Manfredi Matassa

La sicurezza cibernetica come funzione pubblica

FrancoAngeli

SDP Studi di Diritto Pubblico

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, inoltre, 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 pubblicati nella Collana sono stati pertanto sottoposti a un processo di *double blind peer review* che ne attesta la qualità scientifica.

Manfredi Matassa

La sicurezza cibernetica come funzione pubblica

FrancoAngeli

SDP Studi di Diritto Pubblico

Il volume è stato finanziato dall'Unione europea - Next Generation EU, Missione 4
Componente 1, PRIN 2022 "Public Order and Cyber security",
codice CUP B53C24007730006.

Isbn e-book: 9788835184294

Rien n'est possible sans les hommes;
rien n'est durable sans les institutions.
Jean Monnet, *Mémoires*, Fayard 1976

Indice

Abbreviazioni

AAI: Autorità amministrative indipendenti
ACN: Agenzia per la cybersicurezza nazionale
AgID: Agenzia per l'Italia Digitale
AISE: Agenzia informazioni e sicurezza esterna
AISI: Agenzia informazioni e sicurezza interna
ANAC: Autorità nazionale anticorruzione
ANSSI: Agenzia Nazionale per la Sicurezza dei Sistemi (Francia)
ARPA: Advanced Research Projects Agency (USA)
Blue OLEx: Blueprint Operational Level Exercise
BSI: Ufficio federale per la sicurezza delle informazioni (Germania)
CEDU: Convenzione europea dei diritti dell'uomo
CER: Critical Entities Resilience (direttiva UE)
CERT: Computer Emergency Response Team
CESIS: Comitato esecutivo per i servizi di informazione e sicurezza
CGUE: Corte di Giustizia dell'Unione europea
CIC: Comitato Interministeriale per la Cybersicurezza
CIIS: Comitato interministeriale per le informazioni e la sicurezza
CISA: Agenzia per la Cybersicurezza e per le Infrastrutture (USA)
CISR: Comitato Interministeriale per la Sicurezza della Repubblica
CNAIPIC: Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

CONSOB: Commissione nazionale per le società e la borsa

COPACO: Comitato parlamentare per il controllo dei Servizi di informazione e per il segreto di Stato

COPASIR: Comitato Parlamentare per la Sicurezza della Repubblica

CRA: Cyber Resilience Act

CSA: Cyber Solidarity Act

CSIRT: Computer Security Incident Response Team

CV: Centro di Valutazione (Ministero della difesa o Ministero interno)

CVCN: Centro di Valutazione e Certificazione Nazionale

CyCLONe: Cyber Crisis Liaison Organization Network

DARPA: *Defense Advanced Research Projects Agency*

DDoS: *Distributed Denial of Service Attack*

DESI: *Digital Economy and Society Index*

DIS: Dipartimento delle informazioni per la sicurezza della Repubblica

DNS: *Domain Name System*

DoS: *Denial of Service Attack*

DPCM: decreto del Presidente del Consiglio dei ministri

ECCC: Europe Cybersecurity Competence Center

ECCG: Gruppo Europeo di Certificazione della Cybersicurezza

eIDAS: electronic IDentification Authentication and Signature (regolamento UE)

FSD: Fornitori Servizi Digitali

GCI: *Global Cybersecurity Index*

GPDP: Garante per la protezione dei dati personali

IA: Intelligenza Artificiale

ICANN: Internet Corporation for Assigned Names and Numbers

ICCC: International Computer Communication Conference

ICT: Tecnologie dell'informazione e della comunicazione

IETF: Internet Engineering Task Force

IGF: Internet Governance Forum

IIC: Istituto Italiano di Cybersicurezza

IoT: *Internet of Things*

IP: *Internet Protocol*

ISAC: Information Sharing and Analysis Center (v. SOC)

ISO: International Organization for Standardization

ISOC: Internet Society

ITU: Unione Internazionale delle Telecomunicazioni

LAP: Laboratori abilitati di prova

MAECI: Ministero degli affari esteri e della cooperazione internazionale

MI: Ministero dell'istruzione

MIMiT: Ministero delle imprese e del *made in Italy*

MiSE: Ministero dello sviluppo economico (oggi Ministero delle imprese e del *Made in Italy*)

MEF: Ministero dell'economia e delle finanze

MUR: Ministero dell'Università e della Ricerca

MIT: Massachusetts Institute of Technology

NCC: Centro nazionale di coordinamento

NCS: Nucleo per la Cybersicurezza

NIS: Network and Information Security directive

NOS: Nulla osta di sicurezza

NPL: National Physical Laboratory (Regno Unito)

OCSI: Organismo di certificazione della sicurezza informatica

OLAF: Ufficio europeo per la lotta antifrode

OSE: Operatori di servizi essenziali

OVC: Organismi di valutazione della conformità

PNRR: Piano Nazionale di Ripresa e Resilienza

PoC NIS: Punto di contatto unico NIS

PPP: Partenariato Pubblico-Privato

PSN: Polo Strategico Nazionale

PSNC: Perimetro di Sicurezza Nazionale Cibernetica

Rete CSIRT: Rete europea dei Computer Security Incident Response Team

Rete NCC: Rete europea dei Centri nazionali di coordinamento

RIRs: Regional Internet Registries

SECC: Sistema Europeo di Certificazione di Cibersicurezza

SISDE: Servizio per le informazioni e la sicurezza democratica
SISMI: Servizio per le informazioni e la sicurezza militare
SISR: Sistema di Informazione per la Sicurezza della Repubblica
SNSC: Sistema Nazionale di Sicurezza Cibernetica
SOC: *Security Operations Center*
SPOF: *Single Point of Failure*
TCP: *Transmission Control Protocol*
TIC: v. ICT
TLD: *Top-level domain*
UAR: Ufficio Affari Riservati
UCLA: University of California
UCSE: Ufficio centrale per la segretezza
WEF: World Economic Forum

1.
Inquadramento del campo di indagine

1. Le componenti della sicurezza cibernetica

Nell'ultimo ventennio il tema della sicurezza cibernetica[1] è stato oggetto di numerosi studi che hanno coinvolto trasversalmente quasi ogni ambito del sapere. Tuttavia, solo recentemente è emerso il ruolo fondamentale attribuito alla scienza giuridica – in specie al diritto amministrativo – per il conseguimento degli obiettivi prefissati in materia di cibersicurezza. Prima di poter affrontare il tema della regolazione di questa nuova materia, i giuristi del nuovo millennio che hanno inteso approfondire l'argomento sono stati chiamati a misurarsi con l'estrema variabilità della nozione di 'cibersicurezza' a seconda del contesto del suo utilizzo.

L'individuazione del bene giuridico tutelato dalla sicurezza cibernetica rappresenta già di per sé una sfida niente affatto banale. Infatti, anche prendendo a riferimento la formulazione del termine in lingua inglese (*cybersecurity*), non risulta chiaro se la 'dimensione cibernetica' richiamata dal prefisso '*cyber*' voglia indicare lo spazio da mettere in sicurezza oppure, *a contrario*, uno strumento necessario per la sicurezza del mondo reale (se non entrambi). Per risolvere tali interrogativi il giurista è chiamato anzitutto a una scelta di metodo capace di unire le nozio-

1. Al fine di prevenire qualsiasi possibile equivoco di tipo terminologico si evidenzia che le espressioni 'sicurezza cibernetica', 'sicurezza informatica' e 'cibersicurezza' – anche nella sua versione anglofona '*cybersecurity*' – saranno utilizzati come sinonimi. Con particolare riferimento a queste ultime, potendo ritenere condivisibili i rilievi recentemente mossi dall'Accademia della Crusca (comunicato n. 16 del 2021 «la cibersicurezza è importante. L'italiano pure»), si è deciso di non utilizzare la dicitura ibrida italiana-inglese 'cyber-sicurezza' al momento preferita dal legislatore italiano.

ni tecniche alle categorie dogmatiche proprie del diritto pubblico[2]. Di fronte alla possibile complessità della materia, la tentazione del giurista potrebbe essere quella di relegare lo studio della componente tecnica alle altre scienze coinvolte e dunque di 'modellare' (se non proprio ritagliare) il concetto di *cybersecurity* attraverso le categorie tradizionali già conosciute. Tuttavia, per le diverse ragioni che saranno esplicitate nel corso di questo primo capitolo, tale approccio potrebbe rivelarsi metodologicamente errato.

Il presente lavoro non intende aggiungere un'ulteriore rappresentazione parziale del concetto di sicurezza cibernetica (questa volta in senso giuridico-pubblicistico) alle decine – forse centinaia – di definizioni elaborate dalla letteratura scientifica degli ultimi vent'anni. Anche se si trovasse una definizione di tale concetto capace di raccogliere soltanto le componenti tecniche strettamente rilevanti e di proiettarle nella dimensione del diritto pubblico, il risultato di un tale complesso lavoro si rivelerebbe privo di qualsiasi utilità pratica.

In breve, si ritiene che il settore della sicurezza cibernetica possa essere compreso soltanto se osservato nel suo insieme, e non invece attraverso un approfondimento isolato delle sue diverse componenti. Ed infatti, non può ignorarsi come molti degli elementi di maggiore interesse per lo studio della materia si trovino proprio tra le intersezioni delle varie scienze coinvolte nella sicurezza cibernetica (oltre che giuridica anche informatica, storica, sociologica e militare-operativa). In altri termini, come ormai avviene sempre più spesso, il progresso in questo nuovo settore richiede un momentaneo abbandono della metodologia riduzionista in favore di un approccio più che mai eclettico[3].

2. Tra la sterminata letteratura volta ad affrontare il tema del rapporto fra diritto e tecnica si rimanda, prestando particolare attenzione ai problemi posti dall'evoluzione tecnologica, a V. Frosini, *Cibernetica, diritto e società*, Edizioni di Comunità 1973; Id., *Il diritto nella società tecnologica*, Giuffrè 1981; R. Borruso, *Computer e diritto. Problemi giuridici dell'informatica*, Giuffrè 1988; N. Irti, E. Severino, *Dialogo su diritto e tecnica*, Laterza 2001; N. Irti, *Il diritto nell'età della tecnica*, Editoriale Scientifica 2007; A.C. Amato Mangiameli, *Tecno-regolazione e diritto. Brevi note su limiti e differenze*, in «Il diritto dell'informazione e dell'informatica», n. 2, 2017, pp. 147-167; G. Ziccardi, *Il computer e il giurista*, Giuffrè 2015 e F. Faini, S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, Giappichelli 2019. Con un taglio più specifico cfr. anche M. De Benedetto, *Qualità della legislazione tra scienza, tecnica e tecnologia. Prime riflessioni*, in «Osservatorio sulle fonti», n. 2, 2022, pp. 383-396.

3. Sull'eclettismo come 'obbligo metodologico' negli studi ricollegati all'approfondimento della *web society* si rimanda in generale a C. Cipolla (a cura di), *Perché non possiamo non essere eclettici: il sapere sociale nella* web society, FrancoAngeli 2013.

Richiamando le idee poste alla base del pioneristico lavoro di Albert-László Barabási pubblicato all'inizio di questo secolo[4], l'umanista non può osservare le nuove minacce tecnologiche nella stessa prospettiva con cui gli antichi cartografi indicavano i confini dell'ignoto (e cioè attraverso la dicitura '*hic sunt leones*'). Dal momento che la mancata comprensione dei pericoli della rete non permetterebbe al giurista di tradurre correttamente le misure tecniche richieste in norma giuridica, il ciberspazio non può più essere considerato per gli odierni specialisti della sicurezza alla stregua di uno spazio indeterminato, indefinito, popolato da fiere e mostri. Occorre, dunque, partire dall'assunto secondo cui lo strumento più naturale ed efficace di difesa volto a proteggere la comunità dalle minacce della rete sia un'adeguata conoscenza della componente tecnica della materia.

In tale prospettiva, se è vero che scegliere una definizione equivale già di per sé a perorare una causa[5], la principale finalità del capitolo in esame sarà quella di individuare le ricostruzioni del concetto di 'sicurezza cibernetica' maggiormente idonee ai fini dell'inquadramento della materia nel campo del diritto pubblico.

In tale ottica, il presente lavoro si sviluppa secondo un percorso logico e argomentativo ben definito, che muove dalle basi concettuali appena delineate per giungere gradualmente ad affrontare le questioni più complesse e attuali del settore. Nella fase iniziale vengono chiariti i fondamenti teorici della materia e ricostruite le coordinate storiche ed evolutive del ciberspazio, così da fornire al lettore un solido quadro di riferimento. Si affrontano quindi i primi snodi critici, a cominciare dal rapporto tra la tradizionale sovranità territoriale degli Stati e la nuova dimensione cibernetica, per comprendere come il potere pubblico si riconfiguri di fronte alle sfide poste dalla rete globale. Successivamente, l'analisi si concentra sui profili organizzativi della sicurezza cibernetica, mettendo in luce la complessa architettura di governance del settore: vengono esaminati gli assetti nazionali – dal ruolo centrale della Presidenza del Consiglio e del comparto intelligence fino alle funzioni "interstiziali" svolte dall'ACN e dagli altri attori istituzionali e privati – e parallelamente il contesto sovranazionale, con particolare riguardo al quadro normativo e istituzionale europeo (dal ruolo di ENISA ai nuovi meccanismi di cooperazione introdotti dalla direttiva NIS2). Nella parte finale, l'attenzione è invece rivolta ai meccanismi di tutela degli interessi essenziali e alle garanzie predisposte per conciliare le esigenze di sicurezza con i principi dello Stato di diritto:

4. Il riferimento è al primo lavoro sulla 'scienza delle reti' compiuto da A.-L. Barabási, *Link: la scienza delle reti*, Einaudi 2004, p. 6.

5. Si fa riferimento al concetto espresso da C.L. Stevenson, *Ethics and Language*, Yale University Press 1944, p. 210, secondo cui «to choose a definition is to plead a cause».

vengono analizzati il sistema dei controlli e delle sanzioni, nonché strumenti speciali di salvaguardia come il cosiddetto *golden power* esercitabile dallo Stato in settori strategici.

Se l'obiettivo generale è quello di rappresentare la sicurezza cibernetica come funzione pubblica intrinsecamente composita e multilivello, questa parte del lavoro intende approfondire alcuni temi logicamente anteposti rispetto all'oggetto principale del lavoro come, ad esempio, la relazione tra sovranità territoriale e spazio cibernetico[6]. Segnatamente, in questo primo paragrafo è possibile mettere a fuoco le due componenti essenziali poste alla base della nozione di *cybersecurity* (ossia la sicurezza e la cibernetica).

1.1. La componente della sicurezza (nella prospettiva cibernetica)

Alcuni tra i problemi interpretativi più complessi legati alla nozione di *cybersecurity* discendono dalla circostanza per cui all'interno del significante 'sicurezza' sia possibile rintracciare diversi significati eterogenei. Il

6. Tra la sterminata letteratura volta ad approfondire la territorialità come presupposto di esercizio della sovranità si vedano, senza alcuna pretesa di esaustività o di completezza, C. Schmitt, *Il* nomos *della terra nel diritto internazionale dello "*Jus publicum europeaum", Adelphi Milano, 1991; D. Donati, *Stato e territorio*, Athenaeum 1924; N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Laterza 2006; S. Cassese, *Territori e potere. Un nuovo ruolo per gli Stati*, il Mulino 2016. Con particolare riferimento ai temi oggetto di questa ricerca, si ritiene opportuno evidenziare come il rapporto fra sovranità territoriale e spazio cibernetico sia spesso (e in taluni casi forse anche impropriamente) ricondotto *tout court* a quello della sovranità digitale. Tra i principali contributi sul significato dell'espressione 'sovranità digitale' si rimanda a G. Finocchiaro, *La sovranità digitale*, in «Diritto pubblico», n. 3, 2022, pp. 809-827, la ripercorre con attenzione il dibattito mettendo in evidenza tra le numerose questioni affrontate come il termine 'sovranità' trovi utilizzo «per la sua grande capacità suggestiva, ma in maniera inappropriata: nella maggior parte dei casi, infatti, piuttosto che di sovranità, si tratta di potere» (p. 810); V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in «Il diritto dell'informazione e dell'informatica», nn. 4-5, 2015, pp. 683-696 riconduce l'espressione al significato tradizionale di sovranità, ossia come «potere di controllare, *de iure* e *de facto*, un vero spazio, le attività che ivi si svolgono, coloro che vi rientrano come tale spazio è organizzato, amministrare poteri di polizia, giudiziari e di sicurezza di tale spazio» (p. 683); L. Floridi, *The fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in «Philosophy & Technology», 2020, pp. 369-378 attribuisce invece al concetto di sovranità un significato ben distinto da quello tradizionale, ossia quello di «*control of the digital*» (spec. p. 371). Più in generale, per uno studio attuale e di ampio respiro sull'argomento, non può che rimandarsi a O. Pollicino, *Potere digitale* (voce), in «Enciclopedia del diritto», I tematici, vol. Potere e Costituzione, Giuffrè Francis Lefebvre 2023, pp. 410-446.

termine deriva dal latino '*sine cura*' (senza preoccupazione) e già nel linguaggio comune, prima ancora che giuridico, si presta a diverse interpretazioni a seconda che sia inteso in modo oggettivo o soggettivo[7]. Nel primo caso il concetto è utilizzato per fare riferimento a una condizione dettata da circostanze fisiche o giuridiche tali da rendere ragionevolmente improbabile, ma comunque possibile in funzione di un rischio[8], il verificarsi di determinati eventi non desiderati[9]. Nel secondo caso, invece, l'espressione trova utilizzo come riferimento alla percezione del non verificarsi di un evento non voluto in funzione di una determinata circostanza. In altri termini, nella sua accezione più ampia l'espressione sicurezza viene impiegata per descrivere un contesto in cui esiste un rischio ridotto di pericolo (senso oggettivo) o una percezione di assenza di timore (senso soggettivo).

L'intrinseca polisemia del termine rimane inalterata – se non addirittura accentuata – anche nel diritto pubblico, all'interno del quale la nozione di sicurezza sembra osservabile solo dopo aver collocato il concetto in un determinato «paradigma»[10] o «dimensione»[11]. Partendo dall'assunto con-

7. Per un'analisi più puntuale delle possibili declinazioni del concetto a seconda della percezione in senso oggettivo o soggettivo si veda R. Ursi, *La sicurezza pubblica*, il Mulino 2022, pp. 16-18 (secondo cui la dicotomia oggettivo-soggettivo è sovrapponibile con quella mezzo-risultato); G. Pistorio, *Sicurezza* (voce), in «Digesto delle discipline pubblicistiche», VIII, 2021, pp. 339-363 e M. Dogliani, *Il volto costituzionale della sicurezza*, in «Astrid Rassegna», n. 22, 2010, pp. 1-2 (il quale riconduce la duplice sfumatura del sostantivo ai due significati principali originari dell'aggettivo latino '*securus*').

8. Sul punto si rimanda alla riflessione di A. Sterpa, *La libertà dalla paura. Una lettura costituzionale della sicurezza*, Editoriale Scientifica 2019, p. 49, il quale descrive come «inutile» la sicurezza in un contesto cui «non ci sarebbe alcun rischio che un comportamento non prevedibile e non previsto operi alterando l'ordine immutabile delle che cose che garantisce la sicurezza collettiva». Per un approfondimento più generale sul concetto di 'società del rischio' si rimanda invece al pensiero di U. Beck, *La società del rischio. Verso una seconda modernità*, Carocci 2000, p. 25 secondo cui «[n]ella modernità avanzata la produzione sociale di ricchezza va sistematicamente di pari passo con la produzione sociale di rischi […]. [In essa emergono] problemi e conflitti che scaturiscono dalla produzione, definizione e distribuzione di rischi prodotto dalla scienza e dalla tecnica».

9. Tale significato in senso oggettivo si ricava, ad esempio, nelle espressioni 'sicurezza del lavoro', 'sicurezza stradale', 'sicurezza alimentare' o 'sicurezza dei trasporti'.

10. Per un approfondimento sull'evoluzione dei 'paradigmi giuridici della sicurezza' in Italia si rimanda all'analisi di R. Ursi, *La sicurezza pubblica*, cit., pp. 15-46. Segnatamente, l'autore descrive la nascita e lo sviluppo del concetto di sicurezza pubblica attraverso l'evoluzione del costituzionalismo moderno individuando quattro differenti paradigmi: securitario (nato dallo scambio tra sicurezza e libertà del cittadino posto a fondamento dello Stato assoluto), legalitario (ricollegato a nuova visione liberale del rapporto fra sicurezza e libertà), sociale (dettato dalla nascita di un nuovo modello di sicurezza sociale disegnato dal *Welfare State*) e preventivo (frutto invece della crisi dello stesso).

11. Si fa riferimento alle diverse prospettive individuate da T.F. Giupponi, *Le dimen-*

diviso per cui la sicurezza sia «un concetto generico e vuoto, che se non è specificato o riempito non significa nulla»[12], la scienza giuspubblicistica ha così sviluppato diversi metodi di indagine utili ai fini dell'individuazione di nuovi concetti di sicurezza. Tali ricostruzioni condividono la stessa idea di base, quella per cui il significato giuridico di sicurezza possa essere ricercato soltanto all'interno del rapporto fra individuo e autorità statale, ma si distinguono a seconda del paradigma utilizzato per osservare il fenomeno.

In particolare, volendo procedere con una *summa divisio*, è possibile distinguere gli approcci basati su una prospettiva relazionale positiva da quelli invece frutto di un ragionamento in negativo: nel primo caso il contenuto della sicurezza può essere ricavato una volta «parametrato, raffrontato rispetto a un profilo di valutazione, soggettivo (sicurezza di chi (del singolo, della collettività), sicurezza rispetto a chi (agli altri individui, allo Stato) e oggettivo (sicurezza rispetto a cosa)»[13]; mentre nel secondo caso il significato di sicurezza viene costruito 'in negativo' partendo dall'individuazione del rischio quale unico elemento sempre e comunque speculare al concetto di sicurezza[14].

Sulla base di quanto fin qui rappresentato possono mettersi in luce i principali ostacoli da superare ai fini dell'individuazione di una definizione utile di sicurezza cibernetica. In primo luogo, poiché entrambe le precedenti ricostruzioni proposte sono elaborate partendo dall'idea tradizionale di sovranità statale, uno dei problemi più evidenti va riferito alla distorsione del concetto di potere pubblico all'interno dello spazio cibernetico (argomento che sarà oggetto di adeguato approfondimento nel corso del par. 2). In secondo luogo, indipendentemente dall'approccio metodologico prescelto per attribuire significato al concetto di 'sicurezza

sioni costituzionali della sicurezza, Bologna 2008, *passim.*, riassunte attraverso una *summa divisio* tra sicurezza esterna e sicurezza interna, sicurezza individuale (sicurezza da) e sicurezza collettiva (sicurezza di) e tra sicurezza materiale e sicurezza ideale.

12. N. Bobbio, *Eguaglianza ed egualitarismo*, in «Rivista internazionale di filosofia», 1976, p. 322.

13. In questi termini G. Pistorio, *Sicurezza* (voce), in «Digesto delle discipline pubblicistiche», VIII, UTET 2021, p. 342, mentre l'idea di una prospettiva 'relazionale' della sicurezza è da attribuire a G. Peces-Barba, *Teoria dei diritti fondamentali*, Giuffrè 1993.

14. Sul punto si rimanda alle riflessioni di A. Sterpa, *La libertà dalla paura. Una lettura costituzionale della sicurezza*, cit., p. 22, secondo il quale: «[i]l filo rosso che percorrendo le distinte direttrici tiene insieme il concetto è senza dubbio da costruire in negativo: in tutti i casi la sicurezza è invocata per contrastare un rischio (ossia un fenomeno che è percepito come tale) che minaccia l'individuo o la comunità nella sua integrità. Quindi, la sicurezza si definisce concretamente guardando a ciò che combatte ossia al rischio che vorrebbe neutralizzare: la scelta del rischio concretizza la qualità della sicurezza».

cibernetica', il giurista sarà in ogni caso chiamato a misurarsi con diversi concetti dall'elevata componente tecnica. Segnatamente, nella prospettiva di un metodo 'relazionale in positivo' sarà necessario definire il 'cosa' proteggere (se la sicurezza della rete o la sicurezza dei computer), il 'chi' (se il cittadino-utente, la *web-society* o l'apparato pubblico), il 'dove' (se una dimensione virtuale o materiale), il 'come' (con quale potere), da 'chi' (se da un privato, da uno Stato o entrambi) e da 'cosa' (distinguendo tra *cyber-attack*, *cyber-war* e *cybercrime*); mentre, seguendo una prospettiva 'relazionale in negativo', l'interprete sarà chiamato a individuare in concreto possibili rischi derivanti dalle 'minacce informatiche'. Compito, quest'ultimo, non meno complesso del precedente se si tiene in considerazione la circostanza per cui l'ultimo Global Risk Report del World Economic Forum (WEF) abbia ritenuto i rischi della *cybersecurity* nel breve periodo più pericoloso della crisi delle risorse naturali e, nel lungo periodo, dei danni ambientali su larga scala causati da calamità naturali[15].

Su tali premesse, il significato di sicurezza cibernetica non sembra ricavabile attraverso il solo utilizzo delle categorie e dei metodi tradizionali utilizzati dalla scienza giuspubblicistica. Nell'affrontare questo tema il giurista non potrà dunque utilizzare un approccio meramente relazionale con l'intento di proiettare nella dimensione cibernetica dei concetti già noti, ma sarà costretto ad approfondire alcuni concetti essenziali di informatica giuridica. Del resto, cercare di comprendere un ambiente virtuale attraverso le sole categorie conosciute nel mondo reale sarebbe un compito decisamente arduo (se non impossibile).

1.2. La componente della cibernetica

La parola antica *kybernetes* (κυβερνήτης) indica, nella sua accezione ristretta, il pilota di una nave[16]. La radice *kyber* sta per 'dirigere' e ha trovato nel mondo antico un impiego metaforico volto a rappresentare il timoniere di una città o di uno Stato[17] (dal medesimo tema derivano i

15. World Economic Forum, *The global risks report 2023 (18th edition)*, 2023, 6, p. 11, reperibile su *www3.weforum.org* (visitato il 12 luglio 2024).

16. Per un'analisi di ampio respiro sul concetto v. F. Zini, *Cibernetica* (voce), in A. C. Amato Mangiameli, G. Saraceni (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli 2023, pp. 68-71.

17. Il termine *kybernetikos* (κυβερνητικός) è stato utilizzato da Platone, *Il gorgia* (a cura di P. Ubaldi), La Nuova Italia 1933, p. 124 (511) per indicare la relazione tra l'abilità persuasiva di un oratore e quella di un *kybernetikos* (maestro pilota) dettata dalla capacità del primo di guidare e influenzare le menti degli altri attraverso la retorica. In termini più

latini '*gubernare*' e '*gubernator*'). Dopo un iniziale periodo di disuso nel linguaggio moderno, l'espressione è stata riutilizzata nel suo significato classico dal fisico francese André-Marie Ampère durante la prima metà dell'Ottocento per fare riferimento all'«arte di governare in generale»[18] o alla «strategia rispetto alla quale è condotto l'esercito [di una Nazione]»[19]. Tuttavia, tra la fine degli anni Quaranta e l'inizio degli anni Cinquanta del secolo scorso, la medesima espressione si è diffusa in forma anglicizzata (*cybernetics*) per fare riferimento a un nuovo campo della scienza volto a studiare i processi riguardanti «la comunicazione e il controllo tra animale e macchina»[20]. L'idea alla base della cibernetica sviluppata da Norbert Wiener alla fine degli anni Quaranta è stata rivoluzionaria: non solo si è individuato un chiaro parallelismo tra i meccanismi di comunicazione e di relativa elaborazione delle informazioni tipici di uomini e macchine, ma si è inteso sostenere scientificamente la convinzione per cui nel nuovo secolo le informazioni potessero essere comunicate, oltre che tra uomo e uomo,

sintetici, utilizzando le parole di V. Frosini, *Cibernetica, diritto e società*, Edizioni di Comunità 1968, p. 17, in tale accezione il termine cibernetica può essere inteso come «l'arte di governo del timoniere».

18. A.-M. Ampère, *Essai sur la philosophie des sciences, ou exposition analytique d'une classification naturelle de toutes les connaissances humaines, Seconde partie,* Paris 1843, p. 141: « […] Ce n'est donc qu'après tontes les sciences qui s'occupent de ces divers objets qu'après tontes les sciences qui s'occupent de ces divers objets qu'on doit places celle dont il est ici question et que je nomme Cybernétique, du mot *κυβερνήτης*, qui, pris d'abord, dans une acception restreinte, pour l'art de gouverner un vaisseau, reçut de l'usage, chez les Grecs même, la signification, tout autrement étendue, de l'art de gouverner en général».

19. Ivi, p. 143: «[…] On reconnait avec la même facilité ceux du point de vue troponomique dans la cybernétique, qui est, à l'égard du gouvernement des nations, ce qu'est la stratégie relativement à la conduite d'une armée»

20. N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, MIT Press 1948; Id., *The human use of the human beings*, Houghton Mifflin Company 1950; Id., *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri 2012. La scelta di indicare la nascente scienza con il termine '*cybernetics*' è considerata un omaggio a matematico J.C. Maxwell, il quale già nel secolo precedente ebbe l'idea di utilizzare il termine *governor* (*guber*) per indicare un meccanismo di regolazione delle macchine industriali funzionante anche in assenza di interventi umano. Oltre agli studi compiuti da Wiener non è possibile ignorare il contributo delle altre menti illuminate del Ventesimo secolo che hanno permesso un progresso significativo nel campo di ricerca della scienza cibernetica ossia, senza alcuna pretesa di esaustività, A.M. Turing, *On computable numbers, with an Application to the Entscheidungsproblem*, in «Proceedings of the London Mathematical Society», n. 1, 1937, pp. 230-265; C.E. Shannon, *A Mathematical Theory of Communication*, in «Bell System Technical Journal», n. 3, 1948, pp. 379-423 e W.S. McCulloch, W.H. Pitts, *On how we know universals: the perception of auditory and visual forms*, in «Bulletin of Mathematical Biophysics», n. 3, 1947, pp. 127-147.

anche tra uomo e macchina, tra le macchine e l'uomo e tra macchina e macchina[21]. L'impulso di Wiener ha permesso così negli anni successivi la ricerca di una 'teoria unificata dei sistemi complessi' che ha influenzato – tra gli altri – matematici, fisici, ingegneri, biologi, neuroscienziati, sociologi, filosofi e da ultimo anche i giuristi[22].

In definitiva, essendosi ormai perso il significato classico e olistico di *kybernetes*, la scienza cibernetica descrive oggi una vasta quantità di campi di studio intenti ad analizzare qualsiasi interazione tra animale (e, dunque, l'uomo) e macchina. Nel linguaggio comune il prefisso *'ciber'*[23] è così attualmente utilizzato sia per proiettare nella dimensione virtuale delle nozioni del mondo reale già note (ciber-atleta, ciber-bullo o ciber-criminale), sia per fare riferimento a concetti del tutto nuovi determinati dall'interazione tra uomo e macchina (ciber-spazio, ciber-attacco o per l'appunto ciber-sicurezza).

21. Come riporta l'attenta analisi di M. Mirti, *Il cyberspace: caratteri e riflessi sulla Comunità Internazionale*, ESI, 2021, p. 27, Wiener esemplifica questo concetto attraverso delle idee di notevole interesse: «*se son pigro e la mattina, invece di alzarmi dal letto, schiaccio un bottone che apre i caloriferi, chiude la finestra e accende un fornello elettrico sotto la caffettiera, io invio un messaggio agli elementi di questi apparecchi. Se il bolliuova elettrico fischia dopo un certo numero di minuti, esso invia a me un suo messaggio. Se il termostato registra una temperatura eccessiva nella camera e chiude il calorifero si può dire che il messaggio funzione come sistema di comando del calorifero stesso*» (N. Wiener, *Introduzione alla cibernetica. L'uso umano degli esseri umani*, cit.).

22. Tra i primi studi italiani volti ad approfondire la relazione tra diritto e cibernetica si vedano V. Frosini, *Il diritto artificiale: note sui rapporti tra cibernetica e giurisprudenza*, in «Anales de la cátedra Francisco Suárez», n. 5, 1965, pp. 83-99; Id., *La giuritecnica: problemi e risposte*, in «Informatica e diritto», n. 1, 1975, pp. 26-35; Id., *Cibernetica, diritto e società*, cit.; M.G. Losano, *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Einaudi 1969; L. Lombardi Vallauri, G. Tratteur, *Giurisprudenza e cibernetica*, in «Rivista internazionale di filosofia del diritto», p. 3, 1969, pp. 423-439; M. Lupoi, *Giuscibernetica, informatica giuridica. Problema per il giurista*, estr. da *Quaderno del Foro Italiano*, Società editrice del Foro Italiano 1970. Come ricordato da ultimo da L. Previti, *La decisione amministrativa robotica*, Editoriale Scientifica 2022, p. 15, lo stesso tema è stato approfondito anche da L. Loevinger, *Jurimetrics: The next step forward*, in «Minnesota Law Review», n. 5, 1949, pp. 455-493, il quale ha fatto riferimento al rapporto fra diritto e metodo scientifico utilizzando il concetto di 'giurimetria'.

23. Sebbene nel linguaggio comune sia spesso impropriamente attribuito lo stesso significato, si ritiene opportuno evidenziare come in realtà il prefisso '*Cyber*' non sia sinonimo, e dunque liberamente interscambiabile, con il prefisso '*e*' (da *electronic*). Segnatamente, come già evidenziato, nel caso della cibernetica si presuppone in qualche modo un'interazione tra uomo e macchina, mentre nel caso dell'elettronica si fa più in generale riferimento a delle attività svolte senza scambi o contatti fisici (si pensi ad esempio alle frequenti espressioni *e*-democracy, *e*-commerce o ancora *e*-business)

Ricostruire il significato dei termini ricompresi nella prima categoria risulta un compito abbastanza agevole, in quanto l'interprete è chiamato a proiettare nel mondo virtuale dei fenomeni già conosciuti e circoscritti nel mondo reale. Per chiarire meglio il concetto è possibile ricorrere agli esempi indicati *supra*: il ciberatleta è identificabile nell'atleta che per professione gareggia in competizioni 'videoludiche' (e-*sports*), il ciberbullo rappresenta la manifestazione in rete del fenomeno del bullismo e, infine, il cibercriminale è definibile come colui che si avvale dello strumento informatico per compiere o aver facilitata la commissione di un reato.

Le nozioni collocate nella seconda categoria non risultano invece altrettanto chiare, in quanto una volta entrate a contatto con la dimensione cibernetica assumono un significato nuovo, non più coincidente rispetto all'originale. Così come il significato di ciberspazio e ciberattacco non può ricavarsi dalle espressioni 'spazio' o 'attacco', quello di cibersicurezza non può desumersi partendo dal tipico rapporto fra cittadino e autorità pubblica definito dalla scienza giuspubblicistica. Poiché i concetti fin qui richiamati hanno significati tra loro distinti, ma non per questo indipendenti, esigenze di chiarezza espositiva suggeriscono di proseguire l'analisi del concetto di cibernetica soltanto dopo un approfondimento di alcuni elementi essenziali.

1.3. Alcune notazioni sul metodo della ricerca

Il primo inquadramento della materia offerto nelle precedenti pagine introduce all'interno della ricerca diversi problemi straordinariamente complessi, molti dei quali annoverati tra le sfide di questo secolo. La capillare diffusione dell'«infosfera»[24] nella società moderna impedisce di relegare il tema della sicurezza cibernetica alla sola dimensione della tutela dell'individuo, argomento già di per sé poco esplorato nella letteratura giuridica, ma richiede riflessioni più vaste che vanno necessariamente riferite anche alla sopravvivenza delle organizzazione complesse (tra cui gli Stati-nazione).

Se già l'ampiezza e la profondità delle questioni coinvolte sembra di per sé idonea a sostenere la necessità di un abbandono della 'metodologia riduzionista', non è tuttavia possibile esimersi da un confronto con ulteriori questioni di ampio respiro. Qualsiasi pretesa di ricostruzione ordinata della materia richiede, infatti, di misurarsi con alcuni interrogativi

24. Il riferimento è al noto lavoro di L. Floridi, *Pensare l'infosfera. La filosofia come design concettuale*, Raffaello Cortina 2020.

logicamente anteposti al tema principale di questo lavoro (si pensi all'ultratrentennale dibattito riferito al ruolo dello Stato nel ciberspazio o, ancora, alla distinzione tra guerra cibernetica, crimini informatici e attacchi informatici), sia con altri che assumono un rilievo centrale con riferimento ad angoli visuali specifici della materia (si pensi al rapporto fra sicurezza cibernetica, governo della Rete, polizia preventiva, difesa dello Stato e sicurezza nazionale).

In questo contesto, qualsiasi lavoro monografico richiede necessariamente di individuare una precisa traiettoria di ricerca capace di bilanciare esigenze di completezza e omogeneità della trattazione (che suggeriscono di rappresentare le radici culturali e meta-giuridiche della materia) con altre di sinteticità, speditezza e rigore metodologico (che impongono invece di collocare la riflessione giuridica sempre e comunque al centro dell'opera)[25]. Partendo da tale assunto, non sorprende affatto notare come i lavori che hanno guidato la prima fase del dibattito giuspubblicistico abbiano preferito affrontare il tema mettendo a fuoco questioni specifiche, quali il collegamento tra sicurezza cibernetica e polizia preventiva[26] o i meccanismi di collaborazione tra soggetti pubblici e privati[27].

Se da un lato è vero che qualsiasi tentativo di analisi congiunta delle numerose questioni ricollegate alla materia finirebbe inevitabilmente per 'diluire' le argomentazioni giuridiche in un *mare magnum* di informazioni non sempre di interesse, dall'altro non può tuttavia ignorarsi come l'assenza di una riflessione di ampio respiro sugli stessi fondamenti della materia rappresenti un non trascurabile limite per lo sviluppo di questo campo di studi. Infatti, nonostante l'idea della sicurezza cibernetica come nuova funzione pubblica sia ormai ben radicata nella letteratura amministrativista, nell'attuale dibattito non si è ancora sviluppata una riflessione neppure sugli elementi essenziali di quest'ultima. Segnatamente, dal momento che la stessa natura dell'attività che l'amministrazione è chiamata a svolgere risulta ancora oggi in larga parte oscura, qualsiasi studio dell'apparato di sicurezza cibernetica richiede un previo inquadramento volto a misurarsi con i seguenti interrogativi: esiste una funzione unitaria di sicurezza cibernetica o quest'ultima è un insieme di più funzioni (anche tradizio-

25. In questo senso, S. Civitarese Matteucci, *L'identità delle scienze giuridiche nel mondo giuridico 'plurale'. 'Questa è l'acqua'*, in «Diritto pubblico», n. 2, 2013, pp. 441-463 ricorda che nell'ormai mondo giuridico 'plurale' la riflessione giuridica non è chiamata alla ricerca di nuovi metodi, ma a valutare il diritto come insieme di norme, pratiche e linguaggi.

26. E. Buoso, *Potere amministrativo e sicurezza nazionale cibernetica*, Giappichelli 2023.

27. S. Rossa, *Cybersicurezza e pubblica amministrazione*, Editoriale Scientifica 2023.

nali)? Alla riflessione sull'unitarietà (o anche soltanto l'omogeneità) della funzione sul piano orizzontale occorre aggiungere *in secundis* un'analoga riflessione sul piano verticale: la funzione di sicurezza cibernetica europea fino a che punto è sovrapponibile con la dimensione italiana in cui la medesima attività è stata espressamente ricondotta nell'ambito della sicurezza nazionale?

Poiché nei primi anni di studio della materia questi interrogativi sono rimasti di fatto inesplorati, il lavoro in esame è stato realizzato con la volontà di indicare un sentiero che possa favorire lo sviluppo di un confronto più che con l'ambizione di concludere sul nascere un dibattito.

Sulla base di quanto rappresentato, l'obiettivo principale di questo volume sarà quello di approfondire il rapporto fra la moderna funzione di sicurezza cibernetica e le funzioni di sicurezza tradizionalmente affidate allo Stato (con particolare riferimento alla sicurezza nazionale). Come ricaduta, dopo aver individuato i caratteri fondamentali della sicurezza cibernetica sarà possibile procedere nel tentativo di inquadrare tale inedita funzione nel quadro dell'ordinamento multilivello. Ciò, segnatamente, con l'intento di comprendere se la funzione di sicurezza cibernetica nel suo insieme possa intendersi come una funzione pubblica riconducibile *tout court* allo Stato, ma con benefici diretti anche a livello euro-unionale, o invece come una funzione amministrativa condivisa in alcune sue parti con l'Unione Europea. Cionondimeno, nessuno di questi argomenti può essere affrontato senza una previa analisi di alcune questioni preliminari rispetto all'analisi che si intende svolgere, a partire dagli antichi – ma straordinariamente attuali – interrogativi sul rapporto fra ciberspazio e pubblici poteri.

2. Ciberspazio e potere

Il termine '*cyberspace*' venne utilizzato per la prima volta nella prima metà degli anni Ottanta da William Gibson – romanziere considerato padre del genere letterario '*cyberpunk*' – e descritto come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione […]. Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità, linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati»[28]. Per

28. Sebbene la prima comparsa dell'espressione '*cyberspace*' sia da attribuire al racconto "la notte che bruciammo Chrome" (W. Gibson, *Burning Chrome*, in «Omni», vol. 46, 1982, pp. 72 ss.), la citazione è riferita al successivo e più fortunato romanzo "Neuromante" (*Id.*, *Neuromancer*, Ace 1984, p. 62).

quanto affascinante nel contesto di un romanzo fantascientifico, la «definizione artistica»[29] proposta non contiene alcun elemento utile per una ricostruzione del significato dell'espressione. Del resto, non potendo neppure lontanamente immaginare la futura centralità che avrebbe acquisito l'idea del ciberspazio, è possibile presumere come in quel periodo nessuno – tantomeno Gibson – sentisse l'esigenza di elaborare una chiara definizione del concetto. Peraltro, partendo dall'assunto per cui il ciberspazio degli anni Ottanta abbia ben poco (se non proprio nulla) in comune con quello attuale, un simile tentativo sarebbe stato in ogni caso di scarsa utilità ai fini del raggiungimento degli obiettivi perseguiti da questa ricerca.

Quello del *cyberspace* deve ritenersi infatti un concetto dinamico e in continua evoluzione che, non potendo essere racchiuso in una definizione precisa e rigorosa, si presta solamente a una 'fotografia' o a una descrizione riferita a uno specifico momento storico[30]. Si tratta di una dimensione che cambia costantemente in relazione alle evoluzioni tecnologiche e alle sue modalità di utilizzo, e questi cambiamenti influenzano a loro volta il modo in cui le persone comunicano e interagiscono online. Esiste, dunque, un moto circolare e perpetuo interno al ciberspazio in cui i cambiamenti sociali suggeriscono una modifica sul piano tecnologico che, una volta realizzata, impatta inevitabilmente sulla società creando degli ulteriori sconvolgimenti. Partendo, dunque, dall'assunto per cui lo spazio cibernetico si presti maggiormente a essere raccontato più che racchiuso in una definizione, si ritiene opportuno ripercorrere i principali eventi che hanno permesso la nascita di Internet[31] in modo da poter cogliere i riferi-

29. Così, M. Mirti, *Il cyberspace: caratteri e riflessi sulla Comunità Internazionale*, cit., pp. 14-15.

30. Si pensi che soltanto poco più di dieci anni fa, quando ancora non vi era una percezione diffusa circa le pericolose implicazioni della rete nel mondo reale, il governo canadese propose la seguente definizione "amichevole" di ciberspazio: «the electronic world created by interconnected networks of information tecnology and the information on those networks it is a global commons where […] people are linked together to exchange ideas, services and friendship» (Public Safety Canada, *Canada's cyber security strategy*, *Government of Canada*, reperibile su *https://www.publicsafety.gc*).

31. Anche se nel presente lavoro le espressioni di 'Internet' e 'spazio cibernetico' sono utilizzate in modo flessibile, spesso sovrapponendo il loro significato, va comunque chiarito come i concetti non siano del tutto equivalenti. Sintetizzando al massimo, Internet è una rete di computer (o meglio, come si vedrà, una 'rete di reti') che permette lo scambio di informazioni a livello globale composta da determinate infrastrutture, protocolli e tecnologie; lo spazio cibernetico, invece, è un termine più ampio che si riferisce alla dimensione digitale nel suo insieme costituita dall'interconnessione delle di tutte le reti (tra cui Internet). In tale prospettiva, il rapporto fra i due concetti può ricostruirsi sia attraverso un rapporto da genere a specie, in cui Internet viene inteso come una parte del *cyberspace*

menti culturali, sociali e politici che hanno successivamente alimentato il dibattito sulla sovranità del ciberspazio.

2.1. L'origine e il funzionamento di Internet

La rete oggi conosciuta come Internet è nata all'inizio degli anni Sessanta nell'ambito di un progetto militare statunitense che ha raccolto il lavoro scientifico di diversi studiosi[32]. Una «antica leggenda»[33] riconduce la nascita della rete alla volontà del Governo americano di finanziare un sistema di comunicazioni in grado di resistere a un eventuale attacco nucleare sovietico nel corso della Guerra Fredda, ma in realtà Internet prende forma grazie al lavoro svolto congiuntamente e autonomamente da numerosi studiosi. Per quel che sembra una coincidenza, infatti, alcuni tra i più importanti centri di ricerca di eccellenza di quegli anni decisero – senza neppure comunicare tra loro – di progettare un modello di rete decentralizzato diviso in molteplici punti tra loro collegati, i 'nodi'. Parallelamente al pioneristico impegno con cui, nei primi anni Sessanta, Paul Baran disegnò un sistema di comunicazione 'a prova di bomba' per l'amministrazione militare americana[34], tra il 1961 e il 1967 alcuni ricercatori di spicco del MIT furono chiamati a dirigere il centro di ricerca informatico dell'ARPA[35] con l'intento di trovare una soluzione all'enorme spreco di

(il quale include anche reti locali e intranet, sistemi di comunicazione militari e governativi, giochi online e ambienti virtuali), sia attraverso una relazione mezzo/risultato (in cui Internet viene inteso come un mezzo attraverso cui accediamo all'ambiente virtuale).

32. Per uno studio approfondito sull'origine di Internet si rimanda a B.M. Leiner *et al.*, *A brief history of the Internet*, in «ACM SIGCOMM computer communication review», n. 5, 2009, pp. 22-31; K. Hafner, M. Lyon, *Where wizards stay up late: The origins of the Internet*, Simon & Schuster 1998 e W. Isaacson, *The innovators: How a group of inventors, hackers, geniuses and geeks created the digital revolution*, Simon & Schuster 2014.

33. In questi termini A.-L. Barabási, *Link: la scienza delle reti*, cit., p. 157. Nelle stesse pagine l'autore spiega come tra i primi disegni di un'infrastruttura decentrata e frammentata concettualmente molto simile all'attuale Internet sia possibile inserire il lavoro svolto da Paul Baran, lo studioso incaricato dal Governo statunitense alla creazione di una 'rete a prova di attacco nucleare', ma nonostante il suo indubbio contributo teorico il progetto è stato dopo poco abbandonato.

34. Le idee alla base del lavoro di Baran sono state diffuse agli inizi degli anni Sessanta in un paper (P. Baran, *On Distributed Communications Networks*, Rand 1962) e poi successivamente sviluppate in dodici volumi.

35. Per *Advanced Research Projects Agency* (ARPA) si fa riferimento all'Agenzia statunitense istituita nel 1958 come risposta al lancio sovietico del primo razzo Sputnik. Nel 1971 il nome venne cambiato in *Defense Advanced Research Projects Agency* (DARPA), per poi tornare all'originaria denominazione nel 1993 e cambiare ancora nel 1996. Oggi

risorse federali dettato dall'impossibilità di far comunicare i dispositivi dei centri di ricerca[36].

Il primo esperimento di successo ebbe luogo il 29 ottobre 1969 quando, alle 22:30 circa, alcune lettere digitate su un computer dell'Università della California apparvero sullo schermo di un dispositivo dell'Università di Stanford. Sebbene l'esperimento ottenne un successo soltanto parziale – la comunicazione si interruppe infatti dopo l'invio delle prime due lettere della parola «l-o-g-i-n» – l'importanza del progetto divenne ormai chiara. Internet venne così svelato al mondo nel successivo ottobre del 1972 in occasione dell'*International Computer Communication Conference* (ICCC).

Il meccanismo utilizzato è stato quello della 'commutazione dei dati a pacchetto' (*packet switching*), ossia – semplificando all'estremo – un metodo di trasmissione volto a dividere i dati trasmessi con l'intento di ricomporli una volta raggiunto il destinatario. Così, nel rendere le informazioni intelligibili soltanto al momento del loro invio e della successiva ricezione, la prima infrastruttura ha di fatto impedito a qualsiasi soggetto intermediario la possibilità di filtrare il contenuto delle informazioni (principio noto come *end-to-end principle*)[37].

l'Agenzia non ha la stessa posizione di forza del passato in quanto l'originario controllo sui progetti di sviluppo militare e sulle ricerche più avanzate è stata persa a seguito dell'affidamento dei programmi spaziali alla NASA. Il Progetto della prima rete di computer pioniera (ARPANET) è descritto da L. Roberts, *Multiple Computer Networks and Intercomputer Communication*, in «Proceedings of the first ACM symposium on Operating System Principles», 1967, pp. 3.1-3.6.

36. Sebbene quello di Internet sia considerato un progetto statunitense, va evidenziato come anche il National Physical Laboratory (NPL) del Regno Unito ha condotto negli stessi anni (1964-1967) delle ricerche arrivando alle medesime conclusioni degli studi d'oltreoceano. Per un approfondimento sul tema veda J. Bing, *Building Cyberspace: A Brief History of Internet*, in L.A. Bygrave, J. Bing (eds.), *Internet Governance: Infrastructure and Institutions*, Oxford University Press 2009, pp. 8-47.

37. L'*end-to-end principle* è per quel principio fondamentale della rete che attribuisce il controllo e la complessità delle operazioni agli estremi di una rete o di un sistema, piuttosto che distribuiti in modo centralizzato. Secondo il principio '*end-to-end*', la rete dovrebbe fornire solo un servizio di trasmissione dei dati tra due dispositivi, senza interferire con il contenuto dei dati stessi o con le operazioni specifiche che vengono eseguite su di essi. In altre parole, i fondatori della rete hanno inteso trasporre nel linguaggio di Internet gli ideali liberali che pervadevano la società americana già nei primi anni Sessanta, immaginandola come un a dimensione neutrale e trasparente rispetto ai dati che attraversa. Per un approfondimento sul funzionamento *dell'end-to-end design si* rimanda al contributo di J.H. Saltzer, D.P. Reed, D.D. Clark, *End-to-end arguments in system design*, in «ACM Transactions on Computer Systems (TOCS)», n. 2, 1984, pp. 277-288.

La creazione di un sistema di comunicazione decentralizzato è stata possibile grazie all'introduzione di strutture intermedie tra mittenti e riceventi – note come «sottoreti» – preposte a garantire la compatibilità delle informazioni tra i diversi nodi della rete. Per completare l'infrastruttura è stato introdotto successivamente un particolare protocollo denominato *Transmission Control Protocol/Internet Protocol* (TCP/IP) volto a rendere possibile la comunicazione di tutte le diverse componenti della rete[38]. In estrema sintesi, come dimostrato dalla stessa sua denominazione, la tecnologia Inter[connected]-Net[works] raggiunge il suo scopo in quanto 'insieme di reti' o, più precisamente, come la 'rete delle reti'.

Quel che rileva maggiormente in questa fase introduttiva non è tanto la comprensione della componente tecnica della Rete, che risulterà comunque estremamente utile per lo studio di diversi concetti che verranno affrontati nel corso della trattazione, quanto piuttosto la rappresentazione del particolare contesto all'interno del quale Internet si sviluppa. Tale tecnologia deve ritenersi infatti «frutto dello Stato innovatore»[39] (facendo riferimento Stati Uniti), il quale ha garantito ai 'padri dell'Internet' tutte le risorse e gli strumenti necessari per costruirla in modo orizzontale; attraverso un dialogo aperto e creativo tra tutti gli esperti che fossero in grado di offrire un valido contributo.

L'originaria gestione della 'rete delle reti' informale, basata su un approccio *bottom-up*, si è rivelata tuttavia uno dei principali problemi che la comunità internazionale ha dovuto affrontare nel corso della costante ed esponenziale crescita di Internet e degli interessi ad esso ricollegati (in ordine: scientifico, militare, commerciale ed economico e di sicurezza nazionale). In una diversa prospettiva, ed è questo uno dei punti centrali che si intendono affrontare, risulta inevitabile interrogarsi su quale sia oggi il ruolo degli Stati nella *governance* di un sistema costruito da una ristretta comunità di scienziati sotto il coordinamento degli Stati Uniti.

38. Volendo essere più precisi si tratta, in realtà, si due componenti separati: l'*Internet Protocol* si occupa dell'indirizzamento dei pacchetti di dati su Internet, assegnando indirizzi IP univoci ai dispositivi in modo da determinare il percorso necessario per il raggiungimento della destinazione desiderata, mentre il *Transmission Control Protocol* gestisce la consegna affidabile dei dati tra i dispositivi collegati.

39. L'utilizzo dell'espressione «Stato innovatore» come riferimento al ruolo promotore degli Stati Uniti nello sviluppo della tecnologia è da attribuire al noto lavoro di M. Mazzucato, *Lo Stato innovatore. Sfatare il mito del pubblico contro il privato*, Laterza 2005.