ORDINES
Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730
NUMERO 1 – GIUGNO 2023

CASIMIRO CONIGLIONE

Il volto criminale dell'informatica

S. PIETROPAOLI, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, Giappichelli, 2022, pp. 114

ORDINES
Per un sapere interdisciplinare sulle istituzioni europee

1/2023

CASIMIRO CONIGLIONE*

Il volto criminale dell'informatica

S. PIETROPAOLI, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, Giappichelli, 2022, pp. 114

L'opera in esame offre un'interessante analisi sulle diverse "ombre" della rivoluzione tecnologica.

Nella letteratura informatico-giuridica riecheggia spesso la nota metafora del Giano bifronte: il Dio romano dai due volti, che guarda contemporaneamente sia al presente sia al passato. La metafora della divinità romana si sposa assai bene con la rivoluzione tecnologica poiché – come bene argomentato dall'Autore nell'*Introduzione* – "maggiore è il potenziale di una certa tecnologia, superiori sono i vantaggi che essa offre e, allo stesso tempo più gravi sono le conseguenze legate al suo cattivo uso" (p. XI).

In forza di ciò, Pietropaoli nei sei capitoli del volume analizza queste "ombre" della rivoluzione tecnologica, evidenziando le conseguenze negative nel caso di un uso scorretto o non conforme dei dispositivi tecnologici: a causa della loro natura tecnica, infatti, si possono amplificare gli effetti negativi nei confronti di singoli utenti, della società, degli Stati.

Nel primo capitolo (pp. 1-22), l'Autore – prima dell'esegesi delle diverse fattispecie incriminatrici – pone un'interessante e condivisibile scelta terminologica: propone infatti di distinguere fra "reati necessariamente informatici", in cui l'utilizzo delle tecnologie è presupposto necessario e fondamentale per configurare il comportamento penalmente rilevante, e "reati occasionalmente informatici", in quanto l'utilizzo dei dispositivi tecnologici è un elemento accidentale, poiché il comportamento illecito può essere perpetrato anche in modalità *offline* (cfr. p. 3).

Ciò premesso, Pietropaoli analizza gli elementi costitutivi (elemento oggettivo, soggettivo e nesso causale) e accidentali (come, ad esempio, le aggravanti) dei reati informatici introdotti dalla l. 547/1993 e dalla l. 48/2008 (legge di ratifica della Convezione di Budapest sulla criminalità informatica). L'analisi ragionata dei reati informatici del codice penale è integrata anche dalla giurisprudenza, facendo emergere – in certi casi – evidenti contrasti interpretativi fra dottrina e interpretazione giudiziale.

* Dottorando in Lavoro, Sviluppo e Innovazione, Unimore - Fondazione Marco Biagi.

Due specifici *focus* sono dedicati a condotte criminali di difficile configurazione e interpretazione, che nel corso del tempo si sono evoluti, assumendo contorni sempre più sfumati: il *phishing*, che è assimilabile alla truffa informatica e ha variegate forme di manifestazione, è un reato in cui il soggetto attivo tenta di carpire i dati della vittima per propri fini (cfr. pp. 17-20); nel *pharming*, invece, l'autore del reato – sempre con l'intenzione di impossessarsi dei dati della vittima, attraverso un attacco *cracking*, modifica la *cache* DNS (*Domain Name System*) – inganna l'utente sulla veridicità del sito (e come se, ad esempio, si creasse una pagina esteticamente uguale a quella di un istituto di credito, ma con finalità ovviamente assai differenti: in questo caso, l'obiettivo sarebbe quello di carpire il PIN o altri dati bancari; cfr. pp. 20-21).

Nel secondo capitolo (pp. 23-46), Pietropaoli evidenzia forme note e meno note di *cybercrimes*, ossia reati che possono essere commessi *offline*, ma che *online* hanno una diversa carica offensiva.

A questo proposito, l'Autore analizza diverse fattispecie che – in un modo o nell'altro – condividono il bene giuridico tutelato, ovverosia la dignità e il benessere psico-fisico del soggetto passivo del reato: il *cyberstalking*, il *sexting* e *sextortion*, la pedopornografia, il cosiddetto *revenge porn* (espressione, come opportunamente si sottolinea, alla quale è preferibile quella di "pornografia non consensuale": p. 29) e l'*hate speech*. Pietropaoli esamina, poi, il fenomeno delle *fake news*, che non sono propriamente un fenomeno di rilevanza penale ma – a causa della persistenza, della viralità e della profilazione attuata dalle *big tech* – possono sconvolgere gli equilibri democratici del *démos*, manipolando gusti, preferenze e orientamento politico degli utenti del web (cfr. pp. 35-37).

La parte conclusiva del capitolo è dedicata alla trattazione dei *ransomware* e del *cyberlaundering*. Il *ransomware* è un *malware* assai potente installato sul sistema operativo della vittima che cripta, ossia rende illeggibili, i file: l'autore del reato, sostanzialmente, richiede un riscatto alla vittima per "decriptare" i file e – attuando un ragionamento squisitamente penalistico – l'applicazione delle diverse norme penali non sempre è di agevole applicazione (complice anche il divieto di interpretazione analogica delle leggi penali), poiché dipende fattivamente dalla condotta della parte attiva del reato; il *cyberlaundering*, invece, è una "nuova" forma di riciclaggio del denaro che sfrutta i *bitcoin* e le *cryptovalute*. In sintesi, ciò che viene sfruttata, in questa fattispecie incriminatrice, è la dematerializzazione del denaro (cfr. pp. 41-46).

Nel terzo capitolo (pp. 49-66) l'Autore si sofferma sulla guerra cibernetica, descrivendo le nuove modalità di condotta del fenomeno bellico, le *cyberweapons* e i *cyberwarrios*.

Dopo aver commentato il Manuale di Tallin e la sua versione aggiornata (che, si ricorda ad ogni buon conto, costituisce un insieme di atti di *soft law*), ossia il Manuale di Tallin 2.0, ed evidenziando le criticità giuridiche e politiche di questo Manuale che disciplina la *cyberwar* (cfr. pp. 53-58), l'Autore indaga in dettaglio le diverse *cyberweapons* come i *malware* analizzando, a questo proposito, il caso *Stuxnet*. Siffatto *malware*, che rientra all'interno delle condotte di *cyberattack*, è stato in grado di manipolare nel 2010 le centrifughe della centrale nucleare di Natanz, in Iran, alterando i dati di controllo del sistema (l'autore dell'attacco, oggi, è ancora sconosciuto; pp. 58-61). Ciò sta a dimostrare che – contrariamente a quanto si possa ipotizzare – un attacco cibernetico non è meno violento rispetto a un attacco "classico": anch'esso è in grado di produrre effetti collaterali gravissimi.

Ci si concentra poi sulla figura dei *cyberwarriors*. Questi combattenti possono essere sia di natura statale sia di natura parastatale.

Nel primo caso, i militari appartengono alla forze armate di uno Stato (l'unica entità, almeno in linea teorica, a detenere l'uso della forza nei casi di autodifesa o nei casi in cui il Consiglio di Sicurezza delle Nazioni Unite deliberi un attacco) e, come negli Stati Uniti d'America, possono organizzarsi attraverso un'apposita struttura di comando: ad esempio, il CYBERCOM (US *military's Cyber Command*) è una struttura politico-militare che collabora con le altre agenzie di sicurezza come la CIA nei casi di azioni esterne o con FBI o NSA nei casi di azioni interne.

Nel secondo caso gli Stati, per eludere il divieto dell'uso della forza armata, possono ingaggiare dei gruppi parastatali, evitando così sia il coinvolgimento diretto sia la responsabilità internazionale (ciò incentiva anche il fenomeno della c.d. *war by proxy*, ossia la "guerra per procura"); Pietropaoli offre un esempio particolarmente significativo, riportando un caso di *patriotic hacking* nel conflitto in corso fra Federazione Russa e Ucraina: la *cybergang* bielorussa "Conti", nota per la creazione di temibili *ransomware*, si sarebbe schierata a favore delle forze armate russe a discapito di quelle ucraine (cfr. p. 64).

Un'ultima annotazione, poi, è dedicata ai fenomeni di *hacktivism*, ossia soggetti che politicamente non sono legati a nessun governo, bensì esprimono esigenze politiche attraverso gli attacchi informatici per disobbedienza civile, protesta o agitazione. Tra queste forme di *hacktivism*

la più celebre, indubbiamente, è quella di *Anonymous* (cfr. pp. 64-66): questo gruppo decentralizzato, fondato nel 2003, si propone come un baluardo di resistenza nei confronti di imprese e governi autoritari, con il preciso scopo di tutelare la libertà di manifestazione del pensiero e i diritti umani.

Il quarto capitolo (pp. 69-82) – attraverso un'interessante ricostruzione storica (che prende avvio con l'indagine sulla *lex Gabinia* e, dunque, il conferimento dei pieni poteri a Pompeo Magno [106 a.C. – 48 a.C.] per sconfiggere la pirateria in Cilicia) e giusfilosofica – tratteggia la figura del pirata informatico: questi può essere inteso come un soggetto ambiguo poiché, da una parte, viola le leggi sul diritto d'autore (*copyright*) e, dall'altra parte, lotta contro il monopolio dell'industria culturale, mirando a favorire un'informazione e una conoscenza libera dai monopoli delle *big tech* industriali-culturali (cfr. pp. 73-75).

In questo contesto l'Autore esamina il *cyberterrorism*, facendo emergere i lati oscuri della rete. Infatti, nel *dark web* (la parte del *World Wide Web* non indicizzata, raggiungibile solo attraverso specifici *software*, configurazioni o accessi autorizzativi) le organizzazioni terroristiche non solo reclutano e addestrano i diversi adepti, ma pubblicano materiale propagandistico e/o violento contro i diritti umani. Inoltre, usufruiscono del *dark market* per l'acquisito di beni o servizi, ovvero per autofinanziarsi (cfr. pp. 78-82).

Il quinto capitolo (pp. 85-97) intende verificare se è possibile l'accertamento di un illecito con l'ausilio delle nuove tecnologie. L'Autore analizza, più in specifico, le potenzialità offerte dall'informatica forense, una branca della scienza digitale forense legata alle prove acquisite da computer e altri dispositivi di memorizzazione digitale (per un'ampia trattazione si rinvia a R. Brighi [a cura di], *Nuove questioni di informatica forense*, Roma, Aracne, 2022). Oltre a ciò, l'attenzione è spostata verso la già menzionata Convenzione di Budapest che ha comportato, in particolare, la riscrittura dei mezzi di ricerca della prova disciplinati dal vigente codice di procedura penale (ispezione, perquisizione, sequestro e intercettazioni), per adattarli a una società sempre più tecnologica (cfr. pp. 89-94).

Il *focus* di questo capitolo è dedicato al celeberrimo caso di Garlasco del 2007 (cfr. pp. 94-97). Gli agenti e gli ufficiali di Polizia Giudiziaria, com'è noto, non rispettarono gli accorgimenti tecnici per il mantenimento della genuinità e della rapida conversazione della *digital evidence* (il c.d. trattamento *quick freeze*), con la precisa conseguenza che l'imputato non poté dimostrare il suo alibi, mentre la Pubblica Accusa si trovò nell'impossibilità di confutare l'alibi dell'imputato. Ciò sta a dimostrare che la *digital evidence*

è ormai un accessorio fondamentale per l'accertamento della verità processuale.

Il sesto e ultimo capitolo (pp. 99-114) esamina invece la *cybersecurity*, definita come l'insieme di "tutte quelle strategie volte a proteggere la dimensione digitale da un pericolo (o dalla minaccia di un pericolo) generato in modo intenzionale o non intenzionale da soggetti non sempre identificabili" (p. 99). In forza di ciò, Pietropaoli – dopo l'accurata analisi delle normative europee, che posero le basi per le attuali strategie di *cybersecurity* – rivolge l'attenzione al contesto italiano e, in modo particolare, alla "legge perimetro" del 2019 nonché alla recente creazione dell'ACN (Agenzia per la cybersicurezza nazionale).

Il perimetro nazionale, ai sensi dell'art. 1 del d.l. 105/2019 (convertito con l. 133/2019), è identificato nei "sistemi informatici e i servizi informatici sia delle amministrazioni pubbliche, sia degli enti locali e degli operatori pubblici e privati […] da cui dipende l'esercizio di una funzione essenziale […]". Oltre a ciò, la legge identifica criteri e condizioni per l'individuazione dei soggetti autorizzati a stare nel perimetro cibernetico, nonché le diverse entità del pregiudizio che i sistemi informatici possono subire in caso di malfunzionamento, interruzione o utilizzo improprio delle reti, in cui può esserci un pregiudizio per la sicurezza nazionale. È, altresì, prevista anche la collaborazione di diversi organismi fra i quali il COPASIR (Comitato parlamentare per la sicurezza della Repubblica; cfr. pp. 108-110).

Con il d.l. 82/2021 e il d.p.c.m. 223/2021 la tutela dello spazio cibernetico nazionale è affidata all'ACN, che ha funzioni di prevenzione, monitoraggio, analisi e risposta a incidenti o attacchi di natura informatica che possono pregiudicare il perimetro nazionale. Collabora, d'intesa con il Ministero della Difesa, con la NATO ed assume anche le vesti di Autorità nazionale di certificazione della cybersicurezza, potendo emanare sanzioni nei casi in cui vi siano violazioni (cfr. pp. 111-114).

In conclusione, l'opera mostra assai bene i diversi pericoli legati all'utilizzo delle nuove tecnologie, che coinvolgono – come si è illustrato – utenti, società e anche gli Stati. Ciò nonostante, il volume non assume una visione "tecnofobica", ossia ostile ai dispositivi tecnologici, bensì adotta uno spirito critico costruttivo, confidando in una maggiore formazione e informazione di utenti e professionisti nell'informatica forense e nella *cybersecurity*, affinché non sia oscurato il volto positivo delle nuove tecnologie.