RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0255 • articolo sottoposto a peer review • pubblicato in anteprima il 22 dic. 2025

Gaia Fiorinelli

La recente "disciplina penale" del *cybercrime* tra armonizzazione internazionale e interventi nazionali: convergenze parallele?

La tutela penale del cyberspazio è stata, per lungo tempo, il terreno privilegiato di una politica criminale quasi esclusivamente "armonizzata" a livello internazionale ed europeo. Negli ultimi anni, tuttavia, emergono due tendenze divergenti. Da un lato, nella dimensione globale si registra una rilevante evoluzione con l'adozione della Convenzione ONU contro il Cybercrime (2024) e la *Draft Policy on Cyber-Enabled Crimes* (2025) dell'Ufficio del Procuratore della Corte Penale Internazionale, che qualificano il cybercrime come una minaccia rilevante nell'interesse dell'intera comunità internazionale. Dall'altro lato, si moltiplicano in questa materia le iniziative unilaterali dei legislatori statali, soprattutto in aree percepite come strategiche per la sicurezza e l'interesse nazionale (ad esempio, attacchi *ransomware*, FIMI, disinformazione). La ricerca analizza criticamente questa sovrapposizione di interventi penalistici, assumendo il concetto di (cyber)sicurezza come prisma interpretativo che scompone – ma al tempo stesso connette – la politica criminale in materia di *cybercrime*, tra equilibrio geopolitico globale e tutela della sicurezza nazionale.

Cybercrime – Cybersicurezza – Diritto penale – Armonizzazione – Sicurezza nazionale

The emerging criminal law framework on cybercrime between international harmonization and domestic interventions: Parallel convergences?

The criminal-law protection of cyberspace has long been the privileged domain of a criminal policy that was almost exclusively "harmonized" at the international and European levels. In recent years, however, two diverging trends have emerged. On one hand, the global dimension has seen further developments with the adoption of the UN Convention against Cybercrime (2024) and the Draft Policy on Cyber-Enabled Crimes released by the Office of the Prosecutor of the International Criminal Court (2025), which classify cybercrime as a significant threat to the interests of the international community as a whole. On the other hand, unilateral initiatives by national legislators have multiplied in this field, particularly in areas perceived as strategic for security and national interests (e.g., ransomware attacks, FIMI, disinformation). This research critically examines the overlapping layers of criminal-law interventions, using the concept of (cyber)security as an interpretive lens that both breaks down – and at the same time connects – criminal policy in the field of cybercrime, situated between global geopolitical balance and the protection of national security.

Cybercrime – Cybersecurity – Criminal law – Harmonization – National security

L'Autrice è ricercatrice TD-A in Diritto penale presso la Scuola Superiore Sant'Anna di Pisa

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

Sommario: 1. La "storia" della tutela (penale) del cyberspazio. Dall'armonizzazione internazionale ed europea all'abbandono del diritto penale. – 2. Prima traiettoria evolutiva: la riscoperta del diritto penale (globale) per la protezione della cybersicurezza. – 3. Seconda traiettoria evolutiva: *pur un linguaggio nel mondo non (più) s'usa*. L'emergere dei legislatori penali nazionali nel cyberspazio. – 4. La recente trasformazione del diritto penale italiano: dal contrasto al *cybercrime* alla tutela della cybersicurezza nazionale. – 5. Riflessioni conclusive: riconciliare *sicurezza* e *diritti* nella politica criminale multilivello del cyberspazio.

1. La "storia" della tutela (penale) del cyberspazio. Dall'armonizzazione internazionale ed europea all'abbandono del diritto penale.

Per elaborare un'analisi critica delle più recenti traiettorie evolutive della "disciplina penale" del *cybercrime*, è indispensabile ripercorrerne brevemente gli antecedenti storici e la relativa impostazione politico-criminale[1]. Al riguardo, è ben noto come la criminalità informatica rappresenti una delle prime aree nelle quali – nel contesto trans-nazionale ed europeo – si sono sperimentati i moduli dell'armonizzazione (sostanziale) e della cooperazione (procedurale) penale[2]. Anzi, per lungo tempo la tutela penale del cyberspazio è stata concepita come oggetto di una politica criminale *necessariamente* coordinata al di sopra del livello statale, in ragione della dimensione strutturalmente trans-nazionale delle tecnologie informatiche e digitali e, dunque, del relativo uso criminale[3]. Ciò è tanto vero che, nel corso degli anni, sono stati adottati ben otto trattati per il contrasto al *cybercrime*, in seno a sei diverse organizzazioni internazionali, di portata regionale[4].

Limitando l'attenzione ai soli strumenti rilevanti per l'ordinamento italiano, deve però evidenziarsi sin d'ora come i diversi interventi di armonizzazione che si sono susseguiti in questo

1. Per una prospettiva storica su questa materia, cfr. Brodowski 2021.
2. Cfr. Chiavario-Perduca 2022, p. 1, i quali sottolineano, rispetto allo sviluppo della cooperazione penale, il "peso" del "vertiginoso progresso tecnologico in certi settori di alta specializzazione, con la sua idoneità ad agevolare, tra l'altro, movimenti illeciti di capitali e ad aprire la strada a forme sempre più sofisticate di reati 'informatici'".
3. Cfr. in generale Wang 2025; Flor 2023; Spiezia 2023; Schjolberg 2008.
4. Cfr. Wang 2025, p. 236: vi rientrano il Consiglio d'Europa, la Comunità degli Stati Indipendenti (CIS); l'Organizzazione per la Cooperazione di Shanghai (SCO); la Lega araba; la Comunità economica degli Stati dell'Africa occidentale (ECOWAS); l'Unione Africana (AU).

settore siano stati contraddistinti – quantomeno in una prima fase – da un approccio ben più *pragmatico* che *assiologico* al contrasto della criminalità informatica. Con ciò si intende sottolineare, nello specifico, come l'avvicinamento delle disposizioni penali *sostanziali* sia stato generalmente concepito, in tali strumenti, come mero presupposto servente per una più efficace cooperazione *procedurale*, piuttosto che per l'effettivo perseguimento di una politica criminale comune[5]. In questo senso, si è non a caso rilevata in dottrina l'assenza di una vera e propria "azione collettiva globale" contro la cyber-criminalità e, dunque, si è discusso di un'armonizzazione "frammentata"[6].

Un approccio di questo tipo emerge, a ben vedere, già nella prima Raccomandazione OCSE del 1986[7] in materia di *computer-related crime*, la quale muove da una ricognizione delle soluzioni elaborate a livello nazionale, per concludere suggerendo l'adozione di un approccio coordinato, a livello internazionale, idoneo a consentire l'efficace funzionamento degli strumenti di cooperazione giudiziaria e scongiurare l'esistenza di "*computer crime heavens*"[8]. Analoga è anche la visione che emerge dalla Raccomandazione R(89) 9 del Consiglio di Europa[9], nella quale l'armonizzazione del diritto penale sostanziale, pur se non priva di una qualche autonomia concettuale, è direttamente strumentale all'obiettivo di facilitare la cooperazione a livello internazionale.

Un'impostazione similare contraddistingue, a ben vedere, anche la stessa Convenzione del Consiglio d'Europa sulla Criminalità informatica, firmata a Budapest nel 2001[10], la quale – nel suo Preambolo – allude appunto allo scopo primario di promuovere la cooperazione degli Stati parte nel contrasto alla criminalità informatica. Secondo quanto si legge nella Relazione esplicativa, la definizione di un *common minimum standard* nell'ambito del diritto penale sostanziale è intesa a facilitare il contrasto al *cybercrime* sia a livello nazionale che internazionale, quale presupposto per promuovere il ricorso agli strumenti della cooperazione giudiziaria e dello scambio di conoscenze e di esperienze nella trattazione dei casi[11]. Con ciò non s'intende certo negare l'importanza delle definizioni e delle disposizioni di carattere sostanziale contenute nella Convenzione: nondimeno, è noto come le differenti sensibilità dei legislatori nazionali in relazione alla criminalizzazione dei comportamenti illeciti e alla protezione dei diritti fondamentali online abbiano limitato la definizione degli obblighi sostanziali di criminalizzazione al "minimo comune denominatore" rinvenibile tra gli Stati parte, riservando alla legislazione procedurale un ben più ampio ambito applicativo[12]. In questo senso, si è discusso di un modello pragmatico di "armonizzazione flessibile"[13], che coniuga l'esigenza di uniformità con il rispetto delle peculiarità giuridiche e culturali di ogni Stato e che, come si anticipava, non può intendersi, a dispetto delle intenzioni, come una politica criminale globale di contrasto alla criminalità informatica.

Volgendo lo sguardo alla produzione legislativa dell'Unione europea in questo ambito, deve richiamarsi la norma generale di cui all'art. 83 TFUE,

5. In questa direzione, cfr. Brunhober 2022, p. 245.
6. Cfr. in questo senso Wang 2025, p. 236; Brunhober 2022, p. 244; Clough 2014, p. 730.
7. Cfr. OCSE, *Computer-related crime: analysis of legal policy*, Paris, 1986.
8. *Ivi*, p. 64 ss.
9. Cfr. Consiglio d'Europa, Comitato dei Ministri, *Raccomandazione n. R(89)9 del Comitato dei Ministri agli Stati Membri sul crimine informatico*, adottata dal Comitato dei Ministri in data 13 settembre 1989 alla 428ª riunione dei Deputati dei Ministeri, nonché European Committee on Crime Problems, *Computer-related crime*, Council of Europe Publishing and Documentation Services, 1990.
10. Cfr. Consiglio d'Europa, *Convenzione sulla criminalità informatica*, Budapest, 2001.
11. Cfr. Consiglio d'Europa, *Explanatory Report to the Convention on Cybercrime*, 2001, p. 7.
12. Cfr. in generale Clough 2014. L'ambito di applicazione delle disposizioni procedurali è individuato dall'art. 14 della Convenzione, non soltanto con riferimento alle fattispecie penali introdotte nella Sezione relativa al diritto penale sostanziale, ma anche agli altri reati commessi utilizzando tecnologie informatiche, e persino a tutti i casi nei quali sia necessaria la raccolta delle prove in formato elettronico.
13. Cfr. in questi termini Clough 2014, p. 709.

che ora funge da cornice sistematica per tutti gli interventi dell'Unione in materia penale. In essa, la "criminalità informatica" è appunto annoverata tra le materie nelle quali può esplicarsi la competenza penale dell'Unione europea, in ragione della sua intrinseca "dimensione transnazionale" e della sua "particolare gravità", nonché dell'esigenza di contrastarla "su basi comuni". Prima della vigenza di tale disposizione, già la Decisione Quadro n. 222 del 2005[14] si poneva l'obiettivo di migliorare la cooperazione tra le autorità giudiziarie degli Stati membri, proprio mediante il ravvicinamento delle relative legislazioni penali nel settore degli attacchi contro i sistemi di informazione. Com'è noto, la traiettoria di intervento inaugurata dalla Decisione Quadro è stata poi ulteriormente sviluppata con la Direttiva 2013/40/UE, la quale ugualmente si propone l'obiettivo di "ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione", attraverso l'introduzione di norme di diritto sostanziale preordinate alla definizione delle fattispecie rilevanti e all'introduzione delle relative sanzioni: tutto ciò, nella prospettiva di "migliorare la cooperazione fra le autorità competenti"[15].

Com'è stato rilevato, se l'obiettivo primario del diritto penale transnazionale, al quale sono ascrivibili tutte le iniziative considerate, è quello di "promuovere la cooperazione interstatale", le disposizioni di diritto penale sostanziale non possono che risentire di questa "dipendenza" dalle norme procedurali, mancando di un solido sostrato valoriale condiviso[16].

In parallelo con le ultime fasi di tale evoluzione, a livello europeo si è tuttavia affermato un diverso modello d'intervento, che ha progressivamente affiancato (e poi quasi sostituito) le precedenti misure di repressione della criminalità informatica, segnando per certi versi la fine della centralità del diritto penale in questo ambito. Si fa riferimento, com'è noto, alla gestione "preventiva" della "sicurezza informatica", o cybersicurezza[17], che ha segnato il passaggio dal precedente approccio "difensivo"/"deterrente" – imperniato, per l'appunto, sul ricorso al diritto penale – a una diversa impostazione di stampo "protettivo"/"offensivo", fondata sulla previsione di obblighi di protezione delle infrastrutture cibernetiche da parte dei rispettivi titolari[18].

Esula beninteso dalla presente analisi una più diffusa ricostruzione del diritto extra-penale della cybersicurezza. Il tema merita un cenno, tuttavia, per due essenziali ragioni. Da un lato, perché esso segna (quanto meno nel contesto europeo) il passaggio a un modello "integrato", "proattivo e reattivo"[19] di difesa della sicurezza informatica: e ciò sul presupposto che per "ridurre drasticamente il *cybercrime*" sia necessario e più efficace, in luogo dello strumentario penalistico, lo sviluppo di risorse industriali e tecnologiche adeguate a garantire e rafforzare preventivamente la resistenza e la resilienza delle infrastrutture digitali[20]. Dall'altro lato, perché la stessa politica europea in materia di cybersicurezza ha attribuito a tale concetto una valenza polisemica – da mero requisito tecnico a vera e propria condizione di esistenza e di tutela dei diritti nel cyberspazio[21] –, che ha profondamente

14. Cfr. la Decisione Quadro 2005/222/GAI del Consiglio relativa agli attacchi contro i sistemi di informazione, del 24 febbraio 2005.
15. Cfr. la Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. Con riferimento alle competenze penali dell'UE in materia di criminalità informatica, cfr. in generale Picotti 2011.
16. Cfr. Brunhober 2022, p. 244. Cfr. anche Sieber 1998, per il primigenio collegamento tra i due profili dell'armonizzazione (sostanziale) e della cooperazione (procedurale).
17. In argomento cfr. Flor 2019.
18. In questi termini cfr. Chesney 2020.
19. Cfr. Flor 2019, p. 456.
20. Cfr. la Comunicazione congiunta al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1, 7 febbraio 2013.
21. Cfr. De Vergottini 2019.

condizionato le stesse scelte statali in materia di tutela della sicurezza nazionale[22], con alcuni riflessi sulle opzioni politico-criminali *domestiche* e non più trans-nazionali.

Limitandoci ad alcuni cenni, già la prima "Strategia dell'Unione europea per la cybersicurezza: un ciberspazio aperto e sicuro" del 2013[23] rilevava l'esigenza di "sicurezza" del cyberspazio rispetto a "incidenti, attività dolose e abusi": da proteggere, dunque, tanto da "attacchi criminali, di natura politica o terroristica, o commissionati da uno Stato", quanto da "calamità naturali e errori non intenzionali". Le priorità strategiche affiancavano, tuttavia, alla riduzione del *cybercrime* mediante il diritto penale anche nuovi obiettivi di cyber-resilienza, cyber-difesa e cybersicurezza, da perseguirsi mediante interventi coordinati di carattere politico, economico e tecnologico, che consentissero "una protezione forte e una promozione efficace dei diritti dei cittadini" quale condizione della "sicurezza" del cyberspazio[24]. Ma il collegamento assiologico e funzionale tra cybersicurezza e "sicurezza" risulta ancora più esplicito nella successiva Comunicazione del luglio 2017, "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"[25], nella misura in cui essa considera le "attività informatiche dolose" non più soltanto come minacce di consistenza "economica", eventualmente idonee a pregiudicare "il mercato unico digitale", ma anzitutto quali operazioni capaci di compromettere "il funzionamento stesso delle nostre democrazie, le nostre libertà e i nostri valori"[26].

In parallelo, a mutare sono anche i "soggetti" dai quali provengono le "cyber-minacce": non più solamente i "criminali motivati dal profitto", ma anche attori che agiscono per "motivazioni politiche e strategiche", la cui azione diventa tanto più allarmante alla luce del rilievo che "nella stragrande maggioranza dei casi, le possibilità di rintracciare i criminali sono minime e quelle di poter procedere ad azioni penali ancor più esigue"[27]. I pilastri strategici sono perciò individuati, tra gli altri, nel rafforzamento della resilienza agli attacchi, nella certificazione dei requisiti di cybersicurezza, nel potenziamento della risposta politica e di cyber-difesa. È significativo che l'obiettivo della creazione di una "deterrenza cibernetica efficace" non sia più perseguito mediante interventi sul piano del diritto penale sostanziale, ma soltanto attraverso la promozione di miglioramenti procedurali nell'identificazione degli autori degli attacchi e il miglioramento dell'effettiva "capacità di risposta" delle autorità di contrasto, anche attraverso la cooperazione investigativa e giudiziaria[28].

Analogamente, pure la coeva Risoluzione del Parlamento Europeo in materia di criminalità informatica[29], muovendo dal rilievo che il *cybercrime* non comporti soltanto pregiudizi economici, ma rappresenti attualmente una "minaccia" per "i diritti fondamentali delle persone fisiche" e "per lo Stato di diritto", articola la strategia di risposta tra prevenzione, responsabilizzazione dei fornitori di servizi e intensificazione della cooperazione di polizia e giudiziaria, anche con i Paesi terzi, nulla dicendo in materia di diritto penale sostanziale. Infine, anche nella successiva Strategia Europea per la Cybersicurezza del 2020[30], si rende ancor più esplicito che la "la cibersicurezza è parte integrante della sicurezza degli europei"[31] e che le minacce informatiche possono altresì pregiudicare

22. Cfr. Longo 2024, p. 203 ss.; Borriello–Fristachi 2022, p. 157 ss.
23. Cfr. ancora la *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*. Cfr. anche, in generale, Porcedda 2023, p. 45 ss.
24. Cfr. nuovamente la *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro.*
25. Cfr. la Comunicazione congiunta al Parlamento europeo e al Consiglio, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450, 13 settembre 2017; in argomento, cfr. Porcedda 2023, p. 49 ss.
26. Cfr. la Comunicazione *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE.*
27. *Ibidem*.
28. *Ibidem*.
29. Cfr. la Risoluzione del Parlamento europeo del 3 ottobre 2017, *Lotta alla criminalità informatica*, (2017/2068(INI)).
30. Cfr. la Comunicazione congiunta al Parlamento europeo e al Consiglio, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020) 18, 16 dicembre 2020; cfr. ancora l'analisi di Porcedda 2023, p. 51 ss.
31. Cfr. ancora la Comunicazione *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*.

la salvaguardia dei diritti e delle libertà fondamentali dei cittadini. Anche in questo caso, il contrasto della cyber-criminalità si traduce in una serie di iniziative strategiche di resilienza e sovranità tecnologica, rispetto alle quali il contrasto della criminalità informatica è potenziato sul profilo della cooperazione, della diplomazia informatica e della cyberdifesa, in parallelo con la promozione di un cyberspazio "globale" e "aperto" che attribuisce anche agli Stati un obbligo di comportamento responsabile.

In altre parole, nella dimensione trans-nazionale ed europea, alla sempre maggiore consistenza valoriale del concetto di cybersicurezza corrisponde un progressivo arretramento della centralità del diritto penale sostanziale nella sua protezione, in parte in conseguenza dell'evidente mancanza di effettività di tale strumento, ma in parte anche per la crescente preponderanza della dimensione politica e strategica nella tutela delle infrastrutture digitali.

2. Prima traiettoria evolutiva: la riscoperta del diritto penale (globale) per la protezione della cybersicurezza

Ebbene, così sinteticamente ricostruita la "storia" recente del diritto del *cybercrime*, deve rilevarsi come – dopo oltre un decennio di tendenziale silenzio da parte dei legislatori, quantomeno nel contesto "regionale" europeo – negli ultimi anni si registri, invece, una "riscoperta" del diritto penale quale strumento di tutela del cyberspazio, persino su un duplice piano: da un lato, al livello propriamente *globale* e, dall'altro, nel contesto della legislazione penale *nazionale*. È proprio su tali tendenze che s'intende ora concentrare l'attenzione.

Muovendo dalla riscoperta del diritto penale al livello internazionale, i due principali strumenti che "ricollocano" nella dimensione globale la politica criminale di contrasto ai *cybercrime* sono la Convenzione delle Nazioni Unite contro il *cybercrime*, approvata nel 2024[32], e la *Draft Policy on Cyber-Enabled Crimes under the Rome Statute* dell'Ufficio del Procuratore della Corte Penale Internazionale, pubblicata nel 2025[33]. Si tratta, a ben vedere, di due strumenti coerenti con la visione espressa dall'Unione europea nella Strategia per la Cybersicurezza del 2020, relativa alla presa d'atto della dimensione "globale" del cyberspazio e, dunque, del necessario ruolo del diritto internazionale nella costruzione e nella tutela della cybersicurezza: tuttavia, entrambi tali strumenti, anziché focalizzarsi sul comportamento *degli Stati* nello spazio cibernetico, riguardano e definiscono la responsabilità *penale* individuale per la commissione di reati informatici.

Com'è noto, la Convenzione ONU contro il *cybercrime* è stata approvata dall'Assemblea Generale delle Nazioni Unite il 24 dicembre 2024 ed è stata poi denominata "Convenzione di Hanoi" a seguito della cerimonia ufficiale di apertura alla firma, avvenuta appunto ad Hanoi lo scorso 25 ottobre 2025. I lavori dell'*Ad Hoc Committee* incaricato della sua redazione sono durati oltre quattro anni e hanno richiesto una significativa opera di mediazione tra gli Stati, portatori di divergenti posizioni politico-criminali e di distinte "sensibilità" nel bilanciamento tra istanze di repressione della cyber-criminalità e garanzia dei diritti fondamentali[34]. All'esito di tale processo, l'approvazione del testo è stata salutata con favore dai primi commentatori, proprio in ragione della precedente "mancanza di uno strumento al tempo stesso universale e di portata generale nell'affrontare tutti gli aspetti dello specifico fenomeno criminale preso di mira"[35], nonché quale definitivo suggello del "processo di internazionalizzazione" nel contrasto alla criminalità cibernetica[36].

Benché il contenuto della Convenzione si sia infine assestato, nella parte del diritto penale

32. Cfr. United Nations, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, 24 dicembre 2024.
33. Cfr. *Draft Policy on Cyber-Enabled Crimes under the Rome Statute*, pubblicata il 6 marzo 2025 dall'Ufficio del Procuratore presso la Corte Penale Internazionale.
34. Per un primo commento alla Convenzione cfr. Balsamo 2025.
35. *Ivi*, p. 244.
36. Cfr. in questi termini Mattarella 2025, p. 252.

sostanziale, su un elenco di fattispecie in buona parte sovrapponibile con quello della Convenzione di Budapest, nondimeno si ritiene che la Convenzione di Hanoi si differenzi dalle precedenti iniziative, nella misura in cui essa risponde – quantomeno a livello "aspirazionale" – al perseguimento di un'ideale di sicurezza cibernetica *globale*, rispetto al quale l'armonizzazione della legislazione penale sostanziale riveste una funzione cruciale e autonoma[37], non più dipendente dalle sole esigenze di cooperazione. Di tale mutamento di prospettiva si ha evidenza, ad avviso di chi scrive, sin dal Preambolo della Convenzione, che si apre con il dichiarato intento di perseguire "una politica penale globale per la protezione della società dalla cyber-criminalità", da attuarsi sia mediante una definizione condivisa delle fattispecie di reato, sia mediante un rafforzamento dei poteri di cooperazione internazionale.

Anche la struttura e i contenuti della Convenzione parrebbero confermare tale impressione. A differenza della Convenzione del Consiglio d'Europa – che colloca la tutela dei diritti e delle libertà fondamentali all'art. 15 e, dunque, tra le disposizioni comuni al solo diritto *procedurale* – la Convenzione di Hanoi situa la protezione dei diritti fondamentali (art. 6) tra le disposizioni generali, preliminari non soltanto alle norme processuali, ma anche agli obblighi di criminalizzazione, dei quali i diritti umani vengono così a costituire fondamento e limite. Nella medesima direzione, anche la lista delle fattispecie presenta alcune innovazioni rispetto al catalogo dei reati contemplato dalla Convenzione di Budapest, espressive di un'originale impostazione politico-criminale: tra tutte, ad esempio, (i) l'esplicito riconoscimento della connotazione "di genere" del *cybercrime*, del quale la fattispecie di "Non-consensual dissemination of intimate images" (art. 16) costituisce rilevante quanto inedito precipitato, nel contesto internazionale; e (ii) la definizione di circostanze aggravanti, per i reati che abbiano ad oggetto "critical information infrastructures" (art. 21). Del resto, non meno rilevanti, nella medesima prospettiva, sono le successive disposizioni in materia di assistenza e protezione delle vittime (art. 34) e di definizione delle "misure preventive" finalizzate a "ridurre le *opportunità*, presenti e future" di commissione di *cybercrime* (art. 53), tra le quali rientrano: iniziative di *public awareness*, il coinvolgimento dei *service provider*, la protezione dei c.d. *ethical hacker*, la reintegrazione dei cyber-criminali, o ancora la prevenzione della violenza di genere nel contesto digitale e la protezione delle persone vulnerabili. Proprio tali previsioni, espressive di una "strategia ampia di contrasto a tale fenomeno criminale", sono state individuate dai primi commentatori come il "valore aggiunto" e il tratto distintivo della nuova Convenzione[38].

Nella medesima direzione pare collocarsi anche la *Draft Policy on Cyber-Enabled Crimes under the Rome Statute*, pubblicata il 6 marzo 2025 dall'Ufficio del Procuratore presso la Corte Penale Internazionale. Prescindendo da una specifica disamina del contenuto della *Draft Policy* e dalle soluzioni tecniche che tale documento propone rispetto ad alcune questioni interpretative cruciali nel diritto (penale) internazionale[39], ai fini della presente indagine interessa piuttosto sottolineare come, anche in questo contesto, la dimensione "globale" della reazione – e l'affermazione dell'"impegno dell'Ufficio a condurre indagini rigorose e perseguire i reati *cyber-enabled*" – corrisponda proprio a una diversa considerazione della portata lesiva di tali reati. Invero, affermando che anche gli "unlawful and harmful uses of cyberspace"[40] possano rientrare nella giurisdizione della Corte dell'Aia, la *Draft Policy* implicitamente rileva come anche le violazioni informatiche possano attualmente rientrare tra quei *core crimes* che "minacci[ano] la pace, la sicurezza ed il benessere del mondo", come previsto dallo Statuto di Roma. In altre parole, coerentemente con il mandato della Corte, l'attenzione "internazionale" sui *cybercrime* dipenderebbe dalla relativa *gravità* e attitudine offensiva e non, invece, dalla dimensione transnazionale: invero,

37. Cfr. in questa prospettiva Wang 2025.
38. Cfr. in questi termini Balsamo 2025, p. 247 ss., nonché Mattarella 2025, p. 262, nel senso che la Convenzione introdurrebbe, in questo modo, "un diritto penale vittimologicamente orientato, sagomato anche sulle esigenze dei soggetti a vario titolo colpiti dal reato".
39. Cfr. in argomento l'analisi di Ambos 2015.
40. Cfr. la *Draft Policy*, cit., p. 4.

è anzitutto la natura *globale* e *vitale* dell'interesse protetto ad attrarre anche gli attacchi informatici entro l'ambito applicativo del "diritto punitivo della Comunità internazionale", in quanto potenzialmente costituenti "crimini contro la pace e la sicurezza del genere umano"[41].

3. Seconda traiettoria evolutiva: *pur un linguaggio nel mondo non (più) s'usa*. L'emergere dei legislatori penali nazionali nel cyberspazio

Come si anticipava, nella citata "riscoperta" del diritto penale quale strumento di contrasto alla criminalità cibernetica è possibile individuare anche una seconda traiettoria evolutiva. Si allude, in particolare, alla recente tendenza di alcuni legislatori nazionali a ricorrere sempre più spesso e in modo unilaterale al diritto penale per la protezione del cyberspazio (statale) rispetto a "minacce ibride"[42], talvolta – come si vedrà – pure attribuendo una proiezione applicativa extraterritoriale al diritto nazionale. Con il risultato che, se sino ad ora – come si è visto – la criminalità informatica ha rappresentato àmbito d'elezione del paradigma dell'armonizzazione penale, ora l'interprete è invece chiamato a riorientarsi in una "Babele" della tutela penale della sicurezza cibernetica.

Il punto di partenza di tale evoluzione – si ritiene – è il medesimo che è stato posto a fondamento della strategia europea per la cybersicurezza, nelle sue diverse fasi: la presa d'atto che, nel momento presente, la cyber-criminalità non costituisca più soltanto una minaccia per interessi economici individuali, ma possa minare la stabilità della società nel suo complesso, pregiudicare il funzionamento delle istituzioni e la tutela dei diritti dei cittadini, sì che la cybersicurezza diviene componente essenziale di quel concetto di "sicurezza" che storicamente rappresenta – non senza criticità – *cornice* e *fine* dello stesso intervento penale nazionale.

Muovendo da tale premessa, e riservando al prosieguo alcune considerazioni critiche, basterà per ora rilevare come, in prospettiva comparata, attualmente si moltiplichino le iniziative di criminalizzazione di "cyber-attacchi" o c.d. "minacce ibride", specialmente in aree ritenute strategiche per la sicurezza e l'interesse nazionale. Senza alcuna pretesa di esaustività, si forniranno alcuni esempi di tale tendenza politico-criminale.

Un primo essenziale riferimento è, in questa prospettiva, il *National Security Act 2023* adottato nel Regno Unito, che innova le disposizioni penali relative alla protezione della sicurezza nazionale, introducendo specifiche fattispecie per i casi di *espionage, sabotage* e *foreign interference*, quando realizzati nel dominio informatico[43]. Rilevante è, ad esempio, la fattispecie di cui alla Sect. 12 (*Sabotage*), che sanziona con l'ergastolo le condotte di danneggiamento (anche di sistemi elettronici e informatici) pregiudizievoli per la sicurezza o l'interesse nazionale, quando realizzate per conto di un potere estero (*foreign power*). Del pari, anche le fattispecie di *Espionage (Part I)*, benché non contengano un riferimento espresso all'uso di strumenti digitali, sono state riformate al preciso scopo di reagire alla "complessità delle moderne relazioni internazionali in un mondo interconnesso" e alle nuove opportunità di attacco rese possibili dalle nuove tecnologie[44]. Com'è stato rilevato anche dai primi commentatori, si tratta di fattispecie mediante le quali s'intende rafforzare la protezione della sicurezza nazionale contro minacce che, in considerazione dell'attuale evoluzione tecnologica, generalmente si realizzano proprio (e soltanto) nel dominio cibernetico (c.d. *cyber-espionage*); i paradigmi d'incriminazione prescelti si contraddistinguono per il ricorso a elementi piuttosto indeterminati (tra tutti, l'interesse o la sicurezza nazionale), nonché per l'arretramento della soglia d'intervento penale, derivante dal riferimento anche ad atti preparatori[45]. Al riguardo, è peraltro significativo sottolineare che, per espressa previsione, tali fattispecie si applicano *in ogni caso*, indipendentemente dalla nazionalità dell'agente e dal fatto che la condotta

41. Cfr. essenzialmente Vassalli 1999, p. 10.
42. Cfr. Sanz-Caballero 2023 e Billing–Feldtmann 2024.
43. Per un primo commento cfr. Scott 2024.
44. Cfr. National Security Act 2023, *Explanatory Notes*, in www.legislation.gov.uk, p. 7.
45. Cfr. Kendall 2024 e Scott 2024.

abbia avuto luogo nel territorio dello Stato, con una dichiarata proiezione extra-territoriale.

Un intervento del tutto analogo è riscontrabile anche in Polonia. Con legge del 17 agosto 2023[46], infatti, è stata approvata una modifica delle disposizioni penali relative al reato di *espionage*, allo scopo di adattarle al "costante mutamento della situazione geopolitica, al progresso tecnologico e al continuo cambiamento delle modalità operative dei potenziali autori"[47]: in particolare, la fattispecie è stata modificata per riformulare la stessa definizione dei comportamenti costituenti "spionaggio" (art. 130 del Codice penale polacco), nonché per criminalizzare espressamente la diffusione di disinformazione, e introdurre un significativo inasprimento delle pene. Allo stesso modo, anche nei Paesi Bassi è stata introdotta nel 2025 una riforma del Codice penale per criminalizzare nuove forme di spionaggio[48], tra le quali rientra anche il *digital espionage*, a tutela della sicurezza nazionale e delle infrastrutture critiche. Inoltre, il medesimo intervento normativo ha modificato diverse *computer-related offences*, per prevedere una circostanza aggravante per il caso in cui siano state realizzate per conto di un potere estero. Ancora, negli USA è stato di recente proposto il *Cyber Conspiracy Modernization Act*[49], che intende emendare il *Computer Fraud and Abuse Act* per criminalizzare espressamente, a livello federale, la c.d. *conspiracy* riferita ai *cybercrime*: con l'effetto, dunque, di creare un regime apposito e più severo per le condotte coordinate e organizzate, con un ulteriore arretramento della soglia dell'intervento penale (al livello dell'accordo-associazione), a tutela dell'ordine pubblico digitale[50].

Peraltro, lungo la medesima direttrice, non può non segnalarsi come in diversi Stati si registri altresì la progressiva attribuzione di poteri di intervento e contrasto della cyber-criminalità a organi appartenenti al comparto della sicurezza, della difesa e dell'*intelligence*, in luogo (o a completamento) delle tradizionali prerogative del magistero penale: è il caso, ad esempio, di un'imminente proposta che sarà a breve presentata in Germania[51], nonché di quanto già avvenuto in Giappone, dove, con la *Active Cyber Defense Law* del 2024, il concetto di cybersecurity è stato identificato con la "sicurezza nazionale e del popolo avverso attacchi informatici provenienti dall'esterno" ed è stato introdotto un modello di *active cyber defence* che coniuga misure tecniche e informative per la prevenzione e, soprattutto, la neutralizzazione dei cyber-attacchi[52].

Tratto comune a tutti gli interventi appena menzionati – per quanto possa osservarsi nei limiti dell'inevitabile cursorietà dell'indagine – è, in definitiva, il fatto che si tratti di iniziative "unilaterali" dei legislatori penali nazionali, i quali – quasi per la prima volta, nel dominio della criminalità cibernetica – non intervengono nel solco di indicazioni di armonizzazione a livello internazionale o europeo, ma elaborano autonome strategie politico-criminali, accomunate da alcuni stilemi che, utilizzando il lessico del diritto penale italiano, richiamano in vario modo la tutela della "personalità dello Stato", vale a dire degli interessi fondamentali della collettività, dalla sicurezza all'integrità nelle relazioni esterne. Del resto, già nella prospettiva del diritto costituzionale si è rilevato che l'attuale contenuto del concetto giuridico di cybersicurezza interessi tanto "complessivamente l'ordinamento statale", quanto "in dettaglio le sue componenti", dal momento che una qualsivoglia "aggressione tecnologica" è ora da ritenersi in grado di minacciare ad un tempo "la fruibilità dei diritti" da parte dei singoli soggetti appartenenti a un ordinamento, ma anche "gli interessi dello Stato"

46. Per un commento cfr. Burczaniuk 2024.
47. *Ivi*, p. 306.
48. Cfr. Government of Netherlands, *Legislation to be broadened to make more forms of espionage a criminal offence*, 18 marzo 2025.
49. Cfr. Congress of the United States of America, Cyber Conspiracy Modernization Act.
50. Cfr., in ordine al modello della *conspiracy*, Johnson 1973.
51. Cfr. Bundesministerium des Innern, *Strengthening cyber security – Federal Cabinet adopts key measures for increasing cyber security*, 27 agosto 2025.
52. Cfr. Mochinaga 2025.

nel suo complesso[53]. Di conseguenza, in parallelo con (e a prescindere da) il ruolo del diritto internazionale, è in definitiva con il diritto (penale) nazionale che gli Stati si trovano a reagire alle attuali minacce ibride, con un nuovo mosaico di incriminazioni che accomuna problematicamente regimi democratici e autoritari[54] e che non risulta più armonizzato a livello sovranazionale.

4. La recente trasformazione del diritto penale italiano: dal contrasto al *cybercrime* alla tutela della cybersicurezza nazionale

Un analogo riassestamento assiologico si registra, del resto, anche nel contesto nazionale. È ben noto, infatti, come storicamente il legislatore italiano sia intervenuto in maniera organica nell'ambito della criminalità informatica con la legge n. 547/1993[55] e con la successiva legge n. 48/2008[56], adeguando l'ordinamento alla prima Raccomandazione del Consiglio d'Europa e, successivamente, alla Convenzione di Budapest. È altrettanto noto, però, come, in occasione del primo di tali interventi, il legislatore abbia ritenuto che "la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo"[57]. Si è deciso, quindi, di "ricondurre i nuovi reati alle figure già esistenti che ad essi, pur nella loro autonomia, appaiano più vicine", giacché "le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice"[58]. Secondo tale impostazione, dunque, le fattispecie riconducibili alla categoria della "criminalità informatica" sono state inserite nel codice penale in modo piuttosto disorganico e sono risultate, perciò, difficilmente riconducibili, nel loro complesso, a una strategia politico-criminale unitaria. A partire dal 2023, invece, si è registrato un deciso mutamento di prospettiva, che risulta del tutto coerente con quanto si è già evidenziato rispetto ad altre esperienze nazionali. Con il d.l. 105/2023[59], infatti, la materia della "criminalità informatica e cybersicurezza" è stata addirittura oggetto di un decreto-legge, a segnalarne l'urgenza politico-criminale. Ai fini che ora interessano, basterà sottolineare come tale intervento abbia collocato la criminalità informatica realizzata ai danni di sistemi pubblici nell'alveo delle fattispecie soggette ai poteri d'impulso e coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo, al contempo autorizzando una serie di ulteriori strumenti investigativi, tra i quali le operazioni sotto copertura, nonché aprendo un canale informativo tra la "funzione" pubblica di cybersicurezza e le Procure.[60] Ancora più significativa è, nella medesima direzione, la legge 90/2024, che è intervenuta su più livelli a modificare le disposizioni penali relative alla cyber-criminalità[61]: per quanto ora più rileva, tale intervento ha determinato un'omogenea *specializzazione* delle fattispecie generali, introdotte anni addietro per recepire le indicazioni sovranazionali, al fine di costituire una reazione organicamente più severa rispetto alle condotte lesive della sicurezza

53. Cfr. De Vergottini 2019, p. 76.
54. Cfr. Sanz-Caballero 2023.
55. Rubricato "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
56. Che costituisce ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.
57. Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia. – "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (XI Legislatura, divenuto legge 23 dicembre 1993, n. 547).
58. Cfr. ancora la Relazione del Disegno di legge n. 2773 e, in dottrina, Pecorella 2006.
59. Decreto-legge 10 agosto 2023, n. 105, "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione", convertito con modificazioni dalla legge 9 ottobre 2023, n. 137.
60. In generale, con riferimento a tale intersezione, cfr. Ricotta 2023.
61. Su questi temi cfr. Fiorinelli–Giannelli 2024 e i diversi contributi ivi raccolti.

informatica pubblica, al tempo stesso proiettando anche su tale forma di criminalità i paradigmi di contrasto tipici della lotta alla criminalità organizzata e al terrorismo, nel segno di una nuova emergenza politico-criminale[62]. Anche l'introduzione di una nuova fattispecie per la criminalizzazione dei c.d. attacchi *ransomware* (art. 629, co. 3, c.p.)[63] costituisce indice della progressiva "autonomizzazione" delle scelte di incriminazione in questa materia, a ulteriore riconferma dell'attuale priorità politico-criminale attribuita dagli Stati al contrasto delle minacce ibride, anche indipendentemente dagli strumenti di armonizzazione e cooperazione.

Il disallineamento rispetto ai paradigmi condivisi a livello transnazionale ed europeo risulta ancora più marcato in alcuni disegni di legge recentemente presentati in Parlamento, relativi alla (opportuna) definizione di una strategia nazionale per il contrasto agli attacchi *ransomware*. In estrema sintesi, le diverse proposte legislative (C.2366; S.1441; C.2318)[64], d'iniziativa di diverse forze politiche, convergono sulla ritenuta necessità di introdurre un sistema "integrato" per il contrasto e la gestione delle estorsioni informatiche, affiancando alla nuova fattispecie penale introdotta nel 2024 ulteriori misure extra-penali, tra le quali, ad esempio, un generale divieto di pagamento del riscatto per i soggetti inclusi nel c.d. Perimetro di Sicurezza Nazionale Cibernetica; l'istituzione di una task-force nazionale; la previsione di incentivi e di un fondo nazionale di supporto per le vittime di attacchi *ransomware*; la disciplina delle cyber-assicurazioni[65]. Prescindendo, anche in questo caso, da una più dettagliata disamina dei singoli disegni di legge, interessa soprattutto sottolineare il rilievo *diretto* che tali disposizioni proporrebbero di attribuire all'interesse e alla sicurezza nazionale nella concreta gestione e repressione degli attacchi, sul presupposto della "vulnerabilità del Paese" nel "panorama geopolitico" e della correlata necessità di "rafforzare la resilienza nazionale"[66]. Questa specifica impostazione emerge con chiarezza, infatti, dalla previsione – comune ai diversi d.d.l. – che il divieto di pagamento del riscatto sia derogabile con una "specifica determinazione del Presidente del Consiglio dei ministri" qualora l'attacco comporti "un rischio grave e imminente per la sicurezza nazionale", nonché dalla contigua previsione che proporrebbe di attribuire al vertice dell'Esecutivo altresì il potere di classificare un attacco *ransomware* come incidente che compromette la sicurezza nazionale, indipendentemente dal soggetto che l'ha realizzato, anche al fine della eventuale attivazione di misure di intelligence con finalità di contrasto in ambito cibernetico. Addirittura, in una direzione simile a quella rilevata in prospettiva comparata, si propone di prevedere che gli ufficiali di polizia giudiziaria delle forze dell'ordine possano svolgere le attività sotto copertura "anche su reti, sistemi informativi e servizi informatici utilizzati per compiere reati informatici posti al di fuori dei confini nazionali", con una proiezione extraterritoriale delle attività di contrasto. Nella convergenza tra diritto penale, discrezionalità politica e attività di intelligence si coglie la complessità dell'attuale "sistema di governo" della cybersicurezza nazionale, che si articola in un assetto "integrato e multilivello" di poteri pubblici, espressivi di un complesso equilibrio tra Stato-apparato e Stato-Nazione[67]. In prospettiva penalistica l'impatto appare duplice: da un lato, l'attrazione della cyber-criminalità all'area della criminalità *lato sensu* politica, in conseguenza della "politicizzazione" degli interessi protetti, come si dirà meglio nel paragrafo seguente; dall'altro lato, il moltiplicarsi di poteri (anche d'indagine) non

62. Sia consentito rinviare a Fiorinelli 2024.

63. In argomento, cfr. Corasaniti 2025.

64. Si fa riferimento ai disegni di legge: C. 2366 "Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione"; S. 1441 "Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione"; C. 2318 "Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione".

65. In generale, per una simile impostazione cfr. Teichmann 2025; Corasaniti 2025.

66. Cfr. il citato disegno di legge S. 1441.

67. Al riguardo, nonché in relazione ai rapporti tra sicurezza e cybersicurezza, è essenziale il rinvio a Macchia–Sferrazzo 2025; Giupponi 2024; Giupponi 2023; Carotti 2020; Lanzillo 2018.

soggetti alle garanzie penalistiche, ma rispondenti a valutazioni e opportunità politiche e strategiche. Ciò è particolarmente rilevante, ove si consideri come – a differenza di alcune esperienze comparate – nell'ordinamento italiano non si distingue il regime giuridico in base alla provenienza (estera o meno) dell'attacco. Un'impostazione ancor più marcatamente "difensiva" si rinviene, infine, negli ulteriori disegni di legge di recente presentazione (C.2607, C.2425, C.2417)[68] che propongono di introdurre una generale riforma della disciplina delle operazioni delle Forze Armate nello spazio cibernetico. Prendendo ad esempio il d.d.l. C. 2242, il "tema della difesa e della sicurezza dello Stato in ambito cibernetico" è individuato come area *trasversale*, nella quale gli attacchi alle infrastrutture critiche e quelli comunque "vitali" per gli interessi nazionali determinano la convergenza, in un'area pure coperta dalle rilevanti disposizioni penali, del codice dell'ordinamento militare, delle disposizioni in materia di Perimetro di Sicurezza Nazionale Cibernetica, dell'architettura nazionale di cybersicurezza, dell'intelligence in ambito cibernetico, nonché della Strategia nazionale di cybersicurezza. Il contenuto essenziale di tali proposte consiste nell'abilitare il comparto della difesa rispetto alle minacce cibernetiche relative alla sicurezza nazionale, in allineamento con l'intelligence, con l'attribuzione di un "ruolo preminente" allo "strumento militare" nello spazio cibernetico. Anche in tali disegni di legge emerge, dunque, il sempre più marcato collegamento della cybersicurezza con la "sicurezza nazionale" e i suoi "apparati", a tutela della stessa "sovranità" dello Stato, ora sviluppato secondo il diverso (ma non meno rilevante) paradigma della difesa militare.

5. Riflessioni conclusive: riconciliare *sicurezza* e *diritti* nella politica criminale "multilivello" del cyberspazio.

La disamina di tutti i più recenti interventi penalistici che si sovrappongono nell'ambito della criminalità informatica parrebbe suggerire come proprio il concetto di (cyber)sicurezza costituisca un efficace prisma interpretativo dell'attuale congerie di vettori giuridici, in quanto tale concetto aiuta a scomporre – ma al tempo stesso a connettere – le distinte traiettorie politico-criminali individuate in materia di *cybercrime*, nella tensione tra la ricerca di un equilibrio geopolitico globale e la tutela della sicurezza nazionale. A livello internazionale, infatti, il passaggio da un approccio regionale a un'impostazione globale riflette, come si è detto, l'emersione – almeno in senso aspirazionale – di un interesse realmente *comune* alla "pace e alla sicurezza nel cyberspazio"[69], perseguito per la prima volta mediante gli strumenti del vero e proprio diritto internazionale (penale). A livello nazionale, invece, come pure si anticipava, la connessione sempre più profonda tra il contrasto della criminalità informatica e la tutela penale della sicurezza nazionale è alla base della recente "riscoperta" del diritto penale, in parallelo con quel progressivo collegamento tra repressione criminale e cyber-difesa, che fa convergere nel settore della cybersicurezza uno spettro di poteri pubblici che si estendono dall'attività amministrativa, alla giurisdizione penale, fino al dominio militare. La categoria concettuale della sicurezza (riferita al dominio cibernetico) riconnette, dunque, le traiettorie di intervento che si affastellano *in subiecta materia*, dal momento che, tanto nella prospettiva internazionale, quanto a livello statale, la protezione (penale) dell'infrastruttura informatica e digitale è intesa quale strumento di

68. Si fa riferimento ai d.d.l.: C. 2607 "Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e altre disposizioni in materia di operazioni delle Forze armate in ambito cibernetico"; C. 2425 "Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e all'articolo 1 della legge 21 luglio 2016, n. 145, nonché introduzione dell'articolo 7-quater del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, concernenti lo spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato e le operazioni delle Forze armate in ambito cibernetico"; C. 2417 "Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e altre disposizioni in materia di difesa dello spazio cibernetico e di operazioni delle Forze armate in ambito cibernetico".

69. Cfr. Wang 2025.

tutela della società nel suo complesso e della stessa sicurezza interna ed esterna degli Stati[70].

Ciò nondimeno, non può trascurarsi come i concetti di sicurezza internazionale e di sicurezza nazionale possano convergere sul piano teorico-ideale, ma nella prassi rischino di trovarsi spesso in una relazione di tensione o di potenziale conflitto: anzi, proprio le impostazioni più marcatamente "difensive" del cyberspazio registrate a livello statale, tanto più ove esse assumano anche un raggio d'azione extraterritoriale ovvero sviluppino pratiche di cyber-difesa attiva, rischiano di trasformarsi in fattori d'insicurezza, capaci di alterare l'equilibrio cibernetico globale. Ciò è a dire, in altre parole, che, nel più ampio quadro geopolitico, anche le recenti politiche penali si prestano a essere lette quali tracce di quel "protagonismo degli Stati" che contraddistingue l'attuale *race for the cyberspace*[71], con una potenziale tensione tra il livello nazionale e il livello internazionale.

D'altra parte, e soprattutto con riferimento agli ordinamenti statali, s'impone anche una diversa riflessione, a partire dalla centralità della cybersicurezza nelle recenti opzioni di politica criminale. Come si è visto, proprio entro tale cornice assiologica si colloca la reviviscenza di fattispecie di sapore "politico", che riportano alla luce l'esigenza di riconsiderare il "diritto penale del *cybercrime*" attraverso la lente dei diritti fondamentali, non più come *oggetto* di tutela, ma come *limite* alle scelte di incriminazione[72]. Proprio l'aggancio teleologico al concetto di "sicurezza nazionale", infatti, può far temere la tendenziale impermeabilità di tali iniziative politico-criminali – intese in senso ampio – al bilanciamento con altri diritti costituzionalmente garantiti, in tutta coerenza con il paradigma della legislazione penale dell'emergenza. In questa prospettiva, era stato già rilevato come la riflessione penalistica nel suo complesso non abbia ancora adeguatamente valutato in che misura la repressione penale della cyber-criminalità comprima – attraverso le stesse disposizioni *sostanziali* e non soltanto attraverso l'ampliamento dei poteri d'indagine – le libertà individuali: proprio in quanto materia di diritto penale "armonizzato", essa soffrirebbe al contempo il duplice limite di un debole ancoraggio in positivo a beni giuridici da tutelare, così come di un altrettanto debole ruolo dei diritti fondamentali quale limite alle scelte di incriminazione[73]. Se tale rilievo risulta senz'altro condivisibile, nel caso ora in esame la prospettiva che si apre pare ancora diversa: proprio l'ancoraggio *forte* al bene giuridico della "sicurezza nazionale" – variamente intesa al crocevia tra personalità interna e internazionale dello Stato, ordine pubblico, interesse pubblico – ha condotto diversi Stati a "rispolverare" fattispecie per lungo tempo inutilizzate (con lessico italiano: lo spionaggio, le "intelligenze con lo straniero", il disfattismo, i vari attentati all'integrità e all'indipendenza dello Stato, connessi o meno con un *foreign power*) e storicamente controverse, in quanto costruite attorno a beni giuridici di consistenza inafferrabile, come l'interesse politico o la sicurezza dello Stato, ritenuti dalla dottrina ben poco compatibili con i principi costituzionali in materia penale[74]. Non è questa la sede per una più compiuta disamina della categoria del "reato politico": sia consentito però rilevare come le più recenti riforme del *cybercrime* (anche e soprattutto nel panorama comparatistico) evochino proprio tale categoria concettuale e i ben noti, "radicali" problemi che essa solleva nell'ordinamento costituzionale[75]. Del resto, meritevole di un'eguale attenzione critica pare anche la parallela tendenza a fare della sicurezza non già oggetto ma, per così dire, "fine" e "modalità" della tutela, con l'erosione delle competenze dell'autorità giudiziaria, a favore di apparati d'ordine per definizione meno "garantiti",

70. Cfr. Brighi–Chiara 2021, pp. 19-20, e von Solms–van Niekerk 2013, p. 97 ss.

71. Cfr. Barozzi Reggiani 2025, p. 21, che riferisce alla *race for the cyberspace* non soltanto la componente "attivo-offensiva", ma anche quella "passivo-difensiva".

72. Cfr. Brunhober 2022, nonché in prospettiva più ampia Gohdes 2024.

73. Cfr. Brunhober 2022, p. 246.

74. Cfr. Insolera 1990, p. 457.

75. Cfr. in argomento l'analisi di Pulitanò 1989.

come quello di intelligence[76] o lo stesso comparto militare[77]. Anche a prescindere dall'arretramento delle garanzie che tale riassetto dei poteri potrebbe comportare, pare comunque essenziale evidenziare questa tendenza alla de-giurisdizionalizzazione del contrasto agli attacchi informatici, anche per la sua possibile collisione con la rinnovata architettura internazionale in materia di criminalità cibernetica, per le ragioni che già si anticipavano. In definitiva, emerge la necessità – di certo non nuova – di riconciliare *sicurezza* e *diritti*, nello sviluppo di una più organica politica criminale per il cyberspazio: ancor prima, però, è necessario aver ben chiaro quali (e quante) *sicurezze* e quali (e quanti) *diritti* ora convergano nello stesso concetto di cyberspazio e nella sua *governance* multilivello.

Riferimenti bibliografici

K. Ambos (2021), *International criminal responsibility in cyberspace*, in N. Tsagourias, R. Buchan (a cura di), "Research Handbook on International Law and Cyberspace", Edward Elgar Publishing, 2021

A. Balsamo (2025), *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime*, in "Diritto penale e processo", 2025

G. Barozzi Reggiani (2025), *La* race for the cyberspace *degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, in "Rivista italiana di informatica e diritto", 2025, n. 2

F. Billing, B. Feldtmann (2024), *The Role of Criminal Law Approaches Against Hybrid Attacks*, in "Bergen Journal of Criminal Law and Criminal Justice", vol. 12, 2024, n. 2

G. Borriello, G. Fristachi (2022), *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in "Rivista di Digital Politics", 2022

R. Brighi, P.G. Chiara (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in "federalismi.it", 2021

D. Brodowski (2021), *The Emerging History of Transnational Criminal Law Relating to Cybercrime*, in N. Boister, S. Gless, F. Jeßberger (eds.),"Histories of Transnational Criminal Law", Oxford University Press, 2021

B. Brunhober (2022), *Criminal Law of Global Digitality. Characteristics and Critique of Cybercrime Law*, in M.C. Kettemann, A. Peukert, I. Spiecker (eds.), "The Law of Global Digitality", Routledge, 2022

P. Burczaniuk (2024), *The crime of espionage in new terms, i.e. in light of amendment to the Criminal Code of 17 August 2023*, in "Internal Security Review", vol. 30, 2024, n. 16

B. Carotti (2020), *Sicurezza cibernetica e Stato-nazione*, in "Giornale di diritto amministrativo", 2020, n. 5

R. Chesney (2020), *Cybersecurity Law, Policy, and Institutions (version 3.0)*, University of Texas Law, Public Law Research Paper No. 716, 2020

M. Chiavario, A. Perduca (2022), *Cooperazione giudiziaria internazionale in materia penale*, Giappichelli, 2022

J. Clough (2014), *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, in "Monash University Law Review", vol. 40, 2014, n. 3

G. Corasaniti (2025), *Strategie di contrasto al* ransomware *e nuove frontiere della criminalità informatica*, in "Il diritto dell'informazione e dell'informatica", 2025, n. 1

76. Cfr., al riguardo, essenzialmente Salvi 2023.

77. Cfr. in proposito, per una disamina dei poteri connessi alla "funzione di cybersicurezza", Macchia–Sferrazzo 2025, p. 123 ss.; Forgione 2022.

G. de Vergottini (2019), *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in "Rivista AIC", 2019

G. Fiorinelli (2024), *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024

G. Fiorinelli, M. Giannelli (a cura di) (2024), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, in "Rivista italiana di informatica e diritto", sezione monografica, 2024, n. 1

R. Flor (2023), *Cyber-criminality: le fonti internazionali ed europee*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), "Trattato di diritto penale – *Cybercrime*", Giappichelli, 2023

R. Flor (2019), *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in "Diritto di internet", 2019

I. Forgione (2022), *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in "Diritto amministrativo", 2022, n. 4

A.R. Gohdes (2024), *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence*, Oxford University Press, 2024

T.F. Giupponi (2024), *Il governo nazionale della cybersicurezza*, in "Quaderni costituzionali", 2024, n. 2

T.F. Giupponi (2023), *Sicurezza e potere*, in "Enciclopedia del Diritto. I tematici V", Giuffrè, 2023

G. Insolera (1990), voce *Spionaggio*, in "Enciclopedia del diritto", vol. XLIII, Giuffrè, 1990

P.E. Johnson (1973), *The Unnecessary Crime of Conspiracy*, in "California Law Review", vol. 61, 1973, n. 5

S. Kendall (2024), *Espionage law in the UK and Australia: balancing effectiveness and appropriateness*, in "The Cambridge Law Journal", vol. 83, 2024, n. 1

M.L. Lanzillo (2018), *Lo stato della sicurezza. Costituzione e trasformazione di un concetto politico*, in "Ragion pratica", 2018, n. 1

E. Longo (2024), *La disciplina della cybersecurity nell'Unione europea e in Italia*, in F. Pizzetti, M. Orofino, A. Iannuzzi, S. Calzolaio, E. Longo (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024

M. Macchia, G. Sferrazzo (2025), *Sicurezza e rischio tecnologico. La funzione di* cybersecurity, in "Diritto amministrativo", 2025, n. 1

A. Mattarella (2025), *Diritto penale e nuove tecnologie: dalla Convenzione Onu contro i reati informatici alle sfide dell'intelligenza artificiale*, in "Diritto penale e processo", 2025

D. Mochinaga (2025), *Rising sun in the cyber domain: Japan's strategic shift toward active cyber defense*, in "The Pacific Review", vol. 38, 2025, n. 2

C. Pecorella (2006), *Il diritto penale dell'informatica*, Cedam, 2006

L. Picotti (2011), *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in "Rivista trimestrale di diritto penale dell'economia", 2011

M.G. Porcedda (2023), *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis,* Oxford University Press, 2023

D. Pulitanò (1989), voce *Delitto politico*, in "Digesto pen.", III, Utet, 1989

F.N. Ricotta (2023), *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in "Rivista trimestrale di diritto penale contemporaneo", 2023

G. Salvi (2023), *Intelligence e potere*, in "Enciclopedia del Diritto. I tematici, V", Giuffrè, 2023

S. Sanz-Caballero (2023), *The concepts and laws applicable to hybrid threats, with a special focus on Europe*, in "Humanities and Social Sciences Communications", 2023

S. Schjolberg (2008), *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, in "Cybercrime Law", 2008

P.F. Scott (2024), *'State threats', security, and democracy: the National Security Act 2023*, in "Legal Studies", vol. 44, 2024, n. 2

U. Sieber (1998), *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME Study*, 1998

F. Spiezia (2023), *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, in "Sistema penale", 2023

F. Teichmann (2025), *Ransomware extortion in Europe: legal responses and mitigation strategies*, in "International Cybersecurity Law Review", vol. 6, 2025, n. 3

G. Vassalli (1999), *Statuto di Roma: note sull'istituzione di una Corte penale internazionale*, in "Rivista di Studi Politici Internazionali", vol. 66, 1999, n. 1

R. von Solms, J. van Niekerk (2013), *From information security to cyber security*, in "Computers & Security", vol. 38, 2013

X. Wang (2025), *Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers?*, in "Leiden Journal of International Law", vol. 38, 2025, n. 2