatto per la identificazione dei soggetti pubblici da includere, attraverso il decreto di recepimento italiano, all'interno dell'alveo di applicazione della Direttiva NIS 2.

Come è noto, infatti, tale Direttiva (UE) 2022/2555 ha imposto alcuni obblighi di *cybersecurity* in capo agli Stati – l'adozione di una strategia nazionale di cybersicurezza e la designazione di apposite autorità nazionali in materia – e altri in capo a particolari soggetti privati, attualmente distinti dalla Direttiva NIS 2 in soggetti "essenziali" e soggetti "importanti".

Il decreto di recepimento n. 38 del 2024 conferma l'ampio ambito di applicazione delle disposizioni in materia di cybersicurezza. Esso individua i soggetti sulla base dell'importanza che rivestono, con la conseguenza che taluni di questi, pur non rientranti per dimensione, possono esserlo per importanza. Va ricordato, peraltro, che la direttiva NIS 2, differentemente dalla NIS 1 che, come è noto, è intervenuta in un contesto diverso, poiché precedente alla pandemia e alla guerra in Ucraina, ha allargato lo sguardo a molti soggetti, con un concetto di sicurezza che va proporzionato alla realtà che si vive.

Dal quadro normativo sinteticamente tracciato emerge, poi, un elemento ulteriore, e cioè che la platea dei destinatari non può essere indicata nella sua globalità, ma in un certo senso va "costruita". E questo rispecchia quell'approccio sistemico necessario, che conferma come non possa essere sufficiente mettersi singolarmente in sicurezza, ma occorre mettere in sicurezza l'intero sistema.

Si ritorna, allora, alla necessità di una cooperazione a più livelli. E alla possibilità di cogliere l'opportunità di trasformare gli obblighi di legge in processi di efficienza. Così, ad esempio, per quanto riguarda gli obblighi di notifica degli incidenti. Le modalità e i tempi di notifica hanno come scopo "secondario", in realtà, quello di allineare i soggetti coinvolti dalla Legge sulla Cybersicurezza ad alcune delle previsioni normative all'interno del decreto legislativo di recepimento a livello nazionale della Direttiva NIS 2.

L'obbligo di notifica degli incidenti permette all'Agenzia per la Cybersicurezza Nazionale di avere un panorama più dettagliato e preciso di quello che accade in Italia e, in particolare, ai soggetti destinatari. Consente, però, anche di svolgere una serie di attività di natura reattiva a supporto del soggetto. È interessante, infatti, osservare come l'impianto derivante dalla direttiva NIS 2 crei un rapporto di obbligo reciproco tra i soggetti, in una sorta di supporto legato a un'analisi del rischio.

Nell'impianto legislativo si scorgono, così, non irrilevanti spazi di collaborazione, anche se occorre scongiurare il rischio che essi siano offuscati dalla logica "obbligo-sanzione" che comunque permea la disciplina.

2. *La cybersicurezza in materia di appalti pubblici*

Un settore nel quale, in particolare, proprio il tema della collaborazione pubblico-privato può trovare spazi significativi è quello degli appalti per la *cybersecurity*.

È noto che l'esistenza già di strumenti di natura collaborativa può contribuire a incrementare il dialogo fra soggetti pubblici-acquirenti e privati-fornitori, producendo non pochi vantaggi. Si mostra, infatti, un profilo problematico non indifferente relativo all'asimmetria informativa che può determinarsi in un appalto di tecnologia, ridimensionabile probabilmente solo attraverso un rafforzamento delle competenze dei funzionari nell'ambito della disciplina degli acquisti pubblici di cybersicurezza, unitamente al ricorso agli appalti innovativi.

Un rischio particolarmente avvertito negli appalti pubblici di beni e servizi informatici è quello del cosiddetto *vendor lock-in*, ovvero la dipendenza dell'am-

ministrazione da fornitori specifici, in particolare soggetti privati titolari di tecnologie proprietarie. Tale rischio può limitare la concorrenza e compromettere la continuità amministrativa. Per contrastarlo, è opportuno che le amministrazioni ricorrano a clausole contrattuali che impongano standard di interoperabilità, apertura dei formati e trasferibilità dei dati, in coerenza con le indicazioni dell'ACN e con i principi del Codice dell'amministrazione digitale.

Come la dottrina ha avuto modo di osservare, infatti, occorre gestire on attenzione il cambiamento, conducendo la pubblica amministrazione a operare con una capacità strategica per esercitare una «funzione-obiettivo», vale a dire stabilendo un fine da raggiungere sinergicamente insieme ai fornitori e indicando con quali mezzi e risorse conseguirlo. Solo così lo Stato può "smarcarsi" dalla situazione, per così dire, di "sudditanza" nei confronti dei privati, soprattutto delle grandi imprese produttrici di tecnologia. Aspetto essenziale in un settore, quale quello della cybersicurezza pubblica, che è caratterizzato da sensibili interessi sottesi.

Emerge, allora, in modo significativo il concetto di "sovranità digitale", che non rileva soltanto sul piano teorico come guida collaborativa con i soggetti privati, ma anche su quello concreto per l'individuazione di alcuni progetti funzionali a raggiungere una maggiore autonomia pubblica, evitando l'oligopolio delle grandi imprese tecnologiche.

È interessante osservare come la legge sulla cybersicurezza introduca nella disciplina dei contratti pubblici di beni e servizi informatici alcuni criteri di *cybersecurity*, definiti dal legislatore come l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela degli interessi nazionali strategici.

Tali elementi essenziali di cybersicurezza sono da individuarsi con specifico Decreto del Presidente del Consiglio dei ministri da emanarsi entro 120 giorni dall'entrata in vigore della legge, all'interno del quale vi sono anche i casi in cui, per la tutela della sicurezza nazionale, debbano essere previsti criteri di premialità per le proposte o le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi – individuati nel medesimo decreto – tra quelli che hanno accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

È altresì da osservare come nel Codice dei contratti pubblici di più recente approvazione (d.lgs. 31 marzo 2023, n. 36) il concetto di cybersicurezza compaia nell'art. 19, co. 5 e nell'art. 108, comma 4.

Nella prima disposizione (rubricata "*Principi e diritti digitali*"), comma 5 si prevede che: «*le stazioni appaltanti e gli enti concedenti, nonché gli operatori economici che partecipano alle attività e ai procedimenti di cui al comma 3, adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali. Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento*».

Nella seconda, invece, che: «*nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici*».

Per quanto concerne l'ambito di applicazione della disposizione, si può osservare come esso non sia limitato alle sole forniture aventi ad oggetto dispositivi che hanno la finalità di garantire la sicurezza cibernetica delle infrastrutture digitali pubbliche, ma a tutti gli appalti finalizzati all'approvvigionamento di beni e servizi informatici, purché connessi alla tutela degli interessi nazionali strategici. Si tratta di disposizione introdotta in sede parlamentare in accoglimento delle indicazioni fornite dall'Autorità per la Cybersicurezza Nazionale in audizione parlamentare.

Non mancano criticità, segnalate in dottrina.

Innanzitutto, si concede alle stazioni appaltanti una notevole discrezionalità nella valutazione degli elementi di cybersicurezza. La formula adoperata, secondo la quale esse possono attribuire, nella valutazione degli elementi qualitativi delle offerte attinenti all'approvvigionamento di beni e servizi informatici, «*specifico e peculiare rilievo*» nella valorizzazione degli «*elementi di cybersicurezza*» rischia di essere troppo generica. Con la conseguenza che, come è stato notato, si sconfini in arbitrio delle stazioni appaltanti, in mancanza di coordinate adeguate all'esercizio del potere. È stato, così, osservato che la disposizione «risulta insufficiente dal punto di vista contenutistico» e tale da dover necessariamente essere integrata dalle altre disposizioni rilevanti in materia, onde evitare che la discrezionalità delle stazioni appaltanti sconfini in un esercizio arbitrario di poteri pubblici idoneo a ingenerare incertezza e potenziali disparità di trattamento tra operatori economici» (Rossa, 2023:133).

A ciò si aggiunga la mancanza di un idoneo coordinamento tra l'art. 108, comma 4, del Codice e la direttiva NIS II. Il paragrafo 7 della Direttiva ha previsto che nell'ambito della strategia nazionale per la cibersicurezza, «*gli Stati mem-*

bri adottano in particolare misure strategiche riguardanti: a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi ICT utilizzati da soggetti per la fornitura dei loro servizi; b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi ICT negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source».

In definitiva, non sembra dubitabile che il sistema normativo sia ancora insufficiente per regolamentare il fenomeno e che la disciplina del Codice vada, necessariamente, integrata.

Per quanto concerne, poi, la reale possibilità che vi sia cooperazione tra gli attori, è necessario implementare quanto già il sistema offre, in relazione alle forme di partenariato pubblico-privato, in particolare il partenariato per l'innovazione.

Tale possibilità, per quanto rilevante, impatta, però, contro alcune criticità che possono limitarne in modo significativo l'attuazione.

Innanzitutto, l'elevato livello di competenze tecniche e amministrative richiesto per gestire questo tipo di appalti, oltre a una conoscenza ampia della materia e a una visione organica, in grado di consentire la scelta migliore per raggiungere l'obiettivo posto.

Poi, non può essere trascurata l'ulteriore difficoltà derivante dalla necessità di una buona propensione al rischio insito negli appalti innovativi e la c.d. amministrazione (o burocrazia) "difensiva".

Infine, la necessità di impiegare consistenti risorse economiche. Un possibile esito negativo nella ricerca di una soluzione innovativa, così come la non utilità pratica della soluzione sviluppata, può determinare un impiego infruttuoso di risorse pubbliche.

È indubitabile che una consapevole utilizzazione di queste tipologie determina vantaggi non indifferenti, potendo l'Amministrazione collaborare per la creazione di beni e servizi che siano *ab initio* già rispettosi dei requisiti che servono al soggetto pubblico per soddisfare l'interesse perseguito. Si consente, così, una più proficua interazione tra pubblico e privato, poiché si configura una relazione già a monte nella fase di creazione e del *design* del bene o del prodotto, stabilendo *a priori* le caratteristiche che possono servire all'Amministrazione, anziché intervenire in un momento successivo nel tentativo di modificare o implementare beni o servizi già esistenti.

Si potrebbe, in tal modo, concretizzare attraverso gli appalti innovativi, specialmente quelli di partenariato per l'innovazione, il concetto di *cybersafe by design*, ovvero lo sviluppo di prodotti e servizi digitali rispettosi di *standards* di

cybersicurezza già dalla loro progettazione, per fronteggiare il rischio crescente di attacchi e vulnerabilità dei sistemi al quale si assiste progressivamente.

3. *Intelligenza artificiale, cybersicurezza e decisione amministrativa*

Il rischio crescente di attacchi cibernetici trova significativa conferma nell'osservazione del dato empirico.

Come evidenziato dal Rapporto Clusit (Associazione Italiana per la Sicurezza Informatica) 2024, la Pubblica Amministrazione ha subito un numero di attacchi con un ritmo leggermente inferiore rispetto agli altri settori, i quali sono probabilmente considerati maggiormente lucrativi da parte delle organizzazioni criminali in cerca di profitto immediato.

Occorre, però, sempre ricordare il monito, di frequente ripetuto, di non domandarsi "se" si subirà un attacco, ma "quando" si subirà. Dinanzi all'accresciuto attivismo da parte dei *cyber* criminali, ogni potenziale bersaglio deve partire dal presupposto che, prima o poi, finirà nel mirino degli *hacker*.

In quest'ottica, le strategie di difesa non possono non ispirarsi alla logica *detection and response*: rilevare l'attacco il prima possibile e contrastarlo efficacemente.

Può essere utile, allora, compiere qualche riflessione proprio sul ruolo che l'Intelligenza Artificiale può assumere nel garantire la cybersicurezza.

Come è stato evidenziato, l'integrazione dell'I.A. nella *cybersecurity* può rappresentare una rivoluzione nel campo della sicurezza digitale, offrendo l'opportunità di potenziare le difese contro le minacce informatiche sempre più frequenti[5]. La sua capacità di analisi precisa e prontezza nel rispondere alle nuove sfide si rivela una forza non indifferente nella lotta contro i criminali informatici.

Vero è che, però, si è ancora alla ricerca di un equilibrio tra le capacità dell'Intelligenza Artificiale e le competenze umane per costruire sistemi di difesa robusti, adattivi ed etici. Non può essere trascurata l'importanza di un adeguato bilancia-

[5] Il decreto-legge 14 giugno 2021, n. 82 ("*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*"), convertito con modificazioni dalla legge 4 agosto 2021, n. 109, all'art. 7, comma 1, lett. m)-*quater* inserita dal disegno di legge A.C. 2316-A intitolato "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*", prevede che L'Agenzia per la Cybersicurezza Nazionale promuove e sviluppa ogni iniziativa finalizzata a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale.

mento tra innovazione e gestione del rischio, in modo da poter affrontare in maniera consapevole le sfide delle minacce in evoluzione e delle tecnologie emergenti.

Da un lato, allora, investire nella ricerca e nello sviluppo delle tecnologie di Intelligenza Artificiale per sfruttarne il potenziale e migliorare le misure di *cybersecurity* sembra elemento di fondamentale importanza. Dall'altro, però, è essenziale una cooperazione tra esperti di I.A. e di *cybersecurity* per garantire un panorama digitale sicuro di fronte alle minacce in costante mutamento.

Non si può non ricordare che, quando si affronta il tema dell'Intelligenza Artificiale, sono intercettati numerosi saperi e sollecitate non poche questioni, generando altresì interrogativi delicati. Ne è conferma anche la Relazione al recente disegno di legge italiano in materia di Intelligenza Artificiale, che esordisce affermando che «*l'intelligenza artificiale presenta un lato oscuro che contiene semi di ogni specie, ma anche germi di ogni tipo*».

La frase ben rappresenta la delicatezza della tematica e sottende alla fondamentale esigenza, sempre più pressante, di un effettivo "controllo" da parte dell'uomo sul fenomeno.

Non v'è dubbio che nel campo del diritto e, in particolare, del diritto amministrativo, non pochi sono i vantaggi che possono derivare da un impiego diffuso delle tecnologie di intelligenza artificiale, come la riduzione dei rischi di disparità di trattamento; una più attenta osservanza della legge; la prevenzione dei fenomeni corruttivi; una maggiore completezza dell'istruttoria (Viola, 2018; Galetta- Corvolan, 2019; Benetazzo, 2020; Otranto, 2021; Marchetti, 2021; Di Ciommo, 2023). Con la conseguenza che la decisione amministrativa potrebbe divenire più prevedibile e maggiormente in grado di garantire una maggiore certezza giuridica.

Può esserci, però, un *deficit* per quanto riguarda il rispetto delle garanzie.

Tra le varie criticità segnalate, in particolare, vi sono due profili che appaiono maggiormente complessi da affrontare.

Il primo è quello dell'imputabilità della decisione adottata dall'algoritmo, che deve restare in capo all'organo titolare del potere decisionale e, in coerenza con il principio di immedesimazione organica, deve consentire una piena verifica della logicità e della correttezza degli esiti prodotti dall'algoritmo.

Il secondo è quello del pieno rispetto dei diritti del privato nel procedimento amministrativo.

Il principio di trasparenza ne può soffrire in maniera significativa, soprattutto perché esso deve necessariamente essere inteso in modo diverso rispetto a quello tradizionale, pur rimanendo ferma la sua rilevanza nell'attività della pubblica amministrazione. Viene inevitabilmente da chiedersi se sia possibile davvero rag-

giungere la piena comprensibilità della decisione algoritmica e quanto il principio di trasparenza possa porsi come baluardo per un effettivo controllo al potere di matrice tecnologica.

Non è dubitabile che la diffusione delle nuove tecnologie sta profondamente conformando lo svolgimento della funzione amministrativa. È nota, infatti, in particolare nell'attività delle Pubbliche Amministrazioni, la difficoltà di conciliare l'utilizzo dei sistemi di Intelligenza Artificiale con l'esercizio della discrezionalità amministrativa, poiché alla maggior complessità della decisione discrezionale che il sistema di I.A. è deputato a adottare corrisponde una minore "spiegabilità" tecnica del funzionamento dell'algoritmo e dell'*iter* logico giuridico seguito dal sistema, con inevitabili riflessi sul ruolo della motivazione che ancor più deve assolvere alla sua funzione di garanzia non solo delle posizioni giuridiche soggettive del cittadino interessato, ma anche dell'effettiva imparzialità e del buon andamento della pubblica amministrazione sanciti dall'art. 97 della Costituzione.

4. *Il principio di trasparenza nella decisione algoritmica*

Si assiste, insomma, come è stato affermato anche dalla giurisprudenza amministrativa, alla necessità di tradurre in linguaggio giuridico la regola tecnica e di poter cogliere i criteri di valutazione. Elemento indispensabile per evitare il rischio di «una nuova forma di burocrazia tecnologica, in cui la proposta algoritmica viene validata solo formalmente dal funzionario che assume la decisione» (Lo Sapio, 2024), in quanto egli in concreto risulta privo dell'abilità di metterne in discussione il risultato[6].

Ancora una volta, è da ribadire l'importanza della formazione del personale affinché sia capace di comprendere la logica ed il funzionamento dei sistemi, così come richiesto dalla normativa europea.

Ma non solo.

[6] La giurisprudenza amministrativa ha avuto modo di intervenire sul tema dell'utilizzo degli algoritmi nella decisione pubblica. Con la sentenza della sez. VI, 13 dicembre 2019, n. 8472, il Consiglio di Stato ha chiarito che l'uso di algoritmi nella formazione di graduatorie non esonera l'amministrazione dall'obbligo di garantire trasparenza e conoscibilità delle regole decisionali. Più recentemente, con la sentenza della sez. VI, 15 marzo 2021, n. 2270 lo stesso Consiglio ha ribadito che la decisione automatizzata deve restare soggetta a verifica e controllo da parte dell'amministrazione, la quale ne conserva la piena responsabilità.

Si mostra rilevante un'attività di supporto al decisore pubblico nell'individuazione delle opzioni possibili, con una decisione che assume, così, i caratteri di una decisione "mista", in cui l'interazione umano-macchina è indispensabile.

Essa, però, assume forme differenti poiché può risentire della distinzione preliminare tra algoritmi deterministici (c.d. "*rule-based*") e algoritmi di autoapprendimento (c.d. "*machine learning*").

I primi, basati appunto su una logica deterministica, seguono criteri stabiliti a monte dall'amministrazione e, di conseguenza, il processo decisionale rimane in capo all'amministrazione, seppur portato a termine dalla macchina, in quanto il potere di scelta è esercitato a monte mediante l'individuazione dei criteri e l'attribuzione di rilevanza ai diversi fattori.

I secondi determinano invece uno spostamento dalla sfera umana alla macchina stessa, rendendo più difficile risolvere le problematiche relative alla legalità dell'algoritmo, dal momento che è assente l'intervento umano nel processo di elaborazione dei dati. In tale ipotesi, infatti, è unicamente il *software* a determinare l'assetto degli interessi o dei rapporti, anche formalmente, non essendo previsto l'intervento del funzionario-persona fisica.

È evidente altresì come i secondi, considerata la maggiore difficoltà di ricostruire il percorso logico seguito dal *software*, tendano a rendere più complesso il pieno rispetto delle garanzie e del principio di trasparenza.

Infatti, come si diceva in precedenza, la differenza tra le diverse modalità per l'adozione di una decisione automatizzata impatta in modo significativo sul principio di trasparenza, che svolge sempre più il ruolo di elemento fondamentale nell'attività delle pubbliche amministrazioni.

Le indicate difficoltà di tradurre la regola tecnica in regola giuridica si amplificano quando i meccanismi di intelligenza artificiale si rapportano all'esercizio della discrezionalità amministrativa. La nota distinzione tra attività vincolata e discrezionale della pubblica amministrazione costituisce elemento da considerare. Nel primo caso, infatti, stante la limitata possibilità decisionale che residua alla pubblica amministrazione rispetto a quanto disposto dalla legge, l'applicazione dell'algoritmo determina minori difficoltà. Nel secondo caso, invece, si determina un rapporto di proporzionalità inversa, per il quale alla maggiore complessità della decisione discrezionale che il sistema di intelligenza artificiale deve adottare corrisponde la minore spiegabilità tecnica del funzionamento dell'algoritmo e dell'*iter* logico giuridico seguito dal sistema.

L'obbligo di motivazione per tutti i provvedimenti amministrativi costituisce di certo una garanzia di trasparenza. Ma essa può non essere sufficiente, pro-

prio perché è difficile offrire una risposta alla domanda su come debbano essere interpretate le nozioni di conoscibilità e comprensibilità delle decisioni automatizzate. La naturale complessità nella comprensione tecnica del funzionamento del *software* che restituisce la decisione robotizzata richiede un adattamento dei meccanismi e degli istituti del procedimento amministrativo, al fine di conciliare obblighi con le modalità di funzionamento degli algoritmi, in modo compatibile con quanto prescrive l'articolo 97 della Costituzione italiana. Ne deriva un diverso atteggiarsi anche del principio di trasparenza, che deve andare oltre la mera esplicabilità della decisione algoritmica, per consentire di cogliere le modalità relative alla trasposizione tra linguaggio tecnico e linguaggio giuridico.

La giurisprudenza, nel confrontarsi con tali problematiche, ha avuto modo di sottolineare come «le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere e che pertanto, al fine di assicurare l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento, deve seguitare ad essere il dominus del procedimento stesso, all'uopo dominando le stesse procedure informatiche predisposte in funzione servente e alle quali va dunque riservato tutt'oggi un ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo»[7].

Anche quando è stata evidenziata l'importanza di una maggiore diffusione delle procedure automatizzate all'interno del procedimento amministrativo, in quanto in grado di «migliorare la qualità dei servizi resi ai cittadini e agli utenti» e si è aperta la strada alla possibilità di utilizzare l'algoritmo anche per attività connotata da ambiti di discrezionalità, è stata tuttavia sottolineata l'importanza di un adattamento necessario in quanto non può essere applicata in modo indiscriminato all'attività amministrativa algoritmica «tutta la legge sul procedimento amministrativo, concepita in un'epoca nella quale l'amministrazione non era investita dalla rivoluzione tecnologica». Anche considerando come «la fondamentale esigenza di tutela posta dall'utilizzazione dello strumento informatico c.d. algoritmico sia la trasparenza»[8].

[7] T.A.R. Lazio, Roma, sez. III bis, 10 settembre 2018, n. 9224.
[8] Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472.

Non è mancata la sottolineatura che vi è un collegamento tra l'utilizzo degli strumenti di I.A. con i canoni di efficienza ed economicità dell'azione amministrativa (art. 1 legge 241/90) e con il principio costituzionale di buon andamento dell'azione amministrativa (art. 97 Cost.), affermando che «occorre sfruttare le rilevanti potenzialità della c.d. rivoluzione digitale» e che «il ricorso ad algoritmi informatici per l'assunzione di decisioni che riguardano la sfera pubblica e privata può determinare un guadagno in termini di efficienza e neutralità». Con la conseguenza che gli algoritmi potrebbero divenire un utile strumento attraverso il quale «correggere le storture e le imperfezioni che caratterizzano tipicamente i processi cognitivi e le scelte compiute dagli esseri umani, messi in luce soprattutto negli ultimi anni da un'imponente letteratura di economia comportamentale e psicologia cognitiva. In tale contesto, le decisioni prese dall'algoritmo assumono così un'aura di neutralità, frutto di asettici calcoli razionali basati su dati». Significativamente, però, si ribadisce la necessità del rispetto di alcune garanzie, e cioè la "piena conoscibilità", la "imputabilità" della decisione, la possibilità di "controllo" dell'*iter* seguito.

Afferma il giudice amministrativo che la «conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti. Ciò al fine di poter verificare che i criteri, i presupposti e gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato». Più specificamente, secondo il Consiglio di Stato, tale conoscibilità deve intendersi sia con riferimento alla p.a. che decide di affidarsi ad una procedura basata su un algoritmo, sia avendo riguardo al destinatario degli esiti della decisione automatizzata[9]. E ciò anche per consentire un pieno sindacato da parte del giudice amministrativo.

5. *Verso una nuova sovranità digitale?*

Non sembra dubitabile, allora, che i cambiamenti in atto possano avere un significativo impatto sulla decisione amministrativa, non più inquadrabile all'interno delle consuete categorie dogmatiche.

[9] Cons. Stato, n. 8472/2019 cit.

Non si può non ricordare che nell'ordinamento italiano il processo di transizione digitale è risalente nel tempo. Già nel 2005, infatti, all'amministrazione digitale è stato dedicato un "codice" (d.lgs. n. 82/2005, c.d. "CAD") che ha fatto emergere "diritti di cittadinanza digitale" (art. 17, comma 1 quinquies), nozione evanescente nei confini, ma che ben rappresenta la sempre più marcata modificazione delle categorie conosciute. All'art. 41 del Codice si afferma che «*le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione*».

Si tratta di un processo, come noto, in rapidissima evoluzione. Basti pensare che l'art. 3-*bis* della legge n. 241/1990, innovato dal "decreto legge Semplificazioni" n. 76/2020, stabilisce come per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati. Oppure, ancora, all'introduzione della nuova "*Carta della cittadinanza digitale*" (art. 1, l. 7 agosto 2015, n. 124) o del c.d. principio del "*digital first*" (art. 1, comma 1, lett. b, l. n. 124/2015, cit.) che rendono percepibile il mutamento delle relazioni sociali per effetto dell'avvento delle nuove potenzialità di internet, già definito dalla dottrina come «uno spazio sociale dilatato, senza precedenti nella storia dell'umanità […], dove si mescolano soggetti e fenomeni diversi, dove i ruoli possono cambiare vorticosamente e molti interessi trovarsi in conflitto» (Rodotà, 2020).

Insomma, non sembra dubitabile che lo svolgimento della funzione amministrativa sia stato profondamente inciso e conformato dalle nuove tecnologie. E ciò nella fase istruttoria, di partecipazione procedimentale[10] o con riguardo alla forma dell'atto e agli adempimenti necessari per la piena efficacia dello stesso.

Il dato normativo offre, comunque, anche spunti interessanti sia a livello europeo che a livello nazionale.

Come è noto, il Parlamento europeo ha, infatti, approvato il regolamento sull'intelligenza artificiale, che si propone di offrire maggiori garanzie di sicurezza e di rispetto dei diritti fondamentali dei soggetti coinvolti.

L'Unione europea ha optato per l'adozione del regolamento, così come accaduto, fra l'altro, con il GDPR per la disciplina in materia di protezione dei dati,

[10] Si pensi, ad esempio, alla possibilità per i cittadini di realizzare «*la partecipazione con modalità telematiche ai processi decisionali delle istituzioni pubbliche*», ai sensi dell'art. 1, comma 1, lett. c) della legge n. 124/2015, anche attraverso l'utilizzo di forme di consultazione preventiva sugli schemi di atti da adottare, che richiamano il modello americano delle legislative *rules* assoggettati al *notice and comment*.

in modo da determinare vincoli uniformi e direttamente applicabili su tutto il territorio dell'Unione, con l'obiettivo di fissare un quadro normativo omogeneo e tendenzialmente rigido per gli Stati membri.

Si tratta di una disciplina normativa che risponde direttamente alle proposte dei cittadini che hanno partecipato alla Conferenza sul futuro dell'Europa (COFE), finalizzate, in particolare, a rafforzare la competitività dell'UE nei settori strategici; realizzare una società sicura e affidabile, contrastando la lotta alla disinformazione; promuovere l'innovazione digitale, garantendo la supervisione umana e l'uso affidabile e responsabile dell'IA, stabilendo salvaguardie e garantendo la trasparenza; utilizzare l'IA e gli strumenti digitali per migliorare l'accesso dei cittadini alle informazioni, comprese le persone con disabilità.

Il Regolamento non pregiudica le competenze degli Stati in materia di sicurezza nazionale e utilizza un approccio "basato sul rischio", classificando l'impatto dei sistemi di I.A. come rischio "inaccettabile", con riferimento ai sistemi di categorizzazione e identificazione biometrica, ai sistemi che manipolano il comportamento umano o sfruttano le vulnerabilità delle persone; rischio "alto" per i sistemi che possono arrecare danni alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia e allo Stato di diritto (ad esempio assistenza sanitaria, banche, ecc.), alcuni sistemi di contrasto, migrazione e gestione delle frontiere, giustizia e processi democratici (come nel caso di sistemi usati per influenzare le elezioni); rischio "minimo", in caso di videogiochi o filtri spam. Si prevede, inoltre, un sistema di sanzioni e una serie di misure a sostegno dell'innovazione.

È interessante, tuttavia, notare che il legislatore europeo vieta l'uso dei sistemi di *deep learning* senza supporto umano per le attività classificate ad alto rischio. Non definisce, però, tali sistemi, ma fornisce i criteri per individuarli, anche specificando i settori di riferimento. Rimane, tuttavia, da chiarire se il procedimento amministrativo possa essere incluso nelle attività ad alto rischio.

Osservando quanto previsto anche a livello nazionale, si manifesta una tendenza di sistema da considerare per possibili ulteriori sviluppi.

Il disegno di legge sull'intelligenza artificiale[11], di recente approvato in Senato, conferma un approccio secondo cui l'algoritmo deve essere di supporto alla

[11] Disegno di legge n. 1146 ("*Disposizioni e delega al Governo in materia di intelligenza artificiale*").

decisione. Si prevede, infatti, che «*l'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale*»[12].

L'obiettivo del disegno di legge è la promozione di «*un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità*»[13] e migliorare le condizioni di vita dei cittadini e la coesione sociale. Nella Relazione al disegno di legge si esplicita la volontà di perseguire l'obiettivo del bilanciamento tra opportunità e rischi, promuovendo l'utilizzo delle nuove tecnologie, ma fornendo, allo stesso tempo, soluzioni per la gestione del rischio fondate su una visione antropocentrica[14].

In particolare, poi, l'art. 13 regola l'utilizzo dell'Intelligenza Artificiale nel settore dell'attività della pubblica amministrazione come strumento capace di garantire il buon andamento e l'efficienza dell'attività amministrativa dando, tuttavia, centralità al principio dell'autodeterminazione e della responsabilità della persona che la utilizza. L'intelligenza artificiale diviene così strumento per l'incremento della efficienza delle amministrazioni; la riduzione dei tempi di definizione dei procedimenti; l'incremento della qualità e quantità dei servizi erogati. Anche se, però, si ribadisce la necessità di assicurare agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo.

Sembra importante ribadire che l'utilizzo dell'intelligenza artificiale deve essere in funzione strumentale e di supporto all'attività provvedimentale, rispettando l'autonomia e il potere decisionale del soggetto che resta l'unico responsabile dei provvedimenti e dei procedimenti.

Impianto che trova sostanzialmente conferma in un'altra disposizione normativa, della quale è stata notata la rilevanza, trattandosi di una novità significativa per il riferimento espresso all'Intelligenza Artificiale, e cioè l'art. 30 del d.lgs. n. 36 del 2023, recante il "Codice dei contratti pubblici".

[12] Art. 13 ("*Uso dell'intelligenza artificiale nella pubblica amministrazione*") comma 2.

[13] Art. 1.

[14] Il testo si compone di 26 articoli, che disciplinano l'integrazione dell'Intelligenza Artificiale in settori critici quali sanità (art. 7) e lavoro (art. 10), informazione e riservatezza dei dati personali (art. 4), sviluppo economico (art. 5), professioni intellettuali (art. 12), attività giudiziaria (art. 14), investimenti nel settore con un'autorizzazione di spesa di 1 mld di euro (art. 21), tutela degli utenti (art. 23), diritto d'autore, per la disciplina specifica delle opere create con l'ausilio dell'IA (art. 24) e, infine, tutela penale (art. 25), con l'introduzione di una circostanza aggravante per i reati commessi mediante l'impiego di sistemi di Intelligenza artificiale, di circostanze aggravanti speciali per determinati reati e l'introduzione di una nuova fattispecie penale.

Tale disposizione al comma 1 così recita: «*per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'Intelligenza Artificiale e le tecnologie di registri distribuiti, nel rispetto delle specifiche disposizioni in materia*».

Essa, pur essendo una norma settoriale, sembra possedere una rilevanza sistemica.

Anche in tal caso, è interessante osservare come i redattori del nuovo codice hanno scelto di effettuare un'elencazione di una serie di principi destinati a governare l'utilizzo di sistemi di Intelligenza Artificiale da parte delle stazioni appaltanti. Sono, così, enunciati i quattro principi fondamentali della conoscibilità, comprensibilità, non esclusività e non discriminazione[15].

Viene, in tal modo, ribadito un principio di "non esclusività della decisione algoritmica", dal momento che il contributo umano deve poter avere l'ultima parola in merito alla correttezza o, meglio, in ordine alla legittimità della scelta, appunto controllando, validando o smentendo la decisione automatizzata.

La vera sfida consiste però nel rendere effettivamente praticabili i principi enunciati, per garantire spazio alla c.d. "riserva di umanità", ovvero a un intervento umano nel corso del procedimento e dare piena operatività, nell'ambito dell'attività della pubblica amministrazione, al modello "*human in the loop*", che appare indispensabile per sfruttare caratteristiche peculiari dell'uomo, come la capacità di interpretare un contesto e prendere decisioni guidate da principi etici (Pajno, Bassini et al., 2019)..

Allo stesso tempo, però, evitando di incorrere in rischi considerevoli, come ad esempio quello del fenomeno della c.d. *Black Box*, che sfugge a qualunque tentativo di esplicazione *ex post*, mantenendo inalterato lo standard di intelligibilità delle decisioni adottate dalle pubbliche amministrazioni, conciliando gli obblighi di legge, quale quello di motivare i provvedimenti amministrativi, con una decisione che sempre più assume i caratteri di una decisione "mista".

[15] Il comma 3 precisa, infatti, che: «*le decisioni assunte mediante automazione rispettano i principi di: a) conoscibilità e comprensibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata; b) non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; c) non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici*».

Come è stato efficacemente sottolineato, il mutare della forma del rapporto tra cittadino ed amministrazione finisce per costituire la precondizione per una modificazione della sostanza dell'agire pubblico e della struttura della decisione. L'uso dell'A.I. è, allora, estremamente utile nel momento in cui potenzia l'intelligenza naturale del funzionario pubblico, incrementando efficienza e garanzia[16]. Ma, al contempo, evitando che si configuri una "Amministrazione invisibile", spettatrice delle decisioni ad essa stessa imputabili (D'Angelosante, 2015; Civatese Matteucci, Torchia, 2016).

Pur con non poche difficoltà, una applicazione dell'intelligenza artificiale in funzione di garantire la cybersicurezza è da indagare in modo approfondito.

La cybersicurezza è caratterizzata dall'essere fenomeno eterogeneo e trasversale. E, in tale contesto, si evidenzia l'importanza di cogliere un aspetto della sovranità intesa come "sovranità digitale", concetto non così agevole da definire con rigore, potendosi intendere come la capacità dello Stato di esercitare un controllo efficace sui dati, sulle infrastrutture e sulle tecnologie digitali, al fine di garantire sicurezza, autonomia e tutela dei diritti fondamentali[17].

Emerge, così, il *novum* che finisce per impattare le tradizionali categorie ricostruttive delle funzioni statali e delle correlate modalità di decisioni (dal livello normativo a quello amministrativo e organizzativo) per ottenere schemi operativi che riescano a conciliare, tutela dei diritti, libertà ed equilibri politici, con l'obiettivo sicurezza. Di qui la conseguente valorizzazione della cooperazione fra pubblico e privato per ottenere il risultato, nella consapevolezza della oggettiva distanza che intercorre fra le competenze tecniche della parte privata e di quella pubblica. E ciò non solo nella sua dimensione "orizzontale", fra l'acquirente pubblico e i fornitori privati, con i quali le Amministrazioni dovranno in ogni caso confrontarsi anche nell'utilizzo delle infrastrutture pubbliche, una volta terminate e a regime, ma anche nella dimensione "verticale", che concerne i livelli di governo nazionali e sovranazionali e gli stessi Stati fra loro, al fine di rafforzare l'intelaiatura esistente delle politiche sul digitale e sulla cybersicurezza pubblica, apportandovi modifiche in grado di rendere tutto il sistema più resiliente. Si tratta di una cooperazione che deve transitare nel concetto di "collaborazione orien-

[16] Ribadendo, così, l'attualità della considerazione secondo la quale «*technology that is not human-centered will not be a solution*» (Dangel, Hagan, Williams, 2018).

[17] In ambito amministrativo, questa nozione implica la responsabilità pubblica nella regolazione dei flussi informativi e nell'orientamento dell'innovazione digitale, anche mediante strumenti di *soft law* e cooperazione regolatoria (De Minico, 2022; Ramajoli, 2021).

tata dallo Stato", il che impone un impegno pubblico per ottenere un incremento delle competenze manageriali e strategiche.

La *cybersecurity*, nel richiedere un approccio completo e continuo, rende necessario, come detto, investire in soluzioni avanzate per garantire una protezione efficace delle risorse digitali. Le organizzazioni devono migliorare costantemente le proprie difese, adottando soluzioni di sicurezza avanzate e sensibilizzando i dipendenti sui rischi.

È un metodo composito che interviene almeno su tre ambiti: quello tecnico, quello normativo, che deve seguire quello tecnico, e quello della *governance* per predisporre un'architettura multilivello.

Quanto sia operazione complessa, lo dimostra però anche la recente legge n. 90/2024, quando nell'art. 8 si occupa del "*rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza*".

La necessità di una struttura che provveda a svolgere una serie di compiti è allo stato operazione non facile e lo testimonia il comma 2 nella ricerca di un centro operativo (referente per la cybersicurezza) che sia nella condizione di ottenere il risultato.

La riflessione sul grado di effettività dell'impianto normativo, che è trasversale alle opzioni del legislatore, in questo caso ancora di più si impone per cogliere la concreta incidenza nel risolvere una problematica che, come è noto, attinge a livelli nazionali e sovranazionali.

Anche osservando la direttiva NIS 2, si può notare come in uno dei "considerando" si spiega che per raggiungere un comune livello elevato di cybersicurezza è necessario applicare le nuove misure a una parte più ampia dell'economia al fine di dare una copertura completa a quei servizi essenziali e vitali per lo svolgimento delle principali attività sociali ed economiche nel mercato interno.

Insomma, per affrontare le sfide complesse che attengono all'evoluzione delle minacce, alla mancanza di competenze e al c.d. "*IoT*" ("*Internet of things*") con aumento del numero di dispositivi vulnerabili e la conseguente creazione di nuove superfici di attacco, sembra che la strada sia obbligata.

Rinforzare attraverso nuove previsioni e regolamentare in modo adeguato gli strumenti che l'ordinamento già offre per allargare gli spazi, ancora limitati, previsti dalla disciplina della *cybersecurity* pubblica alla collaborazione fra pubblico e privato tende al raggiungimento del fine ultimo della politica pubblica sulla cybersicurezza: non soltanto proteggere le infrastrutture digitali, ma giungere a un contesto istituzionale di *cyber* resilienza in cui tutti gli attori coinvolti, interagendo e collaborando fra loro in vista del raggiungimento di un obiettivo

comune stabilito dallo Stato, diventino consci dei rischi. La cybersicurezza, quale componente fondamentale per il buon funzionamento delle società moderne, influenzando ogni settore, dalla finanza alla sanità, dalla produzione industriale alla protezione della *privacy* individuale, è destinata a crescere di importanza con l'aumento della digitalizzazione e della connettività globale. La protezione delle informazioni, la prevenzione degli attacchi informatici e la gestione delle vulnerabilità richiedono un impegno costante, una cooperazione internazionale e una continua innovazione tecnologica.

Insomma, è richiesto un "cambio di passo". In questo senso, in varie sedi si sottolinea la limitatezza della visione che inquadra i fenomeni all'interno della *compliance*, senza considerarli opportunità di trasformazione in processi di efficienza e di efficacia, anche se, forse, occorre un "percorso" più lungo per accompagnare la Pubblica Amministrazione.

Come è intuibile, nel far ciò il ruolo dello Stato appare imprescindibile.

In tal senso, non può non condividersi l'affermazione che si tratta di «un ecosistema simbiotico basato su relazioni cooperative fra i soggetti pubblici e i soggetti privati. In questo modo si potrà giungere a una co-creazione di valore, indirizzata a fini sociali, che non sia il frutto di mere decisioni "calate verso il basso" (top-down) ma di strategie condivise (bottom-down) in vista del raggiungimento di un fine comune» (Rossa, 2023: 214).

Bibliografia

Bavetta F., *Direttiva NIS 2: l'innalzamento dei livelli di cybersicurezza a livello europeo*, in MediaLaws, n. 3, 2022, 405 ss.

Benetazzo C., *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazion*e, in www.federalismi.it, 16, 2020.

Casonato C., *Tecnologie digitali e diritti fondamentali*, in «Dir. pubbl.», 2020, 339 ss.

Dangel S., Hagan M., Williams J.B, *Designing Today's Legal Education for Tomorrow's Lawyers: The Role of Legal Design, Technology and Innovation*, September 2018.

D'Angelosante M.*, La consistenza del modello dell'amministrazione "invisibile" nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in Civitarese Matteucci S., Torchia L. (a cura di), *La tecnificazione*, Firenze University Press, Firenze, 2016.

De Minico G.*, Sovranità digitale*, *sovranità dei diritti*, in «Giur. cost.», 2022, 923 ss.

Di Ciommo I.P., *La prospettiva del controllo nell'era dell'Intelligenza Artificiale: alcune osservazioni sul modello Hu-man In The Loop*, in www.federalismi.it, n. 9, 2023.

Galetta D.U., Corvalán J.G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in www.federalismi.it, n. 3, 2019.

Losano M., *Diritto e democrazia nell'era digitale*, in «Pol. dir.», 2021, 145 ss.
Marchetti B., *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in «BioLaw Journal – Rivista di BioDi-ritto», 2, 2021.
Mazzucato M., *Lo Stato innovatore. Sfatare il mito del pubblico contro il privato*, Laterza, Roma, 2014.
Otranto P., *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in www.federalismi.it, 7, 2021.
Pajno A., Bassini M., De Gregorio G., Macchia M., Patti F.P., Pollicino O., Quattrocolo S., Simeoli D., Sirena P., *Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in «BioLaw Journal», 3, 2019, p. 205 ss.
Ramajoli M., *Funzione amministrativa e nuove tecnologie*, in Studi in onore di G. Falcon, vol. II, 2021.
Rodotà S., *Il diritto alla conoscenza*, Relazione conclusiva al Seminario alla Scuola per Librai tenutosi presso la Fondazione Cini a Venezia, in www.scuolalibraiuem.it
Rossa S., *Cybersicurezza e pubblica amministrazione*, Editoriale Scientifica, Napoli, 2023.
Salvaggio S.A., González F., *The European framework for cybersecurity: strong assets, intricate history*, in «Int. Cybersec. Law Rev.», 4, 2023, 137 ss.
Tosoni L., *Direttiva NIS, così è l'attuazione italiana*, in *AgendaDigitale.eu*, 15 gennaio 2021.
Viola L., *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in www.federalismi.it, 21, 2018.
Violini L., *Sicurezza e diritti nella giurisprudenza costituzionale*, in «Quad. cost.», 2022.

Capitolo Quinto

Cybersecurity e tutela penale. Quali prospettive?*

Roberto Flor

Introduzione

Con la legge 28 giugno 2024, n. 90 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici") il legislatore penale ha inteso apportare modifiche al sistema codicistico dei reati informatici.

Al di là della rilevanza mediatica di tale intervento, elevato alla stregua di un "giro di vite" contro il *cybercrime*, seguito poi a stretto giro dalla legge 23 settembre 2025, n. 132 ("Disposizioni e deleghe al Governo in materia di Intelligenza artificiale"), il suo impatto, sul piano del diritto penale sostanziale, appare davvero limitato ad un generale inasprimento della risposta sanzionatoria e a taluni "correttivi", fra cui, per citare solo alcuni esempi, l'introduzione di una nuova ipotesi di reato (art. 629, comma 3), nel tentativo di rispondere alla diffusione (soprattutto) di *cyber-attacks* "*ransomware*", di cui si dovranno attendere le prime applicazioni giurisprudenziali per vagliarne effettività ed efficacia, e l'abrogazione, in particolare, dell'art. 615-*quinquies* c.p. che, in verità, viene collocato fra i reati contro il patrimonio (*ex* art. 635-*quater*.1) con la previsione di due nuove circostanze aggravanti. Oppure si pensi al reato di truffa di cui all'art. 640 c.p., che viene arricchito da un ulteriore comma (2-*ter*), se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.

La l. n. 132/2025 appare rilevante, in questo contesto, in quanto lo sviluppo di sistemi e di modelli di intelligenza artificiale avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza,

* Il presente contributo, con l'aggiunta di una bibliografia essenziale, costituisce l'intervento svolto al Convegno "Modelli di *cybersecurity* e prevenzione dei *cyber crimes*. Aporie della legislazione vigente, problematiche applicative e prospettive *de iure condendo*", organizzato in data 24 gennaio 2025 dall'Unità di ricerca dell'Università degli Studi di Napoli Federico II (Responsabile scientifico Prof. Giacomo Di Gennaro), nell'ambito del Progetto PNRR Serics Hard Disc – Spoke 1.

la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati. Le disposizioni in essa contenute, inoltre, sono volte a valorizzare l'intelligenza artificiale anche come risorsa per il rafforzamento della cybersicurezza nazionale.

Proprio al fine di garantire il rispetto dei diritti e dei princìpi espressi da tale atto normativo deve essere assicurata, quale precondizione essenziale, la cybersicurezza durante tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.

Fra il resto la medesima legge ha introdotto alcune aggravanti speciali per "l'aver commesso il fatto mediante l'impiego di sistemi di I.A." e inserito, nel lungo elenco di circostanze previste all'art. 61, c. 1, c.p., l'aggravante comune di cui al n. 11-*decies*, che si applica ai casi in cui il fatto sia stato commesso «mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

Con il presente lavoro, anche alla luce dell'entrata in vigore di queste ultime novità legislative, si intendono proporre alcune brevi riflessioni relative all'esigenza di tutela penale di beni giuridici di nuova o nuovissima generazione, rispetto a tradizionali e innovative forme di aggressione. Beni espressione altresì di inedite forme di manifestazione dei diritti fondamentali, tenendo ben presente la necessità di trovare un fil rouge tra le proteiformi definizioni di "cybersecurity".

1. *Cybersecurity e tutela penale*

La c.d. *cybersecurity*, dunque, non può rappresentare solo una questione o, peggio, un ostacolo, di ordine tecnico. Al contrario, la sua rilevanza nella costellazione sempre più variegata dell'ecosistema digitale la eleva ad una innovativa espressione dei diritti fondamentali e se non ad un diritto fondamentale. Questo approccio è confermato anche nella letteratura straniera, che sempre più spesso fa riferimento a «*Human-Centric Approach to Cybersecurity*» (Deibert, 2018), oppure a «*Cybersecurity as a human rights*» (Shackelford, 2019) o, ancora, ponendosi la

seguente questione, almeno nel panorama europeo: «*New right to cybersecurity?*» (Chiara, 2024)[1].

In effetti, mentre si assiste ad una generale condivisione sull'importanza della *cybersecurity*, non vi è consenso unanime relativamente all'approccio "metodologico", "contenutistico" e "definitorio" a tale concetto, almeno sul piano del diritto penale sostanziale.

Non è raro imbattersi, in letteratura, in argomentazioni che sovrappongono piano diversi, confondendo la *cybersecurity* nel contesto della sicurezza nazionale (se non internazionale) – ossia del perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale – la *cybersecurity* nel contesto pubblico e la *cybersecurity* nel settore privato, ovvero *cyberscurity* intesa quale risultato di un processo organizzativo rispetto alle componenti strutturali del concetto stesso di *cybersecurity*.

La legge n. 90/2024 contiene, infatti, da un lato misure di rafforzamento della *cybersicurezza* nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario e, dall'altro lato, interventi nell'ambito dei reati informatici.

Si tratta di una legge che, per il vero, si inserisce in un contesto europeo in cui l'Unione europea stessa lavora su vari fronti per promuovere la resilienza informatica, ivi compresa la resilienza operativa digitale per il settore finanziario (si pensi solo, a titolo esemplificativo, al regolamento UE/2022/2554).

Dopo la legge n. 547/1993 (prima normativa in materia di *cybercrime*) e la legge n. 48/2008 (di attuazione della Convenzione del Consiglio d'Europa sulla criminalità informatica – Convenzione *Cybercrime*) non si è assistito ad ulteriori interventi di carattere sistematico, e tanto meno risponde a simile esigenza la legge n. 90.

[1] In questo contributo l'autore concentra l'analisi su "three legal challenges brought about by a theoretical framework for development of a new right to cybersecurity. They regard: i) the need for a new right to cyberse-curity against the background of the existing fundamental right to security (Art. 6 EU Charter of Fundamental Rights, CFR); ii) the actual content of this new right; and, iii) how such a new right could be implemented".

La legislazione penale italiana *in subiecta materia*, infatti, è stata sin dall'origine caratterizzata da un insieme di norme incriminatrici eterogenee, frutto di interventi spesso settoriali o frammentari imposti, da un lato, dalla necessità di colmare alcune lacune emerse nella prassi applicativa, dall'altro lato di dare attuazione alle fonti internazionali ed europee.

Si pensi che per più di 30 anni l'art. 615-*ter* c.p., fattispecie fulcro nel microsistema dei reati informatici, non ha subito modifiche, tanto che si sono susseguite diverse tesi riguardanti il suo oggetto giuridico. È stato sostenuto, inizialmente, che la fattispecie tutelasse la privacy, intesa non più solo nel significato riduttivo di «*the right to be let alone*», il domicilio informatico, ovvero configurasse un reato plurioffensivo, a tutela anche dell'integrità del sistema, dei programmi, dei dati e delle informazioni. Il nostro legislatore poi, nel 2008, non ha ritenuto necessario modificare la formulazione originaria dell'art. 615-*ter* c.p., confermando pertanto le scelte di politica criminale degli anni '90.

Oggi, anche dopo il limitato intervento del legislatore del 2024 (vedi *infra*), l'individuazione dell'oggetto giuridico tutelato deve avvenire attraverso l'interpretazione sistematica e teleologica di questa fattispecie da porre in relazione ad altri reati, tra cui quelli *ex* artt. 615-*quater*, 617-*quater*, 617-*quinquies* e 617-*sexies* c.p.

Nell'era dell'interconnessione, della comunicazione globale e dell'infosfera, nonché dell'accessibilità e della fruibilità delle risorse attraverso la rete e qualsiasi strumento di comunicazione anche mobile, lo "spazio informatico" è rapidamente passato da una dimensione privata o singola ad una "dimensione pubblica". In altri termini all'interesse del singolo si affianca quello super-individuale o di natura collettiva a che l'accesso a tali spazi, ai sistemi e ai dati informatici ed alla stessa rete avvenga per finalità lecite e in modo tale da essere regolare per la sicurezza degli utenti, pur mantenendosi quale «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost.» e strumentale per l'esercizio degli stessi diritti fondamentali dell'individuo.

Per cui, da un lato, è innegabile che una componente di tale "area riservata" riguardi la facoltà, il potere, il diritto del titolare di gestire in modo autonomo le utilità e le risorse del sistema informatico, nonché i contenuti delle comunicazioni informatiche (o telematiche), indipendentemente dalla loro natura; dall'altro lato, appare indispensabile un bilanciamento con le esigenze connesse alla "sicurezza informatica". Sia quest'ultima che la "riservatezza informatica", dunque, contribuiscono a delineare un livello anticipato e preventivo di protezione rispetto al momento dell'effettiva lesione dell'integrità delle informazioni, dei programmi o dei sistemi informatici, nonché alla presa di cognizione dei contenuti dei dati

ivi archiviati o trattati, anche di natura riservata o segreta. Simile prospettiva di tutela, che valorizza i profili funzionali della sicurezza informatica, è direttamente rafforzata da dati normativi, espliciti ed autonomi. In primis, l'art. 615-*ter* c.p. offre protezione penale solo ai sistemi protetti da "misure di sicurezza". Le diverse tesi interpretative sul "ruolo" di tale elemento costitutivo convergono su almeno una argomentazione comune e insuperabile: la legge penale non definisce la natura delle misure protettive e non richiede che esse siano efficaci e idonee. A tali misure, dunque, il legislatore sembra aver ragionevolmente affidato il compito di manifestare lo *ius excludendi alios* del titolare dello spazio informatico. In secondo luogo, l'art. 615-*ter*, comma 2, n. 3, c.p. prevede un aumento della pena e la procedibilità d'ufficio se dal fatto derivi la «distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti». La legge n. 90/2024 ha apportato un sensibile inasprimento sanzionatorio per le ipotesi aggravate di cui al comma 2, prevedendo la pena della reclusione da 2 a 10 anni inserendo, proprio nell'ipotesi di cui al n. 3, dopo le parole: «ovvero la distruzione o il danneggiamento» le seguenti: «ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare».

Questa locuzione, da un lato e sul piano sistematico, pare voler rafforzare la già stretta connessione fra riservatezza, integrità e sicurezza informatiche, offese o messe in pericolo dalle condotte previste dall'art. 615-*ter* c.p. Dall'altro lato, il legislatore è caduto nel medesimo errore del legislatore del 2013 quando, questo ultimo, con la legge n. 119/2013 (di conversione con modificazioni del d.l. n. 93/2013) ha introdotto nell'art. 640-*ter* c.p. un nuovo comma, che sanziona ancora oggi la frode informatica commessa mediante sostituzione (furto o indebito utilizzo) dell'identità digitale in danno di uno o più soggetti. L'espressione "furto" di identità digitale sembra richiamare (impropriamente) le condotte di sottrazione e impossessamento previste dall'art. 624 c.p., che sono tecnicamente riferite ad un oggetto fisico-materiale, espresso dal termine "cosa".

Riproporre a più di dieci anni di distanza l'espressione "sottrazione […]" riferita ai dati sembra confermare un difetto di comprensione della "regola tecnologica", essendo i dati, per loro stessa natura, insuscettibili di sottrazione ed impossessamento.

La rapidità dell'evoluzione tecnologica ha sempre rappresentato una sfida per il diritto e, in particolare, per la legislazione e la giurisprudenza penale. Proprio la comprensione della regola tecnologica costituisce e probabilmente costituirà un fattore determinante, in quanto deve entrare nelle scelte di politica criminale,

come la tecnologia entra e entrerà sempre più frequentemente fra gli strumenti investigativi e decisori, gli elementi costitutivi della fattispecie incriminatrice, le note modali di realizzazione della condotta, nonché quale oggetto di tutela se non di espressione essenziale dell'oggettività giuridica, anche quale spazio immateriale e a-territoriale attraverso cui persone, enti ed istituzioni prestano le loro attività ed i loro servizi e garantiscono la regolarità dei rapporti giuridici. La comprensione della regola tecnologica dovrebbe guidare altresì l'interpretazione della fattispecie legale, nel limite dei possibili significati penalmente rilevanti del testo, per evitare "acrobazie" ermeneutiche espressione di approcci decisamente "*vintage*", nascosti in argomentazioni solo apparentemente di stampo evolutivo ma, di fatto, risultato persino di applicazioni analogiche *in malam partem* dettate da una serie di fattori contingenti, fra cui la preoccupazione di lasciare vuoti di tutela penale. Il rischio da evitare è quello "scollamento" fra il contesto tecnologico-sociale, le scelte del legislatore e l'interpretazione delle singole disposizioni.

Deve aggiungersi che, per quanto attiene ai "fatti" tipizzati dai delitti di danneggiamento informatico, anche dopo l'intervento del legislatore del 2024, la dimensione del bene giuridico tutelato non sembra potersi ridurre al patrimonio del titolare dei sistemi o dei dati, che rimane sullo sfondo. Essa è invece estesa all'integrità e alla disponibilità dei dati e dei sistemi informatici e telematici se non persino, per quanto riguarda le incriminazioni di cui agli artt. 635-*ter* e 635-*quinquies* c.p. – strutturati come delitti di attentato – l'ordine pubblico. L'elemento comune e l'area di intersezione fra dimensione individuale e dimensione collettiva del bene tutelato, è costituita dall'interesse a non subire indebite interferenze nella sfera di rispetto e disponibilità di "spazi informatici", indipendentemente dalla qualità (natura) o dalla quantità di dati e informazioni o dalla natura o dimensione dello spazio informatico di pertinenza di uno o più soggetti "titolari", ovvero dal potere di determinare, in sé, il "destino" di tali aree informatiche in cui si manifesta la personalità umana. Il rafforzamento della tutela penale della riservatezza e sicurezza informatiche era comunque già assicurata sia dalla fattispecie ostacolo di cui all'art. 615-*quater* c.p. – che sanziona condotte prodromiche all'accesso abusivo ad un sistema informatico o telematico tramite una decisa anticipazione della punibilità – sia dalla norma di cui all'art. 615-*quinquies* c.p. (ora confluita sostanzialmente nel nuovo art. 635-*quater*.1) sia, infine, dalle citate disposizioni di cui agli artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p. Con riferimento a queste ultime è facile notare come la stessa innovazione tecnologica abbia contribuito ad ampliare il raggio di tutela della segretezza della comunicazione, costituzionalmente garantito dall'art. 15 Cost., andando oltre la segretezza

del contenuto della comunicazione e attraendo nella sua orbita i dati esterni alle comunicazioni.

A prescindere dalle funzioni che si vogliono attribuire alla tutela penale della sicurezza informatica – positiva e negativa – comunque orientate ad assicurare la tutela dell'interesse alla riservatezza informatica ed alla generale correttezza dello svolgimento dei rapporti giuridici, essa deve trovare un bilanciamento con l'esigenza di garantire la libertà di circolazione dei dati e delle informazioni, nonché con la loro libera accessibilità e fruibilità. Tale bilanciamento risulta essere più complesso per la crescente vulnerabilità dei sistemi informatici, dei dati e delle informazioni in essi archiviati, dovuta a forme di aggressione sia "tradizionali" che "tecnologiche" che si evolvono con lo stesso sviluppo tecnologico.

L'esigenza di assicurare tutela penale della sicurezza informatica non corrisponde ad una necessità costruita artificialmente, ma esprimerebbe il bisogno «di assicurare una condizione condivisa nella società dell'informazione».

2. *Semantica tecnica e componenti strutturali della definizione di cybersecurity. Verso un comprehensive concept di un bene giuridico collettivo meritevole di protezione penale*

Appare ora necessaria una ulteriore precisazione, di carattere non solo terminologico. A fenomeni "in costante movimento", come quelli riconducibili al settore della *cyber-criminality*, dovrebbero corrispondere, da un lato, settori dell'ordinamento ad elevato coefficiente di adattamento e, dall'altro lato, un diritto giudiziale flessibile. In campi nuovi o "sperimentali" queste caratterizzazioni del sistema giuridico potrebbero, al contempo, trasmettere un senso di instabilità e di irritazione. Ma proprio la specificità di tali campi o settori necessita del ricorso ad una semantica tecnica che possa riempire termini "tradizionali", comprensibili al giurista ed all'opinione pubblica, con contenuti adattabili al nuovo contesto tecnologico, attenendosi quanto più fedelmente possibile sia al testo redatto dal legislatore, sia ai significati correnti di un termine attribuiti dalla realtà o, meglio, dalla regola tecnologica. Nell'ambito delle ICTs la concezione dello "spazio", inteso quale "area" fruibile dall'utente per il trattamento di dati e informazioni, si basa sull'immaterialità dell'ambiente, che non sempre può essere delimitato entro confini fisici (*server*, singolo sistema o *device*, *smartphone* ecc.) o territoriali. Esso può assumere una duplice dimensione. La prima può essere definita "globale" o "pubblica" e viene tendenzial-

mente utilizzata per descrivere Internet o, meglio, il *World Wide Web*, ossia ambiti "aperti" a tutti gli utenti. La seconda, invece, è di carattere "individuale" o "privato" e identifica un'area riservata ad uno o più soggetti legittimati ad accedervi attraverso diverse modalità di autenticazione.

Il concetto di *cybersecurity* (inteso sia riferito alla sicurezza nazionale – nell'ambito della quale si assiste ad una estensione ad un ampio numero di "operatori" di un complesso insieme di obblighi, con penetranti poteri preventivi, prescrittivi e sanzionatori delle Autorità governative e indipendenti – sia in quello relativo al settore pubblico o privato) non può che essere concepito come un *comprehensive concept* e, in linea con questo approccio "integrato", che comprende l'*information security*, dunque, esso esprime anche – e forse in modo preminente – l'interesse alla protezione contro le minacce alla riservatezza, all'integrità, alla disponibilità ed all'affidabilità di dati e informazioni, nonché dei *computers*, di ogni *device* o di ogni rete o sistema attraverso cui tali dati e tali informazioni vengono trattati.

Cybersecurity che, in tal senso, da un lato si distingue dalla nozione di *cybersafety*, la quale sembra includere i rischi connessi agli *informational contents* dei dati e delle informazioni trattati nel *cyberspace*, con ripercussioni dirette e indirette sull'uomo; dall'altro lato, può essere intesa quale processo proattivo e reattivo volto proprio alla protezione ideale dell'interesse degli uomini e delle organizzazioni ad essere liberi da minacce, in specie da quelle alla *CIA-Triad* – la triade *Confidentiality, Integrity* e *Availability* – che costituisce, al tempo stesso, il fulcro, la *core area* della *information security* o *cybersecurity* e il modello guida della sua governance, a cui può collegarsi l'esigenza di protezione dell'affidabilità di sistemi informatici, reti, dati e informazioni ivi contenuti o tramite di essi trattati.

In estrema sintesi, la nozione di *cybersecurity* potrebbe essere edificata su almeno tre livelli, tutti meritevoli di protezione, pur tenendo presente le esigenze afferenti alla "sicurezza nazionale": 1. infrastrutturale (*devices, hardware, software* e reti); 2. informazionale (ossia riguardante il patrimonio informativo della persona o dell'ente, non necessariamente di carattere personale); 3. personale "in senso stretto" (che riguarda la *data protection*, ossia la tutela dei dati personali).

Questa possibile costruzione di un modello concettuale di cybersecurity coinvolge altresì non solo le mere attività di gestione e prevenzione dei rischi interni al cyberspazio, ma sembra includere indistintamente la dimensione virtuale così come quella reale, per cui risulta necessario ridefinire il ruolo dello Stato e delle

istituzioni pubbliche, sia a livello nazionale che sovranazionale, in relazione alla tutela della cybersicurezza[2].

La dimensione europea della cybersicurezza, infatti, ha acquisito sempre maggiore rilevanza. Con l'adozione del pacchetto legislativo in materia, e con particolare riferimento alla direttiva (UE) 2022/2555 (direttiva NIS2) l'Unione ha delineato un quadro giuridico che mira a innalzare notevolmente il livello minimo di sicurezza delle reti e delle informazioni in tutto il territorio europeo. La sfida non è più quella di una mera armonizzazione tra le differenti legislazioni nazionali, ma quella di ottenere dei benefici comuni attraverso l'istituzione di infrastrutture comuni e di forme di cooperazioni tra Stati membri[3].

Queste riflessioni, però, non possono che partire dalla obiettiva rilevanza di un approccio proattivo e reattivo nella tutela penale della *CIA-Triad*, in uno scenario evanescente ed estremamente mutevole in cui è forse davvero giunto il momento, riprendendo le parole di Rodotà, «di pensare ad un sistema di diritti per il più grande pubblico che l'umanità abbia mai conosciuto».

Questa ricostruzione dogmatica, che giunge all'indomani della legge n. 90/2024, tramite la quale il legislatore penale sarebbe potuto intervenire in modo sistematico sul sistema dei reati informatici, pur valorizzando la tutela di beni collettivi, lungi dal voler limitarsi a contribuire a delimitare la "tipicità" delle fattispecie incriminatrici, vuole offrire un contributo alla elaborazione di un concetto "sostanziale" e "prepositivo" di *cybersecurity*, capace di assurgere, nella prospettiva di riforma o di adeguamento del sistema penale sostanziale e processuale, a parametro razionale di orientamento delle scelte anche di politica criminale, nella consapevolezza di un necessario e costante dialogo fra discipline, in quanto la scienza penale, in generale, «è fatta da diversi attori che usano oggi molti linguaggi, tra i quali ci sono anche la dogmatica classica e quella moderna, ma sempre più forti sono gli apporti della comparazione e di saperi extragiuridici». La scienza e il sapere tecnologico dovrebbero influenzare il diritto, in un'ottica di interazione reciproca per la comprensione dei diversi linguaggi. Oggi è proprio la complessità dei linguaggi tecnico-scientifici a mettere il legislatore ed il giudice in una condizione di inferiorità cognitiva, che nel peggiore dei casi si traduce in un approccio casistico culturalmente arretrato rispetto al livello di progresso tecnologico raggiunto. È condivisibile la conclusione a cui giunge una

[2] Si veda R. Ursi (a cura di), *La sicurezza nel cyberspazio*, FrancoAngeli, Milano 2023.
[3] R. Ursi, (a cura di), *La sicurezza nel cyberspazio*, op. cit., pp. 13-16.

parte della dottrina nell'affrontare, più in generale, il problema dei rapporti tra scienza e diritto e delle controversie tecnico-scientifiche nel diritto e nel processo penale, ossia che si tratti di un «paradosso al quale oggi non ci si può sottrarre». Si tratta di «saperlo gestire, guardandosi dal duplice pericolo che la scienza espropri il diritto, e che il diritto ignori o rinneghi la scienza. Impresa realizzabile in linea di astratto principio, ma difficile nei fatti».

Lo stesso adeguamento, nella prospettiva di una interpretazione evolutiva degli elementi strutturali della fattispecie incriminatrice, a nuove manifestazioni fenomeniche del contesto tecnologico è soluzione percorribile e maggiormente efficace, in molti casi, rispetto ad un approccio interventistico del legislatore penale che potrebbe scontare evidenti criticità di fronte alla rapidità del progresso tecnico. Ma ciò può valere solo in presenza di fattispecie già in astratto suscettibili di plurime chiavi di lettura sotto il profilo dell'oggettività giuridica/offensività[4].

Bibliografia

Chiara P.G., *Towards a right to cybersecurity in EU law? The challenges ahead*, in «Computer Law & Security Review», 53, 2024.

Deibert R.J., *Toward a Human-Centric Approach to Cybersecurity*, Cambridge University Press, 2018.

Flor R., *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, in Militello, Spena, (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, G. Giappichelli Editore, Torino, 2018, 463-481.

Flor R., Marcolini S., *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino, 2022.

Shackelford S., *Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace*, in «Stanford Journal of International Law», 17-55, 2019.

[4] Per ogni ulteriore approfondimento si consenta di rinviare a Flor, *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, in Militello, Spena, (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, G. Giappichelli Editore, Torino, 2018, 463-481; Flor, Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino, 2022.

Sezione Seconda

Capitolo Sesto

Il percorso europeo per il rafforzamento della sicurezza informatica

Simon Pietro Romano

La direttiva NIS2 e il consolidamento della cybersicurezza in Europa

La direttiva NIS2 rappresenta oggi uno dei passaggi più rilevanti nel percorso europeo di rafforzamento della sicurezza informatica. Essa costituisce un'evoluzione significativa rispetto alla prima direttiva NIS, superando le frammentazioni e le diversità di applicazione presenti nei singoli Stati membri. L'obiettivo è creare un quadro normativo omogeneo e integrato, capace di garantire un livello minimo di sicurezza in tutti i settori strategici, favorendo la protezione delle infrastrutture critiche, la resilienza dei servizi essenziali e la continuità delle attività economiche e sociali.

Il cambiamento introdotto dalla NIS2 non si limita agli aspetti tecnici o strettamente regolamentari, ma incide profondamente sulla cultura organizzativa e sulla governance della sicurezza informatica all'interno delle organizzazioni. La direttiva promuove principi fondamentali quali responsabilità, trasparenza e cooperazione tra diversi livelli e attori aziendali, ridefinendo il modo in cui le organizzazioni percepiscono e gestiscono i rischi digitali. In questo contesto, la sicurezza informatica smette di essere vista come un mero obbligo normativo o come un costo accessorio, delegabile al solo reparto IT, e viene riconosciuta come un investimento strategico essenziale. Garantire la protezione dei dati, dei sistemi e dei servizi diventa quindi una componente imprescindibile della gestione complessiva dell'organizzazione, con impatti diretti non solo sulla continuità operativa, ma anche sulla reputazione, sulla fiducia dei clienti, sui rapporti con partner e fornitori, sul rispetto degli obblighi legali e contrattuali.

L'introduzione di responsabilità diretta per i vertici aziendali e manageriali rafforza ulteriormente questa prospettiva, inducendo un cambiamento culturale profondo: la cybersecurity viene integrata nei processi decisionali, nella pianificazione strategica e nella definizione delle priorità aziendali. Non si tratta più di affrontare la sicurezza come una questione "tecnica", ma di considerarla un fattore chiave per la resilienza complessiva dell'organizzazione. Ciò significa investire in strumenti di prevenzione, sistemi di monitoraggio avanzati, audit continui,

piani di risposta agli incidenti e formazione costante del personale. Ad esempio, un attacco ransomware che colpisca una banca o un'azienda energetica può avere conseguenze immediate sulla disponibilità dei servizi, ma anche effetti economici significativi, fino a milioni di euro di perdite, senza contare il danno reputazionale e la perdita di fiducia dei clienti. Analogamente, la divulgazione non autorizzata di dati sensibili in un ospedale o in un'istituzione universitaria può compromettere la privacy degli utenti e comportare sanzioni legali considerevoli, oltre a minare la credibilità dell'organizzazione.

Allo stesso tempo, la trasparenza e la cooperazione, sia all'interno dell'organizzazione che tra enti pubblici e privati, consentono una gestione più consapevole del rischio, favorendo lo scambio di informazioni sugli incidenti, la condivisione di best practice e la costruzione di una resilienza sistemica. La condivisione di indicatori di compromissione, l'adozione di protocolli comuni per la segnalazione degli eventi e la collaborazione tra dipartimenti tecnici, giuridici e di governance diventano strumenti indispensabili per ridurre al minimo gli impatti economici, legali e reputazionali derivanti da violazioni o attacchi informatici. In definitiva, la NIS2 non si limita a imporre obblighi: essa guida le organizzazioni verso un modello di sicurezza integrata, in cui la protezione dei sistemi digitali non è più considerata un onere tecnico o normativo, ma un elemento strategico della gestione del rischio e della sostenibilità organizzativa. L'adozione di questa prospettiva consente alle organizzazioni di affrontare il futuro digitale con maggiore resilienza, capacità di adattamento e consapevolezza dei propri punti deboli, contribuendo a costruire un ecosistema europeo della cybersicurezza più sicuro, coordinato e proattivo.

Uno degli elementi chiave introdotti dalla NIS2 riguarda l'ampliamento significativo dei soggetti coinvolti dalla normativa, con l'obiettivo di garantire una protezione più estesa e coerente del sistema digitale europeo. Non sono più soltanto gli operatori di servizi essenziali (OSE) a essere considerati, come avveniva nella precedente direttiva, ma anche un'ampia gamma di fornitori di servizi digitali, gestori di infrastrutture critiche e un numero crescente di organizzazioni la cui attività, pur non essendo definita strategica in senso stretto, può avere conseguenze sistemiche rilevanti in caso di incidenti informatici. Questo approccio riflette la consapevolezza che, nell'attuale ecosistema digitale, anche servizi apparentemente marginali possono generare effetti a cascata su altre infrastrutture e sull'economia complessiva. Esempi concreti di operatori di servizi essenziali comprendono le reti energetiche, ospedali e strutture sanitarie, servizi idrici, banche e istituti finanziari, oltre a enti della pubblica amministrazione che

gestiscono funzioni critiche per la vita dei cittadini. Ma la NIS2 estende la sua attenzione anche alle infrastrutture ICT, ai fornitori di servizi di telecomunicazione, al settore alimentare e persino alla ricerca scientifica, sottolineando come la continuità operativa di questi ambiti sia fondamentale per garantire la resilienza dell'intero sistema socio-economico. Il criterio centrale adottato dalla direttiva per l'inclusione di tali soggetti è l'impatto sistemico che una compromissione dei loro servizi potrebbe avere: si valuta non solo il danno diretto che un incidente può provocare all'organizzazione stessa, ma anche le ripercussioni sulla vita quotidiana delle persone, sulla sicurezza pubblica, sulla stabilità economica e sulla continuità dei servizi essenziali. In questo modo, la NIS2 riconosce la crescente interconnessione delle infrastrutture e dei servizi digitali, imponendo obblighi di sicurezza proporzionati alla criticità del servizio offerto e alla potenziale gravità degli impatti di un incidente, creando un quadro normativo capace di prevenire, monitorare e mitigare rischi a livello sia locale che transnazionale.

In Italia, il recepimento della direttiva NIS2 è coordinato dall'Agenzia per la Cybersicurezza Nazionale (ACN), che assume un ruolo centrale e strategico nell'intero processo di attuazione. L'ACN non si limita a definire linee guida generali, ma interviene concretamente nell'identificazione, catalogazione e classificazione delle entità soggette agli obblighi normativi, creando un quadro nazionale coerente e aggiornato delle organizzazioni considerate essenziali o importanti per la sicurezza informatica del Paese. Questo processo viene svolto in stretta collaborazione con le autorità settoriali competenti per ciascun ambito, assicurando che le specificità di ogni settore (energia, sanità, telecomunicazioni, trasporti, servizi finanziari, ricerca, tra gli altri) siano correttamente valutate. La raccolta delle informazioni avviene tramite portali dedicati e moduli standardizzati, che consentono di ottenere dati omogenei e confrontabili tra le diverse organizzazioni. Ogni entità deve designare un punto di contatto responsabile della sicurezza, figura chiave nella gestione dei rischi, nella comunicazione con l'ACN e nella supervisione delle misure adottate internamente. Questa catalogazione non ha un valore puramente burocratico: permette di costruire un quadro chiaro, dettagliato e aggiornato, utile a pianificare interventi mirati, a monitorare l'efficacia delle politiche di sicurezza e a garantire una risposta rapida ed efficace in caso di incidenti informatici.

Un aspetto cruciale del lavoro dell'ACN è la capacità di attribuire livelli di priorità differenziati alle varie entità in base alla loro rilevanza strategica e all'impatto sistemico che un eventuale incidente potrebbe generare. In questo modo, le risorse, i controlli e le misure di protezione possono essere concentrate dove il

rischio è maggiore, migliorando la resilienza complessiva del sistema nazionale. Inoltre, le informazioni raccolte vengono integrate nel contesto europeo, favorendo la cooperazione con altri Stati membri e con le agenzie sovranazionali come ENISA, contribuendo alla costruzione di una rete di sicurezza digitale coordinata a livello continentale. Grazie a questo approccio strutturato, l'Italia è in grado non solo di rispondere più efficacemente alle minacce, ma anche di promuovere una cultura della cybersecurity che coinvolge dirigenti, responsabili della sicurezza e personale operativo, rendendo la gestione del rischio un elemento strategico e condiviso all'interno di ogni organizzazione.

Un elemento particolarmente innovativo della direttiva NIS2 riguarda la forte responsabilizzazione dei vertici aziendali e manageriali, che segna un cambio di paradigma significativo rispetto alla gestione tradizionale della cybersecurity. Con la normativa precedente, la sicurezza informatica era spesso considerata una responsabilità tecnica delegata ai team operativi, con limitata attenzione da parte dei dirigenti. NIS2 introduce invece obblighi diretti e specifici per i dirigenti senior, imponendo loro di supervisionare attivamente le misure di sicurezza adottate, di verificare periodicamente l'efficacia dei controlli interni e di garantire che l'organizzazione disponga delle procedure necessarie per rispondere tempestivamente e in modo coordinato agli incidenti. Questa responsabilizzazione riguarda non solo la fase preventiva, ma anche la gestione concreta degli incidenti informatici, comprese le attività di monitoraggio, reportistica e cosiddetta "remediation". Le conseguenze di un eventuale inadempimento sono dirette e significative. Le sanzioni economiche previste dalla direttiva possono arrivare fino al 2% del fatturato annuo dell'organizzazione, un importo che risulta comparabile ai riscatti medi richiesti in caso di attacchi ransomware gravi, sottolineando quanto sia strategico proteggere in anticipo i dati e le infrastrutture critiche. In questo modo, la normativa crea un incentivo concreto per considerare la sicurezza informatica come un investimento strategico piuttosto che un semplice adempimento formale.

L'approccio introdotto da NIS2 ha effetti importanti sul piano culturale: da un lato rafforza la consapevolezza e la responsabilità all'interno dei livelli manageriali, rendendo chi governa un'organizzazione parte attiva nella definizione della postura di sicurezza; dall'altro stimola una mentalità proattiva nei confronti degli investimenti tecnologici, spingendo le aziende e le pubbliche amministrazioni a dotarsi di sistemi di monitoraggio, strumenti di difesa avanzati e programmi di formazione per tutto il personale. La responsabilizzazione dei vertici crea quindi un circolo virtuoso: maggiore attenzione e investimento nella

sicurezza riducono il rischio di incidenti, migliorano la resilienza organizzativa e contribuiscono a proteggere non solo gli asset aziendali, ma anche la fiducia dei cittadini, dei clienti e dei partner commerciali, consolidando un approccio strategico e integrato alla cybersecurity.

Dal punto di vista tecnico, la direttiva NIS2 pone un'enfasi particolare sulla gestione proattiva del rischio e sull'obbligo di notifica rapida degli incidenti informatici, ridefinendo in maniera chiara tempi e responsabilità. Gli enti classificati come operatori di servizi essenziali o fornitori di servizi digitali devono infatti segnalare eventuali incidenti entro 24 ore dalla loro rilevazione, fornendo poi aggiornamenti dettagliati entro 72 ore. Questo sistema di notifiche rapide permette non solo una reazione tempestiva da parte delle autorità competenti, ma consente anche agli altri enti coinvolti di valutare immediatamente la portata della minaccia, predisporre contromisure efficaci e ridurre l'impatto potenziale sugli utenti finali e sul sistema economico. Un aspetto centrale della NIS2 è proprio la condivisione delle informazioni. Questo processo non riguarda solo la mera trasmissione dei dati relativi agli incidenti, ma implica la comunicazione strutturata di indicatori di compromissione (Indicators of Compromise – IoC), che possono includere dettagli tecnici sui malware, vulnerabilità sfruttate o modalità di attacco. La condivisione tempestiva e standardizzata di questi dati permette di prevenire la diffusione di attacchi analoghi verso altre organizzazioni e rafforza la resilienza dell'intero ecosistema digitale europeo, creando un meccanismo virtuoso di apprendimento collettivo. La gestione degli incidenti secondo la NIS2 è articolata in più fasi strettamente coordinate: innanzitutto la rilevazione e l'identificazione della minaccia, seguite dall'analisi tecnica approfondita per comprenderne la natura e le conseguenze; quindi, la notifica agli organi competenti, la documentazione accurata e la reportistica ufficiale, con aggiornamenti continui dei report ogni volta che emergono nuove evidenze o informazioni rilevanti. Questo approccio garantisce trasparenza, tracciabilità e consente alle organizzazioni di apprendere da ogni evento, migliorando progressivamente la postura di sicurezza complessiva.

In Italia, un esempio concreto di gestione integrata degli incidenti è rappresentato dal Security Operation Center (SOC) "HyperSOC" dell'Agenzia per la Cybersicurezza Nazionale. Questo centro raccoglie informazioni provenienti da diversi enti, pubblici e privati, e permette un monitoraggio centralizzato delle minacce informatiche. Grazie ad HyperSOC è possibile coordinare interventi, condividere indicatori di compromissione e supportare la protezione delle infrastrutture critiche in maniera efficace e tempestiva. La presenza di un SOC nazio-

nale consente inoltre di standardizzare procedure, facilitare la cooperazione tra le diverse istituzioni e garantire una risposta rapida agli incidenti che tenga conto delle priorità strategiche, contribuendo a creare un ecosistema digitale europeo più sicuro, resiliente e interconnesso.

Un aspetto centrale della NIS2 riguarda la formazione e la diffusione di una cultura della sicurezza informatica all'interno di tutte le organizzazioni soggette alla direttiva. La normativa non si limita a richiedere lo sviluppo di competenze tecniche avanzate, come la capacità di gestire incidenti, implementare sistemi di protezione o analizzare vulnerabilità, ma sottolinea l'importanza di sensibilizzare l'intero personale aziendale o istituzionale sui principali rischi informatici e sui comportamenti corretti da adottare quotidianamente. Questo approccio implica che ogni individuo, dal personale operativo al management, sia in grado di riconoscere segnali di potenziali attacchi, comprendere l'impatto delle proprie azioni e contribuire attivamente alla protezione delle informazioni e dei sistemi. La direttiva stabilisce che la formazione diventi obbligatoria e parte integrante dei percorsi professionali e accademici, trasformando la cybersecurity in una competenza trasversale che deve permeare l'intera organizzazione. Questo principio si applica non solo ai tecnici informatici, ma anche a dirigenti, manager, figure giuridiche e responsabili di settore, creando un ambiente in cui le decisioni strategiche tengono conto della sicurezza digitale e della gestione del rischio. La promozione di percorsi formativi interdisciplinari, che integrino conoscenze tecniche, normative e manageriali, permette di sviluppare professionalità capaci di operare in contesti complessi, dove la sicurezza informatica non è più un elemento isolato, ma parte integrante della governance organizzativa. Solo attraverso una consapevolezza diffusa e un impegno condiviso è possibile costruire una cultura della cybersecurity solida e sostenibile nel tempo. La formazione continua, unita a esercitazioni pratiche, simulazioni di incidenti e aggiornamenti costanti sulle minacce emergenti, consente alle organizzazioni di anticipare i rischi, ridurre le vulnerabilità e reagire in modo tempestivo ed efficace agli eventi critici. In questo senso, NIS2 promuove un cambiamento culturale profondo, in cui la sicurezza digitale diventa un valore strategico, una responsabilità condivisa e un elemento chiave per garantire resilienza, continuità operativa e fiducia da parte degli utenti, dei clienti e della comunità nel suo complesso.

La classificazione degli enti in operatori di servizi essenziali o in operatori importanti rappresenta uno degli strumenti chiave della NIS2 per la gestione sistematica del rischio informatico. Questa distinzione consente di calibrare in modo mirato gli obblighi normativi, le misure di sicurezza e le risorse disponibili

in funzione del potenziale impatto che un incidente potrebbe avere sull'organizzazione stessa, sugli utenti finali e sull'economia più in generale. Gli operatori di servizi essenziali, come le reti energetiche, gli ospedali, le infrastrutture ICT o i servizi idrici, richiedono requisiti di sicurezza più stringenti e controlli più frequenti, poiché la compromissione di tali servizi può avere conseguenze immediate e sistemiche sulla vita quotidiana della popolazione. Allo stesso tempo, la direttiva non trascura gli altri enti classificati come importanti, ché pur non essendo fondamentali per la sopravvivenza dei sistemi critici, possono comunque influenzare la resilienza complessiva del sistema. Questo approccio permette di allocare le risorse in maniera più efficiente, concentrando gli sforzi e gli investimenti dove il rischio è maggiore, senza generare un falso senso di sicurezza negli ambiti considerati meno critici. In tal senso, la classificazione funziona come un vero e proprio "cuscinetto strategico": garantisce che le infrastrutture più vulnerabili o vitali siano protette prioritariamente, mentre tutti gli altri soggetti rimangono comunque integrati in un quadro complessivo di gestione coordinata della sicurezza. L'obiettivo della direttiva non è dunque quello di eliminare completamente il rischio, un risultato impossibile nel contesto digitale moderno, ma di ridurre al minimo gli effetti negativi degli incidenti informatici. Ciò significa mitigare le interruzioni dei servizi, proteggere i dati sensibili, salvaguardare la continuità operativa e limitare le perdite economiche. Inoltre, un'efficace classificazione e gestione del rischio favorisce la pianificazione preventiva e la reattività agli incidenti, consentendo alle organizzazioni di affrontare le minacce in modo strutturato, coordinato e proporzionato alla loro criticità. Questo approccio integrato contribuisce a rafforzare la resilienza dell'intero ecosistema digitale europeo, promuovendo fiducia, sicurezza e stabilità nei servizi essenziali per cittadini, imprese e istituzioni.

Gli obblighi previsti dalla direttiva NIS2 non si limitano alla semplice implementazione di misure tecniche, ma comprendono un insieme articolato di responsabilità e processi volti a garantire una gestione completa e continua della sicurezza informatica. Tra questi, la gestione accurata della documentazione riveste un ruolo fondamentale: registrare procedure, incidenti, azioni correttive e piani di emergenza consente non solo di dimostrare la conformità normativa, ma anche di creare un archivio operativo da cui trarre lezioni e miglioramenti continui. Parallelamente, la predisposizione di piani di *remediation*, ossia strategie dettagliate per la mitigazione e il recupero in seguito a un incidente, assicura che le organizzazioni siano pronte a reagire in maniera tempestiva e coordinata, riducendo l'impatto sugli utenti, sui servizi e sull'economia. Un altro aspetto

rilevante riguarda la conduzione di test periodici e simulazioni, che permettono di verificare l'efficacia delle misure adottate, identificare vulnerabilità emergenti e allenare il personale a rispondere in modo appropriato a scenari di crisi. Allo stesso tempo, la valutazione dei fornitori e dei partner esterni assume un'importanza crescente: in un ecosistema sempre più interconnesso, la sicurezza di un'organizzazione dipende anche dal grado di affidabilità dei soggetti con cui collabora. La selezione di fornitori conformi a standard di sicurezza elevati e il monitoraggio continuo delle loro pratiche rappresentano quindi strumenti imprescindibili per ridurre i rischi di compromissione attraverso terzi.

In questo contesto, la cooperazione tra enti pubblici e privati assume un ruolo fondamentale e strategico. Non si tratta semplicemente di rispettare procedure comuni, ma di costruire un ecosistema collaborativo in cui la condivisione di informazioni, esperienze e conoscenze diventa uno strumento attivo per aumentare la resilienza complessiva. Condividere best practice permette alle organizzazioni di apprendere dalle esperienze degli altri, evitando di replicare errori già verificatisi e adottando soluzioni collaudate; l'analisi degli incidenti precedenti consente di identificare vulnerabilità sistemiche e comportamenti a rischio, mentre il confronto sulle minacce emergenti facilita la definizione di strategie coordinate per mitigare attacchi comuni. Allo stesso tempo, il monitoraggio degli indicatori di rischio, sia a livello tecnico che organizzativo, permette di reagire tempestivamente a situazioni critiche, riducendo l'impatto di eventuali incidenti e favorendo un approccio proattivo alla sicurezza.

La direttiva NIS2, in questo senso, non si limita a imporre obblighi individuali agli enti soggetti alla normativa, ma promuove una vera e propria cultura collaborativa della sicurezza informatica. La protezione delle infrastrutture critiche e dei servizi digitali non è più considerata un'attività isolata di singole organizzazioni, ma una responsabilità condivisa che richiede trasparenza, fiducia reciproca e un costante aggiornamento delle competenze e delle procedure operative. Ogni ente, sia pubblico che privato, diventa parte di una rete integrata in cui le informazioni scambiate e le esperienze condivise rafforzano la capacità collettiva di prevenire, rilevare e rispondere alle minacce informatiche.

In sintesi, la NIS2 introduce un cambiamento culturale profondo, ridefinendo la sicurezza informatica come elemento centrale della governance e della gestione del rischio. Non si tratta più di un tema marginale o tecnico, confinato ai reparti IT, ma di un fattore strategico che coinvolge dirigenti, responsabili della sicurezza, personale operativo e università nella formazione di figure interdisciplinari capaci di affrontare contesti complessi. La direttiva stimola il ripensamen-

to delle competenze, valorizza la formazione continua, rafforza la collaborazione tra i diversi attori coinvolti e promuove l'integrazione di pratiche di sicurezza nel tessuto organizzativo e decisionale delle istituzioni e delle imprese. In questo modo, l'Europa compie un passo decisivo verso la costruzione di una cultura della cybersicurezza condivisa, in cui la protezione delle infrastrutture digitali e dei servizi critici diventa un pilastro della resilienza, della competitività e della sostenibilità del sistema nel suo complesso, capace di adattarsi rapidamente alle sfide tecnologiche e alle minacce emergenti.

Capitolo Settimo

Competenze e innovazione: il modello delle Accademy

Giorgio Ventre

Mi farebbe piacere impostare il mio intervento trattando di un aspetto importante relativamente a tutto quello di cui si è parlato stamattina, cioè l'aspetto delle competenze e quello dell'innovazione. Un ambito come quello dei crimini informatici e della cyber security richiede chiaramente un aggiornamento continuo e anche una continua tensione per l'innovazione. Devo dire che concordo con quanto diceva il professor Troncone a riguardo del fatto che effettivamente possiamo essere molto fieri come federiciani avendo questo ateneo operato una scelta forte in direzione della multidisciplinarietà, ovvero cercando di rompere le barriere disciplinari e costruire un sapere intersezionale alle settorialità scientifiche.

Sono, infatti, un convinto assertore delle esigenze di eliminare i settori scientifici disciplinari che credo siano veramente una gabbia insostenibile che, tra l'altro, noi accademici ci siamo costruiti attorno ed il caso di SERICS mi sembra andare esattamente nella direzione del superamento delle rigidità dei saperi scientifici. Inoltre, un altro importante passo è stato aprire l'Ateneo alla collaborazione con enti, con organizzazioni, con imprese, perché effettivamente è quello che poi mette noi docenti in grado di creare delle offerte formative e produrre attività di ricerca che alla fin fine poi sono quelle più adatte per voi che seguite questo corso di Scienze criminologiche, investigative e cybersecurity, perché volete una formazione che sia aggiornata, capace, forte, ma anche che sia metodologicamente innovativa. E quindi qui tutto il mio orgoglio federiciano emerge fortissimo.

Quando si parla di competenza nel mondo del digitale, tipicamente si fa un errore. Il primo errore (chi fa questo errore sono essenzialmente gli ingegneri) è quello di pensare che le competenze per il mondo del digitale siano essenzialmente tecnologiche. Questo è vero ma fino a un certo punto. Vi faccio vedere alcune statistiche che sono state elaborate dal Department of Labour degli Stati Uniti su quelle che sono effettivamente delle competenze per i lavori intellettuali e diciamo, in soldoni, questo grafico ci dice che effettivamente queste competenze tecnologiche sono importanti, ma sono ancora più importanti i social e anche *emotional and cognitive skills*. Quindi significa che noi abbiamo bisogno delle

persone che siano preparate non soltanto, appunto, ad affrontare e ad usare la tecnologia, ma anche a collaborare, a renderla disponibile, a comprenderla, digerirla e disseminarne i valori aggiunti.

Bene, ora questo che cosa ci porta? Ci porta a dire che effettivamente quando noi parliamo di tecnologie così evolute, in particolare, con l'arrivo dell'intelligenza artificiale abbiamo sempre di più l'esigenza di interagire con una macchina che, almeno apparentemente, si comporta come ci comportiamo noi. Dico apparentemente perché io sono tra quelli che non ama usare il termine intelligenza artificiale, bensì uso il termine *machine learning*, che è quello più corretto. Però, nonostante questo, noi esseri umani sempre di più andiamo a interagire con dei sistemi che sono molto complessi e che si presentano a noi come se fossero una specie di alter ego, quindi con lo stesso tipo di comportamento. Addirittura, c'è qualcuno che ipotizza uno scenario futuro dove ci siano delle macchine che vanno a sostituire l'uomo, cosa che ritengo difficilissima, almeno in uno scenario decennale. Molto più probabile, invece, uno scenario di collaborazione, ovvero tutti quanti noi saremo sempre più costretti a collaborare con la macchina, anche in task di natura intellettuale, a supporto di quelle che sono le nostre elaborazioni.

E quali sono allora le skills di cui noi abbiamo bisogno?

1) Abbiamo bisogno di capire come la macchina con cui interagiamo si comporti e quindi questo necessariamente richiede delle competenze;
2) abbiamo anche bisogno di capire effettivamente qual è la strategia della macchina, qual è il percorso di funzionamento della macchina;
3) abbiamo anche bisogno di capire come interagire con la macchina.

Ora c'è un problema grosso che tipicamente è sottovalutato sempre dagli ingegneri. Faccio una specie di *mea culpa* culturale. Molto spesso le tecnologie più evolute e più recenti non sono fatte per essere facilmente comprensibili e facilmente utilizzabili dagli esseri umani. Ci sono esempi drammatici. Ne cito uno parzialmente informatico. Voi sapete quale problema è sorto nell'azienda Boeing quando, con il Boeing 737 800 Max, si sono prodotti 2 gravissimi e drammatici incidenti aerei derivanti da una serie di errori a cascata. Diciamo il primo errore:

1) l'aver pensato di trasformare un aereo profondamente e totalmente senza capire quale impatto ci sarebbe stato dal punto di vista della tecnologia del sistema aereo. Questa è la ragione per la quale possiamo attribuire la colpa agli ingegneri aeronautici;
2) altro problema: come addestrare e come sviluppare un software che fosse facilmente utilizzabile dai piloti. E questa responsabilità possiamo attribuirla agli ingegneri informatici;

3) c'è, infine, un altro aspetto che, se mi consentite, riguarda la governance della sicurezza. Il fatto che gli enti che sono preposti negli Stati Uniti per il controllo dell'industria aeronautica e la certificazione hanno attribuito il ruolo di controllore all'azienda che sviluppava l'aeroplano, e quindi un classico corto circuito di controllato che diventa controllore di sé stesso. Tutto ciò ha causato purtroppo una perdita di vite e danni impressionanti, oltre che danni alla stessa azienda, che in questo momento è ancora in una crisi profonda.

Che significa fare trasferimento di conoscenza e formazione? Allora nel Medioevo (parto dal Medioevo perché noi della Federico II abbiamo festeggiato gli 800 anni) la conoscenza era essenzialmente connessa alla lettura e interpretazione delle scritture e occorreva avere una buona competenza a riguardo della logica. Con la rivoluzione scientifica vengono abbandonate le scritture che, con tutto il rispetto, non erano una base di conoscenza scientifica sufficiente, e si comincia, grazie a Galileo, a capire che la conoscenza è basata su dati empirici, cioè esperimenti, prove, metodo e, diciamo, una buona dose di matematica.

Paradossalmente adesso quello che dobbiamo fare è costruire sulla base della conoscenza che abbiamo e che continuiamo a produrre e accumulare; però dobbiamo sempre ricordarci che siamo esseri umani. Cioè, paradossalmente, nel momento in cui noi parliamo con le macchine, dobbiamo assolutamente difendere il nostro modo di ragionare come esseri umani, perché soltanto facendo in questo modo noi riusciremo effettivamente a utilizzare al meglio quello che è il potenziale delle tecnologie che noi stessi sviluppiamo, perché la tecnologia in un certo senso si auto-svilupperà.

Detto questo, qual è il ruolo dell'Università oggi? Fino all'inizio dell'Ottocento, il ruolo dell'università era essenzialmente didattico, quando Federico II crea l'università, la vede come un luogo di apprendimento, non come un luogo di ricerca. Infatti, l'attività di ricerca era essenzialmente sviluppata all'interno delle accademie, era esterna all'università. A Napoli abbiamo uno degli esempi (ahimè, dimenticati) di Accademia, quella fondata da Giovan Battista della Porta, l'accademia dei segreti, che era un'accademia che riuniva questi coraggiosi innovatori ricercatori per cercare di rompere i segreti della natura. Oggi l'università ha un ruolo che si concentra su tre punti che sono: l'insegnamento, la ricerca e il trasferimento tecnologico. Però, mentre fino a poco tempo fa queste tre cose erano viste soltanto debolmente interconnesse, oggi, queste tre cose devono essere fondamentali, cioè non si può fare insegnamento senza fare ricerca decente e non si può fare ricerca decente senza fare trasferimento tecnologico; perché soltanto

capendo quali sono le conseguenze e i risultati delle nostre attività di ricerca possiamo effettivamente avere un impatto sul nostro territorio.

E il campus di San Giovanni nasce con questa filosofia. Nasce, in teoria, in origine, come una estensione. Abbiamo deciso con il precedente rettore Manfredi di attivare all'interno di questo campus delle attività che fossero essenzialmente attività di collaborazione con le imprese.

Che cosa noi facciamo oggi nell'Ateneo federiciano? Per chi non c'è mai stato, vi invito a visitarlo, perché effettivamente è uno spazio divertente, molto dinamico. L'idea è quella di fare attività di didattica tradizionale, ma affiancare a queste attività di didattica tradizionale tutte attività di didattica e di innovazione sviluppate in collaborazione con le imprese.

Vi faccio vedere un po' delle imprese che sono attualmente presenti nel campus, a vario termine e a vario titolo, con diverse tipologie di collaborazione. Come vedete, all'interno di questo lungo elenco di imprese e di soggetti c'è anche, appunto l'ACN, che sarebbe l'autorità per la cyber sicurezza nazionale che, come stesso loro hanno detto stamattina, ha localizzato da noi un centro di *high performe computing* dedicato agli aspetti della cyber sicurezza e che sarà gestito insieme con il Cineca.

Ora, noi, in questo campus, che cosa facciamo? Facciamo tre cose. (i) Facciamo formazione, anche se a me fa più piacere definirla come trasferimento di competenze; (ii) facciamo trasferimento tecnologico; (iii) e poi facciamo programmi di creazione e di accelerazione delle start up.

Sulla formazione, noi abbiamo lanciato questo modello, quello delle Accademy. Le Accademy nascono con questa idea. Resto convinto che la qualità della formazione accademica italiana e quella della Federico II sia eccellente, altrimenti non ci spiegheremmo perché tantissimi talenti e colleghi che sono formati alle nostre università hanno un successo così forte all'estero, altrimenti sarebbe un'evidente contraddizione. Però, un problema che in realtà non è un problema, bensì un limite e che noi siamo consapevoli di avere, attiene la formazione accademica italiana la quale è prevalentemente metodologica; ciò costituisce un'assicurazione sulla vita professionale perché fa sì che tu hai delle competenze che durano più tempo nel tempo, e sono anche autonome (per esempio permettono di sviluppare una capacità di critica circa la tecnologia), però per altro verso, esse effettivamente sono poco pratiche.

Invece di cambiare, allora, l'università, che è difficile e forse anche sbagliato, abbiamo cercato di affiancare ai corsi universitari dei corsi che tendono a complementare queste competenze attraverso l'interazione con le aziende ed è così che

nascono l'esperienza di Apple, quella di Cisco, Deloitte, peraltro non soltanto nel settore della tecnologia digitale, perché cito altre Accademy che stanno avendo un grande successo, quello del polo nazionale Agritech, quello sui nuovi farmaci del polo nazionale, quello sull'ingegneria strutturale, eccetera, eccetera.

Un'Accademy di cui parlo veramente, brevemente, è quella della Apple, ma ne parlo semplicemente perché vorrei essenzialmente concentrarmi sulle differenze di approccio tra la formazione che noi diamo a livello universitario e la formazione che diamo attraverso queste Accademy. Nell'Accademy di Apple utilizziamo una metodologia *challenge base learning*, cioè, è una metodologia estremamente sperimentale, pratica, che chiede che i discenti partecipino ad attività di formazione, andando a sviluppare software e andando a risolvere challenge. Il che significa quindi che l'apprendimento è molto pratico, cioè noi, nell'Apple Accademy non usiamo testi, non usiamo power point, ma cerchiamo di fare in modo che i ragazzi apprendano le tecnologie cercando di sviluppare progetti, partecipando direttamente allo sviluppo di progetti, e questo cambia anche il ruolo del docente. Infatti, i nostri docenti, che non sono docenti della Federico II, sono stati docenti che sono stati arruolati con competenze sia sul piano della formazione che sullo sviluppo di tecnologie.

Noi parliamo di Mentor, perché in realtà il docente diventa un accompagnatore di questa fase di apprendimento, che vede lo studente assolutamente protagonista. I nostri spazi sono assolutamente stati disegnati per favorire questo. Non ci sono le aule classiche con i banchi e con le cattedre, ma abbiamo piuttosto spazi che favoriscono la collaborazione e tutti i progetti che i nostri ragazzi sviluppano sono di gruppo. Non abbiamo voti, ma abbiamo un'analisi delle competenze e dell'auspicabile accrescimento delle competenze che noi facciamo anche con degli strumenti di elaborazione molto complessa. Abbiamo poi degli spazi che fanno sì che questi ragazzi, dopo la fase in questi laboratori possano continuare a lavorare con noi, e quindi abbiamo degli spazi che definiamo spazi di *coworking*, che aiutano e supportano sempre la capacità degli studenti di lavorare in gruppo. E poi abbiamo tanti altri spazi al servizio che sono stati progettati proprio per fare in modo di creare questa esperienza di sviluppo collaborativo tra mentor e studenti e tra studenti. Questo si traduce nel fatto che ogni anno noi abbiamo 300 studenti. Questi studenti ogni 3 mesi sono chiamati a sviluppare un progetto. L'Accademy dura 9 mesi e ogni 3 mesi gli studenti sono chiamati a sviluppare un progetto. E questo progetto è tipicamente un app. Ogni anno vengono prodotte dai nostri studenti 140-150 app e di queste una cinquantina/sessantina vanno a finire in Apple store e sono di proprietà degli studenti. Cioè,

non sono di proprietà della Federico II e men che meno di Apple. Per questo c'è questo concetto di *challange base learning*, la risoluzione di un problema è non soltanto fatta dallo studente, ma lo studente è il proprietario della soluzione che propone, e questo lo rende protagonista.

Chiaramente noi facciamo una grande attenzione anche a collaborare con le imprese, perché il fine nostro ultimo è quello di dare non soltanto delle opportunità di lavoro ai nostri studenti, ma noi vogliamo dare agli studenti la capacità di scegliersi il lavoro che desiderano. Abbiamo circa 350 aziende di tutto il mondo che collaborano con noi, che vanno da Ferrari fino ad Asos fino alla stessa Apple e altre aziende internazionali. E in questo, diciamo, si innesca la seconda fase di quello che noi facciamo all'interno del campo di San Giovanni, che è la fase connessa all'innovazione. Perché per noi la collaborazione con le imprese funziona non soltanto se noi condividiamo questi progetti di formazione, ma se noi collaboriamo con le imprese per portare ad esse innovazione.

Noi seguiamo questo modello dell'*open innovation* dove effettivamente le aziende non fanno attività di ricerca o non soltanto al proprio interno, ma cercano di aprirsi per cercare di coinvolgere all'interno dei propri processi di innovazione soggetti esterni, perché l'innovazione oggi è talmente veloce che è difficile confinarla o ridurla all'interno di una stanza chiusa. Oggi le grandi aziende multinazionali digitali fanno un po' di innovazione al proprio interno, ma comparano tantissima innovazione all'esterno. È il caso di Cisco, Apple, ecc.

Quindi noi facciamo attività di collaborazione con le aziende che sono sia internazionali, ma anche grandi aziende italiane come Enel, Eni, Terna, Leonardo, eccetera.

L'ultima cosa di cui voglio parlare è l'importanza di aggiungere a queste 2 gambe, la terza gamba che è quella delle startup. Le startup e gli spinoff sono importanti nella vita di una università per una serie di fattori. In primo luogo, perché sono un modo concreto e pratico di fare trasferimento tecnologico, cioè un giovane ricercatore, un giovane Professore che ha un'idea, ha realizzato un prototipo, riesce così a creare qualcosa di concreto che poi può andare a finire sul mercato, direttamente o attraverso una grande azienda che acquista queste competenze. In secondo luogo, perché migliora la capacità del nostro sistema industriale di attrarre e di mantenere i nostri talenti. Il problema che noi abbiamo tantissimi ragazzi che escono dalle nostre lauree e vanno all'estero è perché si sentono apprezzati all'estero, sono valorizzati immediatamente, a fronte delle nostre imprese nelle quali non vedono spazi di crescita professionale e riconoscimento professionale. E questo è tristissimo. Paradossalmente, noi stiamo vedendo che i

ragazzi che escono dai nostri corsi di laurea, sia le Accademy ma anche i corsi di laurea, sono molto più affascinati dalle start up piuttosto che dalla grande impresa tradizionale, dove loro si sentono molto costretti e con poca capacità di crescita e poca capacità di portare dei propri contributi. E infine, perché comunque sono dei fattori di innovazione.

All'interno di San Giovanni abbiamo non l'incubatore della Federico II, che è la città della scienza, almeno per il momento, però noi abbiamo la capacità di fare programmi di accelerazione di queste startup che noi sviluppiamo in collaborazione con diverse imprese e aziende che sono sul territorio.

Ecco, questa è la storia che volevo raccontare. Diciamo, c'è una verticale specifica sulla cyber security che prevede un Accademy con Accenture sulla cyber sicurezza e che quest'anno è stata anche patrocinata dall'Agenzia per la cyber security nazionale. Abbiamo attività di ricerca sulla Cyber security con Accenture, con Leonardo e con altre imprese. E quindi questo diciamo fa vedere come effettivamente l'ecosistema che abbiamo realizzato come Federico II a San Giovanni, effettivamente funziona molto bene anche in un settore così verticale, così specifico come quello della cyber security. D'altra parte, la ragione per la quale abbiamo aderito sin dall'inizio alla proposta di produrre o, meglio, partecipare ad un corso di laurea magistrale in Scienze criminologiche, investigative e di cybersecurity è perché siamo convinti che l'aspetto della cybersecurity aziendale e delle organizzazioni istituzionali amministrative e non costituirà in futuro la sfida da affrontare quotidianamente. Grazie per la Vostra attenzione.

Capitolo Ottavo

L'evoluzione dell'architettura nazionale in materia di sicurezza cibernetica e il ruolo dell'ACN

Gianluca Ignagni

Buongiorno, rivolgo innanzitutto un grande ringraziamento al Dipartimento di Scienze Politiche della Federico II e al professor Di Gennaro, perché le iniziative come questa sono molto importanti per contribuire a elevare i livelli di consapevolezza che costituisce un elemento decisivo per la resilenza del Paese.

Gli ultimi anni sono stati caratterizzati da un'intensa digitalizzazione della società, che ormai pervade tutti i campi della nostra vita. Questo processo di digitalizzazione è stato portato avanti mettendo al centro l'attenzione alla facilità d'uso e alla rapidità, ma con scarso interesse per i principi di sicurezza. Si tratta di una impostazione che scontiamo, poi, nella quotidianità, perché il numero degli attacchi continua ad aumentare di pari passo con l'aumento della superficie digitale esposta. Questo ci deve essere di lezione, soprattutto rispetto alle più recenti – e alle future – innovazioni tecnologiche. Ci troviamo già in una fase avanzata di diffusione dell'intelligenza artificiale e, avendo l'esperienza di altre tecnologie, è necessario non farsi cogliere impreparati, ma adottare fin da principio un concetto di *security-by-design* e *security-by-default*. In altre parole, dobbiamo far sì che le applicazioni di intelligenza artificiale che useremo domani nascano, già oggi, con la cybersicurezza come primaria preoccupazione. Si tratta di un approccio indispensabile per gestire con lungimiranza questa tecnologia, che ha impatti di varia natura, da quella etica a quella tecnologica, nonché di sicurezza. Se pensiamo che da molti l'intelligenza artificiale è paragonata all'invenzione e alla diffusione dell'energia elettrica, è evidente che occorre adottare il giusto approccio.

Tornando all'aumento della superficie digitale e conseguentemente degli attacchi informatici, occorre fare una riflessione più generale. Si leggono dati non sempre omogenei, poiché si risente della mancanza di definizioni condivise. Più nel dettaglio, manca una tassonomia comune a livello internazionale su cos'è un attacco informatico e su quali sono le specifiche tipologie. Rileva ricordare, poi, che di sicurezza cibernetica si parla spesso sotto profili diversi e, chiaramente, a profili diversi corrispondono anche dati diversi. Perché un conto è il dato relativo al reato informatico – e quindi le cifre riguardano i reati che vengono denunciati

– altro conto è quello che concerne gli attacchi cibernetici. Tale affermazione è valida anche in un sistema come quello italiano, in cui ogni attacco informatico finisce generalmente per costituire un reato. Nonostante questa precisazione sulla non perfetta coincidenza tra i dati forniti da soggetti diversi, si può comunque dire che le tendenze sono sostanzialmente le stesse. In questo contesto, ritengo importante evidenziare come il legislatore abbia individuato l'Agenzia per la cybersicurezza nazionale (ACN) quale *hub* nazionale delle notifiche di incidenti cyber: riceve, cioè, le segnalazioni degli incidenti informatici previste dalla normativa cyber (in particolare, il Perimetro di sicurezza nazionale cibernetica, la legge n. 90/2024 e la NIS). Questo perché, ovviamente, avere un centro unico di raccolta di tali informazioni ne consente l'analisi e l'elaborazione, ma anche le necessarie attività di controllo, prevenzione e allertamento.

L'aumento degli attacchi è estremamente rapido se pensiamo che, limitandoci a quelli che risultano all'ACN, tra il 2023 e il 2024 complessivamente sono raddoppiati. Che tipi di attacchi vediamo? Si può fare una fondamentale distinzione, sul piano tecnico, tra diverse categorie. Una delle più rilevanti numericamente è costituita dagli attacchi DDoS, ovvero quegli attacchi che impediscono la disponibilità di un servizio online e che vengono, prevalentemente, portati avanti per finalità di attivismo, risultando molto legati alle tensioni geopolitiche. Questi attacchi tendono a non avere un impatto particolarmente significativo da un punto di vista informatico, anche perché è possibile irrobustire le difese delle organizzazioni per prevenirli.

Attacchi particolarmente pericolosi sono i *ransomware* che colpiscono per l'80% le piccole e medie imprese. Ciò dipende, in larga parte, dal fatto che queste spesso sono meno protette e presentano un livello più basso di maturità cyber. Occorre, inoltre, segnalare che non sempre l'impatto dei *ransomware* diventa noto perché, al fine di non avere un danno di immagine, alcuni soggetti non lo riportano. Sul *ransomware*, e sugli eventuali obblighi di denuncia, si potrebbe fare un approfondimento a parte – pure a livello universitario e di ricerca – anche in merito al pagamento (o meno) del riscatto e alla tematica delle assicurazioni. A ogni buon conto, l'ACN ha una visibilità più definita sul fenomeno *ransomware* quando questo va a colpire delle infrastrutture critiche, ad esempio gli ospedali. Al riguardo, abbiamo avuto alcuni casi concreti in cui da un attacco *ransomware* è derivato il blocco dei reparti di rianimazione o delle sale operatorie. In questi casi l'impatto effettivamente diventa particolarmente significativo e carico di conseguenze.

È importante soffermarsi anche sul tipo di attori principali che l'ACN ha visto muoversi. Gli attori malevoli possono essere statuali e non statuali, cosa

che determina delle differenze significative. Per quanto riguarda il *ransomware* tendenzialmente siamo in un ambito criminale e gli attori sono prevalentemente non statuali. Ma vi è una terza categoria della minaccia, alla quale non ho ancora fatto riferimento, che è la più pericolosa, benché numericamente meno rilevante, perché è quella maggiormente impattante, cioè gli APT. I cosiddetti *Advanced Persisten Threat* sono attacchi di natura persistente che richiedono una particolare sofisticatezza; vengono portati avanti in genere da attori statuali o parastatuali, sostanzialmente con finalità di spionaggio o, in alcuni casi, perfino di *disruption*. Difatti, nel momento in cui un attaccante riesce a ottenere il pieno controllo di un sistema, può sia esfiltrare dati, sia provocarne l'inefficienza o alterarne il funzionamento. Ciò rischia di avere, ovviamente, impatti notevoli, teoricamente anche con ripercussioni in ambito cinetico, specie se vengono coinvolte infrastrutture critiche o altri *target* strategici. Come detto, tra tensioni geopolitiche e attacchi informatici possono esserci collegamenti diretti o indiretti.

Un ulteriore elemento di attenzione, a tale proposito, riguarda le tecnologie non sicure e la loro presenza nella *supply chain*. Le tecnologie non sicure, infatti, spesso finiscono per rappresentare uno dei principali vettori degli attacchi, così come le catene di approvvigionamento. Proprio questo è stato uno degli aspetti di novità introdotti dalla direttiva NIS2, che ha previsto di dedicare attenzione all'intera filiera e alla *supply chain* di prodotti e servizi cyber. Quando pensiamo alla cybersicurezza dei grandi operatori è chiaro che, trattandosi di attori strutturati e attenti alla materia, questi hanno in essere misure di sicurezza informatica particolarmente elevate. Lo stesso però non si può sempre dire dei loro fornitori e, data l'elevata interconnessione dei sistemi, un attacco può coinvolgere un grande operatore passando proprio per la sua catena di approvvigionamento. Un altro tema che anche i grandi *player* non possono ignorare è il fattore umano, che rimane il principale vettore sfruttato dagli attaccanti. Le carenze nelle competenze e nelle pratiche di igiene informatica sono, a tutti gli effetti, il "tema dei temi" perché lo riscontriamo costantemente come uno dei problemi maggiori.

Analizzando quali siano i beni che vengono messi a rischio dagli attacchi informatici, abbiamo già parlato delle funzioni e dei servizi essenziali garantiti attraverso le infrastrutture critiche. Ma non possiamo dimenticare, come richiamato anche dal professor Colapietro, che possono risultare compromessi anche i diritti costituzionali, quale ad esempio il diritto alla salute. Quando avviene un attacco *ransomware* a una struttura ospedaliera è proprio questo diritto a esser messo in discussione perché, se l'attacco va in porto, impedendo l'accesso alle cure non viene di fatto garantito l'esercizio del diritto alla salute. Ma gli attacchi

possono arrivare a esporre al pericolo anche i beni più importanti per la comunità nel suo complesso, come la sicurezza nazionale. Se pensiamo a un attacco capace di bloccare l'intera rete di distribuzione dell'energia elettrica nel Paese, è evidente che è la stessa sicurezza nazionale a essere messa a repentaglio.

Passando a quanto l'ACN ha potuto riscontrare nei suoi primi tre anni di vita, possiamo iniziare a delineare un quadro d'insieme. Tendenzialmente tra gli elementi che risultano piuttosto costanti, ci troviamo a confrontarci con sistemi obsoleti. Ciò dipende sia dalle difficoltà di sostituzione, sia da una scarsa attenzione alla cybersicurezza. Molto spesso, infatti, il sistema obsoleto ha un problema intrinseco, poiché non è più aggiornabile e, quindi, risulta maggiormente esposto alle vulnerabilità. A ciò si aggiungono le carenze quali-quantitative del personale dedicato alla cybersicurezza, e più in generale del personale impiegato nella gestione dei sistemi. Abbiamo riscontrato, infatti, significative lacune nella definizione e nell'implementazione delle politiche di sicurezza, politiche che permetterebbero di rafforzare la resilienza contro gli attacchi. Tutta questa situazione, e mi riallaccio alle parole del professor Romano, è alla radice una questione di mentalità. Se gli amministratori delegati delle aziende e i vertici delle Pubbliche Amministrazioni non hanno un adeguato livello di consapevolezza cyber, il risultato è che non si investe abbastanza e ciò, a cascata, ha riflessi sulle carenze nelle policy.

Come reagire e cosa si può fare per ovviare a questi problemi? La risposta chiaramente deve essere multi-stakeholder e multilivello, oltre che globale. Multilivello perché la risposta deve avvenire sicuramente su più piani: regolatorio, per quanto riguarda la prevenzione, l'allertamento e l'accompagnamento, ma anche su un piano tecnologico, oltre che della formazione e della consapevolezza, nonché sull'impiego delle risorse e nell'ambito della collaborazione internazionale.

Sul piano regolatorio cosa abbiamo visto? Seguo questa materia da una decina d'anni e ho potuto assistere a un'evoluzione dell'architettura nazionale di sicurezza cibernetica, proprio tramite l'utilizzo degli strumenti normativi. Molto è cambiato anche riguardo alle diverse Istituzioni che hanno compiti attinenti alla cybersicurezza. La prima normativa in materia è una direttiva del Presidente del Consiglio dei ministri del 2013, adottata con DPCM, con la quale veniva creato il primo Nucleo per la sicurezza cibernetica per la gestione degli incidenti, nell'ambito di un ufficio di diretta collaborazione del Presidente del Consiglio dei ministri, l'Ufficio del Consigliere militare.

Nel 2017, poi, l'architettura cambia: non solo viene rielaborata la prima strategia nazionale di sicurezza cibernetica, ma si inizia a determinare uno sposta-

mento delle competenze istituzionali per i profili di resilienza all'interno del Dipartimento delle informazioni per la sicurezza (DIS). In questo contesto, anche il Nucleo per la sicurezza cibernetica viene spostato all'interno del DIS, ovvero di quell'Organismo di intelligence che ha funzioni di coordinamento rispetto alle due Agenzie (AISE e AISI). Il DIS, poi, assume anche ulteriori nuovi compiti in questo ambito, come il *Computer Security Incident Response Team* (CSIRT), cioè la struttura che è deputata a livello nazionale alla gestione degli incidenti, che riceve le notifiche, e il Punto di contatto con l'UE previsto dalla direttiva NIS1. Così facendo, progressivamente, viene attribuito al DIS un ruolo centrale nella sicurezza cibernetica del Paese.

Si arriva, infine, nel 2021 all'emanazione del DL n. 82, poi convertito con la legge 4 agosto 2021, n. 109, con il quale viene ridefinita l'architettura istituzionale cyber e viene istituita per la prima volta un'agenzia specializzata, l'ACN, quale Autorità nazionale per la cybersicurezza, recuperando un divario di diversi anni rispetto ai principali Paesi europei. Vengono, inoltre, ripartite le varie competenze in materia cyber: la resilienza viene seguita dall'ACN, la prevenzione e il contrasto al *cyber-crime* dalle Forze di polizia, e in particolare dalla Polizia postale e per la sicurezza cibernetica, la difesa militare dello Stato dal Ministero della difesa, la *cyber-intelligence* dagli Organismi di informazione e, come elemento trasversale, la *cyber-diplomacy* è presidiata dalla Farnesina. Viene, altresì, istituito presso l'ACN il Nucleo per la cybersicurezza, che rappresenta il punto di collegamento e di coordinamento in materia, prevedendo la responsabilità in capo al Presidente del Consiglio dei ministri. Nasce, inoltre, un dedicato Comitato interministeriale – il Comitato interministeriale per la cybersicurezza – che costituisce la sede di coordinamento a livello politico-strategico, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

Negli anni abbiamo assistito anche a una costante integrazione del quadro europeo con quello del nostro Paese, attraverso il succedersi di direttive e regolamenti a livello UE e di DPCM e norme di rango primario in ambito nazionale. Questo spostamento verso l'alto nelle fonti impiegate per la disciplina della sicurezza cibernetica rappresenta un aspetto importante che può suscitare riflessioni e approfondimenti in ordine al progressivo rilievo che questa materia ha assunto per la tutela dell'ordinato vivere civile, divenendo la "sicurezza delle sicurezze". A livello UE, il progressivo spostamento dall'utilizzo delle direttive a quello dei regolamenti è legato anche all'esigenza di raggiungere una maggiore omogeneità tra i 27 Stati membri, visto che la direttiva richiede un recepimento a livello nazionale (consentendo una maggiore autonomia per gli Stati membri), mentre

il regolamento è, come noto, direttamente applicabile, per cui l'intervento degli Stati membri è "limitato soltanto" ai necessari adeguamenti degli ordinamenti nazionali. Se pensiamo, infatti, alle ultime norme UE in ambito cyber, solo la NIS2 è stata adottata con direttiva, mentre le altre sono tutte intervenute tramite regolamenti, ad esempio, l'AI Act, il Cyber Resilience Act, il Cyber Security Act; quindi, tendenzialmente tutte le principali innovazioni normative in ambito cyber sono state introdotte con dei regolamenti.

Tornando al rapporto di costante allineamento tra normativa europea e normativa nazionale, abbiamo recepito la direttiva NIS nel 2018, e l'Italia ha fatto poi la scelta – come non molti Paesi europei – di arrivare nel 2019 a costituire un Perimetro di sicurezza nazionale cibernetica (PSNC). Questo perché, come detto prima, tra i beni che possono essere messi a rischio dagli attacchi cyber rientra la sicurezza nazionale. Con il PSNC è stato previsto un insieme di norme volte a tutelare quei soggetti che, con termine poco tecnico, possiamo definire "i gioielli di famiglia", cioè i soggetti maggiormente importanti ai fini della sopravvivenza stessa del Paese e che, pertanto, devono seguire delle norme di sicurezza cibernetica particolarmente elevate. Se per i soggetti che ricadono nella NIS2 la tempistica prevista per assolvere all'obbligo di notifica è di 24/72 ore (entro 24 ore è richiesta una pre-notifica ed entro 72 ore la notifica vera e propria), per i soggetti che rientrano nel Perimetro di sicurezza nazionale cibernetica, il termine per la notifica è entro un'ora o entro sei ore (da quando il soggetto ha avuto conoscenza dell'incidente), a seconda della tipologia di incidente. Un ulteriore aspetto importante riguarda la sicurezza delle tecnologie, che è stata messa al centro del Perimetro, sempre perché ci muoviamo nell'ambito della sicurezza nazionale. Ne è un esempio il fatto che viene previsto lo scrutinio tecnologico dei beni e servizi da acquisire, destinati ad essere impiegati su quei beni, sistemi e servizi del soggetto Perimetro funzionali ad assicurare una funzione o un servizio essenziale per la sicurezza nazionale. È stato, infatti, introdotto un meccanismo – che oggi viene assicurato dall'ACN attraverso il Centro di valutazione e certificazione nazionale (CVCN) – per il quale i soggetti in fase di *procurement* devono notificare l'intenzione di acquisire determinate forniture ICT, rispetto alle quali vengono effettuate delle verifiche tecniche per accertare la sicurezza e l'assenza di vulnerabilità. Tale previsione si collega molto direttamente al tema della sicurezza e dell'affidabilità delle tecnologie su cui mi sono soffermato all'inizio del mio intervento.

Arriviamo, da ultimo, alla legge n. 90 del 2024, composta da due capi: uno relativo alle questioni di natura penale e uno incentrato sul rafforzamento della

resilienza cibernetica. Per quanto concerne questa seconda parte, gli interventi del legislatore sono stati mirati ad assicurare quel costante aggiornamento del quadro regolatorio basato sull'attività di controllo continuativa sull'applicazione delle norme per andare sistematicamente a trovare soluzioni rispetto a quei buchi che la prassi esperienziale ha dimostrato andassero colmati. La prassi aveva, ad esempio, dimostrato che le tecnologie non sicure sono un possibile rischio. Al riguardo, la legge n. 90 ha previsto che, laddove vengono in gioco interessi strategici, tutti i soggetti che sono sottoposti al Codice dell'amministrazione digitale, nonché quelli privati inseriti nel PSNC devono tenere necessariamente conto nelle relative attività di *procurement* degli elementi essenziali di cybersicurezza definiti in un apposito DPCM, adottato su proposta dell'ACN. Questo perché curandosi solo del principio del minor prezzo nel *procurement*, il rischio è di andare al ribasso anche sulla sicurezza. Si tratta di un meccanismo, questo, da disincentivare, per cui è stata introdotta questa nuova disposizione volta a colmare tale divario in tema di sicurezza e delle tecnologie che vengono fornite. La medesima disposizione (l'articolo 14) prevede, altresì, che laddove sia in gioco la sicurezza nazionale e vadano acquisite tecnologie devono essere stabiliti criteri di premialità a favore delle tecnologie nazionali, di quelle provenienti da Paesi UE, NATO oppure da Paesi che con l'UE e con la NATO hanno accordi di collaborazione in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Un altro elemento di novità della legge n. 90 è che ha provveduto a stabilire i rapporti e il bilanciamento tra attività di resilienza e attività giudiziaria. Si tratta di un aspetto particolarmente importante, anche se magari non sempre notato. Qualsiasi intervento che viene effettuato da parte dell'Agenzia come attività di resilienza ovviamente implica la necessità di intervenire sui sistemi impattati per favorire un'immediata ripartenza. Non si può, però, ignorare che nella grande maggioranza dei casi si sta intervenendo su una scena del crimine perché un attacco è anche un reato informatico. In proposito, la legge istitutiva dell'Agenzia aveva previsto un primo meccanismo di collegamento tra resilienza e attività investigativa, prevedendo come la comunicazione – da parte dell'ACN alla Polizia postale – di ogni notifica di incidente ricevuta costituisca adempimento dell'obbligo di cui all'art. 331 del c.p.p (denuncia da parte di pubblico ufficiale e incaricato di un pubblico servizio). Nella legge istitutiva non era però disciplinato il rapporto tra ACN e Autorità giudiziaria. Tale rapporto viene regolato con la legge n. 90, che ha anche introdotto specifici meccanismi di collegamento tra l'Agenzia e la Direzione nazionale antimafia e antiterrorismo (ulteriormente precisati attraverso un dedica-

to protocollo di intesa) oltre che mirate disposizioni per definire anche i rapporti con le Procure, con la previsione della possibilità per il Pubblico ministero di interrompere o ritardare alcune attività di resilienza per non pregiudicare le attività investigative con impatti sul procedimento penale. Gli equilibri e i bilanciamenti sono, infatti, fondamentali in questo contesto perché, ritornando all'esempio fatto prima (l'attacco a una Asl o a un ospedale che blocca l'operatività di una terapia intensiva), c'è sia l'esigenza di tutelare la scena del crimine, sia l'esigenza di far riprendere senza ritardi tutte le attività dell'ospedale. La legge n. 90 ha, pertanto, avuto l'indubbio merito di definire una disciplina molto equilibrata e basata su un corretto bilanciamento tra esigenze concorrenti.

Collegandoci all'importante tema della prevenzione e dell'allertamento, bisogna anche sottolineare la rilevanza dell'attività di accompagnamento. Il fatto che il professor Romano abbia utilizzato alcune *slide* di ACN mi fa molto piacere, perché è sintomatico dell'efficacia delle iniziative di accompagnamento all'applicazione della normativa che stiamo portando avanti, a partire da quella organizzata all'Università Sapienza di Roma con circa 2.000 persone per illustrare la nuova normativa NIS2. In tutti questi casi l'ottica è proprio quella di favorire e accompagnare le aziende, al di là della sanzione, nell'applicazione della normativa.

Sul piano tecnologico, poi, molto si sta facendo nell'ambito della ricerca e dello sviluppo. Si è parlato dell'autonomia tecnologica, delle carenze da un lato e, dall'altro, degli esempi virtuosi di HPC che stiamo realizzando nel Paese. Chiaramente l'attività di ACN non può da sola rappresentare garanzia di sicurezza, ma occorre una complessiva attività di ecosistema, fatta con le altre Amministrazioni, con l'Università, col mondo della ricerca e con il mondo privato. Tra gli esempi di successo possiamo certamente contare l'HPC che stiamo realizzando a Napoli per l'Hyper-SOC, ma anche la vincita di un progetto europeo delle AI Factory per realizzare, a Bologna, un altro computer HPC che permetterà lo sviluppo di strumenti di intelligenza artificiale, anche a favore delle imprese e della ricerca.

In tema di risorse, pur nella limitatezza rispetto al quadro esigenziale, tante cose si stanno facendo, anche grazie ai fondi PNRR, nel cui ambito l'Agenzia è stata designata soggetto attuatore per un intervento da 623 milioni di euro finalizzato al potenziamento della cybersicurezza. Nella legge di bilancio del 2023, poi, sono stati previsti fondi per l'attuazione della Strategia nazionale di cybersicurezza, che prevedono dei fondi strutturali. Fino al 2037 l'insieme di questi fondi sta consentendo, e consentirà, di svolgere molte attività, in particolare per alzare il livello di sicurezza delle Amministrazioni partendo dalla conoscenza delle

proprie infrastrutture IT. Sembra un qualcosa di scontato, ma non lo è. Risulta, infatti, fondamentale capire quali sono gli asset tecnologici di cui si dispone, qual è il livello di sicurezza e, dopodiché, fare tutti gli *upgrade* necessari. Al riguardo, abbiamo un insieme di riscontri di attività fatte che hanno consentito tra il 2022 e il 2024 alle Amministrazioni di raddoppiare i loro livelli di sicurezza cibernetica. Stiamo usando questi fondi anche per progetti quali l'Hyper-SOC, che è stato citato prima, o l'ISAC nazionale. Anche qui c'è un tema di consapevolezza e noi siamo molto soddisfatti della direzione in cui stiamo andando. Per esempio, in tema di ISAC, siamo riusciti a fare in modo che vi sia un sistema di scambio di informazioni di natura strategica e di *best practices* per settori cruciali, come le telecomunicazioni. L'ISAC Telco consente ai vari soggetti di condividere reciprocamente informazioni, cosa non scontata visto che si tratta di aziende spesso in concorrenza tra loro. Questo accade perché si sta acquisendo la consapevolezza che solo attraverso tale condivisione si riesce ad alzare il livello di sicurezza di tutti.

Chiudo sulla formazione. La formazione e la consapevolezza sono assolutamente decisive per alzare i nostri livelli di resilienza e, a tal proposito, posso dire con soddisfazione che sta crescendo l'offerta a livello nazionale di attività informative e formative. È stato citato anche il rapporto di ACN con l'Università Federico II, che è un ottimo esempio di come l'Agenzia collabori con gli Atenei. Ma la nostra attenzione è a 360 gradi e, per questo motivo, l'ACN ha sottoscritto anche un protocollo di collaborazione con il Ministero dell'istruzione e del merito per includere la formazione cyber in tutti i livelli di istruzione.

In conclusione, la cybersicurezza è un percorso. È un percorso che parte dalle tecnologie – e che richiede tecnologie sempre più sicure, attraverso la sicurezza "*by design*" – ma il fattore umano è sicuramente il più determinante. Chiudo con un esempio: ognuno di noi attraversa la strada guardando a destra e sinistra per verificare che non ci sia un qualche pericolo, e che quindi si può procedere in sicurezza. Quando abbiamo davanti un dispositivo, invece, nessuno pensa che ci possa essere lo stesso pericolo se, al posto di una macchina che corre, c'è invece un attore ostile pronto ad attaccarci. Dobbiamo cambiare la mentalità e, ad esempio, quando usiamo un assistente di intelligenza artificiale per farci compilare un *report* aziendale, dobbiamo essere ben consapevoli che stiamo mettendo a disposizione i nostri dati e i dati preziosi dell'azienda, che possono essere utilizzati per mille altri motivi. Li stiamo dando e non sappiamo dove andranno a finire. Ciò testimonia la necessità di un decisivo cambio culturale.

Capitolo Nono

Il ruolo della Polizia informatica e cibernetica nel Paese

Ivano Gabrielli

Grazie per l'invito e soprattutto sono lieto di aver ascoltato gli interventi che mi hanno preceduto la cui qualità mi arricchisce ed è foriera di molte sollecitazioni. Spero di esserne a livello, ovvero di non far scendere in qualche modo l'apprezzamento della mattinata nella quale tutte le relazioni sono state particolarmente interessanti e soprattutto perché il tema che affrontiamo si tinge di questioni diverse con tutto quello che sta accadendo in termini di *cybercrime*.

Cercherò di essere veloce e mi collego ad alcuni interventi che mi hanno preceduto richiamando innanzitutto la Legge 90/2024 in materia di cybersicurezza nazionale che è l'ultimo momento normativo sostanziale che ha riguardato questo settore. È il punto di approdo di tensioni, in quanto scaturita dalla necessità di andare a colmare alcune lacune organizzative che in qualche modo hanno riguardato l'intera materia della sicurezza cibernetica. Sicuramente è una norma che deve essere in qualche modo perfezionata e di fatto qualche intervento precedente ha effettivamente puntualizzato quelli che sono i passaggi da migliorare che dovranno riguardare soprattutto alcune fattispecie. Va detto che tutti gli Stati e anche le stesse Entità sovranazionali, come quelle unionali, stanno normando molto velocemente, probabilmente anche sulla scorta di un'ansia che si sta affacciando rispetto a fenomeni che sopraggiungono e che vengono dipinti o vengono preannunciati come rivoluzionari, assolutamente innovativi o anche talvolta distopici rispetto a quella che è la società in cui viviamo.

C'è un'ansia quindi di normazione in quanto vengono affrontati temi che difficilmente possono essere ricondotti a quella che è la tradizione giuridica, ovvero a quello che è il dato esperienziale tecnico operativo che ad esempio riguarda la nostra competenza, cioè quella di forze di Polizia chiamate a contrastare fenomeni criminali che, perlomeno oggi, si contraddistinguono per due aspetti: per l'alta complessità tecnica e quindi per la difficoltà nell'andare a ricostruire l'elemento probatorio e la ricostruzione del fatto. Un attacco informatico, garantisco per esperienza diretta, è qualcosa di effettivamente molto complesso, che prevede un expertise tecnico-giuridico molto peculiare e tra l'altro deve avvalersi di tecniche forensi innovative per l'acquisizione di *E-evidence* che abbiano la for-

za di reggere all'effettiva conferma in sede dibattimentale. In secondo luogo, gli attacchi informatici hanno sempre più una dimensione internazionale e quindi le relative indagini debbono confrontarsi con regole complesse di diritto internazionale che riguardano, per l'appunto, l'acquisizione della prova, passando attraverso i meandri di convenzioni di cooperazione, soprattutto in caso di indagine d'iniziativa nazionale e non di carattere europeo. Pensate alla complessità di questi iter acquisitivi, spesso supportati da una Magistratura che fatica, così come le Forze di Polizia, ad acquisire confidenza con lo strumento della cooperazione internazionale o con regimi normativi totalmente diversi e con tempi che spesso non sono compatibili con la necessità di andare a garantire, attraverso attività di freezing, la preservazione della prova digitale a livello internazionale quella che sarà l'acquisizione probatoria. Questa è la difficoltà operativa che oggi scontiamo e scontano le forze di Polizia e le Autorità Giudiziarie che in qualche modo sono chiamate a fronteggiare una nuova realtà criminale alla quale, senza andarvi a tediare con quella che è la proiezione organizzativa che testimonia questa difficoltà, abbiamo risposto come Polizia di Stato e Polizia Postale e che viene considerata come un'effettiva realtà emergenziale criminale globale. A tal proposito evidenzio che l'esito di una *Survey* dell'Assemblea Generale Interpol ha visto, di fatto, mettere al primo posto, dell'agenda criminale di tutti i vertici delle forze di Polizia, il contrasto al *cybercrime*.

La dottrina, anche a livello internazionale, intende per *cybercrime* tutte quelle fenomenologie penali che vengono ricondotte in tre macrosettori, in tre macroaree che vengono a loro volta declinate e importate all'interno degli ordinamenti giudiziari. A margine dell'adozione della Convenzione di Budapest avremo, a breve, la firma di una Convenzione ONU specificamente dedicata al *cybercrime*. Le tre macrocategorie riguardano tre aspetti: in primis i reati contro la persona, a partire dal contrasto alla pedopornografia o allo sfruttamento sessuale dei minori, reati commessi tramite la produzione o la registrazione di immagini, la messa in vendita e infine la diffusione o la semplice mera detenzione, il tutto viene considerato *cybercrime*.

In Italia una macroarea, che non tutti gli ordinamenti internazionali considerano riconducibile al *cybercrime* è riferibile, per esempio, ai reati contro la persona quali il *cyberstalking*, inteso come atti persecutori, piuttosto che le molestie, piuttosto che le minacce tutte condotte che in Italia sono considerate illecite e riconducibili al *cybercrime*, cioè appannaggio della nostra struttura con competenza che condividiamo con le altre forze di Polizia. Ancora, viene considerato *cybercrime* tutto ciò che può essere ricondotto alla grande macroarea che com-

prende, a livello internazionale, gli attacchi a sistemi informatici: parliamo di tutte quelle azioni che in qualche modo mirano a violare un sistema informatico. Ci riferiamo a tutti quei reati informatici propri, forse quelli meglio categorizzati nella nostra dottrina che si concretizzano all'interno di un ambiente cibernetico, attraverso l'utilizzo di strumenti cibernetici. Parliamo dell'accesso abusivo a un sistema informatico, cioè la sottrazione di dati piuttosto che il danneggiamento di sistema informatico. Recentemente queste condotte sono state normate e aggravate, sotto alcuni aspetti, soprattutto valorizzando quelle che sono le necessità di tutela del *"core"* cibernetico della nostra società, in riferimento alle infrastrutture critiche, cioè tutte quelle strutture che oggi sono riconducibili all'interno di due perimetri concentrici, il perimetro nazionale di sicurezza cibernetica e il perimetro ridefinito oggi dalla Direttiva 2022/2555 NIS2, così come recepita nel nostro ordinamento. Tutte quelle attività ostili che colpiscono un sistema informatico e tutto quello che viene e può essere condotto in quell'ambito viene ed è considerato un cyber attacco, riconducibile all'alveo del *cybercrime*. Il terzo settore riguarda l'ambito delle frodi informatiche, quindi reati contro il patrimonio che vengono commessi in un ambiente cibernetico con strumenti cibernetici. È il tema delle frodi telematiche, per intenderci, più o meno complesse, più o meno aggravate rispetto a quello che è l'utilizzo, la sottrazione di dati e quant'altro. Questi tre settori, di fatto, oggi integrano quello che è il fenomeno del *cybercrime* e vengono considerati tali a livello internazionale. Il concordare su questa definizione ci permette, in qualche modo, di andare a costruire la cooperazione internazionale di Polizia giudiziaria che consente di fronteggiare un genere di criminalità che, come ho già detto, è connotata, nella quasi totalità dei casi, dall' utilizzo di strumenti che impongono l'acquisizione di elementi probatori oltre il confine nazionale. Questo, ovviamente, si riflette sulla necessità di ripensare anche quelle che sono le strutture organizzative. Attenzione, non è banale parlare di strutture organizzative quando si parla di questo settore. Perché, se osserviamo la struttura delle forze di Polizia, degli apparati giudiziari e soprattutto quella degli enti a carattere sovranazionale, ad esempio Europol, notiamo come la struttura di cooperazione di Polizia Europea ha un centro dedicato al contrasto del *cybercrime* che si chiama EC3 *European Cybercrime Centre,* organizzato in tre divisioni, che sostanzialmente si occupano delle tre macroaree di cui abbiamo già parlato.

Se ci poniamo al di fuori dei tre settori, di fatto, non potremmo utilizzare quella forma di cooperazione internazionale, ma soprattutto se non ci organizziamo internamente con strutture che in qualche modo possano ricondurre ciò

che stiamo fronteggiando in quelle tre macro-materie, in quei tre macrosettori, non riusciremo a poterli fronteggiare efficacemente. In tal senso, per quello che riguarda la struttura della Polizia Postale che ormai da 25 anni si occupa di *cybercrime*, la stessa è articolata in 5 Divisioni: parliamo di una struttura che dal centro coordina 18 centri operativi e 82 sezioni presenti sul territorio nazionale. Mi preme farvi notare, al di là di quelle che sono le competenze della Prima e Quinta Divisione che si occupano rispettivamente del coordinamento e della pianificazione strategica delle risorse umane e del governo e la gestione dei Servizi ICT, di come invece la Seconda, la Terza e la Quarta Divisione di fatto operino all'interno di quelle tre macro aree, rendendo possibile l'attivazione autonoma del canale di cooperazione internazionale, mediante un'azione verticale e specializzata nel contrasto al *cybercrime*. Ma il *cybercrime* è qualcosa di peculiare, cioè un fenomeno criminale che a differenza di altri fenomeni criminali porta con sé aspetti diversi. Abbiamo ascoltato in precedenza l'intervento del dr. Gianluca Ignagni dell'Agenzia per la Cybersicurezza Nazionale che ha parlato e disquisito riguardo a quella che è la minaccia cyber. Ha parlato di minaccia *state sponsored*, di minaccia criminale.

Bene, quando ci riferiamo al *cybercrime* e soprattutto quando parliamo di *Cyber Attacks* e *Financial cybercrime*, siamo fuori dalla tutela di quei macrosettori di cui parlavamo prima. In quel caso i fatti non possono essere soltanto considerati come fatti di reato e affrontati solo con lo strumento penale, da qui la necessità non solo italiana, ma internazionale di creare strutture che in qualche modo fronteggino quella minaccia che non è più soltanto una minaccia criminale, ma deve essere affrontata e letta in maniera multidimensionale. Questo ha comportato, nel tempo, lo sviluppo e la ricerca di forme di coordinamento, ovvero di cooperazione tra vari settori in Italia attraverso il susseguirsi nel tempo di varie fasi, quali da ultimo l'approvazione della Legge 82/2021 che ha istituito l'Agenzia per la Cybersicurezza Nazionale. È un processo evolutivo, badate, che parte dal 2005 e prosegue nel 2013 con il Decreto Monti e, successivamente, nel 2017 con il Decreto Gentiloni e che approda, infine, nel 2021 alla riforma dell'architettura nazionale di sicurezza cibernetica. Quest'ultimo passaggio normativo ha dato la possibilità di approcciare quelle condotte considerate come reati circoscritti ma che avendo le caratteristiche di un attacco di tipo statuale, devono essere considerate come una minaccia che può colpire un servizio pubblico essenziale e quindi deve essere contrastata da una struttura di intelligence. La strategia d'azione deve essere analizzata sotto più profili, coordinando gli interventi e quelle competenze all'interno di un *framework* generale. Questo *framework* si chiama architettu-

ra nazionale di sicurezza cibernetica che vede, per l'appunto, la presenza di più settori, a partire dal settore della *cyber investigation*, *del cyber defense*, della *cyber intelligence* e della *cyber resilience*. Ma questi settori in qualche modo debbono lavorare fianco a fianco portando con sé un fattore determinante: l'intervento di più investigatori. Ciascuna struttura che interviene a margine di un *cyber attacks*, ad esempio nel caso di una violazione di un danneggiamento strutturato oppure nel caso del *ransomware* in danno alla Regione Lazio, per citarne uno dei più famosi, prevedono per l'appunto la possibilità di intervento di più strutture investigative su uno stesso sito, che è il sito di una scena del crimine, ma è anche un punto di analisi per chi dovrà fare *resilience* e rimettere in piedi quel sistema o che dovrà capire cosa è successo per mettere a fattor comune quelle informazioni. È un sito nel quale l'intelligence deve operare per analizzare quello che è successo e per capire se ci troviamo di fronte a una minaccia, magari ibrida, di carattere statuale, che ha necessità di essere fronteggiata magari a livello politico. Oltretutto potrebbe esserci un rischio di tipo militare di difesa dei confini nazionali, qualora quel fatto fosse riconducibile, ad esempio, a una struttura governativa direttamente impegnata o a una struttura militare. Questo significa che gli attori coinvolti devono poter operare insieme, debbono potersi coordinare. Oggi questo coordinamento avviene all'interno di strutture che prevedono tavoli di concertazione di *infoshare* di alto livello, ma anche di cooperazione operativa. Questo impone un'altra cosa, la necessità che quelle strutture abbiano in qualche modo competenze, spesso comuni, spesso sovrapponibili. Un intervento di Polizia Giudiziaria, a margine di un attacco informatico, non è qualcosa di così diverso rispetto all'intervento che fanno i tecnici dell'ACN nel momento in cui debbono ricostruire quello che è successo, anzi è assolutamente sovrapponibile come attività. La stessa capacità di ricostruzione di un fatto deve averla l'intelligence, per individuare gli autori dell'attacco. Le competenze del personale che interviene in quella sede, salvo la parte che poi riguarda la competenza specifica di ciascuna *mission*, sono di fatto sovrapponibili. Questo impone la possibilità, anzi la doverosità, di costruire modelli operativi di interscambio comuni che in qualche modo non si sovrappongano e che oggi sono ulteriormente coordinati a livello normativo.

Questo risultato oggi è garantito dalla legge nr. 90 del 28 giugno 2024, mi riferisco alla parte ovviamente procedurale, che prevede momenti di interscambio informativo. Penso sia la prima norma che prevede, in capo a un Pubblico Ministero, l'obbligo di informare un'Agenzia della Presidenza del Consiglio e di garantire immediatamente il raccordo informativo con l'Organo del Ministero

dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni, che poi è di fatto la struttura del Servizio Polizia Postale che deve garantire in qualche modo, per funzione di ordine e sicurezza pubblica, la conoscibilità di quello che sta succedendo sul territorio nazionale. Bene, questo ci pone di fronte ad alcuni problemi di natura organizzativa e di natura manageriale. Di cosa parliamo? Parliamo della necessità di avere operatori che abbiano le capacità di poter intervenire in maniera sincrona sullo stesso scenario, che possano in qualche modo dirimere le proprie competenze. Oggi le competenze vengono di fatto regolate dagli interventi normativi. Sapete che c'è un obbligo di avviso in capo all'ACN nel momento in cui vengono effettuati atti irripetibili? Sapete che sullo stesso sito possono operare contemporaneamente più realtà? Addirittura, è prevista una reportistica che tra l'altro vede verticisticamente coinvolta oggi la Direzione Nazionale Antimafia e le 26 Procure Distrettuali in caso di reati di competenza distrettuale. L'Ordinamento prevede, quindi, momenti di coordinamento importanti. Il deficit è dal punto di vista operativo, perché creare figure che abbiano la capacità di poter muoversi in un contesto di questo tipo è effettivamente molto complesso. Si tratta di una complessità organizzativa che vivono strutture come l'ACN, la Difesa, l'Intelligence e a maggior ragione strutture come le Forze di Polizia. Reperire e formare personale che abbia questo tipo di capacità oggi è il tema dei temi per il quale effettivamente ci stiamo attrezzando, così come ci si attrezza dal punto di vista di quelle che sono le capacità operative. E qui chiudo il mio intervento, segnalandovi lo sforzo continuo profuso a livello legislativo e normativo per dotare di strumenti investigativi peculiari chi è chiamato a operare in questi contesti particolarmente tecnici, difficili da penetrare. In merito evidenzio una recente innovazione normativa, cioè quella che prevede la possibilità di poter svolgere attività *undercover*. È l'ultimo passaggio di un percorso che ha dato la possibilità di attribuire a determinati soggetti la facoltà di penetrare, per l'appunto, in ambienti di criminalità informatica. Tale necessità è dovuta al fatto, ripeto, di svolgere attività investigative non soltanto nella ricostruzione del fatto ma nella ricostruzione delle responsabilità e quindi nell'individuazione dei soggetti autori di reato: nell'esecuzione di quella che è l'attività investigativa che si manifesta con effetti cinetici in una realtà cibernetica, ovvero virtuale o contemperata e compenetrata come la politica.

A un certo punto questa attività deve portare all'individuazione di responsabili, questo necessariamente è lo sviluppo di un'attività di contrasto e non solo preventiva e questa attività di contrasto oggi passa attraverso strumenti che nel 2005 avevano visto addirittura la possibilità di attribuire all'Organo del Ministe-

ro dell'Interno, quindi ad una compagine specialistica settoriale molto definita e precisa, cioè al Servizio Polizia Postale, la possibilità di fare intercettazioni preventive, attività *undercover*, che oggi si arricchisce della possibilità di svolgere attività diretta, passatemi il termine, attività di *cyber-attack* nei confronti di quelle che sono le infrastrutture che vengono messe in piedi per uso criminale. Quando? e qui la normativa è molto ampia, quando si procede per reati commessi nei confronti delle infrastrutture critiche, non per reati qualificati a monte, perché dà la possibilità di poter svolgere attività che oggi prevedono la facoltà di bucare sistemi informatici, di sostarvi all'interno, di osservare, di costruirne altri. Stiamo parlando di un potere molto forte, simile a quello che viene esercitato, anche questo di recente, dall'intelligence con il permesso e con le previste garanzie funzionali. Facoltà simili ad altre attività, ad altri poteri che altre forze di Polizia hanno o che hanno distribuito su organismi diversi in Italia. Questo oggi lo si può fare. Ovviamente vi è un problema di capacità e di competenze tecniche nel realizzare un'attività di questo tipo. Lo si può fare, ci si pone il problema di poterlo fare nei confini nazionali od oltre i confini nazionali, non conoscendo effettivamente dove sia la risorsa tecnologica che in quel momento è oggetto di attività proattiva. Questo è un problema che dovremo in qualche modo risolvere e per il quale, molto probabilmente, sarà chiamata ad intervenire la giurisprudenza. Ma oggi di fatto, ed è questa la conclusione del mio percorso, parlare di *cybercrime* è parlare di una nuova dimensione di criminalità. Una dimensione che in qualche modo è molto presente, molto aggressiva, molto pericolosa e che ha una dimensione tale per cui gli strumenti che conoscevamo, anche dal punto di vista investigativo, non sono più sufficienti. C'è bisogno di un'attività diversa, di competenze, ma c'è soprattutto bisogno di mettere queste competenze all'interno di un percorso costituzionalmente garantito, che permetta di svolgere un'attività investigativa che non sfori, verso abusi che possano essere pericolosi e rischiosi, nel momento in cui attività di questo tipo hanno la capacità di attingere, di permanere all'interno di sistemi informatici, estrapolando quelli che sono poi gli elementi probatori necessari a ricostruire il fatto e di individuarne le responsabilità.

Capitolo Decimo

Attività di indagine e modalità di acquisizione dei dati tecnici in materia di reati informatici

Vincenzo Molinese

Introduzione

L'utilizzo sempre più diffuso di dispositivi digitali e informatici, accessibili a prezzi contenuti e disponibili in numerose tipologie, ha trasformato radicalmente il modo di condurre indagini e di raccogliere informazioni.

Questi dispositivi, infatti, sono diventati una delle principali fonti di informazione in ambito investigativo e giudiziario. Tuttavia, l'evoluzione tecnologica ha portato anche alla nascita di nuovi illeciti, fornendo spesso supporto ai reati tradizionali e dando origine a situazioni in molti casi al limite, non ancora pienamente regolate sul piano legislativo e procedurale.

1. *Le indagini telematiche: minacce e reati informatici*

Nella conduzione delle indagini telematiche è fondamentale fare riferimento ad alcune precisazioni, in particolare distinguendo tra reato informatico e minaccia informatica. Una "minaccia informatica" rappresenta qualsiasi vulnerabilità, circostanza, evento o azione che possa compromettere, disturbare o causare effetti negativi su reti, sistemi informativi, utenti di tali sistemi o altre persone. Si tratta di un rischio *potenziale* che, pur potendo trasformarsi in un danno concreto, non implica necessariamente un comportamento illecito. D'altro canto, un "reato informatico" è un'azione illegale commessa *tramite* o *contro* sistemi informatico-digitali, violando leggi specifiche in ambito penale. Questo tipo di reato, che può riguardare sia la condotta che l'oggetto materiale del crimine, può essere perpetrato utilizzando tali sistemi come strumenti (*computer-as-a-tool*) oppure colpendoli direttamente (*computer-as-a-target*).

In tale contesto, riveste un ruolo estremamente importante il concetto di "prova digitale" (*digital evidence*). Una fonte di prova digitale si può definire come qualsiasi informazione, con valore probatorio, memorizzata o trasmessa in formato digitale, indipendentemente dal supporto utilizzato.

Le principali caratteristiche della fonte di prova digitale che è opportuno considerare, includono:

- *Immaterialità*. La prova digitale risiede nel contenuto, non nel supporto fisico su cui è memorizzata;
- *Dispersione*. La prova digitale può essere distribuita su più dispositivi, anche geograficamente distanti tra loro;
- *Promiscuità*. La prova digitale può coesistere su dispositivi che contengono altre informazioni non rilevanti per l'indagine;
- *Congenita modificabilità*. La prova digitale è altamente suscettibile a modifiche, alterazioni o manipolazioni.

2. *Minaccia informatica*

Una minaccia informatica è un rischio o una circostanza che *potrebbe* compromettere la sicurezza di reti, sistemi informativi o utenti, causando effetti negativi come perdita di dati, interruzioni di servizio o violazioni della *privacy*. Esempi di minacce possono essere *malware* (software dannoso come *virus*, *worm*, *spyware* e *trojan*, progettati per infiltrarsi nei sistemi, danneggiarli o esfiltrare informazioni), *ransomware* (*malware* che cripta i dati di un dispositivo bloccandone l'accesso fino al pagamento di un riscatto), rischi di *phishing* e *ingegneria sociale* (tecniche di manipolazione che ingannano gli utenti per ottenere informazioni sensibili, come *password* o dati bancari, per cui risulta fondamentale un'adeguata formazione del personale), vulnerabilità ad *attacchi DDoS* (attacchi che sovraccaricano un sistema o una rete con un traffico eccessivo, rendendoli inaccessibili e inutilizzabili), *exploit Zero-Day* (attacchi che sfrutano vulnerabilità sconosciute in *software* o sistemi prima che possano essere risolte), o infine, le *insider threats* (minacce interne causate da dipendenti o collaboratori che, intenzionalmente o per errore, compromettono la sicurezza aziendale). A riguardo, al fine di evitare che tali minacce vengano utilizzate per effettuare attacchi e violazioni di ogni tipo, sono fondamentali attività di *cyber-security*, protezione dei sistemi, monitoraggio e formazione del personale[1].

[1] Concetto di *security awareness*, "consapevolezza" da parte del personale dei rischi e delle problematiche legate alla sicurezza informatica.

3. *I reati informatici*

I reati informatici, come già espresso, sono azioni illecite commesse a danno o per mezzo di strumenti digitali e si possono differenziare in "*cyber-enabled crime*" e "*cyber-dependent crime*" sulla base del loro grado di dipendenza dalla tecnologia per la commissione del crimine.

I crimini "*cyber-enabled*" sono crimini tradizionali che vengono facilitati o resi più efficaci grazie all'uso di strumenti telematici. Si tratta di attività che non dipendono esclusivamente dalla tecnologia, ma la cui efficienza, portata e velocità è aumentata dall'utilizzo di mezzi informatici. Basti pensare alle frodi bancarie e truffe *online* (in cui alle vittime vengono sottratte le credenziali di accesso ai propri conti per derubarle) o *stalking online* (definito *cyber-stalking*, in cui la persecuzione e la molestia avvengono sui social media). In ogni caso, esiste talvolta una corrispondenza tra i reati tradizionali e quelli tipicamente commessi nel *cyberspazio*, spesso anche sancita nel Codice penale. Ad esempio, all'estorsione nel mondo reale possono corrispondere forme digitali come la *sextortion* o la richiesta di riscatto a seguito della cifratura di un sistema tramite *ransomware*[2].

Analogamente, la violazione di domicilio trova un parallelo nell'accesso abusivo a un sistema informatico, mentre gli atti persecutori hanno il loro equivalente digitale nel *cyberstalking* o nel *revenge-porn*.

I crimini *cyber-dependent* sono crimini che non potrebbero essere commessi senza l'uso della tecnologia e inesistenti al di fuori del cyberspazio. Questi crimini dipendono direttamente da Internet, da sistemi informatici o da reti telematiche, e senza l'uso di computer o analoghi dispositivi elettronici, il crimine non esisterebbe. Attività illecite di questo tipo sono riconducibili, ad esempio, all'esecuzione di attacchi DDoS, finalizzati a rendere inutilizzabili e inaccessibili sistemi digitali o alla distribuzione di *malware* e *virus* per danneggiare dispositivi informatici o rubare informazioni.

[2] Un ransomware è una tipologia di malware che blocca l'accesso ad un dispositivo target criptandone i dati, con l'obiettivo di ottenere un riscatto dalla vittima, che deve pagare per ottenere nuovamente l'accesso.

4. *Le modalità di acquisizione dei dati*

Il concetto di dato, in tale contesto, riveste un ruolo fondamentale e di primaria importanza, essendo evidente l'importanza che tali informazioni possono rivestire nei processi infoinvestigativi e giudiziari. Dal punto di vista delle indagini telematiche, le modalità di acquisizione dei *dati informatici* sono molteplici e si possono riferire a due principali macro-categorie:

- la *digitalforensics*, o informatica forense, che riguarda l'estrazione di dati da dispositivi;
- l'OSINT (*Open Source INTelligence*), che consente di ottenere dati e informazioni consultando le cosiddette "fonti aperte", ossia attingendo al materiale disponibile liberamente *online*.

5. *La Digital Forensics*

Le informazioni estratte da un dispositivo, che possono costituire delle fonti di prova a tutti gli effetti, sono soggette a volatilità[3] e fragilità, risultando dunque fondamentale eseguirne una acquisizione, al fine di garantire il valore probatorio dei *bit* estratti dai *device* di interesse. La giurisprudenza, pertanto, incoraggia l'utilizzo di tecniche di informatica forense (*digital forensics*) per l'estrazione di dati, da cristallizzare in copie forensi, consentendo la produzione di elementi giudiziari certi, in relazione alle caratteristiche di *integrità* dei dati, *non-manipolazione*, *riconducibilità* all'autore e *certezza temporale*, rendendo immodificabile la copia forense generata e dall'indiscutibile valore probatorio.

La *digital forensic*, è, dunque, una scienza forense che si occupa di raccogliere e analizzare dati provenienti da dispositivi digitali (computer, dispositivi mobili, ma anche *hard disk*, reti informatiche, database, e perfino dalle immagini) ai fini investigativi e giudiziari, preservandone l'integrità e la validità in sede processuale, con lo scopo di *identificare*, *conservare*, *acquisire*, *documentare* e *interpretare* i dati presenti su uno strumento telematico. Tali attività vengono svolte da personale altamente specializzato, in grado di effettuare operazioni manuali,

[3] La volatilità di un dato si riferisce alla caratteristica della memoria di mantenere o perdere i dati immagazzinati in base alla disponibilità di alimentazione elettrica. In altre parole, indica se i dati vengono conservati o meno quando la memoria non è alimentata.

intervenendo direttamente sui sistemi, oppure utilizzando una suite di software ad-hoc per questo tipo di attività.

5.1. *Conservare il valore probatorio del dato: la Catena di Custodia*

È evidente che, quando si parla di prove digitali contenute su supporti informatici, si possono manifestare diverse problematiche, trattandosi di informazioni facilmente modificabili, oltre che soggette a deperimento e rischio di cancellazione. Infatti, perché una prova digitale sia valida e si mantenga tale anche successivamente alla sua acquisizione (e dunque in ambito giudiziario), è necessario che questa resti inalterata. Una volta raccolta la prova, è necessario che tutti gli interventi avvenuti su di essa, eventuali alterazioni o spostamenti siano tracciati e tracciabili. Ciò può avvenire solamente mediante la redazione della *Catena di custodia*. Tale documento, che descrive l'intero ciclo di vita delle *digital evidences*, permette di seguire l'intero iter percorso dalla prova (riportando in maniera dettagliata luoghi. tempi e soggetti intervenuti), dalla sua raccolta fino al relativo utilizzo in sede di giudizio. Poter verificare se vi sono state manomissioni, oltre che conoscere chi effettivamente è entrato in contatto con la prova, infatti, garantisce la salvaguardia della prova stessa. Inoltre, è necessario che i dati raccolti vengano opportunamente protetti, mediante apposizione di sigilli sia sui dispositivi elettronici originali, sia sulle loro copie, sottolineando che una manomissione dei sigilli potrebbe invalidare la prova stessa. Un'altra fase di estrema importanza della catena di custodia riguarda il *trasporto delle evidenze* in oggetto, le quali, attraverso opportune tecniche e strumentazioni, devono essere isolate da qualsiasi contatto con il mondo esterno (sia dal punto di vista fisico e meccanico, che radio).

Tali attività sono finalizzate a garantire le caratteristiche di riservatezza (dati, informazioni e risorse devono essere accessibili esclusivamente a coloro che ne sono i legittimi fruitori), integrità (dati, informazioni e risorse non devono essere modificabili e alterabili da chi non ne ha diritto), disponibilità (gli utenti devono poter accedere e fruire dei dati, informazioni e risorse di cui hanno legittimamente bisogno in ogni momento), autenticità (dati, informazioni e risorse devono essere fedelmente riconducibili nella forma e nei contenuti al dato originario, ossia a quello presente nel sistema informatico-telematico oggetto d'indagine) e non ripudiabilità (è necessario impedire il disconoscimento di una azione, di un messaggio o di un documento, da parte dell'autore).

Pertanto, l'utilizzo della catena di custodia (COC) nella *Digital Forensics* garantisce che la prova informatica non venga alterata o manomessa. In questo modo, le prove restano attendibili per tutta la durata del processo.

6. *Il domicilio informatico*

Nell'ambito di una perquisizione informatica, è bene sottolineare che possono essere oggetto di acquisizione non solo oggetti fisici presenti sulla scena, ma anche dati collocati in rete, su piattaforme decentralizzate e sul cosiddetto cloud. In tal senso, è opportuno definire il concetto di *Domicilio Informatico*, che fa riferimento a un luogo virtuale riconducibile a una persona fisica o giuridica, dove sono conservati dati, informazioni o strumenti digitali che possono avere valore personale, patrimoniale o legale ed è, di fatto, l'estensione del concetto di domicilio tradizionale nel contesto digitale. Pertanto, non si tratta di un luogo fisico, ma di uno spazio interno di una rete digitale o di un sistema informatico, come un server, una casella di posta, dei profili social-media, un account di *cloud storage*. Nel contesto giuridico italiano, il domicilio informatico è tutelato dall'articolo 615-ter del Codice penale, che disciplina il reato di accesso abusivo a un sistema informatico o telematico. La norma prevede sanzioni per chiunque acceda a un sistema informatico protetto contro la volontà del legittimo proprietario, assimilando la violazione del domicilio informatico a quella del domicilio fisico. Il domicilio informatico è un concetto cruciale nella società digitale, dove la protezione dei dati personali e della privacy assume un ruolo sempre più centrale. Esso rappresenta uno spazio digitale privato e inviolabile, soggetto a specifiche tutele giuridiche per prevenire abusi e accessi non autorizzati. L'estrema varietà e distribuzione dei dati (che possono trovarsi sia su dispositivi fisici che virtuali e non fisicamente individuabili) e dei possibili supporti da cui estrarli, rende, talvolta, molto complicata l'individuazione delle possibili fonti di dato da cui poter acquisire informazioni utili in ambito giudiziario ed investigativo.

6.1. *Le difficoltà del sopralluogo*

In tal senso, risulta fondamentale il sopralluogo che avviene sulla scena del crimine. In primo luogo, è necessario cinturare fisicamente e, laddove possibile e ritenuto opportuno, anche logicamente (cambiando, ad esempio, le password di accesso ai profili social individuati, cercando di congelare le informazioni presenti fino a quel momento) la scena del crimine, determinando il legittimo titolare del domicilio informatico oggetto di indagine, e ragioni che giustificano la loro presenza.

6.2. *Le problematiche del processo di acquisizione forense*

In conclusione, il processo di *acquisizione forense* presenta una serie di problematiche complesse, legate sia alla natura e alla varietà tecnologica dei dispositivi,

sia alle strategie impiegate per proteggerne i dati. L'eterogeneità dell'*hardware* e le diverse tipologie dei sistemi operativi rappresentano una sfida significativa, rendendo difficile standardizzare i metodi di acquisizione. Le tecniche di *anti-forensic*, come la cifratura e la cancellazione automatica dei dati, complicano ulteriormente il recupero delle informazioni dai dispositivi. Si fa riferimento, ad esempio, agli strumenti di comunicazione criptata (*criptofonini*) che sono sempre più utilizzati dalle organizzazioni criminali, in ragione dell'elevato livello di sicurezza e segretezza che riescono a garantire mediante complessi algoritmi di cifratura e molteplici funzionalità di cancellazione del dato, anche da remoto.

In tale ambito, inoltre, i processi in *background*[4] possono alterare lo stato del dispositivo, compromettendo l'integrità delle prove. Anche la scelta della strumentazione giusta per il tipo di device in esame è cruciale, poiché spesso occorre affrontare ostacoli aggiuntivi che includono la necessità di superare password, codici di sblocco e funzionalità avanzate di sicurezza progettate per tutelare la privacy. Infine, l'assenza di risorse forensi adeguate e aggiornate rispetto ai nuovi modelli di dispositivi limita la capacità di condurre analisi complete ed efficaci.

7. *L'OSINT*

Se la *digital forensics* permette di estrarre dati e informazioni direttamente dai dispositivi, seppur talvolta in maniera indiretta, l'enorme varietà di dati disponibile *online* sulle piattaforme digitali liberamente accessibili (come *blog*, *forum*, *social media*, articoli di giornale), mette a disposizione degli investigatori un'enorme quantità di informazioni. A riguardo, la raccolta, la valutazione e l'analisi dei dati provenienti da tali fonti informative (eterogenee e di dominio pubblico) prende il nome di OSINT (*Open Source INTelligence*). L'obiettivo di questa scienza è pertanto quello di raccogliere informazioni pertinenti e di interesse investigativo rispetto ad un determinato *target*, valutandone l'attendibilità (con particolare riferimento alla fonte da cui il dato proviene), l'accuratezza e la validità. Considerando la grande mole di dati che è possibile ottenere attraverso tecniche di questo tipo, è fondamentale selezionarli sulla base della loro rilevanza investigativa e, una volta ottenuto un dataset strutturato, è possibile procedere

[4] Processo che il sistema operativo di un dispositivo esegue in maniera latente, non sempre rilevabile in prima analisi.

all'analisi dei dati, finalizzata a ricostruire attività criminali e scoprire eventuali vulnerabilità di un soggetto, nell'ottica di individuare potenziali canali di aggressione mediante inoculazione di un captatore informatico. In maniera analoga alla *digital forensics*, le attività di OSINT sono svolte da personale altamente specializzato, che utilizza software dedicati, e al contempo, opera manualmente sulle piattaforme digitali oggetto di ricerca.

Conclusioni

La rivoluzione digitale ha influenzato in maniera consistente anche il mondo investigativo e giudiziario (chiamati a preservare e difendere lo Stato di diritto a prescindere dalle evoluzioni della società), che ha dovuto adattarsi e aggiornarsi al dirompente sviluppo tecnologico. Pertanto, l'informatica forense, le *digital investigations*, le attività di OSINT e le relative procedure (che spesso operano in maniera propedeutica e combinata) rivestono un ruolo cruciale nelle attività di indagine e nelle modalità di acquisizione dei dati tecnici in materia di reati informatici, sia per fornire linee guida agli operatori del settore, sia per regolamentare procedure complicate che richiedono specifiche competenze tecniche e professionali.


Raggruppamento Operativo Speciale Carabinieri
CARABINIERI
ATTIVITÀ DI INDAGINE E MODALITÀ DI ACQUISIZIONE DEI DATI TECNICI IN MATERIA DI REATI INFORMATICI
R.O.S.
Napoli, 24 Gennaio 2025
GEN. B . VINCENZO MOLINESE


Raggruppamento Operativo Speciale Carabinieri
CARABINIERI
Indice
MINACCIA INFORMATICA E REATO INFORMATICO
LE MODALITÀ DI ACQUISIZIONE DEL DATO
LA DIGITAL FORENSICS
L'OSINT
CONCLUSIONI
2

Raggruppamento Operativo Speciale Carabinieri

Obiettivi di Indagine: Minaccia Informatica e Reato Informatico

In danno – *Cyber-dependent crime*
Per mezzo – *Cyber-enabled crime*

Minaccia Informatica

- Qualsiasi circostanza, evento o azione che potrebbe compromettere, disturbare o causare effetti negativi su reti, sui sistemi informativi, sugli utenti di tali sistemi o su altre persone.
- Rischio ***potenziale*** che potrebbe trasformarsi in un *danno*, non implica necessariamente un comportamento illecito.

Reato Informatico

- Azione **illegale** compiuta in danno o per mezzo di sistemi informatici o digitali, atta a violare leggi specifiche in ambito penale.
- Caratteristiche della **prova digitale:**
  - Immaterialità, dispersione, promiscuità e modificabilità

3

Raggruppamento Operativo Speciale Carabinieri

Minaccia Informatica

- *Malware*
- *Phishing* e ingegneria sociale
- *Ransomware*
- Attacchi DDoS
- Exploit *Zero-Day*
- *Insider Threats*

Sono fondamentali le attività di *cyber-security*, protezione dei sistemi, monitoraggio e formazione del personale (*security awareness*)

4

REATO INFORMATICO: ALCUNI ESEMPI

CYBER-*ENABLED* CRIMES

Crimini che vengono *facilitati* o resi possibili grazie all'utilizzo di sistemi digitali:

- Frodi bancarie e truffe online
- Cyber-stalking

CYBER-*DEPENDENT* CRIMES

Crimini impossibili da commettere senza strumenti digitali, che possono costituire l'oggetto del reato:

- *Hacking* e accesso non autorizzato
- Distribuzione di *malware*
- Furto di dati e informazioni

5

Raggruppamento Operativo Speciale Carabinieri

LE MODALITÀ DI ACQUISIZIONE DEL DATO

LE MACRO-CATEGORIE:

- ACQUISIZIONE *DA DISPOSITIVI*
  - *Digital Forensics*: accesso **diretto** al dispositivo
- ACQUISIZIONE *ONLINE*
  - OSINT: estrazione da *fonti aperte*

6

Raggruppamento Operativo Speciale Carabinieri

La Digital Forensics

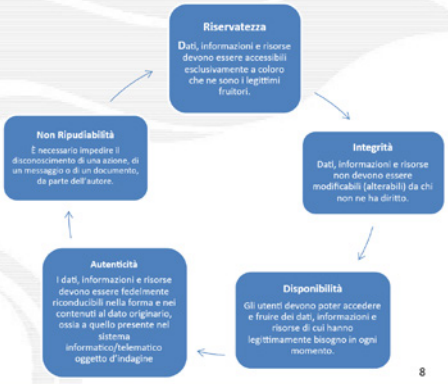
- Scienza forense che si occupa di raccogliere e analizzare dati provenienti da dispositivi digitali ai fini investigativi e giudiziari, preservandone l'integrità e la validità in sede processuale.
- Personale altamente qualificato specializzato nell'utilizzo di *software* dedicati

7

Raggruppamento Operativo Speciale Carabinieri

Conservare il valore probatorio del dato: La Catena di Custodia

- La **catena di custodia** (COC) è l'insieme di uno o più documenti che attesta, in un dato arco temporale, la responsabilità di un soggetto nella custodia e gestione di uno o più reperti.



8

Raggruppamento Operativo Speciale Carabinieri

Il concetto di Domicilio Informatico

- Luogo virtuale riconducibile a una persona fisica o giuridica, dove sono conservati dati, informazioni o strumenti digitali che possono avere valore personale, patrimoniale o legale.
- Strettamente connesso ad un soggetto, rappresenta un'estensione del concetto di domicilio tradizionale nel contesto digitale (account email, social, cloud).
- È tutelato dall'art. 615-ter C.P., che disciplina il reato di *accesso abusivo a un sistema informatico o telematico*.

9

Raggruppamento Operativo Speciale Carabinieri

Il sopralluogo sulla Scena del Crimine

- ***Cinturare*** fisicamente e, laddove possibile e ritenuto opportuno, anche **logicamente** la scena del crimine.
- Determinare il "legittimo titolare" del domicilio informatico.
- Documentare chiunque abbia accesso alla scena del crimine e i motivi che giustificano la presenza.

10

Raggruppamento Operativo Speciale Carabinieri

Le problematiche del processo di Acquisizione Forense

- Hardware molto eterogenei
- Varietà dei sistemi operativi
- Tecniche di anti-forensic, come cifratura dei dati e cancellazione sicura
- Processi in background che possono modificare lo stato del dispositivo
- Strumentazione adeguata al device
- Mancanza di risorse forensi aggiornate, a fronte dei nuovi dispositivi in commercio
- Funzionalità di sicurezza a tutela della privacy, che ostacolano le acquisizioni
- Password e codici di sblocco
- Ripristino delle impostazioni di fabbrica

11

Raggruppamento Operativo Speciale Carabinieri

L'Open Source INTelligence: OSINT

Informazioni reperibili su *fonti aperte.*

- Grande quantità di dati: analizzare attendibilità, accuratezza e validità.
- Effettuato da personale altamente specializzato

12

Raggruppamento Operativo Speciale Carabinieri

CONCLUSIONI

- Mondo investigativo e giudiziario non esente dal dirompente sviluppo tecnologico.
- Ruolo cruciale del concetto di *dato informatico* nei processi info-investigativi.
- Molteplici branche e modalità operative, che spesso operano in maniera combinata, per le attività di **estrazione**, **acquisizione** e **analisi** dei **dati**.

13

RAGGRUPPAMENTO OPERATIVO SPECIALE CARABINIERI

GRAZIE PER L'ATTENZIONE.

Napoli, 24 Gennaio 2025

14

Capitolo Undicesimo

Digital Forensics e investigazione digitale

Francesco Zorzi

Questo intervento è stato svolto nell'ambito di un Convegno interdisciplinare presso l'Università degli Studi di Napoli, Federico II ed è stato rivolto a professionisti del settore informatico, criminologico, giuridico, nonché a studenti e personale delle Forze dell'Ordine. L'orientamento della presentazione ha posto l'accento sull'importanza della formazione e dell'interazione nell'ambito della sicurezza informatica "offensiva", intesa come insieme di tecniche e metodologie utilizzate sia dai criminali informatici che dagli esperti di *digital forensics* per accedere ai dati digitali.

È stato evidenziato come la raccolta delle prove e delle evidenze digitali rappresenti un fattore determinante nell'indagine moderna, proprio per l'evoluzione dell'utilizzo dei dispositivi informatici e la loro presenza nella quotidianità della società moderna. Le tecniche tradizionali di investigazione sono state profondamente stravolte dalla tecnologia contemporanea e dalla "quotidianità digitale", elemento comune sia agli utilizzi leciti e sia a quelli illeciti. Ogni individuo possiede oggi dispositivi mobili protetti da codici di blocco o sistemi biometrici che, pur garantendo una certa protezione dai comuni attaccanti, possono essere comunque violati con tecniche appropriate.

Un aspetto cruciale riguarda la differenza etica tra chi opera nell'ambito della *digital forensics* e chi compie attacchi informatici: dal punto di vista tecnico non esistono sostanziali differenze, mentre la discriminante è puramente etica. Gli esperti forensi intervengono per finalità investigative legittime, mentre i criminali lo fanno per trarre benefici illeciti.

Con l'evoluzione della tecnologia, l'informazione non risiede più esclusivamente all'interno del dispositivo fisico, che funge piuttosto da "porta di accesso" ai dati conservati nel cloud. Applicazioni come Telegram o Instagram, senza connettività, risultano inutilizzabili poiché i dati sono memorizzati remotamente.

Un problema fondamentale per l'attività investigativa è rappresentato dai messaggi effimeri o auto-cancellanti, ormai una funzionalità standard in molte applicazioni di messaggistica. Quando un messaggio si elimina autonomamente dopo un determinato periodo, la copia forense del dispositivo effettuata succes-

sivamente potrebbe non contenere più quel dato. Se, inoltre, il sistema utilizza cifratura avanzata con chiavi temporanee, il recupero del messaggio diventa praticamente impossibile.

Questo scenario introduce il fattore tempo come elemento critico: l'evoluzione tecnologica impone una sempre maggiore tempestività nell'acquisizione delle prove. Gli operatori di polizia giudiziaria in prima linea devono essere in grado di effettuare un'attività di triage immediata, valutando quali elementi siano rilevanti e quali rischino di andare perduti se non immediatamente acquisiti.

I dispositivi mobili contemporanei non contengono solo informazioni intenzionalmente fornite dall'utente, ma un vasto patrimonio di dati comportamentali: abitudini, biometria, movimenti, localizzazioni, sensori di accelerazione. Questo patrimonio informativo può rivelarsi decisivo in casi di omicidio, scomparsa di persone o altri crimini gravi.

Diversi Stati hanno iniziato a sviluppare figure professionali ibride che combinano competenze di criminologia e profiling nell'ambito della *mobile forensics*. Queste figure sono essenziali per:

- comprendere rapidamente quali dispositivi acquisire e quali dati siano prioritari;
- effettuare analisi comportamentali per ricostruire eventi e movimenti;
- identificare eventuali crimini collaterali o connessi all'indagine principale;
- gestire la mole enorme di dati contenuti nei dispositivi moderni (un telefono di un adolescente può contenere oltre 300 GB di dati).

È stato inoltre evidenziato come il lavoro di prevenzione e intelligence sia estremamente complesso e richieda capacità di profilazione avanzate. Ad esempio, fermando una persona per detenzione di stupefacenti, l'analisi forense del suo dispositivo potrebbe rivelare attività di proselitismo terroristico o traffico di esseri umani, crimini ben più gravi del reato contestato inizialmente.

Contrariamente a quanto comunemente si crede, il criminale informatico medio non è necessariamente un esperto di sicurezza informatica. La maggior parte degli attacchi ransomware viene condotta utilizzando strumenti "noleggiati" da organizzazioni criminali che offrono il servizio di *ransomware as a service* (RaaS). Questo modello consente anche a soggetti con competenze tecniche limitate di condurre attacchi sofisticati.

Sono state inoltre evidenziati gli scenari nei quali le vittime di truffe online, in particolare quelle relative a falsi investimenti in criptovalute, siano spesso vittime di molteplici reati collegati:

- truffa (reato principale);

- accesso abusivo ai sistemi informatici;
- sostituzione di persona / furto d'identità;
- riciclaggio di denaro.

In Italia, a differenza di altri Stati, la problematica del furto d'identità digitale non è ancora adeguatamente riconosciuta e perseguita, nonostante sia alla base di molti crimini informatici. Le identità rubate vengono vendute nel darknet e utilizzate per attività di *money muling* e per aprire account presso *exchanger* di criptovalute aggirando i controlli KYC (Know Your Customer).

Un punto centrale dell'intervento ha riguardato la natura delle criptovalute, spesso erroneamente considerate anonime e irrintracciabili. In realtà, le criptovalute come Bitcoin sono basate su blockchain pubbliche, il che significa che ogni transazione è visibile e tracciabile. Il problema è che non è immediatamente possibile associare un *wallet* a una identità reale.

Tuttavia, attraverso tecniche di profilazione e analisi comportamentale, è possibile ricostruire le catene transazionali e identificare gli autori. Il relatore ha fornito esempi concreti di come criminali informatici siano stati identificati grazie a errori banali, come l'acquisto di una pizza o il pagamento di un abbonamento streaming utilizzando fondi provenienti da attività illecite.

Le caratteristiche distintive delle criptovalute rispetto al sistema bancario tradizionale sono:

- irreversibilità delle transazioni: una volta effettuata, una transazione in criptovaluta non può essere annullata;
- pubblicità della blockchain: tutte le transazioni sono visibili pubblicamente, mentre i bonifici bancari richiedono accertamenti per essere letti dalle autorità;
- pseudonimia: i wallet non sono direttamente collegati a identità reali, ma l'analisi delle transazioni e del comportamento può rivelare l'identità.

Nonostante esistano sistemi avanzati di mixing e riciclaggio per confondere le tracce, l'analisi forense delle criptovalute rappresenta uno strumento potente per contrastare crimini come ransomware, traffici illeciti e riciclaggio internazionale.

L'Open Source Intelligence (OSINT) è stata identificata come componente essenziale dell'attività investigativa moderna. Attraverso l'analisi di fonti aperte (social media, siti web, forum), è possibile ricostruire comportamenti, abitudini e connessioni di individui sospetti.

Le risorse in cloud non si limitano dunque ai soli backup, ma includono tutto il "transitato" di dati che può lasciare tracce anche dopo la cancellazione apparente. Spesso i dati cancellati dai dispositivi rimangono accessibili attraverso copie di backup o cache nel cloud, permettendo di ricostruire attività passate.

La capacità di elaborare e profilare grandi quantità di dati è fondamentale per:

- distinguere informazioni rilevanti da quelle irrilevanti;
- identificare pattern comportamentali;
- scoprire crimini collaterali non immediatamente evidenti;
- abbattere i tempi investigativi in situazioni critiche (scomparse, traffico di esseri umani).

Si è rappresentato come le tradizionali ricerche per parola chiave possono risultare inefficaci poiché la ricerca tradizionale per parola chiave presuppone che tutte le informazioni siano nella stessa "lingua", ma in informatica esistono molteplici linguaggi (testo, immagini, audio, video, metadati). Una ricerca efficace richiede la trasformazione e indicizzazione di tutti i contenuti in un formato uniforme.

1) Audio e contenuti multimediali: un telefono moderno può contenere centinaia di messaggi vocali. Strumenti avanzati permettono di convertire gli audio in testo e analizzare le tendenze, ma richiedono investimenti significativi.
2) Strumenti di triage vs copia forense: molti strumenti di triage in realtà effettuano una copia forense completa (full file system) per poter indicizzare e rendere ricercabili i dati. Questo crea problemi giuridici relativi alla distinzione tra ispezione informatica e acquisizione forense.
3) Mole di dati: un telefono di un adolescente può contenere 300 GB o più di dati. La polizia giudiziaria che effettua la copia forense si trova di fronte a un "mondo" di informazioni, con il problema aggiuntivo di dover discernere cosa sia di interesse investigativo e cosa no, nel rispetto della privacy.

Sono stati introdotti gli scenari a confronto in merito alle tecniche preliminari utilizzate come prassi operativa e le relative problematiche tecnico giuridiche:

1) Ispezione informatica vs acquisizione forense: la normativa italiana prevede l'ispezione informatica come attività distinta dall'acquisizione forense, ma nella pratica gli strumenti utilizzati spesso effettuano copie complete, creando zone grigie interpretative.
2) Tempestività vs garanzie difensive: l'esigenza di tempestività nell'acquisizione delle prove (prima che i dati si autocancellino o si perdano) può entrare in conflitto con le garanzie difensive previste per gli accertamenti tecnici irripetibili ex art. 360 c.p.p.
3) Capacità operative delle forze dell'ordine: gli operatori in prima linea spesso non dispongono delle competenze tecniche necessarie per effettuare un triage efficace, determinando il rischio di perdere prove critiche o, al contrario, di acquisire quantità eccessive di dati non pertinenti.

4) Insufficiente riconoscimento del furto d'identità: in Italia, la sostituzione di persona digitale e il furto d'identità non sono spesso identificati, nonostante siano alla base di molteplici crimini informatici e permettano il riciclaggio internazionale.

In conclusione, l'intervento ha evidenziato come l'attività di profilazione e analisi comportamentale sia diventata essenziale nell'investigazione digitale moderna. Il tecnico informatico forense non è e non deve essere confuso con l'investigatore: il primo fornisce gli strumenti e la "lente" per leggere i dati, il secondo deve ricostruire gli eventi e condurre l'indagine.

Il ruolo dei profiler digitali sta emergendo come figura professionale ibrida tra criminologia e informatica forense, particolarmente nell'ambito della *mobile forensics*. Questa figura è necessaria per:

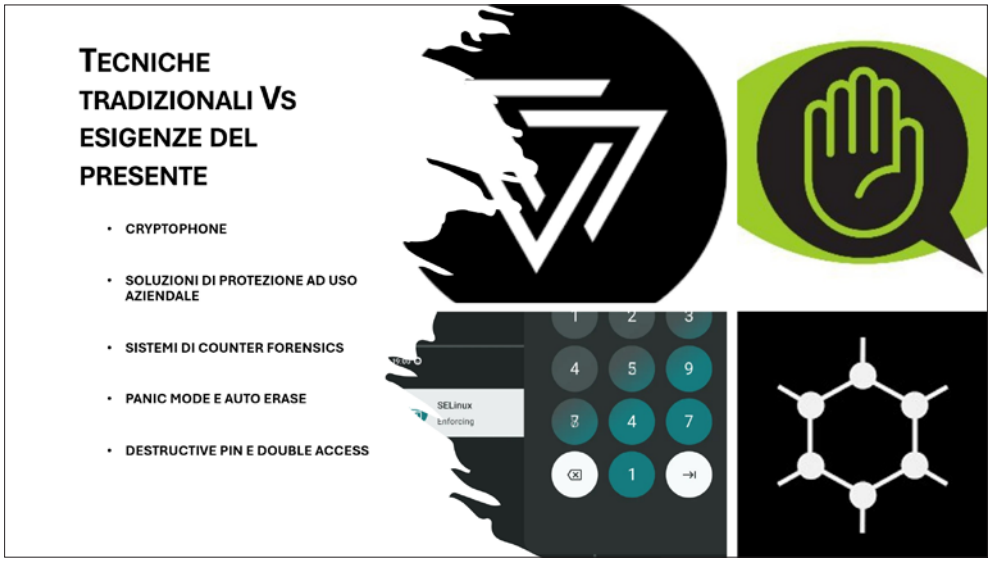
- gestire la complessità e la mole dei dati digitali;
- effettuare triage efficaci in tempi rapidi;
- identificare crimini collaterali o connessi;
- supportare sia le attività investigative che quelle di intelligence.

L'utilizzo illecito delle criptovalute è passato da logiche di finanziamento di attività criminali a strumento trasversale per una stragrande maggioranza di crimini. La capacità di elaborare le transazioni blockchain e correlarle con altre fonti di informazione (OSINT, dati comportamentali, analisi forensi) è fondamentale per contrastare efficacemente la criminalità digitale moderna unitamente alla necessità che il legislatore comprenda profondamente la natura dei crimini informatici, il tutto per fornire strumenti normativi adeguati agli investigatori, evitando zone grigie interpretative e garantendo al contempo il rispetto dei diritti fondamentali e delle garanzie difensive.

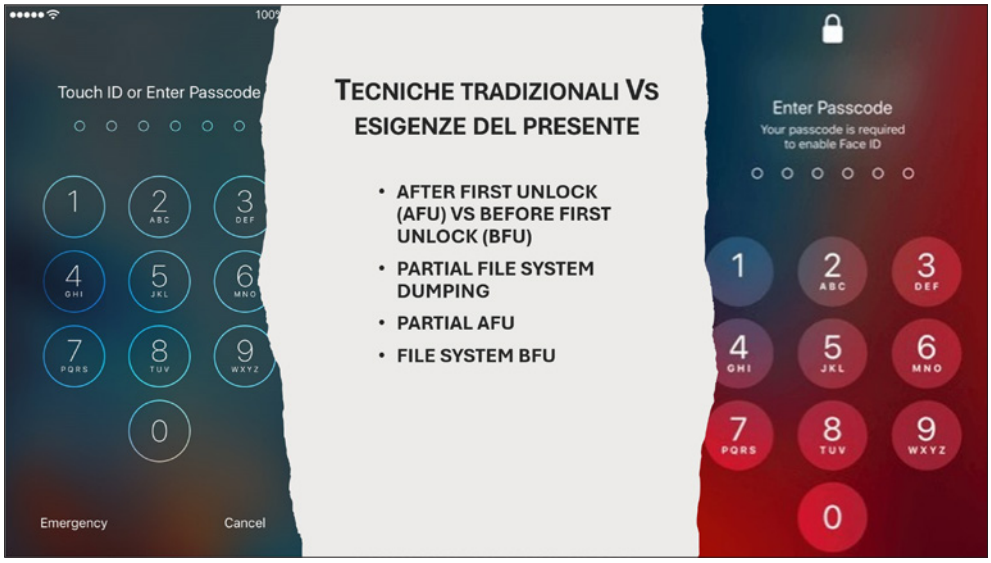

LA RACCOLTA DELLE PROVE INFORMATICHE E DIGITALI
Le tecnologie impiegate ai fini criminali e l'evoluzione delle tecniche operative di acquisizione delle prove
FRANCESCO ZORZI


TECNICHE TRADIZIONALI VS ESIGENZE DEL PRESENTE
• SVILUPPO DEI SISTEMI NATIVI DI PROTEZIONE DEI DISPOSITIVI
• EVOLUZIONE DEI SISTEMI DI MESSAGGISTICA
• EVOLUZIONE DEI SISTEMI DI PAGAMENTO
You set the disappearing message time to 3 hours.
Like as the waves make towards the pebbled shore, so do our minutes hasten to their end


TECNICHE TRADIZIONALI VS ESIGENZE DEL PRESENTE
• METODOLOGIE DI FUNZIONAMENTO CLOUD ORIENTED
• SISTEMI DI CANCELLAZIONE PROGRAMMATA
• SISTEMI DI RIMBALZO DELLE COMUNICAZIONI
wickr


TECNICHE TRADIZIONALI VS ESIGENZE DEL PRESENTE
• CRYPTOPHONE
• SOLUZIONI DI PROTEZIONE AD USO AZIENDALE
• SISTEMI DI COUNTER FORENSICS
• PANIC MODE E AUTO ERASE
• DESTRUCTIVE PIN E DOUBLE ACCESS
SELinux
Enforcing


TECNICHE TRADIZIONALI VS ESIGENZE DEL PRESENTE
• INACTIVITY REBOOT
• WATCHDOG
• INACTIVITY ERASE
• TRAY ERASE
• DOCK ERASE

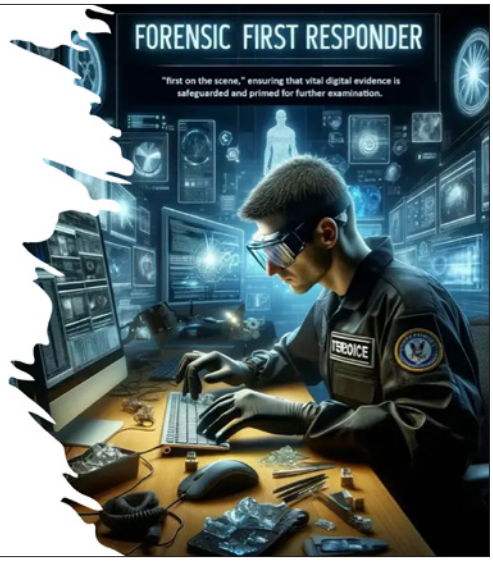

Touch ID or Enter Passcode
Emergency
Cancel
TECNICHE TRADIZIONALI VS ESIGENZE DEL PRESENTE
• AFTER FIRST UNLOCK (AFU) VS BEFORE FIRST UNLOCK (BFU)
• PARTIAL FILE SYSTEM DUMPING
• PARTIAL AFU
• FILE SYSTEM BFU
Enter Passcode
Your passcode is required to enable Face ID


TECNICHE TRADIZIONALI
VS ESIGENZE DEL
PRESENTE
• CONDIZIONI DI SEQUESTRO
• RF SHIELDING
• EMULAZIONE COMUNICAZIONI
• FARADAY BAG


APPLICAZIONI OPERATIVE
DIGITAL INTELLIGENCE
E
COMPUTER FORENSICS

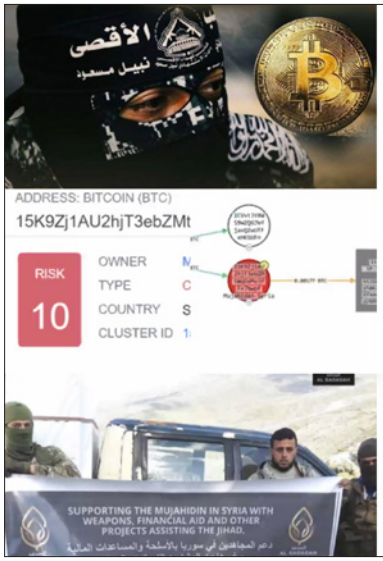
FIRST RESPONDER

- L'IMPORTANZA DEL FIRST LINE APPROACH
- TRIAGE
- MULTIDISCIPLINARITA'



CRIPTOVALUTE

- TIPOLOGIE DI UTILIZZO IN AMBITO CRIMINALE
- L'IMPORTANZA DELL'ACQUISIZIONE PRELIMINARE - TRIAGE
- BLOCK CHAIN SCOUTING



CRIPTOVALUTE ED UTILIZZO CRIMINALE:

- **EVOLUZIONE E CASI DI UTILIZZO**
- **TECNICHE DI CHAIN PARSING**
- **ANALISI E RICOSTRUZIONE DELLE TRANSAZIONI**
- **STUDIO DEL COMPORTAMENTO**

CRIPTOVALUTE: RICERCA, INDIVIDUAZIONE, SEQUESTRO

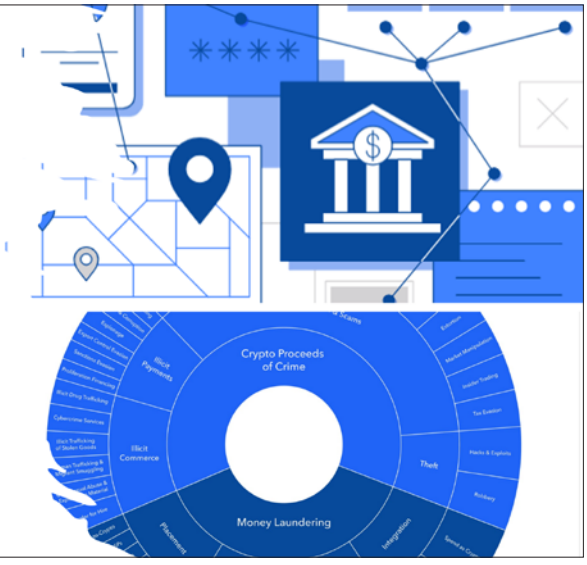
- **L' IMPORTANZA DELLE SOS**
- **IL RUOLO DELLE FIU**
- **BEST PRACTICE NEI SEQUESTRI**

CRIPTOVALUTE: DA VALUTA DI TRANSIZIONE A STRUMENTO

- LA C.O. ED IL NUOVO RICICLAGGIO
- CONVERSIONE SERVICE ORIENTED
- TECNICHE DI FUNDS DELIVERY

CRIPTOVALUTE: APPROCCIO TECNICO

- IMPLEMENTAZIONE DELLE RICOSTRUZIONI BASATE SU MACHINE LEARNING
- APPLICAZIONI A.I. E D.L. NELL'ANALISI FORENSE DELLE TRANSAZIONI
- DATA GATHERING APPLICATO ALLE TECNICHE INVESTIGATIVE




LA RACCOLTA
DELLE PROVE
INFORMATICHE
E DIGITALI
Le tecnologie impiegate ai fini criminali e l'evoluzione delle tecniche operative di acquisizione delle prove
Si ringrazia per la partecipazione
FRANCESCO ZORZI

Capitolo Dodicesimo

Bit-Mafie: criptovalute e riciclaggio

Rosario Patalano

Il riciclaggio è il complesso processo mediante il quale la ricchezza accumulata illecitamente è occultata, trasferita e reinvestita nei circuiti dell'economia legale. Non può esistere una quantificazione univoca del fenomeno ma le stime concordano nell'affermare un'incidenza sull'economia legale significativa e che non tende a dare segnali di contrazione. La criminalità organizzata ha saputo avvalersi delle nuove tecnologie digitali, in particolare il mercato delle *criptovalute*, dove l'operazione di riciclaggio ha potuto sfruttare sia l'anonimato garantito da attività finanziarie decentralizzate (DeFI), sia i vantaggi derivanti da asset fortemente speculativi. Il lavoro analizza gli elementi tecnici alla base del riciclaggio mediante criptovalute, tenta di fornire dati aggiornati sul fenomeno, e ricostruisce il quadro delle misure antiriciclaggio attualmente previste dalla normativa nel mercato DeFi.

Introduzione

Internet è un luogo ideale per il commercio ed è una piattaforma perfetta per le attività di riciclaggio di denaro, poiché le transazioni non rientrano nelle definizioni normative esistenti. Rapido, facile da implementare, difficile da rintracciare ed economico, utilizzando Internet con varie tecniche, è possibile intraprendere tutte le fasi del processo di riciclaggio di denaro, vale a dire le fasi di collocamento, stratificazione o integrazione.

Esistono tre principali tipologie di pagamento informatico: la prima è costituita dai servizi di pagamento via Internet, come i pagamenti mobili, i micropagamenti o i metalli preziosi digitali; la seconda è costituita dalle carte di credito e dalle smart card; la terza è l'online banking. Tuttavia, vi sono altri metodi sempre più utilizzati, come le *dark pool* di criptovalute, il *mining* di criptovalute, la vendita di opere d'arte, i *token non fungibili* (NFT), i bancomat di criptovalute (*crypto ATMs*), nonché la traduzione di beni fisici in beni digitali. Ad essi si aggiungono il gioco d'azzardo online, i giochi e le aste, insieme ai beni virtuali, sempre più frequentemente utilizzati per riciclare denaro. L'apertura di conti e servizi bancari

online può avvenire con l'uso di e-mail che possono essere utilizzate esclusivamente da terminali pubblici, come un Internet café o una biblioteca pubblica, seguire l'accesso e l'utilizzo di un conto.

L'uso di una crittografia di alto livello basata sull'applicazione di metodi che servono a rendere un messaggio intelligibile solo ai soggetti espressamente autorizzati a leggerlo ha reso possibile la nascita e la diffusione delle criptovalute (dette più semplicemente *Bitcoin* dalla più diffusa criptovaluta creata nel 2009) che possono essere create e scambiate tramite una rete decentralizzata di computer, il che significa evitare il coinvolgimento di istituzioni finanziarie o governi in tali transazioni. I criminali possono facilmente camuffare le loro transazioni, inviare *Bitcoin* ovunque, convertirli in contanti e depositarli in banca. I cyber-riciclatori traggono vantaggio per l'incapacità di identificare e autenticare correttamente le parti, oppure dalla mancanza o per le difficoltà di segnalare le transazioni sospette.

Lo scopo di questo lavoro è definire la relazione tra i nuovi strumenti monetari del cyberspazio e l'attività di riciclaggio.

1. *L'attività di cyberlaundering*

Le monete digitali o *virtual currency*[1], tra cui emerge il *Bitcoin*, non potevano sfuggire alle organizzazioni mafiose come strumenti di riciclaggio. L'uso di *Bitcoin* e altre criptovalute da parte della criminalità è un fenomeno complesso e in continua evoluzione. Sebbene una piccola percentuale delle transazioni in criptovalute sia legata ad attività illecite, la criminalità organizzata sfrutta sempre più queste tecnologie per diverse finalità, principalmente a causa della loro natura decentralizzata e della percezione di anonimato. La domanda di transazioni con criptovalute è assecondata da una crescente offerta differenziata di strumenti sempre più sofisticati: dal 2009, data di nascita della prima criptovaluta, il *Bitcoin*, ad oggi, il numero di strumenti è aumentato in modo esponenziale, fino al 2023 si contano più di 40 tipi diversi di *cripto-valute* (tabella 1).

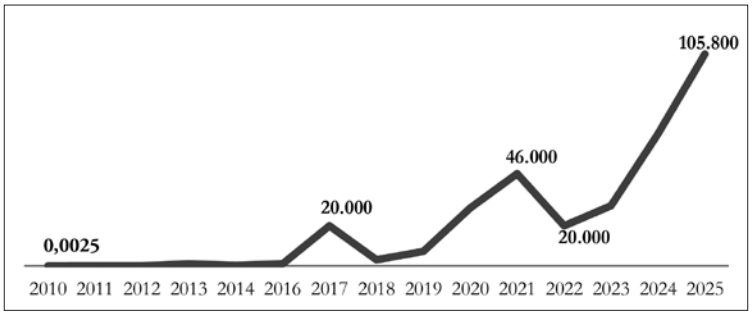
[1] Le *Virtual Currencies* (Valute Virtuali) sono "una rappresentazione digitale di valore che non è stata emessa o garantita da una banca centrale o da un'autorità pubblica e che non è necessariamente collegata a una valuta legalmente istituita (denominata anche fiat money) e che non hanno lo status giuridico di valuta o denaro, ma che sono accettate da persone fisiche o giuridiche come mezzo di scambio e che possono essere trasmesse, immagazzinate e scambiate con mezzi elettronici" (Art. 1, c. 2, D.Lgs. 90/2017).

Tabella 1. Criptovalute attive e non attive (in grassetto corsivo)

Anno	*Criptovaluta*
2009	Bitcoin
2011	Litecoin, Namecoin
2012	Peercoin
2013	Dogecoin, Gridcoin, Primecoin, Ripple, Nxt
2014	Auroracoin, Dash, NEO, MazaCoin, Monero, Titcoin, Verge, Stellar, Vertcoin, Coinye, OneCoin
2015	Ethereum, Ethereum Classic, Nano, Tether
2016	Firo, Zcash
2017	EOS.IO, Cardano, Tron, BitConnect
2018	AmbaCoin, Nervos Network, KodakCoin, PlusToken
2019	Algorand
2020	Avalanche, Polkadot, Shiba Inu, Solana
2021	DeSo, SafeMoon
2023	Arkham, Intel Exchange

Il grafico 1 mostra il valore in dollari di un bitcoin dal 2010 al 2024. Si può notare come abbia subito ampie fluttuazioni in relazione soprattutto alle scelte di regolamentazione e alle ondate speculative. Tra il 2023 e il 2024 il suo valore è aumentato di +98.09%, in cinque anni, l'incremento di valore registrato è stato +1,002.11%, in sette anni è stato +1,717.05%[2].

Grafico 1. Valore in USD di un *Bitcoin* 2010-2024 (valori fine anno). Fonte: https://charts.bitbo.io/price/



[2] Nel corso del 2025 il *Bitcoin* ha mostrato una estrema volatilità raggiungendo nel 2025 il suo massimo storico, toccando i 126.000 dollari. Dopo il picco di ottobre 2025, è iniziata una fase di ribasso. Alcuni report economici negativi (come i dati sull'inflazione negli USA a metà agosto e novembre) e una saturazione del mercato hanno portato il prezzo sotto la soglia di inizio anno, attestandosi nel gennaio 2026 a 89.934 dollari.

Il *Bitcoin*, sin dalla sua genesi nel 2009, ha rappresentato una rivoluzione tecnologica e finanziaria. Concepito come valute digitali decentralizzate e non soggette a controllo governativo, le criptovalute hanno attratto un vasto interesse per le loro potenzialità di innovazione e efficienza.

Garantendo parziale anonimato, basse barriere all'ingresso, negoziabilità globale ed elusività normative, si può affermare che le valute virtuali sono certamente adatte al riciclaggio di denaro. Parallelamente, le stesse caratteristiche intrinseche che le rendono attraenti per gli utenti legittimi – la decentralizzazione, la velocità e l'assenza di confine – hanno sollevato significative preoccupazioni in merito al loro potenziale uso illecito[3].

A differenza dei sistemi finanziari tradizionali, che si basano su intermediari centrali come banche e governi, la rete delle criptovalute opera su un modello *peer-to-peer* ed è basata sulla omonima *blockchain*[4]. Questa architettura elimina la necessità di un'autorità centrale che possa supervisionare, censurare o bloccare le transazioni. Di conseguenza, nessun governo può prenderne il controllo o influenzare la politica monetaria. Per le organizzazioni criminali che operano a livello transnazionale, questa indipendenza rappresenta una garanzia di resilienza e immunità dal controllo statale, un fattore particolarmente rilevante per la raccolta e il deposito di capitali illeciti.

Un altro aspetto fondamentale è l'efficienza transazionale: le transazioni in *Bitcoin* avvengono in modo rapido e con costi potenzialmente molto contenuti, specialmente per i pagamenti internazionali. Mentre un bonifico internazionale può richiedere da tre a sette giorni lavorativi, una transazione in *Bitcoin* si com-

[3] Gli attacchi *ransomware*, che criptano i dati delle vittime e chiedono un riscatto per la decriptazione, hanno quasi universalmente adottato il *Bitcoin* come metodo di pagamento. Secondo un'analisi, il 98% di questi attacchi richiede pagamenti in *Bitcoin*.

[4] La *blockchain* appartiene alle *DLT* (*Distributed Ledger Technologies*) che ha reso possibile lo sviluppo delle criptoattività (o *token*) e, con esse, si è profilata la possibilità di creare un nuovo ecosistema finanziario decentralizzato (DeFi), che funziona senza un'autorità fiduciaria centralizzata e senza intermediari, ovvero quei soggetti su cui fa perno la normativa per il contrasto del riciclaggio. "La DLT consiste in un registro elettronico distribuito sulla rete informatica, condiviso tra i partecipanti (detti nodi), su cui possono essere memorizzate transazioni verificabili e immutabili. L'aggiunta di nuove informazioni al registro non richiede la validazione da parte di un ente centrale di garanzia, ma prevede il raggiungimento di un accordo tra i partecipanti alla rete tramite i c.d. meccanismi di consenso. La blockchain è una specifica categoria di DLT caratterizzata dal raggruppamento delle transazioni in blocchi, concatenati in ordine cronologico (la catena, chain, appunto), per creare un registro non modificabile di tutte le transazioni effettuate" (Gabbiadini - Gobbi - Rubera, 2024: 6).

pleta in circa dieci minuti. Questa velocità, unita alla portabilità e all'immutabilità delle transazioni, riduce i rischi operativi e logistici per chi movimenta grandi quantità di fondi illeciti attraverso i confini.

Con le criptovalute, il processo di riciclaggio ha trovato una nuova frontiera, definita *cyberlaundering*. Il processo tipico consiste nel generare un portafoglio digitale (*wallet*) per ricevere i proventi di attività illecite. Una volta ricevuti i fondi, i criminali impiegano una serie di tecniche di offuscamento per "ripulire" le criptovalute e renderne impossibile la tracciabilità[5]. Contrariamente a quanto comunemente si crede, infatti, le transazioni in *Bitcoin* non sono del tutto anonime, ma piuttosto *pseudo-anonime*. Ogni transazione è registrata in un registro pubblico (la *blockchain*) e può essere visualizzata da chiunque[6]. Le transazioni sono collegate a indirizzi di portafoglio, non a identità personali. Tuttavia, se le autorità riescono a collegare un indirizzo a un'identità reale (ad esempio, attraverso un *exchange* di criptovalute che richiede la verifica dell'identità), è possibile tracciare l'intero flusso di denaro. Aziende specializzate e le forze dell'ordine utilizzano sempre più strumenti sofisticati per analizzare la blockchain e identificare i movimenti illeciti.

La percezione di un "anonimato assoluto" ha costituito la principale attrattiva delle criptovalute per i criminali. Tuttavia, questa percezione si scontra con la realtà tecnica del suo funzionamento. Per contrastare la tracciabilità intrinseca di *Bitcoin,* i criminali hanno sviluppato e utilizzato servizi di *mixer* o *tumbler*, che

[5] Un metodo per mantenere l'anonimato consiste nel depositare i contanti, derivanti da attività illecite su conti correnti intestati a società o titolari di conto e successivamente convertiti in criptovalute. Questo permette di effettuare operazioni illecite, mantenendo l'anonimato e rendendo difficoltosa la tracciabilità delle transazioni.

[6] "La maggior parte degli utenti di criptovalute si affida a nuove forme di intermediari per eseguire transazioni. Il provider globale più noto è il sito web *Kraken*, dove il detentore della chiave pubblica registrata per la criptovaluta autorizza il trasferimento a un'altra chiave pubblica mediante l'uso della chiave privata. Nel mondo delle valute reali, ciò equivale all'incirca alla firma di un assegno o all'utilizzo della procedura PIN/TAN per un bonifico bancario online. Il destinatario decifra i codici ricevuti per ottenere i Bitcoin inviati, che vengono conseguentemente aggiunti al suo portafoglio. I dati della transazione, incluso l'importo in *Bitcoin*, la chiave pubblica del mittente e la chiave pubblica del destinatario, vengono trasmessi a tutti i partecipanti alla rete *Bitcoin* per la relativa verifica. I computer degli altri utenti esaminano i codici individuali dei Bitcoin che, analogamente al DNA, registrano la cronistoria completa della moneta digitale. Questo sistema garantisce la tracciabilità di ogni Bitcoin fino al suo indirizzo originario e documenta le transazioni eseguite. Questo processo può essere visto come una sorta di monitoraggio che rende le transazioni in criptovalute assai più facilmente tracciabili rispetto a quelle in valuta legale" (Nicaso – Rauti – Nasi – Fantacci. 2023: 67-68).

possono essere centralizzati o decentralizzati, mescolando i fondi di più utenti per spezzare il legame tra il mittente e il destinatario di una transazione[7]. L'obiettivo è rendere quasi impossibile per gli osservatori esterni tracciare l'origine dei fondi.

Tuttavia, anche questi strumenti non sono infallibili: i *mixer* centralizzati mantengono un registro delle transazioni che potrebbe essere acquisito dalle forze dell'ordine, compromettendo l'anonimato. Le autorità di regolamentazione hanno sanzionato e, in alcuni casi, smantellato mixer noti come *Blender.io* e *Tornado Cash*. Inoltre, alcuni *exchange* di criptovalute etichettano i fondi provenienti dai mixer come "tainted" (contaminati), bloccando i prelievi verso determinati indirizzi e creando un deterrente per l'uso di questi servizi.

Per eludere le indagini è stata creata una tecnica più recente e complessa, il *chain-hopping,* concepita per eludere le indagini sulla *blockchain*. Consiste nel trasferire rapidamente i fondi tra diverse criptovalute su *blockchain* differenti, utilizzando servizi noti come *blockchain bridges*. L'obiettivo è di "annebbiare la tracciabilità" e complicare il lavoro degli analisti forensi, che devono seguire i fondi attraverso ecosistemi digitali distinti. Nonostante la percezione di anonimato, la natura immutabile e pubblica del registro di *Bitcoin* è diventata un'arma potente per le forze dell'ordine. La *blockchain forensics* è una disciplina investigativa che sfrutta questa trasparenza per tracciare i flussi finanziari illeciti. Gli investigatori utilizzano strumenti specifici per "de-anonimizzare" gli indirizzi, ricostruendo il percorso dei fondi e collegandoli a identità reali o a servizi illeciti. I successi operativi in questo campo sono numerosi.

Il crollo di *Silk Road* nel 2013 è il primo e più emblematico esempio del ruolo del registro pubblico di *Bitcoin* nella risoluzione di un'indagine, e ha segnato un punto di svolta. Nonostante che il fondatore avesse fatto affidamento sulla presunta anonimia del *Bitcoin*, le prove dei trasferimenti di valuta sono state uti-

[7] "I termini *mixer* e *tumbler* descrivono lo stesso servizio. Lo scopo è quello di garantire l'anonimato del mittente e del destinatario di una transazione. Attraverso una serie di transazioni scambiate in rapida successione, è possibile mascherare l'origine delle criptovalute, in modo che il loro trasferimento risulti non-tracciabile, alla stregua di un pagamento in denaro contante. Allo stesso tempo, però, il rischio rappresenta anche un vantaggio, perché a questo punto le monete incriminate si staccano da chi le ha inizialmente collocate nella blockchain. Se le transazioni vengono eseguite sempre tramite la stessa chiave pubblica, può sorgere rapidamente il sospetto di occultamento. Un metodo per fare «perdere le tracce» è quello di scambiare, ad esempio, Bitcoin con altre criptovalute, il che renderebbe eccessivamente complesso il tracciamento delle transazioni perché sarebbe necessario agire su due blockchain differenti" (Nicaso – Rauti – Nasi – Fantacci. 2023: 71).

lizzate contro di lui in tribunale. Un procuratore federale ha liquidato il processo di tracciamento come "niente di molto complicato", poiché si basava su "registri pubblici che mostrano connessioni a uno a uno tra gli indirizzi *Bitcoin*". Questo evento ha dimostrato inequivocabilmente la vulnerabilità dello pseudo-anonimato del *Bitcoin*. Di conseguenza, i mercati successivi hanno iniziato a diversificarsi, e i criminali hanno iniziato a esplorare l'uso di criptovalute con funzionalità di anonimato intrinseche.

Più recentemente, l'FBI ha rintracciato e sequestrato fondi in *Bitcoin* rubati da attori collegati alla Corea del Nord, e la Guardia di Finanza italiana ha sequestrato un portafoglio di criptovalute per un valore di oltre 9 milioni di dollari, riuscendo a seguire le transazioni nonostante i tentativi di offuscamento. Un recente caso investigativo della Guardia di Finanza italiana ha chiarito l'uso di questa tecnica in un presunto caso di riciclaggio, dove oltre 9 milioni di *Tether* (USDT) sono stati convertiti in pochi minuti in *Bitcoin*, *Ethereum* e altre criptovalute, per ostacolare il tracciamento. Nonostante la sofisticazione del metodo, l'analisi forense della *blockchain* ha permesso agli investigatori di seguire i movimenti sospetti e di risalire all'origine illecita dei fondi, portando a un sequestro preventivo.

Le piattaforme di scambio e le autorità di controllo hanno sviluppato la capacità di rilevare specifici "indici di anomalia" che suggeriscono un comportamento criminale[8]. Questi includono: i. modelli di transazione insoliti: trasferimenti frequenti, valori elevati in cifre tonde o operazioni frazionate appena al di sotto delle soglie di segnalazione; *ii.* esposizione geografica: transazioni che coinvolgono giurisdizioni ad alto rischio o con normative antiriciclaggio deboli, spesso incluse nelle liste grigie o nere della *Financial Action Task Force* (FATF); *iii.* dati di identità sospetti: l'utilizzo di documenti falsi o l'incoerenza nei dati KYC (*Know Your Customer*)[9], una tattica che si è evoluta con l'uso di tecnologie

[8] Per condurre queste indagini, le agenzie governative hanno creato unità specializzate e si sono dotate di software di intelligenza avanzati. L'FBI, ad esempio, ha istituito la *Virtual Assets Unit* (VAU) per centralizzare le competenze in materia di criptovalute e fornire supporto tecnologico e analitico alle indagini. A livello italiano, la Guardia di Finanza opera con nuclei specializzati in frodi tecnologiche e polizia valutaria. Queste unità si avvalgono di software di analisi della blockchain forniti da aziende leader di settore come *Chainalysis, Elliptic, TRM Labs e CipherTrace*. Questi strumenti consentono di tracciare le transazioni, valutare i rischi associati agli indirizzi e identificare i flussi di fondi verso entità illecite, come mercati darknet o servizi di riciclaggio. Cfr. Gabbiadini - Gobbi - Rubera, 2024.

[9] È un processo normativo che obbliga le aziende, in particolare quelle finanziarie, a identificare e verificare l'identità dei propri clienti. Questa procedura è fondamentale per la lotta al

come i *deepfake* per aprire portafogli fraudolenti. L'uso di documenti e identità sintetiche per superare i controlli KYC delle piattaforme regolamentate rappresenta un'evoluzione sofisticata del crimine. Questo sposta la responsabilità della conformità sulle piattaforme stesse, che devono implementare strategie antiriciclaggio avanzate, inclusa la due *diligence* sui clienti e il monitoraggio continuo delle transazioni.

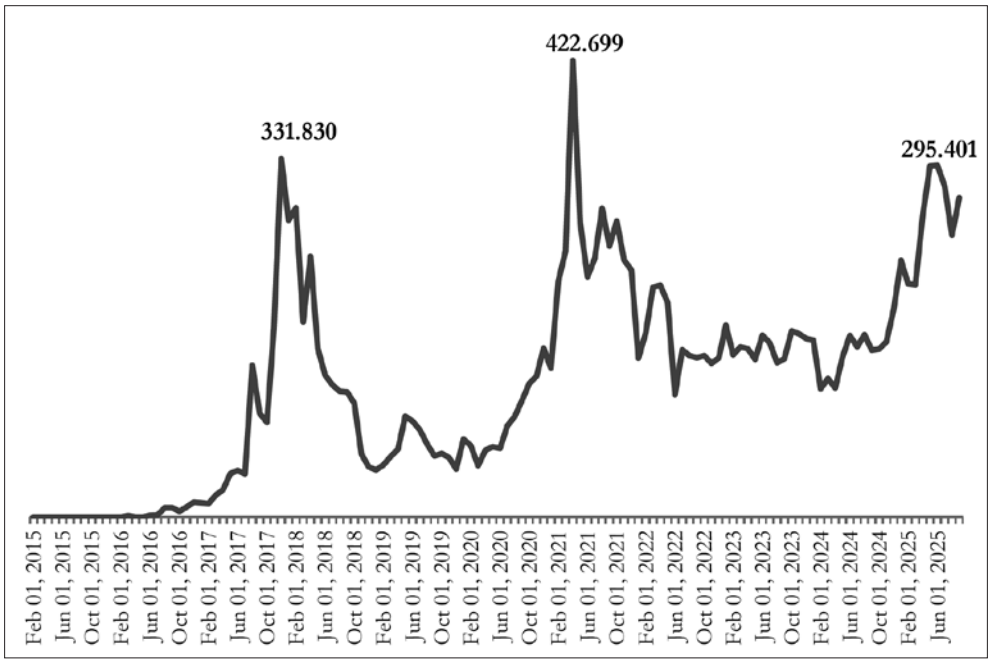
Le operazioni di riciclaggio non avvengono ovviamente utilizzando gli specifici ATM dedicati (se ne stimano circa 1600 in tutto il mondo) in cui depositare valuta e prelevare *Bitcoin*, ma attraverso percorsi più complessi: *i.* il denaro in moneta legale ottenuto dalle attività illecite è depositato su conti correnti intestati a società o singoli e successivamente convertiti in criptovalute. Questo permette di effettuare operazioni illecite, mantenendo l'anonimato e rendendo difficoltosa la tracciabilità e con una serie di transazioni in rapida successione è possibile mascherare l'origine delle criptovalute. *ii.* Un altro metodo per nascondere la tracciabilità è quello di scambiare *Bitcoin* con altre criptovalute, rendendo eccessivamente complesso il tracciamento perché si dovrebbe agire su blockchain differenti. *iii.* È possibile utilizzare un servizio di miscelazione di criptovalute presente sul dark-web, mescolando i *Bitcoin* con quelli di altri utenti e rendendo difficile tracciare l'origine dei fondi ed ottenendo alla fine *Bitcoin* ripuliti con un'origine apparentemente legittima. *iv.* É possibile utilizzare anche transazioni *Peer-to-Peer* (P2P, come *LocalBitcoins* e Paxful) che consentono di comprare e vendere criptovalute direttamente tra utenti evitando la registrazione su piattaforme, con la possibilità di accordarsi sul prezzo e sul metodo di pagamento (bonifici bancari, pagamento in contanti o servizi di pagamento online come *PayPal*). *v.* Possono essere utilizzate carte di debito prepagate, clonate o anonime, che consentono agli utenti di spendere criptovalute in negozi fisici o online, proprio come una carta di debito tradizionale, convertendo automaticamente le criptovalute in valuta al momento della transazione. *vi.* Altre transazioni possono avvenire in mercati on line off-shore, cioè entro giurisdizioni non regolamentate, per scambiare criptovalute con moneta legale. *vii.* Acquisto di beni e servizi in mercati legali (in particolare beni di lusso come gioielli, oro, auto) e rivendita per trarne denaro ripulito. *viii.* Infine convertendo *Bitcoin* in criptovalute con più difficile tracciabilità.

riciclaggio di denaro e al finanziamento del terrorismo, garantendo la conformità alle normative e proteggendo l'azienda e i clienti da attività illegali.

Infatti, a seguito della crescente capacità di tracciamento di *Bitcoin*, i criminali si stanno progressivamente spostando verso criptovalute con funzionalità di anonimato integrate come *Monero* (XMR), creata nell'aprile 2014, che è emersa come la criptovaluta di riferimento per questa transizione. A differenza del *Bitcoin*, che è pseudo-anonimo, *Monero* è progettata per rendere le transazioni completamente anonime e non tracciabili (Calzone, 2017). La tecnologia di *Monero* si basa su tre pilastri per offuscare i dettagli delle transazioni: i. *Ring Signature*: nasconde l'indirizzo del mittente; ii. *Stealth Address*: genera un indirizzo unico per ogni transazione, nascondendo il destinatario; iii. *Ring Confidential Transactions:* nasconde l'importo della transazione.

Questa intrinseca opacità rende *Monero* significativamente più difficile da tracciare per le forze dell'ordine rispetto a *Bitcoin*. La banda *ransomware DarkSide* ha persino incentivato le vittime a utilizzare *Monero* a causa del suo ridotto rischio di tracciamento. Questo fenomeno indica una chiara tendenza della criminalità a migrare verso strumenti che offrono un livello di privacy superiore (il grafico 2 indica il valore in dollari USA del *Monero* tra il 2015 e il 2025).

Grafico 2. Valore in USD di un *Monero* 2015-2025. Fonte: https://www.investing.com/crypto/monero/historical-data



Il confronto tra *Bitcoin* e *Monero*, in termini di attributi tecnici e uso criminale, illustra chiaramente il motivo di questa migrazione (tabella 2).

Tabella 2. Differenze tra bitcoin e Monero.

Caratteristica	*Bitcoin (BTC)*	*Monero (XMR)*
Natura	Pseudo-anonima	Totalmente anonima
Tracciabilità	Registro pubblico e trasparente; ogni transazione è visibile e può essere de-anonimizzata	Registro offuscato; indirizzi e importi nascosti per impostazione predefinita
Funzionalità	Blockchain pubblica	Ring Signature, Stealth Address, Ring Confidential Transactions
Uso Criminale	Inizialmente dominante nei mercati darknet e nel ransomware; ora meno preferito a causa della tracciabilità	In ascesa nei mercati darknet, nel ransomware e nel riciclaggio; preferito per la sua elevata privacy

Le stime sul volume delle transazioni illecite in criptovalute sono state storicamente oggetto di dibattito, con indagini che hanno suggerito percentuali elevate, tuttavia, i dati più recenti e dettagliati forniti da società di analisi specializzate offrono un quadro più preciso. Un report del 2025 di *TRM Labs* indica che, nel 2024, il volume illecito stimato è sceso a 45 miliardi di dollari, rappresentando solo lo 0,4% del volume totale delle criptovalute, in calo rispetto allo 0,9% del 2023. Dati simili sono stati riportati anche da altri analisti, che hanno stimato il volume illecito intorno allo 0,34% del totale. Questa diminuzione in termini percentuali non deve tuttavia mascherare un fatto cruciale: il volume complessivo dell'economia delle criptovalute è cresciuto in modo esponenziale. Nel 2024, il volume totale delle transazioni ha superato i 10,6 trilioni di dollari, con un aumento del 56% rispetto all'anno precedente. Di conseguenza, sebbene la quota percentuale del crimine sia diminuita, il valore assoluto dei fondi illeciti rimane significativo e in evoluzione.

Di seguito, la tabella 3, 4 e 5 illustrano la dinamica quantitativa del fenomeno negli anni recenti, rispettivamente secondo *TRM Labs* e secondo *Chainalysis*[10].

[10] Le stime fornite da diverse fonti di ricerca (come *Chainalysis* e *TRM Labs*) possono variare in modo significativo a causa delle diverse metodologie di raccolta e aggregazione dei dati. Gli operatori di ransomware scelgono il Bitcoin perché è la valuta digitale più facile da acquisire e utilizzare per i pagamenti, anche per le vittime che non hanno mai interagito con le criptovalute. La facilità e la velocità con cui il riscatto può essere trasferito e verificato sulla blockchain superano in molti casi l'esigenza di un anonimato assoluto.

Tabella 3. Volume di transazioni in criptovalute e componente illecita. Anno 2019-2024. Fonte: TRM Labs.

Anno	*Volume Totale delle Criptovalute (Trilioni di USD)*	*Volume Illecito (Miliardi di USD)*	*Percentuale Illecita (%)*
2019	≈3,4	≈21,4	2,1%
2020	≈10	≈10	0,34%
2022	≈4	≈30	0,31
2023	≈6,8	≈ 46	0,9%
2024	≈10,6	≈45	0,4%

Tabella 4. Quota di transazioni illecite effettuate con criptovalute. Fonte: Chainalysis, 2025.

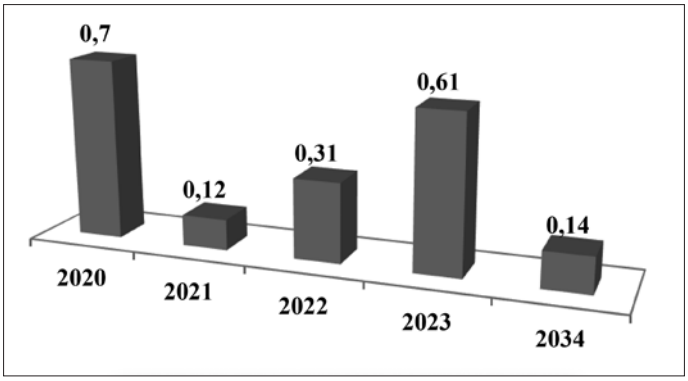


Tabella 5. Valore delle transazioni illecite in Bitcoin, Monero e Stablecoin in miliardi di USD nel 2024. Fonti: TRM, Chainalysis, 2025.

Digital Currency	*Stima dei flussi illeciti in miliardi USD (2024)*	*Percentuale del totale di flussi*
Bitcoin (BTC)	5,4	12% (TRM 2025)
Monero (XMR)		Non determinabile con certezza (privacy coin)
Stablecoins (USDT, USDC, ecc.)	2,58	≈63% (Chainalysis 2025)
Totale Crypto (indirizzi illeciti identificati)	4,09	Total lower-bound: $40.9B (Chainalysis) / TRM: ~$45B

Ma oltre ad uno strumento di riciclaggio l'acquisto di criptovalute, in particolare *Bitcoin*, può rappresentare un ottimo bene rifugio e di investimento, visto che il suo valore ha un trend in ascesa nonostante le larghe fluttuazioni periodiche. Per assicurarsi un valore più stabile sul mercato sono state introdotte le *stablecoin*. A differenza di criptovalute molto volatili come *Bitcoin* (BTC) o

Ethereum (ETH), che possono fluttuare in modo significativo nel giro di ore, le *stablecoin* cercano di mantenere un "ancoraggio" ad un asset di riferimento, solitamente una valuta come il dollaro statunitense o l'euro. L'obiettivo principale delle *stablecoin* è unire i vantaggi delle criptovalute (rapidità, sicurezza, costi ridotti nelle transazioni internazionali, accessibilità globale) con la stabilità di valore delle valute tradizionali. Le *stablecoin* fungono da "ponte" tra il mondo delle criptovalute e quello della finanza tradizionale, i trader possono convertire i loro profitti in *stablecoin* per "mettere al sicuro" il loro valore senza dover uscire completamente dall'ecosistema delle criptovalute e tornare alle valute ordinarie. Si possono distinguere: *i.* le *stablecoin fiat-collateralized* (*Tether, USD Coin, Euro Coin*), supportate da riserve di valuta tradizionale (dollari USA, euro) detenute in conti bancari o in asset equivalenti a basso rischio, come titoli di Stato a breve termine. Per ogni *stablecoin* emessa, l'emittente detiene un importo equivalente nell'asset di riserva; *ii.* le *stablecoin crypto-collateralized* (*Dai*), che sono coperte da altre criptovalute (come *Ethereum* o *Bitcoin*) come garanzia. Per compensare la volatilità del collaterale, queste *stablecoin* sono spesso "sovracollateralizzate", ovvero l'utente deve depositare un valore in criptovaluta superiore a quello della *stablecoin* che vuole coniare; *iii. Stablecoin algoritmiche* (*Terra USD*), che non sono supportate da un collaterale fisico o digitale. Mantengono la stabilità attraverso algoritmi e *smart contract* che regolano in automatico l'offerta di token in base a variazioni della domanda. Se il prezzo scende, il sistema riduce l'offerta; se sale, aumenta l'offerta con l'emissione di nuove monete. Tuttavia, tale sitema non ha mostrato ancora la sua efficienza come dimostra il crollo nel 2022 di *Terra USD*, che ha causato gravi perdite nel mercato *crypto*, dimostrando la fragilità di questo modello se non gestito correttamente; *iv. Stablecoin commodity-collateralized* (*Paxos Gold*, *Tether Gold*), che sono garantite da asset fisici come l'oro o l'argento e ogni *token* rappresenta una quantità specifica della materia prima sottostante, custodita in un caveau. Anche questa tipologia di criptovaluta è soggetta a rischi, in quanto il loro valore fluttua in base al prezzo della materia prima, e quindi non sono del tutto "stabili" come quelle ancorate alle divise più solide.

Un problema non certo trascurabile è la possibilità di creare direttamente criptovalute attraverso l'attività di *mining*, direttamente gestita da organizzazioni criminali. Un primo strumento è il *Cryptojacking* che consiste nel minare criptovalute (spesso il *Monero*, più efficiente da minare su hardware meno potenti) utilizzando le risorse informatiche di terzi, senza il loro consenso. Lo scopo può essere raggiunto o attraverso la diffusione di *Malware* che, una volta installati su un computer o una rete, avviano un programma di mining in background,

all'insaputa dell'utente. I bersagli preferiti sono i server aziendali, i data center o le reti di dispositivi *IoT* (*Internet of Things*), data la loro elevata potenza di calcolo; o attraverso siti web compromessi inserendo script di mining nel codice di siti *WEB*. Quando un utente visita la pagina, il suo browser inizia a minare criptovalute per il criminale, rallentando il dispositivo e consumando energia. Queste operazioni non sono quasi mai il frutto di un singolo hacker, ma richiedono l'impego di reti di *botnet* (centinaia o migliaia di computer, infatti, create e gestite da organizzazioni criminali, per massimizzare la potenza di calcolo e, di conseguenza, i guadagni. La gestione di queste reti richiede infrastrutture complesse e un'organizzazione strutturata, tipica del crimine informatico su larga scala. Le vittime, che possono essere privati cittadini o, più spesso, aziende, subiscono un aumento dei costi energetici, un deterioramento precoce dei componenti hardware e un drastico calo delle prestazioni dei loro sistemi. Sebbene il *mining* in sé sia un'attività legittima, le organizzazioni criminali possono utilizzarlo per riciclare i proventi di altre attività illecite. Questo può avvenire investendo direttamente denaro sporco in grandi *mining farm* (centri di calcolo dedicati al *mining*) per generare denaro pulito in forma di criptovaluta da convertire in valuta ordinaria[11].

[11] Questa attività delle organizzazioni criminali è già ampiamente documentata: nel 2021 la polizia malese ha arrestato sei uomini accusati di aver rubato energia elettrica per un valore di circa 2 milioni di dollari per alimentare un'operazione di mining di *Bitcoin*. Le forze dell'ordine hanno dovuto distruggere oltre 1.000 attrezzature di mining confiscate, un'azione molto mediatizzata per sottolineare la gravità del crimine. Sebbene non sia stato esplicitamente collegato a una nota organizzazione criminale, la natura e la scala dell'operazione suggeriscono un'attività criminale organizzata. Sempre nel 2021, le autorità ucraine hanno smantellato una vasta "mining farm" sotterranea che utilizzava quasi 500.000 kilowattora di elettricità al mese, l'equivalente del consumo di un'intera città. I criminali avevano rubato l'energia da una società statale per il loro profitto, causando ingenti perdite economiche. L'operazione era strutturata e complessa, con implicazioni che vanno oltre il singolo reato. Nel 2020 in Russia sono state segnalate operazioni di mining illegali che si connettevano illegalmente alla rete elettrica nazionale per evitare di pagare le bollette. Spesso queste operazioni erano condotte in luoghi isolati o in ex stabilimenti industriali, e le indagini hanno rivelato una struttura di tipo mafioso per la gestione e la protezione delle attività. Diversi rapporti di intelligence e di sicurezza informatica hanno evidenziato come le organizzazioni criminali russe e cinesi abbiano investito ingenti somme di denaro sporco nella costruzione di gigantesche mining farm. La criptovaluta generata dal mining (come Bitcoin o Ethereum) è intrinsecamente "pulita" in quanto non ha una storia precedente di transazioni illecite. Una volta che le criptovalute vengono coniate, possono essere convertite in valuta fiat, "ripulendo" di fatto l'intero capitale iniziale. Questi casi sono spesso difficili da provare in tribunale, ma le agenzie di intelligence e le forze dell'ordine monitorano regolarmente queste attività come parte delle loro indagini sul riciclaggio di denaro.

In questo modo la criminalità organizzata ha raggiunto il potere di *creare direttamente moneta*, assumendo una maggiore capacità di condizionare l'economia ed estendere la sua egemonia nella società.

Una indagine recente condotta sulla estrazione di Helium ha rivelato una anomalia nella regione di Crotone e nella Locride, in cui la presenza di hotspot per persona è superiore alla media nazionale, pari a 0,59, attestandosi rispettivamente a 2,23 e a 1,44, rivelando la presenza di attività che è sicuramente indirizzata alla creazione di *mining* (Nicaso - Rauti - Nasi - Fantacci, 2023: 91-92).

2. *Conclusioni*

Il crimine organizzato si avvale delle opportunità offerte dalla tecnologia informatica ed è ormai un dato consolidato che il WEB offre al crimine sia nuove fonti di arricchimento illecito sia strumenti per riciclare la ricchezza accumulata illegalmente (Di Nicola - Baratto - Vettori, 2025). Occorre però distinguere la componente mafiosa dal contesto generale del crimine organizzato, in quanto la caratteristica delle mafie è data dalla loro capacità di penetrare nella economia legale, una caratteristica che è invece estranea ad una organizzazione criminale nata per perseguire scopi illeciti particolari senza obiettivi di potere economico su cui costruire consenso sociale e politico. In altre parole, le mafie hanno come obiettivo di diventare parte integrante della economia legale pur avendo fonti di accumulazione illegale, provenienti in primo luogo dal narcotraffico.

La fase attuale di sviluppo del modo di produzione capitalistico consente la formazione di aree di capitalismo criminale, in cui le mafie entrano nell'economia legale e costruiscono in questo modo consenso sociale, divenendo di fatto una vera e propria formazione sociale, in grado di ritagliare spazi di potere economico e politico e governare di fatto intere aree sottratte al controllo degli Stati (Patalano, 2020, 2024; Iezzi P., Razzante R., 2024). Se in alcuni paesi come in America Latina, il fenomeno di formazioni sociali di questo tipo è evidente, nei paesi occidentali, il potere mafioso appare più discreto e subdolo, ma sempre interessato "ad ambiti affaristico-imprenditoriali, approfittando della disponibilità di ingenti capitali accumulati con le tradizionali attività illecite" (DIA, 2023: 4).

L'attività di *cyberlaundering* ha inquietanti possibilità di sviluppo nella creazione di criptovalute mediante l'attività di mining, a cui le organizzazioni criminali possano accedere, anche con rilevanti investimenti, per poter avviare direttamente una fase di creazione monetaria e rivoluzionare completamente il riciclaggio.

Bibliografia

Calzone O., *Servizi di Mixing e Monero*, *Il mondo dell'intelligence,* 2017, www.sicurezzanazionale.gov.it, disponibile on line

Chainalysis, *Crypto Crime Report*, 2025

DIA, Direzione Investigativa Antimafia, *Relazione Secondo Semestre 2023*, Roma, 2023

Di Nicola A. – Baratto G. – Vettori, B., *Criminological definitions of organized crime on the digital test bench: towards a physical–digital framework*, in *Trends in Organized Crime*, 2025, disponible on line https://doi.org/10.1007/s12117-025-09575-3

Gabbiadini R. – Gobbi L. – Rubera E., *Riciclaggio e blockchain: si può seguire la traccia nel mondo cripto?*, in «Questioni di Economia e Finanza», Occasional Papers,893 – Novembre 2024, Roma: Banca d'Italia.

Iezzi P. – Razzante R., *Algoritmo criminale. Come mafia, cyber e AI riscrivono le regole del gioco*, Milano, Il Sole 24 Ore, 2024.

Nicaso A. – Rauti A. W. – Nasi G. – Fantacci L., *The Dark-Web Side of Mafias appalti, crypto e cybercrime. Le mafie adesso: più invisibili e potenti,* Zolfo Editore, 2023.

Patalano R., *Capitalismo criminale. Analisi economica del crimine organizzato*, Torino, Giappichelli, Torino, 2020.

Patalano R., *Criminal capitalism: a new socio-economic formation*, in «Cambridge Journal of Economics», 2024, 48, pp. 329–361.

TRM. 2025. *Crypto Crime Report. Key trends that shaped the illicit crypto market in 2024*, disponibile online: https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

Autori

Andrea Alberico è professore associato di Diritto penale presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Napoli Federico II.

Giovanni Cocozza è professore associato di Diritto amministrativo e pubblico presso il Dipartimento di Scienze Politiche dell'Università degli Studi di Napoli Federico II.

Carlo Colapietro è professore ordinario di Diritto costituzionale e pubblico presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre.

Giacomo Di Gennaro è professore ordinario di Sociologia giuridica e della devianza, insegna criminologia e criminologia applicata al Dipartimento di Scienze Politiche dell'Università degli Studi di Napoli Federico II.

Roberto Flor è professore associato di Diritto penale informatico presso il Dipartimento di Giurisprudenza dell'Università di Verona ove insegna anche Legal Studies and Comparative Law.

Ivano Gabrielli è Direttore del Servizio Polizia Postale e per la sicurezza cibernetica, incardinato nella neoistituita Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, che ha ereditato anche le storiche competenze del Servizio Polizia Postale e delle Comunicazioni.

Gianluca Ignagni è esperto di Cybersecurity ed è Capo Servizio della Divisione Affari giuridici e legislativi, nonché Capo di Gabinetto dell'Agenzia per la cybersicurezza nazionale (ACN).

Vincenzo Molinese generale di Brigata dell'Arma dei Carabinieri, è Comandante del Reparto Investigativo speciale dei Ros, l'unico con competenza centralizzata sulla criminalità organizzata e sul terrorismo.

Rosario Patalano è professore ordinario di Storia del pensiero economico e Storia economica delle mafie e dei Reati finanziari, insegna presso il Dipartimento di Giurisprudenza e di Scienze Politiche dell'Università degli Studi di Napoli, Federico II.

Simon Pietro Romano è professore ordinario di Data Security and Computer forensics e di Network security presso il Dipartimento di Electrical Engineering and Information Technology (Dieti) dell'Università degli Studi di Napoli, Federico II.

Pasquale Troncone è professore associato di Diritto penale dell'economia e Diritto penitenziario presso il Dipartimento di Giurisprudenza e di Scienze Politiche dell'Università degli Studi di Napoli, Federico II.

Giorgio Ventre è professore ordinario di Sistemi di elaborazione delle informazioni e Reti di Calcolatori presso il Dipartimento di Electrical Engineering and Information Technology (Dieti) dell'Università degli Studi di Napoli, Federico II ed è stato il co-fondatore dell'Apple Developer Academy della Federico II.

Francesco Zorzi, ingegnere esperto IT & Cybersecurity, è Senior advisor in Cybersecurity, Chief Technical Consultant Cybersecurity and Forensic DevitaLaw; è Testimone qualificato per la Scuola di Polizia Economico-Finanziaria della Guardia di Finanza; nonché docente specializzato in corsi e seminari in materia di sistemi e applicazioni di sicurezza IT per aziende, infrastrutture critiche e applicazioni pubbliche.

Studi e Ricerche in Scienze Criminologiche, Giuridiche e Sociali

Il tema della sicurezza informatica sta assumendo un ruolo sempre più importante nella contemporaneità che si fonda sulla operatività di una Rete globale dei sistemi e delle informazioni. Una Rete che si sviluppa con infrastrutture che, oltre a coprire il territorio nazionale, si interconnettono in un circuito tecnologico transnazionale. La cybersicurezza, pur nella porosità della legislazione nazionale e sovranazionale, sta divenendo centrale nel più ampio processo di digitalizzazione che sta investendo sia le istituzioni pubbliche che gli attori del settore privato. Sono qui presentati gli atti del convegno "Modelli di cybersecurity e prevenzione dei cyber crimes", tenutosi, nell'ambito Progetto PNRR Hard Disc Spoke 1, il 24 gennaio 2025 presso il Dipartimento di Scienze Politiche dell'Università degli Studi di Napoli Federico II. Il testo raccoglie i contributi di accademici, professionisti e rappresentanti della pubblica amministrazione che, da prospettive disciplinari differenti, si sono confrontati sugli assetti altamente dinamici che intersecano le sfere del diritto, dell'economia, delle relazioni internazionali e della tecnologia, al fine di promuovere un modello di prevenzione di tali fenomeni attraverso una legislazione più armonica.

Giacomo Di Gennaro è ordinario di Sociologia giuridica e della devianza e insegna criminologia e criminologia applicata presso il Dipartimento di Scienze Politiche dell'Università Federico II di Napoli. Coordina il nuovo Corso di Studi Magistrale in *Scienze criminologiche, investigative e cyber crime*, nonché il Master di II livello in *Criminologia e diritto penale. Analisi criminale e politiche per la sicurezza urbana* presso lo stesso Dipartimento. È autore di oltre 160 pubblicazioni a livello nazionale e internazionale; è direttore di diverse collane editoriali e membro di comitati scientifici di riviste. Tra le più recenti pubblicazioni si segnalano, *Il potere delle estorsioni*, Editoriale scientifica 2023; in coll. con R. Aurilia, *Neotenia, competenze adattive alla vita e organizzazione criminale*, in M.L. Iavarone (eds), *Neotenia e plasticità umana*, FrancoAngeli 2025; con Gen.le M. Minicucci, *I frontalieri digitali. Reti e strategie per truffare gli anziani*, Federico II University Press, fedOAPress Napoli 2025.

ISBN 978-88-6887-404-9