La sicurezza nel cyberspazio

a cura di
Riccardo Ursi

Scritti di
Diritto Pubblico

FRANCOANGELI

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

STUDI DI DIRITTO PUBBLICO

Collana diretta da **Roberto Bin**, **Fulvio Cortese** e **Aldo Sandulli**
coordinata da **Simone Penasa** e **Andrea Sandri**

La Collana promuove la rivisitazione dei paradigmi disciplinari delle materie pubblicistiche e l'approfondimento critico delle nozioni teoriche che ne sono il fondamento, anche per verificarne la persistente adeguatezza.
A tal fine la Collana intende favorire la dialettica interdisciplinare, la contaminazione stilistica, lo scambio di approcci e di vedute: poiché il diritto costituzionale non può estraniarsi dall'approfondimento delle questioni delle amministrazioni pubbliche, né l'organizzazione e il funzionamento di queste ultime possono ancora essere adeguatamente indagati senza considerare l'espansione e i modi di interpretazione e di garanzia dell'effettività dei diritti inviolabili e delle libertà fondamentali. In entrambe le materie, poi, il punto di vista interno deve integrarsi nel contesto europeo e internazionale.
La Collana, oltre a pubblicare monografie scientifiche di giovani o affermati studiosi (**STUDI E RICERCHE**), presenta una sezione (**MINIMA GIURIDICA**) di saggi brevi destinata ad approfondimenti agili e trasversali, di carattere propriamente teorico o storico-culturale con l'obiettivo di sollecitare anche gli interpreti più maturi ad illustrare le specificità che il ragionamento giuridico manifesta nello studio del diritto pubblico e le sue più recenti evoluzioni.
La Collana, inoltre, ospita volumi collettanei (sezione **SCRITTI DI DIRITTO PUBBLICO**) volti a soddisfare l'esigenza, sempre più avvertita, di confronto tra differenti saperi e di orientamento alla lettura critica di problemi attuali e cruciali delle discipline pubblicistiche.
La Collana si propone di assecondare l'innovazione su cui si è ormai incamminata la valutazione della ricerca universitaria. La comunità scientifica, infatti, sente oggi l'esigenza che la valutazione non sia più soltanto un compito riservato al sistema dei concorsi universitari, ma si diffonda come responsabilità dell'intero corpo accademico.
Tutti i volumi, pertanto, saranno soggetti ad un'accurata procedura di valutazione, adeguata ai criteri fissati dalle discipline di riferimento.

La sicurezza nel cyberspazio

a cura di
Riccardo Ursi

Il volume è stato pubblicato con il contributo del Dipartimento di Giurisprudenza dell'Università degli Studi di Palermo.

Indice

La sicurezza cibernetica come funzione pubblica

Riccardo Ursi

Sommario: 1. La sicurezza nel cyberspazio. - 2. Il concetto di sicurezza cibernetica in senso ampio: il problema dell'ordine pubblico digitale. - 3. La sicurezza cibernetica in senso stretto: l'interrelazione tra sicurezza, difesa ed *intelligence.*

1. La sicurezza nel cyberspazio

L'evoluzione repentina dei processi tecnologici ha rivelato un connotato ultra-moderno della pubblica sicurezza, sempre più correlata alla definizione e alla distribuzione dei rischi prodotti dalla scienza e dalla tecnica.

Rischio e sicurezza rappresentano nozioni logicamente connesse: se la determinazione del rischio rappresenta sempre l'esito di una valutazione (secondo punti di vista molteplici: sociologici, economici, giuridici) inerente al grado di insicurezza riscontrabile in un dato contesto sociale, il livello di sicurezza è strettamente dipendente dall'assetto funzionalmente predisposto ad abbassare la soglia del rischio.

Come è noto, l'orizzonte giuridico della sicurezza rappresenta una delle cifre costitutive della modernità giuridica, la quale annulla il rischio e l'incertezza strutturalmente sottesi alle dinamiche sociali tramite il paradigma di prevedibilità razionale dei comportamenti collettivi. Tale modello è radicato su coordinate concettuali chiare e definite, quali la spazialità del perimetro statuale, il controllo preventivo-sanzionatorio esercitato da apparati di polizia/sicurezza territoriali, il primato della legge come garanzia dei diritti individuali. Questa concezione della sicurezza risulta, tuttavia, non adatta ad un contesto in cui la tecnologia ha reso i modelli tradizionali non più applicabili, con la conseguente ridefinizione della natura stessa della dimensione politico-giuridica [G. Bombelli, 2017, 11].

Tale assunto si palesa in maniera eclatante in relazione al prodotto più qualificante dello sviluppo tecnologico, ossia Internet e l'universo virtua-

le da esso generato, caratterizzato dall'assenza di confini, dal dinamismo e dall'anonimato. Internet consente di spostare informazioni in modo rapido ed è aperto a tutti gli utenti che desiderano un accesso. Ciò crea nuove opportunità di sviluppo per la società basata sulla conoscenza, ma anche rischi per il suo funzionamento.

Il mondo interconnesso in cui viviamo dipende integralmente dalle informazioni, dall'informatica e dalle comunicazioni. Si tratta di una condizione che se, da un lato, agevola lo sviluppo delle relazioni e rende i sistemi economici, sociali ed istituzionali maggiormente efficienti e performanti, li espone, dall'altro, a numerosi pericoli, dato che la vita quotidiana di ogni cittadino, l'economia nazionale e la sicurezza stessa degli Stati sono ormai indissolubilmente legati alla stabilità e alla sicurezza del cyberspazio [L. Martino, 2018, 62]. Quest'ultimo viene definito come un ambiente globale, caratterizzato dall'uso dell'elettronica e delle ICT per creare, immagazzinare, modificare, scambiare e sfruttare informazioni attraverso reti e sistemi interdipendenti [D. Kuhel, 2009, 28]. In sostanza, come espressamente indicato dalle linee guide ISO/IEC del 2018, si è in presenza di un «*complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*». Queste reti e sistemi informativi risiedono, simultaneamente, nello spazio fisico e nello spazio virtuale, così come all'interno e all'esterno dei confini geografici. In questo senso, il cyberspazio è un ambiente in cui gli esseri umani e le loro organizzazioni utilizzano le tecnologie per agire e produrre effetti rilevanti sia al suo interno sia nell'ambito di altri domini fisici: un nuovo dominio operativo di natura artificiale, trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale).

Il dominio, o spazio, cibernetico è costituito da quella rete di infrastrutture materiali di collegamento e di comunicazione che, attraverso la tecnologia informatica, mette in contatto tra loro un crescente numero di esseri umani e permette loro di attivare e controllare, da ubicazioni remote, macchine e apparati in tutto il mondo. Le coordinate di individuazione di una nozione giuridica del cyberspazio devono tenere conto, dunque, dei profili qualitativi e strutturali dello stesso.

Sul piano qualitativo, risulta agevole rilevare che sono principalmente due gli elementi che contraddistinguono lo spazio cibernetico rispetto a quello fisico: da una parte, esso si presenta come un ambiente indefinito, privo di confini fisici, dove è difficile, se non impossibile, discriminare tra pubblico e privato; dall'altra, esso è in continua evoluzione e implementazione, in relazione alla rapidità dello sviluppo delle tecnologie.

Sul piano strutturale, lo spazio cibernetico si manifesta, invece, come un ecosistema complesso di tre livelli interattivi: quello fisico-infrastrutturale, rappresentato dalle macchine (le architetture delle reti, i *computer*, i *rou-*

ter); quello logico-informativo rappresentato dal volume dei dati gestiti dalle macchine (*database*, *files*, *software*); quello sociale-cognitivo determinato dall'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei *social network*, gli indirizzi IP delle macchine). Quindi, un luogo in cui si realizza l'interazione tra persone, *software* e servizi. Ed in cui il fattore umano è altrettanto importante quanto quello tecnologico [L. Montessoro, 2019, 791].

Negli ultimi trent'anni la crescita di Internet e dell'innovazione che ne è derivata è stata facilitata da un ambiente relativamente privo di controlli. Tuttavia, la profonda integrazione nel quadro sociale del *World Wide Web* ha messo in discussione l'idea tradizionale di sicurezza, intesa come predisposizione di un perimetro normativo funzionale al libero esplicarsi della sfera individuale. Ad essa sembra progressivamente sostituirsi un modello legato al concetto di protezione, caratterizzato dalla disponibilità (anche implicita) a scambiare/sacrificare spazi di libertà personale a fronte della possibilità di operare in un ambiente sociale e tecnologico politicamente e giuridicamente protetto (secondo il paradigma dello Stato preventivo) [F. Pizzolato, 2017, 39].

In questo contesto, per poter affrontare il tema della dimensione giuspubblicistica della sicurezza cibernetica occorre svolgere una ricostruzione che non operi un semplice adattamento delle categorie tradizionali, ma che cerchi di elaborarne di nuove. La vocazione libertaria dello spazio virtuale, frutto della circostanza che esso è, in ultima analisi, il prodotto più rappresentativo di forme estreme di anarco-liberalismo individualista, mal tollera i paradigmi dello Stato westfaliano, sovrano e regolatore, ma dà la stura al consolidarsi di un governo ampiamente nelle mani di poteri privati, senza ricevere la legittimazione di istituzioni nazionali o sovranazionali [S. Mannoni, G. Stazi, 2021, 24]. Queste ultime cercano di inseguire uno sviluppo tecnologico incontrollato attraverso strumenti di regolazione, più o meno vincolanti, e attraverso attività amministrative e giudiziarie che mirano rivendicare spazi di sovranità ed esercizio di poteri pubblici [M. Betzu, 2021, 24]. L'obiettivo non è solo l'autoconservazione dello Stato e delle sue componenti, ma soprattutto la sicurezza degli individui, dei gruppi e delle entità economiche e sociali in una logica neo-hobbesiana. Perché come scriveva Hobbes, senza sicurezza «non c'è posto per l'applicazione del lavoro perché il frutto di esso è incerto, e perciò non si coltiva la terra, non ci si dedica alla navigazione, (…) non si coltiva la storia, le arti, le lettere, i rapporti sociali, e ciò che è peggio si vive in uno stato di continuo timore e pericolo di morte violenta, e la vita dell'uomo è solitaria, misera, ripugnante brutale e breve» [T. Hobbes, 1955, 159-160].

Adattando allo spazio cibernetico questo assunto si potrebbe dire che, senza una rete protetta da pericoli e minacce, al giorno d'oggi anche la vita degli individui è priva di prospettive certe. Cosa si intende per rete sicura, in che modo il Leviatano può ancora svolgere il suo ruolo in un mondo senza

confini, in che senso il diritto può regolare l'azione dei privati e i compiti delle istituzioni pubbliche, sono questioni che si intersecano nella delimitazione del concetto giuridico di sicurezza cibernetica. In proposito, si potrebbe individuare una nozione ampia, che riguarda il livello sociale-cognitivo ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive, e una nozione ristretta, che riguarda la protezione del livello fisico-infrastrutturale e del livello logico-informativo. Nel primo caso la sicurezza attiene alla protezione dei beni giuridici che vengono lesi direttamente dall'uso degli strumenti informatici e che vedono il cyberspazio come ambiente delle condotte lesive nei confronti degli individui; nel secondo caso la sicurezza riguarda precipuamente le aggressioni alle infrastrutture ed ai sistemi informatici il cui effetto è, in varia misura, la lesione di beni giuridici fisici.

In entrambi i casi, i problemi giuridici della sicurezza cibernetica attengono alle modalità di repressione e, soprattutto, di prevenzione delle condotte lesive, ai soggetti, pubblici e privati, investiti della funzione di garantire la sicurezza, ai poteri correlati a tale funzione, nonché alle fonti di regolazione.

2. Il concetto di sicurezza cibernetica in senso ampio: il problema dell'ordine pubblico digitale

Come è noto, l'ordine pubblico come causa e fine della funzione di sicurezza si qualifica come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale (art. 159 d.lgs. n. 112/1998). Come espressamente affermato dalla Corte costituzionale: «tale definizione nulla aggiunge alla tradizionale nozione di ordine pubblico e sicurezza pubblica tramandata dalla giurisprudenza di questa Corte, nella quale la riserva allo Stato riguarda le funzioni primariamente dirette a tutelare beni fondamentali, quali l'integrità fisica o psichica delle persone, la sicurezza dei possessi ed ogni altro bene che assume primaria importanza per l'esistenza stessa dell'ordinamento» (Corte cost. 25 luglio 2001, n. 290).

Tale definizione può essere replicata per il cyberspazio laddove l'azione di protezione riguarda le relazioni umane digitali e i beni digitali. L'avvento della rivoluzione digitale ha determinato il sorgere di nuovi conflitti e ha reso possibili nuovi comportamenti illeciti, che violano o minacciano gravemente sia i diritti e gli interessi tradizionali di persone, gruppi e collettività sia quelli nuovi che proprio nella dimensione cibernetica trovano il loro necessario riconoscimento. Come è stato evidenziato, «accanto alle nuove forme di prevaricazione e di soggezione, correlate a concentrazioni straordinarie di poteri e di corrispondenti forze e capacità di intimidazione, di controllo, di condizionamento delle informazioni, della volontà e delle scelte delle singole persone e dei gruppi sociali, si sono sviluppate e si sviluppano nuove

forme di aggregazione, di condivisione, di partecipazione, che utilizzano le inedite possibilità di incontro, scambio e creazione di comunità e gruppi di interessi, con obiettivi e valori comuni» [L. Picotti, 2019, 38].

In tale contesto, la pacifica e ordinata convivenza può essere minacciata da condotte che vedono nell'ambiente digitale solo la caratterizzazione di un fatto che si può inverare anche nello spazio fisico, ma che trova nel mezzo informatico un'amplificazione dei suoi effetti pregiudizievoli (si pensi, ad esempio, al *cyber*-bullismo, al *sexing*, ma anche alla diffusione perniciosa di *fake news*), così come da condotte che costituiscono, invece, manifestazione esclusiva del cyberspazio (ad esempio, la frode informatica o il furto di identità). La criminalizzazione di tali condotte è avvenuta secondo due linee di sviluppo: da una parte, tramite l'estensione di talune fattispecie già esistenti che trovano nello spazio cibernetico un ambiente differenziato; dall'altra mediante la creazione di ipotesi specifiche, in considerazione delle peculiarità intrinseche della dimensione digitale. Ciò ha permesso la classificazione dei *cyber-crimes* a seconda che si tratti di reati comuni commessi mediante lo strumento informatico (per esempio, la diffamazione sul *blog*), ovvero si tratti di fattispecie nelle quali l'elemento informatico costituisca un elemento imprescindibile e caratterizzante della fattispecie, nel rispetto delle esigenze di tassatività delle norme incriminatrici [L. Picotti, 2011, 831].

Si tratta di condotte che da oltre un trentennio sono oggetto di normazione sovranazionale ed internazionale, che ha trovato il suo suggello più importante nella Convenzione di Budapest sulla criminalità informatica del 2001, recepita in Italia con la legge 18 marzo 2008, n. 48. Obiettivo di questo trattato è quello di perseguire una politica criminale comune e promuovere la cooperazione internazionale, tenendo in considerazione i profondi cambiamenti dovuti all'evoluzione della tecnologia digitale e alla globalizzazione delle reti informatiche e coinvolgendo nella prevenzione e nell'accertamento dei reati informatici non solo gli Stati, ossia organismi pubblici, ma anche il settore privato. L'ordinamento euro-unitario ha seguito la medesima traiettoria muovendosi, dapprima, con strumenti generali di armonizzazione come le decisioni quadro e, dopo il Trattato di Lisbona del 2008, con direttive specifiche, in attuazione a quanto previsto dall'art. 83.1 TFUE, che hanno determinato importanti sentenze della Corte di giustizia come quella sul caso Google del 2014 [R. Flor, 2019, 457].

Il tema riguarda l'attività di repressione degli illeciti e di prevenzione delle condotte lesive, che impongono una rivisitazione delle categorie tradizionali del diritto penale e spingono inevitabilmente ad immaginare un ambito operativo di interrelazioni tra forze dell'ordine e autorità di sicurezza che esorbita i confini statuali. Si tratta di attività amministrative e giudiziarie espressioni di poteri sovrani, la cui efficacia risulta pregiudicata dalla collocazione territoriale dell'autore di simili illeciti, ammesso che lo si possa individuare, e dal fatto che l'intermediario privato che gestisce la rete ha la

disponibilità esclusiva dei dati e dei contenuti sui quali si intende intervenire. In questa prospettiva, soggetti privati, titolari di piattaforme e *providers,* esercitano poteri preventivi e sanzionatori nei confronti dei propri utenti, spesso in maniera sommaria e senza alcuna garanzia procedurale.

Si è pertanto in presenza di un quadro complesso in cui, a fronte di una incrementale domanda di sicurezza generata dai pericoli e dalle minacce provenienti da un mondo virtuale, si registra un indebolimento delle tradizionali funzioni pubbliche statuali e una loro contaminazione forzata. E ciò in quanto il mondo socio-politico ha delegato al mondo privato-imprenditoriale il disegno e la gestione dell'architettura cibernetica, la quale integra una dimensione della sicurezza avulsa dalle categorie giuridiche di cui si è sempre nutrita, ossia la legittimazione, la polarità privato-pubblico, il nesso di spazialità-territorialità [A.C. Amato Mangiameli, 2019, 22]. Lo sforzo di ultraregolazione di tipo globale, basato, da una parte, sulla volontà di approntare omogeneità alle coordinate dell'illiceità e, dall'altra, su un esercizio di una sorta di *soft-power* nei confronti delle *Big-tech*, è sfociato in un sistema normativo che soffre ancora di un modello stato-centrico per la sua implementazione.

Ciò risulta confermato anche nell'esperienza italiana, nella quale la repressione penale dell'illecito cibernetico è fondata, in larga misura, su condotte tipizzate in fattispecie normative non sempre di agevole configurazione e l'attività di prevenzione nei confronti di criminali informatici risulta ancora allo stato primordiale, sia sul piano organizzativo, sia sul piano degli strumenti operativi. Ad eccezione di alcune materie, quali il *cyber*-bullismo o lo *stalking,* in cui la funzione di polizia di sicurezza si qualifica per strumenti di intervento preventivo, per le altre forme di crimini informatici, a causa dei citati limiti ordinamentali, la prevenzione risulta di scarsa o di nessuna efficacia. Tale circostanza riflette la volontà di lasciare alla sola polizia giudiziaria, che peraltro non è sempre adeguatamente attrezzata, il ruolo di perseguire fatti che trovano manifestazione nel cyberspazio.

In questa prospettiva, la prevenzione legata all'ordine pubblico digitale, ossia la sicurezza cibernetica in senso ampio, si è concentrata prevalentemente sulla tutela della riservatezza dei dati, che si sostanzia nella garanzia che il trattamento dei dati sia effettuato in modo da assicurare la sovranità delle informazioni, ossia la capacità di controllare l'integrità, la disponibilità e la circolazione delle informazioni digitali. La tutela dei dati è la precondizione per limitare il crimine informatico e la protezione e la responsabilizzazione del trattamento degli stessi diventa prioritario fattore di sicurezza per prevenire il fenomeno [C. Bigotti, 2014, 116]. Com'è noto, l'azione preventiva, regolativa ed amministrativa è dettata dalla disciplina euro-unitaria disposta dal Reg. UE 679/2016 (il c.d. GDPR), mentre l'azione repressiva si indirizza verso condotte criminali tese a compromettere la riservatezza dei dati, attraverso una loro esposizione al rischio di apprensione da parte di sog-

getti terzi, a determinare la perdita di disponibilità dei medesimi da parte del titolare, oppure a causare una menomazione della loro integrità ed autenticità [V. Manes, S. Mezzacuva, 2019, 168].

3. La sicurezza cibernetica in senso stretto: l'interrelazione tra sicurezza, difesa ed *intelligence*

La protezione *nello* spazio cibernetico si è altresì sviluppata nell'idea della protezione *dello* spazio cibernetico, o meglio di quella porzione che influenza l'ambito degli interessi pubblici considerati rilevanti e vitali per la loro dimensione fisica. In tal senso, l'ordine pubblico digitale viene declinato come protezione degli interessi minacciati da condotte lesive nei confronti dei sistemi e delle reti informatiche: un ambito che coinvolge l'insieme delle tecnologie e delle misure di risposta e mitigazione progettate per tutelare reti, *computer*, programmi e dati da attacchi, danni o accessi non autorizzati, in modo da garantire riservatezza, integrità e disponibilità. Ed è proprio tramite la individuazione degli interessi primari da proteggere che la sicurezza cibernetica si presenta come una funzione pubblica, la quale muovendo da un controllo delle infrastrutture tecnologiche tenta di inibire pericoli e minacce sulle persone.

I criminali informatici sono ormai in grado di sfruttare le vulnerabilità dei prodotti e delle reti informatiche per acquisire illegalmente i dati che transitano nello spazio cibernetico e per compromettere, in tutto o in parte, il funzionamento di servizi o sistemi digitali: è sotto questa prospettiva che la sicurezza cibernetica emerge come prestazione di un servizio essenziale per il mantenimento di attività civili, sociali ed economiche fondamentali dello Stato. Come è stato osservato, «l'ampia gamma di azioni ostili può andare dallo spionaggio agli attacchi veri e propri, con finalità di inibire, alterare o addirittura distruggere dati, *hardware*, reti o eventuali servizi e sistemi ad essi connessi. Generalmente possono essere rivolte ad assetti governativi, economico-finanziari, imprese, infrastrutture critiche o servizi dedicati alla società civile. I possibili effetti da essi generati possono facilmente divenire strategicamente rilevanti oppure influenzare comportamenti, azioni e documentazione collegati anche ad operazioni militari in corso. I protagonisti possono essere entità statuali, gruppi terroristici, organizzazioni criminali o semplici individui dediti alla ricerca di informazioni o alla distruzione/danneggiamento dei sistemi informatizzati e dei dati in essi contenuti» [N. De Felice, 2012, 72]. Si tratta, dunque, di una funzione di sicurezza che interessa, complessivamente, l'ordinamento statale e, in dettaglio, le sue componenti, ossia le imprese e i singoli cittadini. Da questo punto di vista, «la tecnologia non soltanto ha offerto in tempi particolarmente brevi eccezionali occasioni di progresso e quindi di sviluppo delle possibilità di conoscen-

za, di miglioramento culturale, sanitario, tecnologico, economico, ma ha ad un tempo consentito l'affermarsi di modalità aggressive che, se operate con propositi criminali, sono in grado di minacciare sia gli interessi dello Stato che la fruibilità dei diritti dei soggetti di un ordinamento» [G. De Vergottini, 2019, 76].

In definitiva, sussiste un interesse pubblico che denota una funzione statuale: quello di apprestare, contestualmente, mezzi di protezione a favore dello Stato e dei suoi soggetti, relativi alla sopravvivenza, all'incolumità e all'integrità politica, alla stabilità economica e al benessere sociale derivanti dall'utilizzo dello spazio cibernetico [A. Monti, 2020, 79]. In questa prospettiva, si fa strada una dimensione più ristretta della sicurezza cibernetica, che ha una duplice natura: la difesa del "fortino" tecnologico, che protegge quegli interessi di fronte ad attacchi tesi a minarne la stabilità; l'attività di prevenzione, che si coagula nella promozione della resilienza delle infrastrutture rispetto al pericolo, potenziale o attuale, di pregiudizio al funzionamento delle stesse, al fine di inibire o mitigare i danni alle persone, alle imprese di settori nevralgici per la vita economica, o alle istituzioni democratiche. La funzione amministrativa connessa all'ordine pubblico digitale diventa allora l'organizzazione e la raccolta di risorse, processi e strutture volte a proteggere il cyberspazio e i sistemi abilitati da eventi pregiudizievoli [D. Craigen, N. Daikun-Thibault, R. Purse, 2014, 17], al fine di tutelare interessi considerati rilevanti anche ai fini della sicurezza nazionale.

Al riguardo, si deve osservare come la fluidità della rete senza confini non consente di precisare i tratti distintivi tra attività di difesa, ossia protezione dalle minacce esterne, e attività di sicurezza, volta a garantire in termini preventivi l'incolumità di persone e beni [A. Lauro, 2021, 530].

Di fronte alla fisiologica a-territorialità dello spazio cibernetico si individua una sorta di *area di territorializzazione effettuale* dello stesso, in modo da definire un ambito di tradizionale autorità ed esercizio dei poteri correlati: una funzione di tutela che si lega alla natura nazionale (e quindi direttamente o indirettamente territoriale) degli interessi tutelati [N. Tsagourias, 2015, 21]. Tale funzione è contrassegnata, da una parte, dal carattere dinamico della stessa, derivante dalle continue interazioni tra esseri umani e sistemi informatici, e dall'altra, dalla sua complessità intrinseca, in quanto immaginata per fornire protezione nei confronti dell'intera gamma degli eventi pregiudizievoli, siano essi intenzionali ovvero accidentali. In questo senso, la funzione di sicurezza cibernetica si dettaglia: nella creazione di un modello organizzativo complesso e policentrico, idoneo a monitorare e sorvegliare il "fortino"; nel rafforzamento dei potenziali bersagli vulnerabili, consentendo loro di resistere agli attacchi o di impedire le intrusioni; nel costruire sistemi resilienti in grado di continuare a funzionare durante un attacco, riprendersi rapidamente ed, eventualmente, rispondere agli attaccanti.

Ciò posto, si potrebbe ritenere che il concetto di sicurezza cibernetica in senso stretto compendi due tipi di attività di rilievo pubblico: la *cyber-defense*, intesa come resistenza di fronte ad un attacco informatico, e la *cybersecurity*, intesa come prevenzione e resilienza del sistema informatico rispetto ad un potenziale attacco.

Al riguardo occorre precisare che l'attacco informatico può essere definito come un tentativo malevolo e intenzionale, da parte di un individuo o di un'organizzazione, di violare il sistema informativo di un altro individuo o azienda e che esso si caratterizza, prevalentemente, in relazione alla "sensibilità" del bersaglio colpito, alla natura pubblica o privata dei dati e delle informazioni, alla rilevanza degli interessi coinvolti. Come è agevole sottolineare, l'offensività e l'impatto di un attacco appare maggiore se esso è indirizzato verso un operatore di servizi essenziali, pubblico o privato che sia (come quelli del settore dell'energia, del traffico aereo o dei mercati finanziari), oppure verso un fornitore di servizi digitali di primaria importanza.

I *cyber attacks* possono essere distinti anche in base al loro oggetto: mentre negli attacchi "passivi" l'attività malevola è diretta ad acquisire, alterare o danneggiare o a utilizzare abusivamente dati o informazioni, senza incidere necessariamente sulle infrastrutture fisiche o logiche, gli attacchi "attivi", invece, mirano ad alterare o a danneggiare i sistemi informatici e le loro risorse [R. Flor, 2019, 453]. Di conseguenza, le finalità principali di un attacco cibernetico possono essere due: le informazioni e/o la causazione di un danno fisico. Con riferimento al primo ambito, si deve ricordare come, in termini informatici, un'informazione è ogni dato che riduca l'incertezza in ordine allo stato di un sistema; così il sistema operativo di un *computer*, i suoi processi automatizzati, le sue applicazioni (così come i file ivi contenuti) sono classificabili quali informazioni. Con riferimento al secondo ambito, l'esperienza dimostra che un attacco cibernetico può cagionare un rilevante danno di natura fisica, come avviene quando vengono colpiti sistemi con i quali si gestiscono le infrastrutture critiche delle società tecnologicamente avanzate [S. Setti, 2017, 2].

Come è noto, la tipologia di attacchi informatici è molto variegata e diversificata nelle modalità e negli effetti pregiudizievoli realizzati. Tra quelli più diffusi si possono evidenziare quelli che utilizzano i c.d. *malware,* ossia *software* malevoli con i quali si viola una rete sfruttandone le vulnerabilità (come si verifica, in genere, quando un utente seleziona un *link* pericoloso o apre un allegato ricevuto via *e-mail* che installa un *software* dannoso). Una volta all'interno del sistema, il *malware* può bloccare l'accesso alle componenti principali della rete (*ransomware*), installare altri *software* dannosi, ottenere informazioni di nascosto trasmettendo dati dal disco rigido (*spyware*) o interferire con altre componenti e rendere il sistema inutilizzabile. Un'altra forma di attacco ampiamente utilizzata è il c.d. DoS ovvero DDoS (*Distributed Denial-of-Service*), mediante il quale si invadono le risorse di un sistema

al fine di sovraccaricarle, impedire le risposte alle richieste di servizio, ridurre le prestazioni del bersaglio. In ultimo, si segnalano gli attacchi *Structured Query Language (SQL) injection,* mediante i quali si incorpora un codice dannoso in applicazioni vulnerabili, producendo risultati di *query* nel *database* ed eseguendo comandi che l'utente non ha richiesto.

Alla luce di quanto detto, l'attacco cibernetico individua, in prima battuta, in relazione alla sua portata lesiva di interessi, direttamente o indirettamente, di rilevanza pubblica, i compiti di difesa prioritariamente in capo a soggetti pubblici. Si tratta di un'attività, la c.d. *cyber defence*, che si ascrive per il suo carattere peculiare nell'ambito della sicurezza nazionale, e che è destinata a fronteggiare i nuovi conflitti cibernetici, nei quali si misura la capacità dello Stato di proteggere sé stesso, le proprie istituzioni e le strutture economico-sociali ritenute essenziali, contro minacce, spionaggio, sabotaggio, crimini, frodi, furti d'identità ed altre interazioni e transazioni cibernetiche illecite e distruttive.

Al riguardo è stato evidenziato che «la difesa cibernetica ha una sua specificità e importanza da tre punti di vista. In primo luogo, il dominio cibernetico può essere considerato un terreno di scontro ad alta intensità nel quale non è mai stato finora dichiarato un conflitto, ma in cui gli attacchi sono numerosi, vengono attuati da una pluralità di attori statali e no, e possono portare all'attivazione della clausola di difesa collettiva della Nato, con ripercussioni anche nel "mondo reale". In secondo luogo, di conseguenza, il dominio cibernetico vede il formarsi di comandi, agenzie e unità sia nei Ministeri della Difesa dei Paesi alleati sia a livello Nato. Infine, la questione della *cyber defence* apre il campo a riflessioni strategiche nuove su cosa vuol dire difendersi e attaccare, nonché dissuadere un attacco, sia in questo dominio operativo sia negli altri quattro domini pervasi dal *cyberspace*» [A. Marrone, E. Sabatino, O. Credi, 2021, 33].

In proposito occorre altresì evidenziare che l'attività di difesa cibernetica non si limita solo al presidio del "fortino", poiché, come già notato dalla dottrina militare statunitense, per riuscire ad assicurare questo risultato occorre anche assumere un ruolo attivo [P.M. Nakasone, 2019, 12]. In particolare, è importante sviluppare una capacità di difesa cibernetica "attiva" (*active cyber defence*), ossia una capacità proattivamente difensiva, tesa a sfruttare le vulnerabilità altrui (c.d. *exploitation*) per un eventuale contrattacco nello spazio cibernetico. Lo scopo di questa attività è quello di eseguire *penetration test* al di fuori del proprio perimetro informatico e di compiere un'analisi degli effetti malevoli da poter arrecare ad altri sistemi esterni [M. L'Insalata, 2019, 1282]. Come osservato dalla Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico della Camera dei deputati del 2017, «mentre la difesa cibernetica in senso stretto (*cyber defence* o *cyber security*) comprende misure di separazione fisica o di protezione (reti autonome, *firewall*, *antivirus*) e protocolli di sicurezza (procedure, modi di fare), la difesa pro-

attiva (*active cyber defence*) – primo grado verso le capacità di *exploitation* (sondare restando invisibili) e di attacco (produrre danni) nello spazio cibernetico – implica un'interazione attiva con l'esterno per proteggere la propria rete».

In tal senso, se l'*exploitation* rappresenta l'operazione, prevalentemente di *intelligence*, destinata ad acquisire informazioni sugli avversari, restando invisibili, per capire cosa fanno, come possono reagire e cosa possono subire, l'*attack* costituisce un'operazione indirizzata a provocare effetti pregiudizievoli nei confronti dei criminali informatici. Si tratta di quello che è stato definito tecnicamente come *hackback,* secondo il quale la vittima di un attacco informatico costruisce un contrattacco contro l'aggressore, danneggiando il suo sistema prima che possa arrecare ulteriore danno e impedendogli di lanciare futuri attacchi. Secondo l'analisi compiuta dalla dottrina statunitense, l'*hackback* può essere realizzato dirigendo un'ondata di traffico verso i *server* attraverso i quali l'attacco informatico viene instradato, sopraffacendoli temporaneamente e dissuadendoli dal continuare l'intrusione [N.A. Sales, 2013, 1564].

La *cyber defense* si caratterizza, in ultima analisi, per la creazione di modello indirizzato a costruire le c.d. capacità di *Computer Network Operations* (*CNO*), vale a dire quel complesso di capacità/attività nel settore informatico, telematico e cibernetico aventi finalità offensive, difensive e/o di analisi e sfruttamento di dati, sia sul territorio nazionale che fuori dai confini, attraverso l'integrazione delle capacità militari interforze, in armonia con il quadro legislativo nazionale e delle regole internazionali ratificate da ciascuno Stato.

Le CNO si basano sullo sviluppo di tre pilastri fondamentali: a) la *Computer Network Defence* (*CND*) che individua, attraverso attività di analisi e sfruttamento dei dati, una serie di azioni tese a proteggere da attività cibernetiche ostili le infostrutture sensibili e gli assetti rilevanti per la Difesa; b) la *Computer Network Exploitation* (*CNE*) che riguarda quella serie di azioni tese ad acquisire e analizzare dati e informazioni contenute su *computer* e *network* d'interesse, al fine di ottenere un vantaggio; c) il *Computer Network Attack* (*CNA*) che denota le azioni volte a rendere inaccessibili, degradare o distruggere informazioni contenute in rete o nei *computer* degli avversari [D. Murciano, 2012, 85].

In definitiva, se la difesa del "fortino" informatico si muove, sul piano oggettivo e soggettivo, lungo le linee della funzione di sicurezza nazionale e della difesa militare, l'attività di prevenzione, volta a garantire la resilienza del sistema informatico rispetto a potenziali minacce, rappresenta una funzione nuova per la quale si individua un compito pubblico, nel quale regolazione e amministrazione assumono connotati peculiari, e una architettura organizzativa, che si contraddistingue per un modello composito in cui convivono soggetti pubblici dotati di poteri autoritativi e forme di cooperazione con soggetti privati.

La costruzione di una funzione pubblica indirizzata alla prevenzione dei sistemi informatici ha trovato nell'ordinamento europeo un significativo impulso sin dal 2013, che si è tradotto nell'adozione di importanti indirizzi strategici e, più di recente, in una regolazione di dettaglio. Di fronte alle minacce derivanti da attacchi su vasta scala, potenzialmente ostativi della normale e corretta prestazione di servizi essenziali sull'intero territorio europeo, l'obiettivo dell'Unione è stato quello di costruire, da una parte, capacità effettive e coordinate di risposta e di gestione delle crisi, anche tramite apposite politiche e strumenti di più ampia portata, e quello di svolgere, dall'altra, una valutazione periodica sullo stato della cybersicurezza e della resilienza nel contesto europeo, anche per poter effettuare previsioni sistematiche circa gli sviluppi, le prospettive e le minacce future. Al riguardo, si è sottolineata la necessità di effettuare un *enforcement* delle capacità e della preparazione degli Stati membri e delle imprese, nonché un miglioramento della cooperazione, del coordinamento e della condivisione di informazioni tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. Tuttavia, importanti competenze in materia di sicurezza cibernetica restano ancora attribuite ai singoli Paesi, i quali si devono impegnare a «mantenere e sviluppare le capacità degli Stati membri di rispondere in modo globale alle minacce informatiche, compresi gli incidenti transfrontalieri».

Anche in Italia, per fare fronte alle evidenti necessità di sicurezza cibernetica dell'ordinamento, si è registrata a partire dal 2013 una embrionale regolazione (DPCM 24 gennaio 2013, c.d. Decreto Monti), alla quale ha fatto seguito una produzione normativa alluvionale e multilivello, che ha visto nel d.l. n. 105/2019, istitutivo del Perimetro informatico, e nel d.l. n. 82/2021, che ha istituito l'Agenzia per la Sicurezza Cibernetica, due momenti fondamentali di definizione del modello istituzionale di tutela delle reti, dei sistemi e delle comunicazioni elettroniche. L'architettura complessiva che se ne ricava si caratterizza per la stretta connessione tra la nozione di sicurezza nazionale e quella di ordine e sicurezza pubblica e per la partecipazione attiva delle infrastrutture critiche, gestite sia da soggetti pubblici che privati, alle attività di protezione della cybersicurezza [F. Serini, 2022, 268].

In conclusione, la sicurezza cibernetica è divenuta oggi una funzione pubblica sufficientemente definita nei suoi contenuti regolatori, sebbene, in considerazione della complessità e della dinamicità del fenomeno, essa si presenti ancora approssimativa nella sua dimensione operativa.

Il volume, in questo senso, proponendo un'analisi articolata e approfondita di diversi aspetti della tematica, cerca di rispondere all'esigenza di riflettere sullo stato dell'arte e di porre in risalto le principali criticità del sistema nazionale di tutela della cybersicurezza. Si tratta, pertanto, di un punto di partenza per ulteriori ricerche sul tema, il quale nel prossimo futuro non potrà che occupare uno spazio centrale nel dibattito giuspubblicistico.

Bibliografia

Amato Mangiameli A.C. (2019), *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica*, in Amato Mangiameli A.C., Saraceni G. (a cura di), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, II edizione, 1-56.

Betzu M. (2021), *I baroni del digitale*, Napoli.

Bigotti C. (2014), *La sicurezza informatica come bene comune implicazioni penalistiche e di politica criminale*, in Flor R., Falcinelli D., Marcolini S. (a cura di), *La giustizia penale nella "rete"*, Milano, 2015, 97 ss.

Bombelli G. (2017), *Dal moderno all'"ultramoderno"? Intorno al nesso diritto-tecnica-sicurezza*, in Pizzolato F., Costa P. (a cura di), *Sicurezza e tecnologia*, Milano, 3-26.

Brighi R., Chiara P.G. (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, n. 21, 18-42.

Craigen D., Daikun-Thibault N., Purse R. (2014), *Defining Cybersecurity*, in *Technology Innovation Management Review*, n. 10, 13- 21.

De Felice N. (2012), *Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali*, in Gori U., Germani L.S. (a cura di), *Information warfare 2011. La sfida della cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano, 69-82.

De Vergottini G. (2019), *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, n. 4, 76.

Flor R. (2019), *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di internet*, n. 3, 453-469.

Kuehl D.T. (2009), *From Cyberspace to Cyberpower: Defining the Problem*, in F.D. Kramer, S.H. Starr, L. K. Wentz (eds.), *Cyberpower and national security*, University of Nebraska Press.

L'Insalata M. (2019) *Cyberwarfare: gli scenari della guerra informatica*, in Cadoppi A., Canestrari S., Manna A., Papa M. (diretto da), *Cybercrime*, Torino, 1273 ss.

Lauro A. (2021), *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Gruppo di Pisa*, quaderno n. 3, 529-545.

Manes V., Mazzacuva F. (2019), *GDPR e nuove disposizioni penali del Codice privacy*, in *Dir. pen. proc*., n. 2, 168 ss.

Mannoni S., Stazi G. (2021), *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli.

Marrone A., Sabatino E., Credi O. (2021), *L'Italia e la difesa cibernetica*, Documenti IAI 21/12, in www.iai.it

Martino L. (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, n. 1, 61-76.

Montessoro P.L. (2019), *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *Istituzioni del Federalismo*, n. 3/2019, 783-800.

Murciano D. (2012), *Il ciberspazio quale nuovo dominio operativo per lo strumento militare nazionale,* in Gori U., Germani L.S. (a cura di), *Information warfare 2011. La sfida della cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano, 83-90.

Nakasone P.M. (2019), *A Cyber Force for Persistent Operations*, in *Joint Force Quarterly*, n. 92, 10-14.
Picotti L. (2011), *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, n. 4, 827 ss.
Picotti L. (2019) *Diritto penale e tecnologie informatiche: una visione di insieme*, in Cadoppi A., Canestrari S., Manna A., Papa M. (diretto da), *Cybercrime*, Torino, 33 ss.
Pizzolato F. (2017), *Il costituzionalismo alla prova della tecnica: libertà, uguaglianza e sicurezza*, in Pizzolato F., Costa P. (a cura di), *Sicurezza e tecnologia*, Milano, 27-45.
Sales N.A. (2013), *Regulating cyber-security*, in *Northwestern University Law Review*, vol. 107, n. 4, 1503-1568.
Serini F. (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, n. 12, 2022, 241-272.
Setti S. (2017), *Diritto e guerra cibernetica*, in *www.sicurezzanazionale.gov.it.*
Tsagourias N. (2015), *The legal status of cyberspace*, in N. Tsagourias, R. Buchan (eds.), *Research handbook on International Law and Cyberspace*, Cheltenham, 13 ss.

La regolazione della cybersecurity in Italia

Manfredi Matassa

Sommario: 1. Premessa. - 2. Inquadramento del fenomeno. - 3. La disciplina dell'Unione Europea. - 4. L'approccio italiano al tema della sicurezza cibernetica. - 5 (*Segue*): Alcuni cenni sull'architettura nazionale di cybersicurezza. - 6. La visione strategica italiana tra realtà e mito.

1. Premessa

Oggi l'impegno sul fronte della sicurezza cibernetica deve considerarsi un prerequisito essenziale per garantire la sopravvivenza di qualsiasi organizzazione complessa. La storia recente ha dimostrato come un'entità ostile, che sia uno Stato o un insieme di privati, possa ricorrere allo strumento informatico per perseguire gli scopi più eterogenei: basti pensare alle frequenti campagne di disinformazione volte a compromettere lo svolgimento dei processi decisionali indispensabili per la vita di una qualsiasi democrazia, ma anche agli attacchi che hanno determinato la sospensione dell'erogazione dei servizi pubblici essenziali di un intero Paese o ne hanno danneggiato le infrastrutture di difesa. In tale contesto, occorre considerare anche come la sempre maggiore diffusione dell'Internet of Things (IoT)[1] nelle nostre vite quotidiane abbia portato con sé indiscutibili vantaggi, permettendo tuttavia al Cyberspazio di invadere quasi ogni aspetto della vita reale, esponendo così i cittadini alle conseguenze del «mondo delle tecnologie ad alto rischio» [C. Perrow, 1984, 3] in modo spesso inconsapevole.

1. Il concetto di "Internet of Things" (IoT) è stato impiegato per la prima volta nel 1999 dall'ingegnere inglese Kevin Ashton per descrivere un sistema in cui gli oggetti del mondo fisico potessero essere connessi all'internet attraverso dei sensori. Secondo le stime dell'Unione Europea entro il 2024 saranno circa 22,3 miliardi i dispositivi in tutto il mondo connessi all'IoT e gli esempi applicativi di IoT utilizzate già oggi nella vita di tutti i giorni sono innumerevoli: basti pensare alle automobili, alle abitazioni dotate di impianti domotici o anche alle *smart cities*.

In tale scenario, la sicurezza cibernetica si è affermata quale obiettivo primario a tutti i livelli di regolazione. Come verrà meglio approfondito nel prosieguo, l'esigenza di protezione verso le sempre più crescenti minacce cibernetiche ha infatti condotto l'Unione Europea e i singoli Stati membri a dotarsi di strutture organizzative con caratteristiche inedite, dando così vita ad un'architettura di notevole complessità e in costante mutamento. Con particolare riferimento al contesto italiano, pur riscontrando una tardiva presa di consapevolezza circa l'importanza del tema rispetto ad altri Stati europei, si riscontra ad oggi l'ideazione di un modello di gestione degli incidenti informatici virtuoso e con numerosi profili di originalità da ultimo valorizzato dalla pubblicazione della strategia Nazionale di Cybersicurezza 2022-2026. Così, se nel corso dell'ultimo ventennio l'argomento della sicurezza informatica è stato oggetto di numerosi studi che hanno coinvolto trasversalmente quasi ogni ambito del sapere, negli anni recenti è emerso il ruolo di grande rilievo attribuito alla scienza dell'amministrazione per il raggiungimento degli obiettivi prefissati in materia di cybersicurezza. Ancora oggi, tuttavia, lo studio dei profili giuridici della cybersecurity non si dimostra spesso agevole a causa di diversi fattori, su tutti la notevole complessità del modello organizzativo della sicurezza cibernetica in Italia e la non sempre felice formulazione delle disposizioni introdotte nell'ultimo quinquennio.

Su tali premesse si intende fornire al lettore un inquadramento generale del tema della sicurezza cibernetica con l'intento di introdurre alcune questioni che saranno trattate con un maggiore grado di approfondimento all'interno del presente volume. In particolare, oltre a ripercorrere a brevi cenni le principali elaborazioni teoriche che hanno segnato il rapporto tra sovranità e cyberspazio, si intende mettere a fuoco la nozione di "attacco informatico" con l'intento di perimetrare i diversi concetti di "*cyber-attack*", "*cyber-warfare*" e "*cyber-crime* ". Una volta definiti tali concetti preliminari sarà possibile ripercorrere le principali tappe che hanno permesso la costruzione di un'infrastruttura comune di difesa cibernetica europea, con l'intento di avanzare alcune riflessioni conclusive circa i più evidenti punti di forza e di debolezza dell'attuale architettura a livello comunitario e interno.

2. Inquadramento del fenomeno

Come è stato già accennato, la sicurezza cibernetica ha acquisito un ruolo di indiscussa centralità nell'attuale dibattito tra studiosi pubblicisti. Tuttavia, sebbene questo tema sia stato approfondito già a partire dagli anni Novanta in ambiti del sapere tra loro eterogenei e sotto molteplici angoli visuali (da quello informatico a quello sociologico, passando anche da ricerche in ambito operativo-militare), i primi studi in ambito giuridico sul tema risalgono soltanto all'ultimo decennio.

Per individuare le ragioni che hanno portato al tardivo sviluppo di una vera e propria *cybersecurity law* è necessario avviare la disamina del tema partendo da lontano, guardando in particolare il rapporto tra sovranità e cyberspazio. I primi teorici del diritto dell'internet non sono stati infatti chiamati a interrogarsi esclusivamente sul ruolo che le organizzazioni tradizionali avrebbero dovuto assumere di fronte alla progressiva espansione della rete, ma anche su come quest'ultime – ancora profondamente legate al principio di territorialità – potessero esercitare sovranità su un qualcosa di "immateriale" come internet. Non vuole essere obiettivo né ambizione di questo scritto tentare di sciogliere i nodi ancora irrisolti della *vexata quaestio* relativa alla sovranità dell'internet, ma esigenze di completezza della trattazione suggeriscono di delineare le tre precise fasi che hanno segnato tale complesso rapporto nel corso del tempo.

In una prima fase, agli albori della nascita di internet, la sovranità del dominio cibernetico si riteneva attribuita direttamente agli utenti della rete sulla falsariga dei principi racchiusi nella celebre Dichiarazione di Indipendenza del Cyberspazio del 1996. Dichiarazione, quest'ultima, ricordata ancora oggi per aver raffigurato i governi come «stanchi giganti di carne e di acciaio» incapaci di comprendere la portata della rivoluzione in corso in risposta al tentativo del legislatore americano di imporre una politica restrittiva in materia di controllo delle telecomunicazioni. Nella prospettiva degli ideatori di questo primo modello di regolazione della sovranità del *cyberspazio*, a posteriori definito come *cyber as sovereign* [K.E. Eichensehr, 2015, 327], internet era ancora immaginato come uno spazio virtuale lontano dai problemi economici e geopolitici del mondo reale e sembrava destinato ad essere regolato dai suoi stessi utenti senza essere assoggettato al controllo di nessun governo. La spinta cripto-anarchica che ha contraddistinto questo primo modello può essere sicuramente giustificata dal contesto e dal momento storico in cui il pensiero prende forma: a quel tempo il CERN aveva annunciato da appena anni la nascita del *world wide web*, la rete internet connetteva tuttalpiù dieci milioni di computer e il termine "cyberspazio" si riferiva ancora ad un universo alternativo teorizzato in un romanzo fantascientifico [W. Gibson, 1982, 72].

L'inarrestabile espansione di internet della seconda metà degli anni Novanta rese tuttavia ben presto evidente che il pubblico potere non potesse più valutare gli avvenimenti della rete come privi di effetti nel mondo reale. Su queste basi iniziarono così a svilupparsi ricostruzioni incentrate sull'idea secondo cui la rete non fosse uno "spazio" separato rispetto al territorio tradizionale, e non ciò tanto in funzione delle componenti *hardware* necessarie per il suo funzionamento (teoria fin da subito minoritaria nota come "*internet as a place*"), ma in quanto mezzo necessario per comunicare tra giurisdizioni differenti nel mondo reale [J. Goldsmith, 1998, 476]. Secondo tale prospettiva, il ruolo affidato a internet dalla fine del ventesimo secolo non sembra difforme da quello in precedenza attribuito al telefono fisso, al telegrafo e un

tempo ai segnali di fumo (*sic!*). Dunque, anche di fronte all'espansione tecnologica allora in corso, lo Stato avrebbe dovuto continuare ad esercitare la sua indispensabile funzione di soggetto regolatore a tutela di ogni cittadino.

La terza e più moderna elaborazione volta a qualificare il rapporto tra sovranità e cyberspazio raccoglie invece il dibattito sviluppatosi tra alcuni tra i più importanti accademici tra i primi anni Duemila e si distingue per una netta svalutazione del ruolo attribuito ai singoli stati nella regolazione del cyberspazio in favore della creazione di una *global cyber governance* [G. Goldsmith, 2006, 164]. La più recente ricostruzione si smarca così dal concetto tendenzialmente nazionale di sovranità della rete e inquadra il tema come problema da risolvere su scala globale attraverso i tradizionali strumenti di diritto e politica internazionale. Una volta consolidata l'idea secondo cui la sovranità della rete dovesse essere inquadrata nell'alveo dei «*government-to-government issues*» e non nei rapporti «*government-to-individual*» [K.E. Eichensehr, 2015, 329] il tema della sovranità della rete, e conseguentemente anche la sicurezza cibernetica degli Stati, sembra destinato ad interessare studiosi delle relazioni internazionali e dei conflitti più che studiosi dell'amministrazione.

Tale convinzione, volta a intendere la cybersecurity come un argomento poco affine con gli interessi dello studioso della cosa pubblica, sembra rimanere ferma per diversi anni, fino al verificarsi di un attacco informatico di grandi dimensioni proprio nel territorio europeo. Si fa riferimento ai violenti scontri tra la popolazione russofona e le autorità conseguenti alla decisione del governo estone di spostare una statua simbolo dell'era sovietica dalla piazza centrale di Tallin in un luogo meno rappresentativo della città. La risposta alla ferma repressione delle proteste segnò uno spartiacque nella storia recente: un gruppo riconducibile alla Russia avviò un *DdoS attack*[2] dalla durata ventidue giorni che rese impossibile l'erogazione di alcuni servizi pubblici e commerciali essenziali per la vita del Paese (basti pensare al blocco assoluto sistema sanitario, energetico e alla rete dei trasporti).

Questo evento, guardato a posteriori, può ritenersi come un "banco di prova" della guerra cibernetica del futuro. Soltanto pochi anni più tardi, nel

2. Per *Distributed Denial of Service attack* (DdoS) si fa riferimento a un attacco distribuito capace di generare una quantità abbastanza grande di traffico di dati verso un determinato server fino al punto di rallentarne il funzionamento o impedirgli di accettare nuove connessioni. Si tratta di un bombardamento informatico di grande intensità, capace di sospendere il funzionamento di un determinato server per tutta la durata dell'attacco. Rimandando lo studio dell'incidenza degli attacchi *ransomware* nel settore pubblico a contributi più approfonditi in questa sede preme in ogni caso sottolineare come tale tipologia di attacco si sia dimostrata particolarmente efficace contro le pubbliche amministrazioni. La natura spesso riservata dei dati posseduti da quest'ultime permette infatti di portare a termine attacchi ransomware "a doppia estorsione" con cui, oltre alla somma richiesta per la decifrazione delle informazioni presenti nel dispositivo colpito, l'attaccante richiede un riscatto aggiuntivo minacciando di rendere pubblici i dati ottenuti.

gennaio del 2010 il programma nucleare iraniano subì un brusco rallentamento a causa dell'improvviso guasto di parte della strumentazione utilizzata per l'arricchimento di uranio nella principale centrale del Paese. I sistemi di difesa informatici di allora non rilevarono alcuna anomalia e, certe che lo sviluppo di sistemi digitali offline costituisse un valido strumento di difesa, le autorità iraniane non ritennero che l'incidente fosse stato conseguenza delle ingerenze di un soggetto esterno. La causa del malfunzionamento venne scoperta soltanto nei mesi successivi: un malware capace di autopropagarsi (*worm*) dal peso di soli 500 kilobyte, possibilmente introdotto attraverso l'inserimento di una semplice chiavetta USB, che richiese circa 10.000 giorni di lavoro per la sua creazione. Un progetto troppo grande da realizzare per chiunque non fosse uno Stato-nazione.

Con il passare del tempo divennero sempre più frequenti attacchi informatici non più legati a singoli obiettivi militari o strategici, ma elaborati con l'intento di creare danni economici e reputazionali agli Stati attraverso attacchi diffusi e ad ampio spettro. Si pensi, ad esempio, al *malware* noto come *Wanna Cry* che nel 2017 riuscì a infettare in poco tempo più di 200.000 computer in almeno 74 nazioni cifrando le informazioni contenute nei dispositivi attaccati o, ancora, a *Petya* che negli stessi anni riuscì a infliggere danni a imprese europee e statunitensi per una stima di circa dieci miliardi di dollari.

Le implicazioni di questi eventi non furono immediatamente chiare. Se in un primo momento alcuni autorevoli studiosi ricalcarono con fermezza l'idea secondo cui la minaccia cibernetica non potesse essere valutata alla stregua di una minaccia militare in senso stretto [T. Rid, 2013], gli avvenimenti che si verificarono negli anni successivi smentirono quest'idea dimostrando come il cyberspazio fosse ormai asceso alla "quinta dimensione della conflittualità". Si accede così ad un momento storico in cui la sicurezza interna, il benessere economico e la vita democratica di uno Stato iniziano a dipendere dalla stabilità e la sicurezza del cyberspazio [L. Denardis, 2020, 97]. Divenne così ben presto necessario introdurre nuove misure e stanziare ingenti investimenti in materia di cybersicurezza, non tanto per accelerare il percorso di transizione digitale italiano ed europeo, ma per offrire una tutela indispensabile alla stessa sicurezza dei cittadini. In tale contesto, prima di soffermarsi sull'importante ruolo affidato alla scienza dell'amministrazione nel contrasto alle minacce cibernetiche, si ritiene opportuno tuttavia mettere a fuoco il concetto di "attacco cibernetico" e le diverse implicazioni sul piano giuridico ad esso correlate.

Preliminarmente, può evidenziarsi come nell'ultimo decennio si siano registrati in letteratura diversi tentativi volti ad elaborare una definizione di "attacco informatico" abbastanza flessibile da adeguarsi alla continua evoluzione di tale fenomeno. Rinviando la ricognizione delle varie definizioni proposte a studi più approfonditi [O.A. Hathaway et. al, 2012, 822-832], in questa sede ci si può limitare a far luce sull'importante distinzione tra attac-

chi informatici (*cyber-attacks*), guerra cibernetica (*cyber-warfare*) e crimini informatici (*cyber-crimes*). Sul punto va anzitutto chiarito che la ricostruzione maggiormente condivisa inquadra il rapporto tra attacchi informatici e guerra cibernetica in una relazione da genere a specie: entrambi questi fenomeni condividono le medesime due finalità (distruggere o disturbare le operazioni di un network e finalità politiche o di sicurezza nazionale), ma la *cyber-warfare* si contraddistingue per un ulteriore elemento: il verificarsi di effetti equivalenti a quelli causati da un attacco tradizionale. Il crimine informatico, invece, può ritenersi un fenomeno distinto rispetto ai precedenti, in quanto – per essere considerato tale – richiede il coinvolgimento dal lato attivo di attori non statali e la commissione di una condotta tassativamente prevista dalla legge come reato realizzata attraverso l'utilizzo di un sistema informatico. Seguendo tale ricostruzione, un crimine informatico può essere dunque considerato un cyberattacco soltanto nel caso in cui integri in via mediata o indiretta i presupposti di "scopo" che contraddistinguono tale categoria, mentre appare dubbia la possibile coincidenza con il fenomeno della guerra cibernetica (sarebbe in questo caso più corretto parlare di cyberterrorismo visto il coinvolgimento di attori non statali).

In tale conteso, se i concetti di crimine informatico e guerra cibernetica trovano il loro paradigma giuridico di riferimento rispettivamente nel diritto penale e nel diritto internazionale dei conflitti armati, l'attività di prevenzione e risposta ai cyberattacchi può ormai ritenersi una vera e propria funzione pubblica autonoma dai caratteri assolutamente inediti. Difatti, non solo nell'ultimo quinquennio il legislatore ha implementato sul piano della cybersecurity strutture organizzative già esistenti dotandole di mezzi quanto più possibili idonei a fronteggiare le nuove sfide, ma – anche in funzione degli obblighi assunti a livello comunitario – ha istituito diverse strutture *ad hoc* (tra cui una nuova agenzia nazionale istituita nel 2020). Questo percorso ha in poco tempo permesso la costruzione di una complessa architettura che, oltre ad affidare ad operatori privati e cittadini un ruolo determinante nella realizzazione degli obiettivi prefissati, si caratterizza per lo stretto collegamento funzionale con l'infrastruttura comune di difesa disegnata dall'Unione Europea.

3. La disciplina dell'Unione Europea

In premessa, va sottolineato come l'Unione Europea non sia stata tra le prime istituzioni ad acquisire una piena consapevolezza circa la necessità di adottare in tempi rapidi dei modelli regolatori capaci di affrontare al meglio le future sfide di sicurezza cibernetica. Tuttavia, sebbene in netto ritardo rispetto ad altri *competitors* internazionali (su tutti gli Stati Uniti)[3], negli ultimi

3. Gli Stati Uniti hanno inserito la *cybersecurity* tra le priorità del governo federale già nel

anni l'UE è riuscita a creare un sistema di sicurezza cibernetica all'avanguardia attraverso diversi interventi ben calibrati[4].

Il processo che ha portato alla creazione dell'attuale architettura di difesa europea è stato però tutt'altro che lineare. Prima ancora di progettare le misure necessarie per fronteggiare il sempre più preoccupante fenomeno degli attacchi informatici, il legislatore europeo è stato chiamato a perimetrare il concetto di "cybersecurity" in modo da considerare le diverse esigenze (e soprattutto le risorse disponibili) degli Stati membri. Non essendo certamente questa la sede per avventurarsi nella impervia strada della ricerca della più appropriata definizione di cybersecurity[5], bisogna in ogni caso rappresentare come ancora oggi questo concetto risulti declinato in maniera diversa non solo a seconda dell'area di regolazione interessata, ma anche sulla base dei diversi obiettivi perseguiti dagli Stati membri. Per meglio comprendere la questione basta evidenziare come nelle strategie dei diversi paesi UE si riscontri ad oggi la coesistenza di almeno diciotto definizioni diverse di "cybersecurity" [L. Jasmontaite, 2020, 105-106].

Nel contesto fin qui delineato, le apparentemente irrisolvibili difficoltà sul piano terminologico non hanno potuto che riversarsi nell'ambito regolatorio: l'architettura europea di cybersicurezza per lungo tempo non è stata altro che la somma dei diversi interventi settoriali, spesso eterogenei, dando così vita a un quadro giuridico fortemente frammentato. Ne risulta ancora oggi un sistema oltremodo complesso, che per un efficace funzionamento richiede un'implementazione tanto su un piano orizzontale (ogni settore oggetto di regolazione deve combinarsi con gli altri), quanto su quello verticale (in funzione dell'indispensabile ruolo affidato agli Stati membri per il funzionamento dell'architettura) [R.A. Wessel, 2015, 405].

Il primo intervento europeo in materia coincide con la pubblicazione della strategia dell'Unione europea per la cybersicurezza del 2013 con cui sono state delineate tre aree iniziali di intervento: a) miglioramento dei sistemi di sicurezza dei sistemi ICT utilizzati dagli erogatori di servizi essenziali e infrastrutture strategiche; b) miglioramento dei sistemi sicurezza delle comu-

1997 [D.E. Bambauer (2011) 585-591], dimostrando una chiara consapevolezza dell'importanza che avrebbe assunto il tema nel determinare i futuri equilibri tra Stati. A testimonianza della complessità della materia trattata può evidenziarsi come, sebbene gli Stati Uniti figurino nel più recente GCI come il paese più virtuoso in materia di sicurezza cibernetica con un punteggio di 100/100, in letteratura non manca chi descrive l'infrastruttura di difesa informatica americana «a mess if not an outright disaster» [D.E. Bambauer (2021) 172].

4. A sostegno di quanto detto è possibile segnalare che, tra i primi venti Paesi inseriti nella più recente classifica del *Global Cybersecurity Index* (GCI), ben undici Stati sono membri dell'UE.

5. Sul punto si rimanda a una delle definizioni maggiormente accreditate in letteratura, secondo cui «*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign* de jure *from* de facto *property rights*» [D. Craigen *et. al.* (2014) 13-21].

nicazioni, con particolare riferimento alla privacy e alla protezione dei dati personale; c) lotta al cybercrimine. L'intento perseguito dalla prima strategia «di fare dell'ambiente online dell'Unione l'ambiente in linea più sicuro al mondo» dimostra grande ambizione e sfida apertamente, forse in modo troppo ottimista, quell'assunto secondo cui nel cyberspazio non possa esistere un ambiente sicuro al 100%.

Ciò nondimeno, la sempre più crescente evoluzione della capacità offensiva dei mezzi di attacco informatico mostrò ben presto i limiti della strategia di difesa europea. Gli ingenti danni causati dagli attacchi *ransomware* noti come *WannaCry* e *Petya* del 2017 hanno permesso l'avvio di un processo di profondo ripensamento delle politiche in materia di cybersecurity volto a riconoscere un sempre più crescente legame tra la sicurezza cibernetica e benessere di cittadini e imprese operanti nel territorio dell'Unione. Una delle iniziative più virtuose che ha portato all'avvio di tale percorso di rafforzamento va ricondotta alla pubblicazione della seconda strategia europea per la cybersicurezza del 13 settembre 2017, con cui si è disegnato un modello comunitario incentrato sul tre concetti chiave: resilienza, deterrenza e difesa. Tra le principali novità contenute all'interno della menzionata strategia viene manifestato l'intento di riformare l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) istituita nel 2004 in modo da creare un centro di coordinamento di cybersicurezza europeo con importante ruolo consultivo nell'elaborazione e nell'attuazione delle politiche europee. Tale obiettivo, di centrale importanza per il raggiungimento del necessario grado di resilienza agli attacchi informatici, è stato realizzato con il successivo regolamento UE del 2019 noto come *Cybersecurity Act*[6], il quale ha attribuito all'Agenzia un mandato permanente volto a offrire un supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri.

La strategia per la Cybersicurezza dell'UE è stata da ultimo aggiornata nel 2020 sulla base dei nove principi affermati nella *Paris call for trust and security in Cyberspace* del 2018, un'iniziativa che ha coinvolti 81 Paesi (tra cui tutti gli Stati europei e gli Stati Uniti) unitamente alle principali società e organizzazioni internazionali operanti nel settore tecnologico e della sicurezza informatica. La principale novità introdotta dalla più recente strategia riguarda l'istituzione di un'unità congiunta per il ciberspazio (nota come *Joint Cyber Unit* o *JCU*) come piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cybersicurezza all'interno dell'UE, ciò «con particolare

6. Il Regolamento (UE) 2019/881 del 17 aprile 2019 (noto come *Cybersecurity Act*) ha inteso rafforzare il sistema europeo di difesa agendo su due versanti. Da un lato, come già ricordato, ha rafforzato i poteri istituzionali dell'Agenzia europea per la cybersicurezza; dall'altro ha permesso l'istituzione di un sistema europeo di certificazione della cybersicurezza attraverso l'individuazione di parametri minimi di sicurezza informatica per prodotti, servizi e processi ICT (favorendo anche l'acquisto e lo scambio di dispositivi e sistemi tecnologici in Europa).

attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera».

I menzionati documenti strategici si dimostrano di notevole importanza per il funzionamento operativo del sistema di difesa comune, ma il cuore pulsante del quadro normativo europeo in materia di sicurezza cibernetica va ricercato – oltre che nel già menzionato *Cybersecurity Act* – nelle fonti di armonizzazione. Nello specifico, per meglio comprendere il funzionamento dell'infrastruttura europea è possibile far riferimento agli obiettivi fissati dapprima dalla Direttiva 2016/1158[7] (nota come "Direttiva NIS") e successivamente dalla recentissima Direttiva 2022/2555 (nota come "Direttiva NIS II").

La Direttiva NIS rappresenta la prima disciplina UE introdotta con l'intento di innalzare la protezione della rete e dei sistemi informativi degli Stati membri dell'Unione attraverso un approccio orizzontale. Il principale merito della richiamata direttiva è stato quello di elaborare dei criteri di identificazione comuni degli operatori di servizi essenziali europeo, affidando agli Stati membri l'onere di trasmettere e aggiornare con cadenza biennale l'elenco dei soggetti pubblici e privati ricavato sulla base dei parametri indicati dall'art. 5 della Direttiva[8] e dei settori indicati dall'Allegato II[9]. Pertanto, ai fini della NIS non sono ricompresi tutti gli operatori di servizi essenziali intesi in senso ampio, ma soltanto quelli considerati come tali dagli Paesi membri all'esito del procedimento di categorizzazione fissato a monte dal legislatore euro-unionale (prevenendo in ogni caso la possibilità per gli Stati di includere nei settori oggetto di tutela anche soggetti non contemplati dai parametri europei).

Pur dovendo riconoscere alla Direttiva NIS il merito di aver introdotto un nucleo minimo e indispensabile di tutela volto a garantire la continuità dei servizi essenziali a livello europeo, non può ignorarsi come la sempre più crescente evoluzione delle minacce cibernetiche abbia dimostrato alcuni limiti strutturali della disciplina europea. Osservando i parametri per l'individuazione dei soggetti che il legislatore comunitario ha inteso tutelare non può infatti ignorarsi l'assenza di alcuni settori di importanza vitale per la vita e la sicurezza dei cittadini europei: basti pensare che non sono (*rectius*,

7. Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio recante misure per un livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione.

8. Ai sensi dell'art. 5, par. 2, della Direttiva NIS gli stati membri possono identificare gli operatori essenziali sulla base dei seguenti parametri: «a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociale e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; b) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio».

9. L'Allegato II della Direttiva NIS ha individuato sette macrosettori in cui raggruppare gli operatori di servizi essenziali, più precisamente: energia, trasporti, servizi bancari, servizi finanziari e di mercato, sanità, catena di produzione e di distribuzione dell'acqua e infrastrutture digitali.

erano) presenti tra i settori indicati nell'Allegato II operatori pubblici e privati operanti nel settore della Pubblica Amministrazione, dell'ambiente, del settore alimentare, chimico e nucleare Direttiva. Se è vero che alcuni Stati virtuosi – tra cui come vedremo figura anche l'Italia – hanno provveduto in fase di attuazione della NIS ad ampliare il novero dei soggetti coinvolti, il sistema introdotto nel 2016 non sembra in grado di raggiungere gli obiettivi di armonizzazione prefissati per la costruzione di una "fortezza cibernetica europea".

Il legislatore europeo si è dimostrato consapevole dei limiti fin qui descritti e durante la fase di attuazione della NIS ha lavorato sull'elaborazione di un'ulteriore direttiva (nota come Direttiva NIS II) per colmare le precedenti lacune. Il nuovo testo, approvato dal Parlamento Europeo e dal Consiglio lo scorso novembre ed entrato in vigore il 17 gennaio 2023[10], mantiene intatto lo stesso spirito della precedente direttiva ma innalza significativamente il livello di sicurezza delle reti europee partendo proprio dall'assegnazione di nuovi criteri di individuazione dei soggetti da tutelare. La Direttiva NIS II ha inteso affrontare le criticità descritte muovendosi in una duplice direzione: da un lato ha esteso gli obblighi di sicurezza a una ricca platea di operatori di servizi essenziali pubblici e privati dapprima non ricompresi nel perimetro applicativo della NIS (*ex multis*, i soggetti pubblici e privati operanti nei settori della produzione di dispositivi medici, dell'ingegneria aerospaziale della gestione dei rifiuti, della produzione e distribuzione di alimenti, dei servizi postali, ma anche tutta la Pubblica Amministrazione); dall'altro ha sottratto ai singoli Stati il compito di identificare gli operatori di servizi essenziali soggetti alla Direttiva attraverso la formulazione di criteri auto-applicativi maggiormente precisi e uniformi. In conclusione, la Direttiva NIS II sembra destinata a cambiare in modo profondo la realtà europea, ma – come verrà chiarito *infra* – l'Italia potrà procedere con l'attuazione della nuova Direttiva (il cui termine coincide con il 18 ottobre 2024) consapevole di aver già costruito un'infrastruttura di sicurezza cibernetica già in larga parte conforme agli *standard* di tutela richiesti dal legislatore comunitario.

4. L'approccio italiano al tema della sicurezza cibernetica

Nel quadriennio 2018/2021 sono stati registrati a livello mondiale 7144 attacchi informatici, di cui circa 900 hanno colpito l'Europa e ben 185 hanno avuto come target Pubbliche Amministrazioni e società italiane. I dati del rapporto Clusit 2021 fotografano come in Italia il tema della cybersecurity sia una minaccia reale e in continua crescita: nel solo 2021 l'Italia ha inter-

10. Il testo è reperibile su *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823*.