Riccardo Ursi

Introduzione. La sicurezza cibernetica come funzione pubblica[*]

I cambiamenti imposti dal rapido sviluppo tecnologico dell'ultimo trentennio richiedono oggi di affrontare il tema della sicurezza cibernetica partendo da una nuova prospettiva in chiave strettamente giuspubblicistica, richiedendo di inquadrare il fenomeno anche (e soprattutto) come una funzione pubblica. L'emergere di questa inedita prospettiva ha messo il giurista dinanzi a questioni nuove e particolarmente complesse, in quanto lo studio del fenomeno richiede una riflessione sulla nozione stessa di cybersicurezza (nonché, a monte, della stessa definizione di sicurezza). Il concetto di *cybersecurity* oggi non può che essere inteso in modo da coinvolgere non solo le mere attività di gestione e prevenzione dei rischi interni al cyberspazio, ma sembra coinvolgere indistintamente la dimensione virtuale così come quella reale. Del resto, se da un lato l'evoluzione delle reti informatiche globali hanno premesso un progresso notevole sul piano economico e sociale di tutte le principali democrazie occidentali, dall'altra la stessa ha esposto individui, imprese e istituzioni a rischi significativi. In questo contesto, il giurista è chiamato a traslare categorie giuridiche tradizionali all'interno di un di uno spazio non legato a confini geografici, un 'non luogo' in cui gli Stati-nazione – nonostante i più strenui tentativi in senso contrario – si sono trovati privati della possibilità di esercitare la loro sovranità. Il compito di cura della sicurezza cibernetica affidato alle istituzioni pubbliche nazionali ed europei richiede così agli studiosi del nuovo millennio di affrontare con lenti nuove alcuni temi di centrale rilievo dal punto di vista teorico e pratico.

Questo numero monografico si propone l'ambizioso obiettivo di esplorare alcune tra le questioni trasversali più rilevanti nell'attuale dibattito che sta interessando la materia. L'interrogativo probabilmente più rilevante, rivolto a comprendere come possa lo Stato garantire la sicurezza dei suoi cittadini rispetto ai pericoli provenienti dal ciberspazio in assenza di un controllo diretto sul fenomeno da cui proviene il rischio, sembra allo stato dell'arte destinato a rimanere privo di una risposta soddisfacente. Se i tentativi di risposta a tale interrogativo appaiono oggi tutt'altro che soddisfacenti, in questa prima fase di studi della materia risultano già ben definiti quelli che sono i principali interrogativi che i giuristi – accompagnati da studiosi e operatori di altre materie – sono chiamati a svolgere. Tra questi, senza alcuna pretesa di esaustività, risulta inevitabile interrogarsi sulle seguenti questioni

* Scritto non sottoposto alla procedura di referaggio doppio cieco.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760156

messe a fuoco nelle successive pagine: (*i*) il concetto di sicurezza cibernetica può essere riferito allo stesso concetto di 'sicurezza' tradizionalmente affrontato dalla scienza giuridica italiana (ammesso che ne esista uno univoco)?; (*ii*) qual è il rapporto tra ordinamento nazionale ed europeo nel nuovo ordinamento multilivello di *cybersecurity*?; (*iii*) come prima ricaduta, qual è il rapporto tra sicurezza cibernetica e nazionale?; (*iv*) come seconda ricaduta, quale spazio può essere affidato ai provati attraverso forme di partenariato in una materia legata a doppio filo con informazioni classificate?

Alla luce di tali quesiti, risulta necessario ridefinire il ruolo dello Stato e delle istituzioni pubbliche, sia a livello nazionale che sovranazionale, in relazione alla tutela della cybersicurezza. La crescente interdipendenza tra sistemi informatici e infrastrutture critiche ha reso evidente che la protezione dello spazio cibernetico non può essere più ricondotta al tradizionale binomio tra sicurezza interna e sicurezza esterna, ma deve essere affrontata attraverso nuove categorie, prima tra tutte quelle di 'ordine pubblico globale'. Lo Stato, in questo senso, non assume più soltanto il ruolo di garante della sicurezza fisica, ma è chiamato a essere il custode della sicurezza digitale, con la responsabilità di proteggere cittadini, imprese e infrastrutture dall'invisibile minaccia cibernetica.

Tuttavia, questo compito è complicato dal fatto che le tecnologie digitali si sviluppano in un ambiente globale e decentralizzato, rendendo difficile per gli Stati esercitare il loro tradizionale monopolio del potere coercitivo. Di fronte alla complessità e alla globalità delle minacce cibernetiche, che spaziano dagli attacchi informatici alle violazioni della privacy, si richiede una nuova architettura di governance multilivello. Tale architettura deve necessariamente includere non solo le autorità pubbliche, ma anche gli attori privati, le organizzazioni internazionali e la società civile.

In questo contesto, la collaborazione tra pubblico e privato diventa essenziale. Le imprese, infatti, detengono molte delle risorse tecnologiche e delle competenze necessarie per affrontare le sfide della cybersicurezza, mentre lo Stato possiede la legittimità e la capacità di coordinare e regolamentare le attività di difesa del cyberspazio. Il modello emergente sembra quindi orientarsi verso un sistema di (cyber-)resilienza in cui Stato e attori privati cooperano attivamente per prevenire, mitigare e rispondere agli attacchi cibernetici.

Inoltre, la dimensione europea della cybersicurezza ha acquisito sempre maggiore rilevanza, con l'Unione Europea che ha adottato un ruolo di primo piano nella definizione di politiche e regolamentazioni comuni. Con l'adozione del più recente pacchetto legislativo in materia, e con particolare riferimento alla direttiva (UE) 2022/2555 (nota come direttiva NIS2) l'Unione ha delineato un quadro giuridico che mira a innalzare notevolmente il livello minimo di sicurezza delle reti e delle informazioni in tutto il territorio europeo. La sfida non è più quella di una mera armonizzazione tra le differenti legislazioni nazionali, ma quella di ottenere dei benefici comuni attraverso l'istituzione di infrastrutture comuni e di forme di cooperazioni tra Stati membri. La sfida è sicuramente ambiziosa, in quanto è rivolta a trovare un delicato punto di equilibrio tra l'infrastruttura verticale, riferita ai rapporti tra UE e singoli Stati, e orizzontale, riferita al rapporto tra pubblico e

privato, con l'obiettivo di individuare una formula di azione il quanto più possibile efficace. Tuttavia, poiché i soggetti chiamati a sostenere i costi dell'intera infrastruttura europea risultano oggi in larga parte coincidenti con gli stessi onerati ad adempiere ai diversi obblighi previsti dall'attuale architettura livello di cibersicurezza, l'attuale sistema non può che sollevare diverse perplessità circa il sostegno che il settore pubblico dovrà fornire per raggiungere gli obiettivi minimi prefissati.

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)[1].

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[2]. 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[3]. 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.

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

1 Pizzolato 2017: 39.
2 Mannoni e Stazi 2021: 24.
3 Betzu 2021: 24.

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.

Con riferimento alla sicurezza cibernetica in senso ampio, correlata ad una idea di ordine pubblico digitale, 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.

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»[4]. 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 conoscenza, 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»[5].

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. 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[6], 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[7].

4 Cfr. De Felice 2012: 72.
5 De Vergottini 2019: 76.
6 Craigen, Daikun-Thibault, Purse 2014: 17.
7 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[8]. 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.

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.

I contributi inserito all'interno di questo fascicolo, seguendo lo spesso spirito delle relative relazioni tenutesi dagli Autori al Convegno ospitato dall'Università del Piemonte Orientale di Novara, sono stati raccolti e ordinati seguendo l'idea – che si spera che possa rimanere ferma nei successivi studi – dell'eclettismo come indispensabile obbligo metodologico. Senza un reciproco interesse tra la componente tecnica e quella propriamente giuridica della materia, la sicurezza cibernetica è destinata a rimanere un corpo in tutto o in parte estraneo nel proprio campo di studio.

Bibliografia

Betzu M. 2021, *I baroni del digitale*, Napoli: Editoriale Scientifica.

Craigen D., Daikun-Thibault N., Purse R. 2014, "Defining Cybersecurity", in *Technology Innovation Management Review* (10) 17.

8 Tsagourias 2015: 21.

De Felice N. 2012, "Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali", in U. Gori, L.S. Germani (a cura di), *Information warfare 2011. La sfida della cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano: Franco Angeli, 72.

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

Lauro A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *Gruppo di Pisa*, (3) 530.

Mannoni S., Stazi G. 2021, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli: Editoriale Scientifica.

Pizzolato F. 2017, "Il costituzionalismo alla prova della tecnica: libertà, uguaglianza e sicurezza", in F. Pizzolato, P. Costa (a cura di), *Sicurezza e tecnologia*, Milano: Giuffré.

Tsagourias N. 2015, "The legal status of cyberspace", in Tsagourias N., Buchan R. (eds.), "*Research handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 21.