Alberto Oddenino

Pervasività, centralità geopolitica e molteplicità delle istanze di tutela della cybersicurezza: elementi introduttivi[*]

*Abstract***:** Comprendere la cybersicurezza nella moderna società tecnologica e digitalizzata e le istanze di tutela che essa solleva richiede alcune chiavi di lettura preliminari. Il contributo si propone di offrirne tre: esso muove dalla forza espansiva e dalla pervasività della nozione, per evidenziare poi la centralità geopolitica che hanno assunto le sue istanze di tutela, e concludendo con la molteplicità delle dimensioni rilevanti nella considerazione del fenomeno.

Keywords: cybersecurity, globalization, international law, sovereignty, national security

1. La pervasività e la forza espansiva della cybersicurezza nella società contemporanea

Il tema della tutela della cybersicurezza ha assunto una portata sempre più pervasiva nella società contemporanea, in cui la presenza tecnologica è resa essa stessa sempre più capillare e in certo senso ubiqua.

Il progresso tecnologico accompagna da sempre l'evoluzione della società, modificandone radicalmente i valori oltre che abitudini e stili di vita. L'avvento dell'era digitale – caratterizzata da una sempre più vasta interconnessione e da una massiccia elaborazione algoritmica di dati – ha segnato una netta accelerazione di tale processo trasformativo. Ogni attività possiede oggi una propria dimensione digitale, nella quale la tecnologia è divenuta sostrato e strumento spesso imprescindibile. Al contempo, le implicazioni del progresso tecnologico non si limitano alla sfera sociale, poiché lo sviluppo di nuove tecnologie assume un'innegabile rilevanza geopolitica e strategica. Si tratta di un aspetto non nuovo nel panorama internazionale, se è vero che la tecnologia costituisce da sempre

* Contributo non sottoposto alla procedura di referaggio doppio cieco.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760144

terreno di competizione e ambito di elezione per il perseguimento degli interessi strategici, anche in una logica di fusione o almeno di parziale allineamento di interesse fra pubblico e privato[1].

Ciò è tanto più vero nella misura in cui dimensione di collegamento tecnologico è sostrato irrinunciabile per il supporto e lo sviluppo dell'intelligenza artificiale, che nelle sue frontiere più attuali appare portatrice di uno slancio trasformativo senza precedenti per le nostre società, il nostro modello economico e in ultima analisi per lo stesso futuro dell'umanità[2].

Su un piano ancora preliminare si deve ricordare come Internet stessa, la Rete delle reti, risulti "territorio" fortemente conteso: ben lontano da una concezione originaria come spazio di libertà tendenzialmente assoluta, che trovava nell'autoregolamentazione tecnica il solo modello normativo accettabile, la Rete, in ragione delle sue grandi potenzialità strategiche, sociali e commerciali, è oggetto di ambizioni di controllo tecnico ancor prima che di regolazione strutturale e contenutistica[3].

A tali riflessioni ci si riferisce quando si menziona una specifica dimensione geopolitica relativa alla cybersicurezza, ricordando che quella che si gioca sulla Rete non è solo una partita per affermare una prevalenza economica, ma una vera contesa di potere, nella sua accezione più ampia e totalizzante, che coinvolge in modo frontale il tema della sovranità[4].

Peraltro il tema supera di molto la sola dimensione interstatuale o quella riconducibile ad organizzazioni internazionali o organismi sovranazionali, per raggiungere il cuore della *data economy* contemporanea, ponendosi in collegamento con il settore privato, in cui accanto alla dominanza ormai incontrovertibile dei cd. *Big Tech*, fiorisce una ampia congerie di soggetti privati portatori di rilevanti interessi economici legati al commercio e alla circolazione dei dati.

Non deve pertanto sorprendere se la nozione di cybersicurezza, proprio in ragione di questa sua capacità espansiva, abbia assunto crescente centralità nelle valutazioni del potere, tanto pubblico quanto privato.

In piena coerenza con l'evoluzione della società verso la cd. *Risiko Gesellschaft* teorizzata da Ulrich Beck, oggi la valutazione e la gestione dei rischi cibernetici occupa l'agenda tecnologica e regolatoria della più parte degli stati contemporanei.

In prospettiva regolatoria ciò ha condotto a rafforzare un approccio cd. *risk based*, che ha trovato nell'ordinamento della UE un terreno fertile di sviluppo, e che assume oggi una portata sempre più ampia e in certo senso esorbitante, perva-

1 Si tratta di un tema complesso e potenzialmente vastissimo, su cui può bastare in questa sede richiamare la brillante teorizzazione di un nuovo contratto sociale contenuta in Shadmy 2019.

2 In tema si veda da ultimo, fra la ormai vasta letteratura, Aresu 2024.

3 In tema si veda, fra l'ampia letteratura, Muller 2010. Sia consentito rinviare anche a Oddenino 2012.

4 È evidente infatti come la contesa per il controllo della struttura sia propedeutica al controllo dei contenuti. In tema si veda De Nardis 2014, ove si evidenzia come la possibilità di realizzare una penetrante sorveglianza e una raccolta sistematica di informazioni strategiche, anche e soprattutto in dimensione internazionale, sia espressione qualificata di un tale disegno.

dendo di sé, come è noto, non solo l'ambito della *data protection* ma anche il plesso di regolazione oggi dedicato all'intelligenza artificiale.

In definitiva, la cybersicurezza esprime oggi essa stessa una netta attitudine alla esorbitanza, e travalica di molto la tradizionale sua ricostruzione delle origini, che recava un collegamento biunivoco con gli ambiti della Cyber-guerra e del Cyber-terrorismo, per esplicare una capacità di penetrazione di molti altri ambiti collegati con l'ampio concetto strategico di sicurezza nazionale[5].

2. Alla ricerca di una definizione e di una tassonomia per la cybersicurezza

Alla luce di quanto precede si comprende come già la semplice perimetrazione del campo di indagine, e con essa l'individuazione di una nozione univoca di cybersicurezza, non sia agevole. Essa può oggi essere vista come una declinazione della più ampia nozione di sicurezza nazionale, della quale in certo senso rappresenta anche una forma di evoluzione, dotata di notevole potenziale pervasivo.

Per certo, in questo senso, il concetto di cybersicurezza è influenzato dalle esigenze politiche, sociali e culturali di ciascun Paese e, per altro verso, richiede l'adattamento della nozione di sicurezza nazionale ad un sempre mutevole settore digitale. Si ritiene che sempre per questa ragione non è presente, a livello multilaterale, una concettualizzazione univoca della cybersicurezza.

Una certa autorevolezza ha assunto la nozione di cybersicurezza resa dal *U.S. National Institute of Standards and Technology* (NIST), in termini di: "prevenzione del danneggiamento, dell'uso non autorizzato, dello sfruttamento e, se necessario, ripristino dei sistemi elettronici di informazione e comunicazione delle informazioni in essi contenute, al fine di rafforzare la riservatezza, l'integrità e la disponibilità di tali sistemi". Si tratta di una definizione più ampiamente condivisibile in ragione della sua scelta di non distinguere il settore pubblico dal settore privato, né con riferimento agli attori di un possibile attacco, né con riferimento ai potenziali obiettivi. Essa, focalizzandosi esclusivamente sugli eventuali danni all'integrità delle informazioni e dei sistemi informativi, non lascia volutamente emergere altri e più ampi obiettivi, quali ad esempio lo sviluppo delle imprese nel settore digitale, il libero accesso degli individui a Internet, la regolamentazione dei contenuti caricati online, i controlli sul traffico dati anche attraverso *Big Data* e intelligenza artificiale, tutte dimensioni riconducibili alla cybersicurezza, che ne rivelano la multidimensionalità, aspetto su cui si tornerà a breve.

Non deve stupire pertanto se a questa prima definizione di cybersicurezza se ne è affiancata un'altra, più ampia, sviluppata dall'*International Telecommunication Union* (ITU), secondo cui la cybersicurezza è "la raccolta di strumenti, politiche, concetti di sicurezza, garanzie di sicurezza, linee guida, approcci di gestione del rischio, azioni, formazione, migliori pratiche, garanzie e tecnologie che possono essere utilizzate per proteggere l'ambiente informatico, l'organiz-

5 In tema cfr. la ricostruzione tradizionale espressa in Bosco 2013.

zazione e le risorse degli utenti", nella quale rientrano anche "i beni dell'organizzazione e degli utenti" che "comprendono i dispositivi informatici connessi, il personale, l'infrastruttura, le applicazioni, i servizi, i sistemi di telecomunicazione e la totalità delle informazioni trasmesse e/o archiviate nell'ambiente informatico" e, ancora, che "la sicurezza informatica si impegna a garantire il raggiungimento e il mantenimento delle proprietà di sicurezza dell'organizzazione e delle risorse degli utenti contro i rischi per la sicurezza rilevanti nell'ambiente informatico" [6].

Una definizione davvero ampia da cui si deduce come ITU, nella sua qualità di organizzazione internazionale di vertice per il settore delle telecomunicazioni, riconosca l'estrema ampiezza dell'ambito di cybersicurezza nonché la varietà degli approcci e dei possibili rischi per la sicurezza nazionale: di qui la connotazione del tema della tutela della cybersicurezza non solo come semplice insieme di regole, ma come vera e propria strategia *risk based* che pervade l'adozione di atti di *soft* o *hard law* in materia digitale[7].

Alla luce delle incertezze definitorie, può essere meritevole uno sforzo di minima tassonomia. In questa prospettiva le minacce *cyber* possono innanzitutto distinguersi in attive o passive, accidentali o intenzionali.

Le prime nascono da comportamenti che implicano un'alterazione del funzionamento di un bene o di un servizio originariamente previsto, mentre nelle seconde il comportamento non determina alcuna alterazione del funzionamento, ma tende a sfruttare un malfunzionamento o una lacuna nel sistema al fine di operare in maniera illecita.

Accidentali sono invece le minacce determinate da malfunzionamenti o bug dei software o della rete che possono esporre i dati o altri elementi sensibili a rischi, mentre intenzionali sono le minacce rappresentate da comportamenti studiati appositamente per perseguire uno scopo illecito attraverso il cyberspazio.

Quanto ai settori materiali possono essere individuati almeno cinque aree chiave.

Una prima area-chiave per la cybersicurezza, direttamente legata al concetto di sicurezza nazionale inteso in senso tradizionale, è quella della difesa nazionale, che comprende tutto ciò che è legato agli ambiti militare e di intelligence, nella quale

6 Cfr. International Telecommunication Union, "*Overview of Cybersecurity*", Recommendation ITU-T X.1205, aprile 2008, p. 2 par. 3.2.5. Giova sottolineare come le stesse tipologie di attacchi, nel corso degli anni, si siano ampliate parallelamente allo sviluppo tecnologico, ricomprendendo nuovi settori quali i dati sensibili degli utenti o le piattaforme digitali. Resta ferma e fondamentale la distinzione, elaborata dall'ITU stesso, tra attacchi digitali – ad esempio nel caso di *malware* – e attacchi fisici – ad esempio nel caso di danneggiamento di infrastrutture digitali che causi disservizi in un territorio.

7 L'adozione da parte di ITU del *risk based approach* ha condotto ad individuare tre categorie di possibili rischi per la sicurezza nazionale, derivanti da beni e da servizi digitali, e in particolare: i "*service interruption attacks*", che disabilitano, in maniera temporanea o permanente, l'accesso a piattaforme di servizi; gli "*assets compromise*", che danneggiano le infrastrutture e possono cagionare danni su larga scala; i "*component hijacking*", che mirano a prendere il controllo di altri dispositivi da utilizzare per lanciare ulteriori attacchi nel cyberspazio.

sono incluse le infrastrutture utili alla difesa stessa, ai network e ai software collegati e ai loro contenuti quali, ad esempio, le informazioni classificate[8].

La seconda area-chiave nella quale sono possibili cyber attacchi su larga scala, idonei a causare blocchi di funzionamento dalla durata variabile, con conseguenze gravi per i servizi essenziali, è quella legata alle infrastrutture critiche, cioè a quelle infrastrutture utili al soddisfacimento dei bisogni primari della popolazione, quali la fornitura di energia elettrica o le reti 5G, necessarie per la gestione della salute, dell'energia e dei trasporti. L'attacco alle infrastrutture critiche può avvenire in maniera diretta, tramite il tentativo di penetrare al loro interno violando i protocolli di sicurezza, oppure attraverso l'istallazione di *backdoors*, che possono avere natura *hardware* (chip occultati) o *software* (programmi non previsti o creazione di meccanismi che evitano i protocolli di identificazione e di accesso) che rendono possibile l'accesso per soggetti non autorizzati, senza lasciare alcuna traccia di forzatura del sistema[9].

Terza area è quella che attiene allo spionaggio economico che determina l'appropriazione di segreti industriali o la violazione della proprietà intellettuale soprattutto in ambito software. Anche in questo caso, l'accesso fraudolento può avvenire tramite attacchi diretti o, nell'ambito delle catene di fornitura, attraverso l'installazione di *backdoors* nel corso di produzione della componentistica hardware o software utilizzata dall'impresa cui l'attacco è destinato[10].

La quarta area-chiave attiene al settore della *digital information*. Qui gli attacchi informatici possono essere diretti all'acquisizione di dati, come accade quando uno Stato utilizza big data per acquisire informazioni sulle abitudini o preferenze degli utenti di un determinato Paese, oppure diretti alla manipolazione o falsificazione delle informazioni per creare confusione e sfiducia nella popolazione. In questa area si collocano, in particolar modo, le minacce ibride, intese come un tipo di attacco volto a destabilizzare un Paese attraverso meccanismi non convenzionali, quali, ad esempio, la disinformazione o l'acquisizione illecita di dati volti a ottenere informazioni di sicurezza nazionale, utili a facilitare un eventuale attacco di natura convenzionale, quale ad esempio un attacco armato[11].

8 Sui rischi per la sicurezza nazionale derivanti dai tentativi degli hacker di penetrare nei sistemi di difesa per acquisire informazioni relative anche allo sviluppo della componentistica software e hardware nelle apparecchiature militari cfr. si veda ad esempio, *Joint Statement for the Record to the Senate Armed Services Committee – Foreign Cyber Threats to the United States*, 5 gennaio 2017, disponibile a https://www.armedservices.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

9 Una definizione precisa di infrastrutture critiche è data dall'US Patriot Act, secondo cui "le infrastrutture critiche sono quei sistemi o beni, fisici o virtuali, così vitali per gli Stati Uniti che il loro malfunzionamento o distruzione avrebbe un impatto debilitante sulla sicurezza, sulla sicurezza economica nazionale, sulla salute pubblica nazionale o su qualsiasi combinazione di tali questioni" (USA PATRIOT ACT, 2001, 42 U.S.C. §5195c(e)).

10 In tema cfr. National Counterintelligence and Security Center: "Foreign Economic Espionage in Cyberspace", 26 luglio 2018, p. 12. Reperibile in https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

11 Per un'analisi approfondita dell'utilizzo della disinformazione come minaccia ibrida e strumento volto alla destabilizzazione di un Paese si vedano Singer, Brooking 2018.

La quinta e ultima area di operatività dei rischi per la sicurezza informatica riguarda sia l'accesso da parte degli utenti ad internet, quale espressione del diritto alla libertà di informazione ed espressione, sia l'accesso reciproco tra Paesi a informazioni, alla luce del principio di leale cooperazione nei rapporti internazionali. In questi casi, si possono verificare cyber attacchi del tipo *Distributed Denial of Services* (DDOS), che impediscono agli utenti di raggiungere determinati siti o, in generale, di accedere ad internet, causando disservizi o, in alcune occasioni, disinformazione. Si pensi al caso in cui, a ridosso di elezioni politiche, vengano artatamente e illegittimamente oscurati siti di informazione. In alcuni casi può succedere che l'accesso avvenga, in maniera diretta o per il tramite di intermediari privati, da parte di governi stranieri per acquisire informazioni o creare disservizi. Non è infrequente, allora, che vengano poste restrizioni sia in maniera diretta, impedendo l'accesso, oltre i confini nazionali, a siti contenenti informazioni ritenute sensibili, sia in maniera indiretta, impedendo a soggetti stranieri di fare investimenti che, per essere realizzati, richiedono l'accesso a informazioni sensibili[12].

3. La centralità della nozione di sicurezza nazionale, e la tendenza a una determinazione unilaterale delle misure di tutela della cybersicurezza

A fronte di un panorama tanto ricco e complesso, resta evidente che la dimensione del fenomeno, per certo internazionale in ragione della portata globale del fenomeno, vede le risposte tecniche e regolatorie affidate invece a iniziative e sensibilità prevalentemente nazionali.

In questo senso si staglia come assolutamente centrale il rapporto con la nozione di sicurezza nazionale, quale ambito privilegiato di esercizio della sovranità e quale clausola di salvezza anche rispetto alla eventuale assunzione di obblighi internazionali da parte degli stati[13]. Ciò apre ad una interpretazione fortemente unilaterale della nozione di cybersicurezza e a un suo chiaro orientamento in senso geopoliticamente strategico.

Il piano del diritto internazionale resta esile con svariate iniziative di *soft law* [14], accanto a rare emersioni di strumenti giuridicamente vincolanti che sono però del tutto settoriali, come in particolare la Convenzione di Budapest del 2001 sul *cybercrime* elaborata in senso al Consiglio d'Europa[15].

12 Così Meltzer 2020

13 Cfr. GEE, *Report Group of Governmental Experts on Developments in Field of Information and Telecommunications in the Context of International Security*, 14 luglio 2021, UN Doc. A/76/135, par. 7, 14.

14 Nel primo senso si veda su tutto la Risoluzione dell'Assemblea generale delle Nazioni Unite, Creazione di una cultura globale della sicurezza informatica e della protezione delle infrastrutture informatiche critiche, 23 dicembre 2003, n. 58/199, UN Doc. A/RES/58/199.

15 Su questo tema si veda ex multis Mazza 2004. Le azioni del Consiglio d'Europa nel campo della cybersecurity, che hanno due profili principali: la lotta alla criminalità informatica e la protezione delle persone in materia di trattamento automatizzato dei dati personali. Sotto il primo profilo, l'organizzazione di Strasburgo ha iniziato ad occuparsi di criminalità informatica

Le dinamiche internazionali sono piuttosto paradigmatiche di come il settore della cybersicurezza resti un terreno di aspro confronto fra sovranità nazionali, e si presti a qualche strumentalizzazione unilaterale. Ciò è risultato storicamente con particolare evidenza anche in occasione della disputa relativa alla riforma delle *International Telecommunications Regulations* dell'ITU: essa ha visto, nella Conferenza di Dubai del 2012, lo scontro fra visioni e pretese contrapposte, segnando una profonda lacerazione fra gli Stati solidali con la posizione volta al sostanziale mantenimento dello *status quo*, espressa dagli US, e quelli che, come Cina e Russia in particolare, in una logica geopolitica di contropotere, hanno tentato di affermare una visione alternativa, sulla base di dichiarate esigenze di cybersicurezza. Il che evidenzia una volta di può il portato strategico e geopolitico di una nozione che tende a ricalcarsi su quella dell'interesse nazionale[16].

È chiaro come in un mondo globalizzato, e al fine di favorire le dinamiche dello scambio e del commercio internazionale anche dei beni digitali, sarebbe opportuno porre rimedio a una totale discrezionalità nella identificazione delle misure di cybersicurezza da parte dei singoli stati. La disciplina di queste aree di interesse richiederebbe regole armonizzate tra i diversi Paesi, così da evitare che le valutazioni, invero particolarmente discrezionali in quanto legate a informazioni spesso riservate e quindi non conoscibili dai Paesi terzi o da organi sovranazionali, siano strumentali alla creazione di meccanismi protezionistici e di tutela delle imprese interne con conseguente violazione dei principi di libero scambio e libera concorrenza[17]. Tuttavia la clausola di eccezione costituita dell'interesse nazionale costituisce un facile grimaldello per scardinare ogni sistema armonizzato che potesse prendere corpo a partire dalla condivisione di alcuni standard tecnici. Gli stati restano inclini a valutare l'effettiva sussistenza di un interesse di sicurezza nazionale attraverso un approccio caso per caso. Esso si giustifica perché, per un verso, si verificano minacce ambigue e, quindi, difficilmente qualificabili – si pensi a quelle ibride – e, per altro verso, minacce che coinvolgono interessi esclusivi di un Paese che, se dirette contro un Paese diverso, comporterebbero rischi minori[18].

come questione di diritto penale già negli anni '80, a partire dalla promulgazione di due raccomandazioni, relative alla criminalità informatica e al diritto processuale penale legato alle tecnologie dell'informazione. A metà degli anni Novanta, con il consolidarsi delle nuove tecnologie, che hanno portato anche a un loro uso malevolo, il Comitato dei Ministri ha deciso di istituire il Comitato di esperti sulla criminalità informatica (PC-CY), incaricato di redigere un accordo sulla criminalità informatica. La Convenzione che ne è scaturita, conclusa a Budapest il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004, è supportata da un Comitato specifico (T-CY) volto a garantirne l'attuazione attraverso valutazioni, linee guida e altri mezzi, nonché attraverso i programmi di *capacity building*.

16 Sul punto sia consentito rinviare a Oddenino 2013.

17 In tema si rinvia a Oddenino 2017.

18 La natura ambigua dei cyber attacchi ha indotto talora gli Stati ad agire in via preventiva e non sempre proporzionata, ad esempio impedendo ad altri Paesi di accedere ai propri server o alle proprie infrastrutture di rete, oppure limitando eccessivamente il commercio di prodotti dual use, in quanto potenzialmente utilizzabili per sviluppare tecnologie per i cyber attacchi, di software o di hardware potenzialmente idonei a nascondere *backdoors*.

In merito vi è dunque una forte riemersione di sensibilità nazionali sovrane che non trovano facile allineamento. Ciò non fa che riecheggiare una contrapposizione già emersa fra mondo occidentale a resto della comunità internazionale rispetto al tema della applicazione del diritto internazionale al cyberspazio, che merita una indagine comparatistica che evidenzi le diverse sfumature di sensibilità tecnica e giuridica[19].

In tale già articolato scenario, il crescente ruolo del settore privato costituisce un ulteriore elemento di complessità. La nuova realtà internet-based porta con sé nuovi equilibri fra attori pubblici e privati, in quanto sempre più asset di rilevanza strategica per il Sistema Paese sono oggi oggetto di sviluppo, controllo e immissione nel mercato da parte di attori privati o da parte di sinergie pubblico-private. La potenziale dipendenza da altri attori pubblici o privati relativamente alla fornitura e gestione di tecnologie digitali costituisce un fattore di rischio per gli interessi nazionali, e ciò poiché asset strategici controllati da soggetti operanti nel mercato sono maggiormente esposti ad influenze ed operazioni di acquisizione da parte di soggetti potenzialmente ostili. Per questo gli asset rilevanti per la cybersicurezza, particolarmente in dimensione infrastrutturale, sono spesso oggetto dei cd. poteri speciali dei governi rispetto alla penetrazione di investitori stranieri, settore che esso stesso è lungi dall'essere ricostruibile secondo linee sistematiche e armonizzate[20].

4. La molteplicità di angolazioni e di dimensioni sostanziali rilevanti per la cybersicurezza

Una terza chiave di interpretazione, quella della molteplicità, conduce anche a introdurre brevemente gli scritti compendiati in questo volume. Il variegato contesto della cybersicurezza che si è rapidamente tratteggiato si traduce infatti in una molteplicità non solo di piani normativi, ma anche di dimensioni strutturali e sostanziali, che necessariamente trascendono la dimensione squisitamente giuridica, per abbracciare quella tecnica ed economica. Proliferano pertanto le angolazioni da cui muovono le analisi del fenomeno, delle sue potenzialità e delle sfide che esso determina.

In relazione alla prospettiva di protezione si pone un diretto collegamento con il tema della *data protection*, confermando una saldatura che d'altronde discende dallo stesso impianto normativo del GDPR, in cui la cybersicurezza è declinata come elemento qualificante delle istanze di protezione dei dati. Così il contributo di Corso Tozzi Martelli, che approfondisce il rapporto fra la cybersicurezza e il Codice dei contratti pubblici indagando l'opportunità che la nuova normativa italiana (di cui al D.lgs. n. 36 del 2023) offre per rinforzare la protezione dei dati personali

19 In tema cfr. Gargiulo Giovannelli Sciacovelli 2024

20 Paradigmatico è in proposito l'esercizio del cd. *golden power* previsto, con maglie di ampia discrezionalità politica, nell'ordinamento italiano

e la cybersicurezza nel contesto degli appalti; o, ancora, quello che indaga privacy e cybersecurity nel caso delle smart cities, richiedendo la messa a punto di *best practices* adeguate (Maria Notaristefano, Fabio Angeletti, Esli Spahiu).

Una prospettiva in chiave economica è offerta da Alessandra Galassi sui rischi di cybersicurezza in relazione a modelli di sviluppo urbano basati sui c.d. GIS (*Geographical Information Systems*) mentre sempre nella prospettiva di applicazioni materiali si colloca l'analisi di Melissa Capelli su oneri di adempimento e vantaggi competitivi connessi all'applicazione della cybersecurity alla filiera dei servizi nell'ambito turistico.

Prospettive sistemiche legate all'impatto sui modelli di organizzazione e amministrazione sono offerte nel contributo di ampio respiro di Bruno Carotti, nonché da Francesca Castaldo e Federico Serini che approfondiscono l'interazione fra pubblico e privato, proiettando detto rapporto sulla dimensione europea della cybersicurezza, coinvolgendo forme di coregolazione, standardizzazione e certificazione che paiono ormai centrali. Sempre su una prospettiva sistemica policentrica indugia Filippo Galli, che dedica il suo contributo all'organizzazione amministrativa della cybersicurezza nell'ordinamento multilivello.

Una importante dimensione di sicurezza strategica settoriale è al centro del contributo di Matteo Pignatti, dedicato al quadro multilivello della cybersicurezza della infrastruttura ICT in relazione al settore finanziario, ove si evidenziano rischi per la stabilità finanziaria in relazione a cripto-attività, tecnologie a registro distribuito e resilienza delle infrastrutture.

Nella prospettiva della sicurezza nazionale dell'ordinamento italiano si colloca poi Massimiliano Malvicini, che indaga l'evoluzione dell'architettura strategica nazionale in materia di sicurezza cibernetica.

Vi sono infine interessanti prospettive di collegamento fra l'ambito della cybersicurezza e quello della tutela dell'ambiente. Così Teresa Monaco apre una finestra di attenzione sul rapporto fra ambiente naturale e ambiente digitale proponendo una nuova dimensione applicativa del principio di precauzione che dialoga assai bene coi temi della gestione del rischio cibernetico, mentre Maura Mattalia muove dal tema del cambiamento climatico e della governance di Internet per trarre elementi di riflessione sulle potenzialità della governance policentrica anche in relazione alle istanze di cybersicurezza.

In conclusione, una ampia disamina di prospettive che rivela, una volta di più, come il tema della sicurezza cibernetica sia fluido, vario e fortemente evolutivo. I tratti sono labili, i confini mutevoli: forse il tempo consoliderà assetti più certi e prevedibili ma oggi le prospettive e le potenzialità dischiuse dalla tecnologia che pervade il nostro mondo recano inestricabilmente con sé, quasi fosse una faccia nascosta della luna, l'elemento della vulnerabilità: del nostro modello, delle nostre società e, forse ormai, dell'umanità stessa. La spasmodica ricerca di risposte alle istanze di cybersicurezza non è altro che un tentativo del potere di consolidarsi nell'intento di sottrarsi, e sottrarci, almeno un po', a questa vulnerabilità.

Bibliografia

Aresu A. 2024, *Geopolitica dell'intelligenza artificiale*, Milano: Feltrinelli.

Bosco F. 2013, "Cyberterrorismo e Cyberwarfare: profili giuridici e analisi della casistica a livello internazionale, in G. Cassano, G. Scorza e G. Vaciago (a cura di), *Diritto dell'Internet, Manuale operativo*, Milano: CEDAM-Wolters Kluwer, p. 657 ss.

Carotti B. 2020, "Sicurezza cibernetica e Stato-Nazione", in *Giornale di diritto amministrativo*, 5, p. 629 ss.

Cerra R., Crespi F. 2021, *Sovranità tecnologica*, Roma: Centro per l'economia digitale (CED).

De Nardis L. 2014, *The Global war for Internet Governance*, New Haven: Yale University Press.

Egloff F.J. 2022, *Semi-State Actors in Cybersecurity,* New York: Oxford University Press.

Gargiulo p. , Giovannelli D., Sciacovelli A.L. 2024, *Governance e quadri normativi della cybersecurity: Prospettive dei paesi non occidentali e delle organizzazioni internazionali*, Rivista La Comunità internazionale, Quaderno n. 29, Napoli: Editoriale Scientifica.

Ishikawa T., Yarik K. (eds.) 2023, *Public and Private Governance of Cybersecurity: Challenges and Potential*, Cambridge: Cambridge University Press.

Manjikian M. 2023, *Cybersecurity Ethics: An Introduction*, London: Routeldge, Taylor & Francis Group.

Mazza R. 2004, "Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001", in *La Comunità Internazionale*, p. 91 ss.

Meltzer J.P. 2020, "Cybersecurity, digital trade and data flows – Re-thinking a role for international trade rules" in *Global Economy and Development*, Working Paper n. 132, Brookings, p. 7 ss.

Mueller M. 2010, *Network and States. The Global Politics of Internet Governance*, Cambridge, Mass.: MIT Press.

Oddenino A. 2012, "Il problema della governance internazionale della rete" in M. Durante, U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino: UTET, p. 45 ss.

Oddenino A. 2013, "Diritti individuali, sicurezza informatica e accesso della conoscenza in Rete: la revisione delle International Telecommunication Regulations dell'ITU", in *Diritti umani e diritto internazionale*, p. 525 ss.

Oddenino A. 2017, "La violazione dei sistemi informatici contenenti informazioni riservate come illecito internazionale: tra dimensione interstatuale e tutela dei diritti umani" in M. Distefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli: Editoriale Scientifica, p. 13 ss.

Oddenino A. 2018, "Digital standardization, cybersecurity issues and international trade law" in *Questions of International Law*, vol. 51, p. 31 ss.

Pelroth N. 2021, *This Is How They Tell Me The World Ends. The Cyber Weapons Amrs Race*, New York: Bloomsbury Publishing**.**

Rossa S. 2023, *Cybersecurity e pubblica amministrazione*, Napoli: Editoriale Scientifica.

Shadmy T. 2019, "The New Social Contract: Facebook's Community and our Rights" in *Boston University International Law Journal*, vol. 37, p. 307 ss.

Singer p. W. Brooking E.T. 2018, *Like War: The Weaponization of Social Media*, Houghton Mifflin Harcourt: Eamon Dolan.