Filippo Galli

L'organizzazione amministrativa della cybersicurezza nell'ordinamento multilivello

Abstract: Lo studio analizza il quadro giuridico multilivello della cybersecurity, con particolare attenzione al profilo dell'organizzazione amministrativa. Prendendo spunto dall'analogia con le Ecatonarchie della mitologia greca, il contributo esplora le intricate strutture che definiscono il panorama operativo della cybersecurity, sottolineando le difficoltà nel concettualizzare la materia come un sistema giuridico coerente senza un'analisi completa della sua natura in evoluzione. Esaminando i modelli organizzativi all'interno dell'UE e delle discipline nazionali e ricostruendone la *ratio*, lo studio evidenzia l'interazione tra gli approcci tradizionali Stato-centrici e i modelli di governance policentrici emergenti. La trattazione sostiene che, in un contesto di assenza di autorità, il concetto di organizzazione emerge come principio relazionale, cruciale per navigare nelle complessità della poliarchia. L'articolo riflette sulle implicazioni per le future discipline giuridiche, sottolineando la necessità di una governance adattiva che possa rispondere alla rapida evoluzione delle minacce nel dominio digitale.

Keywords: Cybersecurity; Organizzazione amministrativa; Digital Governance; Rete; Multistakeholder Approach.

1. 'Catturare l'Ecatonchiro'. Lo studio della cybersicurezza come sistema coerente di diritto

Nei racconti della teogonia greca sull'origine dell'ordine cosmico[1], si narra che dall'unione primordiale tra Cielo (*Urano*) e Terra (*Gea*) nacquero, tra gli altri, gli Ecatonchiri[2]: esseri colossali e dalle fattezze mostruose, erano dotati, ciascuno (da cui il *nomen* collettivo), di cinquanta paia di braccia e altrettante teste, che li ren-

1 Mi rifaccio, in particolare, alla tradizione esiodea (Hes. *Th*. 148 ss.).
2 Dall'unione delle parole *ἑκατόν* ("cento") e *χείρ* ("mano"), latinizzato in *Centimani*.

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: 10.7413/197054760148

devano "insuperabili per dimensione e potenza"[3]. Della loro forza Zeus si servì per rovesciare la tirannia del padre Crono, lasciandoli infine a sorvegliare i Titani prigionieri nel Tartaro.

All'osservatore che si accosti al sistema amministrativo della cybersicurezza, la figura dell'Ecatonchiro fornisce una sintetica ma pregnante rappresentazione del 'colpo d'occhio'. Le ragioni dell'analogia sono di natura epistemica, nella misura in cui la comune complessità strutturale dei fenomeni si riflette sulle condizioni di conoscibilità degli stessi: come gli autori classici finiscono per contraddirsi nelle reciproche descrizioni della creatura mitica, faticando persino a immaginarne le fattezze, così lo studio in termini strutturali dell'architettura *cyber* sconta preliminari esigenze di chiarificazione concettuale, nonché di una ricostruzione capace di articolarne in modo significativo le eterogenee componenti e i rispettivi indirizzi operativi.

Si pone, pertanto, un fondamentale problema di definizione dell'oggetto d'indagine e financo di *pensabilità* dello stesso, quanto meno nei termini di un *corpus* unitario e provvisto di pur basilare coerenza. 'Catturando l'Ecatonchiro' nel suo insieme, il giurista può tentare una descrizione della cybersicurezza come sistema di diritto 'in azione', rilevandone, al di là della miriade di norme e apparati, regolarità e matrici funzionali. L'analisi complessiva della materia, oltre a rendere conto della sua categorizzazione, è essenziale per comprenderne il funzionamento globale e individuare le migliori soluzioni *de lege ferenda* nel quadro di una disciplina in rapidissima evoluzione.

In questo senso, il presente lavoro si propone di fornire alcune notazioni di carattere teorico-generale con riferimento alla tipologia organizzativa riscontrabile nell'ordinamento multilivello della cybersicurezza, nonché ai relativi moduli operativi e ai sottesi modelli di regolazione sociale.

2. Organizzazione amministrativa e definizione della funzione: le ragioni di un'inversione di metodo

Questione di rilievo all'apparenza contingente, ma foriera di considerazioni circa lo statuto giuridico della cybersicurezza, è la scelta di partire da uno studio dell'organizzazione, privilegiando un'osservazione del fenomeno amministrativo che ne evidenzi tanto il rilievo istituzionalistico di "grandezza sociale"[4], quanto la natura di "stabile e ordinata struttura politico-sociale in cui coesistono e interagiscono persone con ruoli e responsabilità differenti, utilizzando risorse di vario genere (…) per raggiungere determinati obiettivi"[5] e garanzie.

Si è correttamente osservato, in dottrina, che l'aspetto latamente organizzativo, tradizionale appannaggio di una scienza dell'amministrazione oggi in ripresa[6], è

3 Apollod. *Bibliotheca* 1.1.1.

4 Così Romano 1909: 8, difendendo la "personificazione del potere per mezzo dello Stato" dalla facile critica di costituire nulla più che una "fantasia poetica".

5 Gasparri 2024: 1.

6 Matassa 2022: 627 s., D'Alberti 2013: 65.

costitutivo del concetto stesso di *cybersecurity*, il quale, sul piano etimologico, sta ad indicare un'organizzazione di tipo difensivo[7] e, su quello operativo, ha principalmente ad oggetto la protezione di "infrastrutture informatico-digitali di organizzazioni complesse, pubbliche o private"[8], spesso coinvolte in iniziative di coordinamento difensivo ben al di là delle formali indicazioni normative[9]. Spingendosi oltre tali conclusioni, si può rilevare come, per un settore dominato dalla *disruptive innovation*[10] quale la cybersicurezza, tale profilo strutturale concorra alla stessa definizione della funzione, la quale appare costantemente in via di consolidamento. È del resto opinione diffusa, *a fortiori* in discipline di frontiera, che tracciare un confine netto tra l'ambito dell'organizzazione e quello dell'attività amministrativa sia impresa tutt'altro che agevole (e forse nemmeno auspicabile), modellandosi la prima, anche per un basilare principio di strumentalità, in relazione alle finalità sostanziali che la seconda si propone di perseguire[11].

Se, dunque, secondo l'insegnamento di Giannini, "in principio sono le funzioni"[12] (e quindi i bisogni, cui, solo in un secondo momento, segue l'articolazione amministrativa)[13] – e ciò costituisce un assioma sempre valido – in pochi altri ambiti, nella prassi, la struttura finisce per rivelarsi tanto determinante rispetto ai confini della funzione: in altri termini, tra la cybersicurezza *stricto sensu* (la c.d. cyber-resilienza) e il suo frequente impiego come "*umbrella term*"[14] di più o meno connesse istanze securitarie si riscontra una vasta area di "penombra"[15] semantica, popolata da concetti come guerra cibernetica, cybercrimine e *cyberintelligence* e i cui confini restano segnati, in ultima istanza, dalle scelte discrezionali concernenti l'attribuzione agli apparati delle relative competenze.

7 Rossa 2023a: 9 ss. Rossa 2023b: 162 s. Rossa 2022: 428 s.

8 Rossa 2023b: 163.

9 Odermatt 2018: 354 ss., con riferimento al "*multi stakeholder approach*" tipico dell'Unione europea.

10 L'espressione è resa popolare da Bower e Christensen 1995, che la impiegano per descrivere i processi di innovazione tecnologica capaci di rivoluzionare in maniera 'dirompente' il funzionamento di un determinato mercato, portando in ultima istanza alla sua sostituzione o, quantomeno, a quella delle imprese in esso dominanti: "*The technological changes that damage established companies are usually not radically new or difficult from a technological point of view. They do, however, have two important characteristics: First, they typically present a different package of performance attributes – ones that, at least at the outset, are not valued by existing customers. Second, the performance attributes that existing customers do value improve at such a rapid rate that the new technology can later invade those established markets. Only at this point will mainstream customers want the technology. Unfortunately for the established suppliers, by then it is often too late: the pioneers of the new technology dominate the market*".

11 Franchini e Vesperini 2012: 74. In tema di rilevanza giuridica dell'organizzazione amministrativa, che va ben oltre la mera strumentalità rispetto alla relativa attività, si vedano, *ex multis*, Merloni 2009, Rossi 2005, Nigro 1988, Paleologo 1981, Guarino 1977, Berti 1968, Nigro 1966, Bachelet 1965. Il tema è stato recentemente riproposto da Carbone 2024.

12 Giannini 1957.

13 Gasparri 2024: 2 ss.

14 Odermatt 2018.

15 Hart 1958.

Più in generale, assecondando la comune tendenza degli ordinamenti della sicurezza[16], l'amministrazione *cyber* manifesta, al prezzo di una certa ambiguità categoriale[17], una natura "trasversale"[18], capace di curare molteplici interessi pubblici[19] nelle forme ibride dell'approccio *whole-of-society*[20]. A tale dispiegamento corrisponde, di necessità, l'assestarsi di un'idonea organizzazione pubblica, o piuttosto di quella "miriade di organizzazioni"[21] in cui si esprime ogni ramo di amministrazione, disegnando un "complesso di strutture"[22] e di "modelli differenziati"[23] percorso da relazioni eterogenee: un sistema la cui complessità qualitativa si misura nella coesistenza di figure soggettive (quali 'agenzie', 'comitati' e 'gruppi' di vario tipo) profondamente divergenti per natura, compiti e composizione.

In un settore alimentato dalla digitalizzazione, la quale impone regolarmente il ripensamento degli operatori sul piano organizzativo e financo culturale[24], si fa più stridente che altrove il "paradosso tra l'insufficienza esplicativa del tradizionale modello legalitario-burocratico di amministrazione pubblica e la persistente egemonia del quadro teorico statocentrico"[25], laddove, coinvolgendo ormai in ogni sua componente la vita economica e sociale, l'esigenza di protezione sottesa all'esercizio del potere sembra domandare ad un tempo soluzioni di amministrazione classica e di *governance* globale, generando concorrenza tra i rispettivi modelli.

Per tali ragioni, un metodo d'indagine che, con inversione logica, si appunti prioritariamente all'organizzazione della cybersicurezza consentirà non solo di sondarne la concreta consistenza, ma anche di chiarire le finalità della relativa funzione e, auspicabilmente, la capacità dell'amministrazione di assicurarne gli esiti.

3. In principio è il diritto globale, tra gruppi di intervento e norme tecniche

Peculiarità della cybersicurezza come fenomeno ordinamentale è lo sviluppo originario, e quindi la priorità *in tempore* rispetto al successivo intervento (sovra-)

16 Chiti 2016: 545.

17 La quale finisce per forzare la tradizionale semantica del potere pubblico e della sovranità. Cfr. Slack 2016.

18 Lauro 2021: 532.

19 Sola 2022: 391.

20 Ovvero di un approccio che, oltre alle competenti amministrazioni, "vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza. Nella presente visione strategica, infatti, quest'ultima è concepita non solamente come un indiretto beneficia rio delle misure contemplate nel Piano di implementazione della strategia, ma anche come parte attiva. L'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso" (*Strategia Nazionale di Cybersicurezza 2022-2026*: 8).

21 Guarino 1977: 88.

22 D'Alberti 2013: 73.

23 Guarino 1970: 17.

24 Golisano 2022: 824.

25 Di Gaspare 1995: 513.

statale, di sistemi regolatori globali rientranti a pieno titolo tra le manifestazioni del c.d. *global administrative law*[26].

Benché, infatti, il tema resti perlopiù inesplorato in dottrina, anche perché riconducibile in larga misura a fenomeni di *soft law* posti ai margini della rilevanza giuridica[27], la trentennale[28] esperienza dei gruppi di risposta alle minacce cibernetiche, di eterogenea natura e denominazione (oggi perlopiù *Computer Security Incident Response Team* – CSIRT o *Computer Emergency Response Team* – CERT)[29], ha origine al di fuori di ogni inquadramento normativo o burocratico, esprimendosi nondimeno, fin dal principio, in un sistema deformalizzato di coordinamento globale preposto ad attività di *soft regulation* e scambi informativi.

In linea con la "grande trasformazione"[30] innescatasi a partire dalla seconda metà del XX secolo e la conseguente esplosione della globalizzazione giuridica, le singole cellule operative, talora investite di "mandati pubblici nazionali"[31], hanno progressivamente prodotto aggregazioni complesse di "reti (…) di poteri pubblici neutrali"[32], investite di competenze tecniche dalla portata universale (es. CERT/CC e FIRST) o regionale (es. TF-CSIRT) ma pur sempre estranee al circuito politico-rappresentativo e alle sue istituzioni domestiche o internazionali. Ne è risultato un complesso strutturalmente eterogeneo, orientato alla comunione di funzioni[33] tra soggetti equiordinati[34]; un meccanismo di *governance* informale, animato da relazioni *de iure* paritarie e segnato al più dalla sostanziale primazia di organi particolarmente autorevoli (ad es. il CERT/CC con sede a Pittsburgh).

È solo a ridosso del nuovo millennio che la disciplina della cybersicurezza attira le attenzioni crescenti degli attori politici tradizionali, *in primis* di quello comunitario, i quali non di rado, pur avanzando autentiche pretese conformative e proponendo soluzioni organizzative ad esse adeguate, hanno optato per un innesto dei nuovi sistemi amministrativi sull'intelaiatura preesistente, istituzionalizzando ed arricchendo di funzioni pubbliche la rete 'parallela'[35] costituita dai CSIRT nazionali[36].

26 Sul distinguo v. Battini 2008, Cassese 2005.

27 Laddove "[r]ilevante è, dunque, il fatto che riceve un predicato giuridico; irrilevante, il fatto che non riceve un predicato giuridico", esprimendosi in tal modo non "una nota del fatto, ma la impossibilità del giudizio giuridico" (Irti 1968: 103).

28 A partire dalla diffusione del c.d. Morris Worm, nel 1988, su cui v. Ruohonen – Hyrynsalmi – Leppänen 2016: 748 s.

29 Sulle ragioni della diffusione di una doppia denominazione, v. Serini 2021: 251 e Contaldo – Peluso 2018: 70 ss.

30 Battini 2016: 112 ss.

31 Ruohonen – Hyrynsalmi – Leppänen 2016: 749.

32 Ielo 2003: 374.

33 Su cui Ielo 2003: 384 ss.

34 Sulla *governance* tecnica della cybersicurezza cfr. Mueller, M. – A. Schmidt – B. Kuerbis 2013.

35 Accanto a quella "propriamente amministrativa" (Lauro 2021: 532).

36 La disciplina dei CSIRT e della relativa Rete è, da ultimo, prevista dagli articoli 10-13 e 15 della Direttiva (UE) 2022/2555 (NIS 2).

L'intera vicenda disegna, quindi, un caso singolare di 'glocalizzazione del diritto', il quale, inizialmente etichettabile come 'globale', si fa disciplina comunitaria e poi nazionale, cristallizzando via via in formule normative e istituzionali di maggiore cogenza: un percorso dettato dalla novità della relativa funzione, nata, quantomeno con riferimento al Vecchio continente, in un contesto di forte vitalità oltre i confini (e le categorie) dello Stato[37].

4. Il quadro europeo della cybersicurezza: organizzazioni a rete e integrazione decentrata

Nel senso sopra delineato, l'ordinamento amministrativo dell'Unione è il primo ove sia dato riscontrare un'organizzazione in senso proprio operante, nell'ambito della sicurezza informatica, (anche) entro i confini nazionali, mentre il legislatore italiano esiterà a inaugurare una normativa dedicata per almeno un altro decennio[38]. Il regime comunitario in vigore dai primi anni Duemila[39] viene rimaneggiato a più riprese, specialmente a seguito dell'elaborazione di un'apposita Strategia dell'Unione[40], e si articola oggi in un disegno estremamente complesso.

Prendendo a riferimento i due principali criteri di distribuzione delle funzioni amministrative[41], il sistema, nel suo insieme, può declinarsi *ratione materiae* laddove ogni ripartizione sub-settoriale della cybersicurezza è riconducibile alla competenza di chiare figure istituzionali (ENISA per la cyber-resilienza[42], EC3 per il cybercrimine[43], l'Agenzia europea per la difesa con riferimento alla c.d. guerra cibernetica[44]), ma anche rispetto alla tipologia di attribuzioni: così, attorno al nucleo della regolazione *cyber*, costituito da ENISA con le sue funzioni di assistenza, coordinamento, certificazione e formazione, si sviluppano varie "reti" di carattere tecnico-operativo che coinvolgono agenti e strutture decisionali a diversi livelli di intervento (tra cui la rete dei CSIRT[45], il Gruppo di cooperazione[46] e la nuo-

37 Della Cananea 2009.

38 Con il d.P.C.M. n. 66 del 19 marzo 2013 (decreto Monti).

39 Radoniewicz 2022: 73 ss. Lauro 2021: 531 ss., Ruohonen – Hyrynsalmi – Leppänen 2016: 749 ss.

40 *Strategia dell'Unione europea per la cibersicurezza* (JOIN(2013) 01), già preceduta da una comunicazione sulla *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001) 298) e da una *Una strategia per una società dell'informazione sicura* (COM(2006) 251), nonché da un piano di azione e una comunicazione *Proteggere le infrastrutture critiche informatizzate* (COM(2009) 149).

41 Franchini e Vesperini 2012: 75 s.

42 L'Agenzia dell'Unione europea per la cibersicurezza, istituita nel 2004 e disciplinata, da ultimo, con Reg. (UE) 2019/881.

43 Il Centro europeo per il cybercrimine, proposto la prima volta con la comunicazione sulla *Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica* (COM(2012) 140).

44 Su cui cfr. *La politica di ciberdifesa dell'UE* (JOIN(2022) 49).

45 Art. 15 Direttiva (UE) 2022/2555 (NIS 2).

46 Art. 14 Direttiva (UE) 2022/2555 (NIS 2).

va rete per le crisi informatiche EU-CyCLONE[47]); con riferimento ai compiti di formazione e scambio di buone prassi, è sorto un vero e proprio ecosistema europeo delle competenze, che vede un Centro europeo di competenza sulla cybersicurezza (ECCC) attorniato da una Rete di centri nazionali di coordinamento e operante nell'ambito della c.d. Comunità europea della cybersicurezza, una sorta di piattaforma di dialogo al servizio dei portatori di interesse[48]; mentre nell'ambito di quest'ultima, rispetto alle specifiche esigenze di rilancio e coordinamento industriale, si è registrato il varo di un vasto programma di partenariato pubblico-privato sotto l'egida di una *European Cyber Security Organization* (ECSO)[49].

L'intreccio di organi e funzioni traccia un regime di *governance* "distribuita"[50] che, partito da basilari compiti di coordinamento dinamico, ha gradualmente accentuato i propri tratti conformativi secondo un processo di stratificazione burocratica (*bureaucratic layering*)[51] lungo le precedenti infrastrutture di cooperazione informale.

In particolare, benché l'impianto complessivo resti chiamato a convogliare nelle sedi decisionali la più vasta platea di soggetti interessati (*multistakeholder approach*), confermando così la propria vocazione partecipativa, emerge il ruolo preminente di ENISA: un'agenzia europea che, inizialmente impegnata in un'ostica "lotta per il riconoscimento"[52] come autorità di settore, si è vista attribuire crescenti competenze operative e promozionali[53], sino a diventare l'*ubi consistam* di un sistema[54] capace di combinare strategie difensive *risk-based* e azioni mirate *threat-based*[55].

Il descritto complesso regolatorio sconta il carattere composito e multipolare proprio delle amministrazioni europee[56], segnate in ogni direzione da rapporti di "interdipendenza strutturale e funzionale"[57]. Ai fini di un inquadramento tipologico, l'esito appare in prevalenza riconducibile a due modelli organizzativi di notevole efficacia descrittiva, ancorché di scarso rigore dogmatico: la figura della rete[58], "contenitore di relazioni"[59] nel quale si realizza una distribuzione di competenze tra nodi e "punti di contatto"[60] orientati alla comune soluzione di problemi

47 Art. 16 Direttiva (UE) 2022/2555 (NIS 2).
48 Reg. (UE) 2021/887.
49 Fondata nel 2016 e il cui statuto è disponibile all'indirizzo www.ecs-org.eu.
50 OECD 2002.
51 Ruohonen – Hyrynsalmi – Leppänen 2016: 753.
52 Honneth 2002.
53 Ulteriormente accresciute con la Direttiva NIS 2 e il Reg. (UE) 2019/881 (*Cybersecurity Act*).
54 Sulle competenze di ENISA, *ex multis*, Rossa 2023b: 166 ss., Forgione 2022, Parona 2021, Pauri 2017, Eckhardt – Kotovskaia 2023.
55 Backman 2023.
56 Franchini e Vesperini 2012: 120, Chiti 2007, Cassese 2002.
57 Franchini – Della Cananea 2010: 143.
58 Frediani 2010: 103 ss. che ne distingue un senso tecnico e uno metaforico o traslato. V. anche Cassese 2001, Lippi 2001.
59 Perulli 1998.
60 Terminologia impiegata dalle stesse Direttive NIS.

tecnici[61], e il concetto, limitrofo, di integrazione decentrata, ove alla contitolarità di una funzione regolatoria tra uffici comunitari e statali corrisponde l'effettiva riconduzione degli stessi ad un'"amministrazione unitaria"[62], principalmente tramite l'istituzione di agenzie europee con compiti di coordinamento.

In questo senso ENISA, centro polifunzionale di un 'sistema a stella'[63] dal quale dipanano diverse reti, ben incarna il fenomeno dell'*agencification* come esercizio congiunto di funzioni europee[64]. Di qui la predilezione, più che per indirizzi atti a vincolare i soggetti statali, per rapporti operativi che concretizzino una "pratica della loro interdipendenza e complementarietà funzionale"[65], ove l'organismo centrale funga da "centro di gestione, elaborazione e condivisione di informazioni a contenuto scientifico particolarmente elevato"[66]. Anche nel settore della cybersicurezza, pertanto, l'integrazione con l'ordinamento europeo supera la vecchia dicotomia (di rilievo meramente funzionale) tra amministrazione diretta e indiretta, confermando il primato dell'organizzazione come principio ordinante per agglomerati di competenze non dipanabili[67] col solo richiamo alle funzioni[68].

5. Il sistema nazionale di cybersicurezza: direzione centrale e operatività diffusa

Anche nel sistema nazionale di cybersicurezza si riconosce un'amministrazione "multiorganizzativa"[69], se non altro per l'evidente condizionamento da parte delle corrispondenti strutture comunitarie, che ad essa delegano compiti e richiedono uffici di collegamento[70]. In "un contesto ispirato al pluralismo istituzionale"[71], la demarcazione delle attribuzioni non ricalca solo la frammentazione concettuale della funzione di sicurezza (anche in questo caso, con cyberdifesa, cybercrimine e *cyberintelligence* distribuiti tra i rispettivi enti)[72], ma attiene al nucleo stesso della resilienza informatica, la cui *governance*, radicalmente rivista su spinta del PNRR[73], ripropone l'"approccio a tre livelli"[74] – tecnico (ACN, CSIRT), operativo (ACN, NCS) e strategico/politico (Presidenza del Consiglio) – dei programmi di coordinamento in sede europea.

61 Cassese 2001.
62 Franchini e Vesperini 2012: 126.
63 Come osserva da ultimo Rossa 2022: 445 s.
64 Chiti 2021.
65 Chiti 2002: 445 ss.
66 Lamberti 2016: 287.
67 Coerentemente alla condizione dello stato contemporaneo, "congiunto organizzato di amministrazioni diverse" per Giannini 1986: 79.
68 Che, nel caso della cybersicurezza, non è espressamente prevista dai Trattati (Chiara 2023 Odermatt 2018, Pauri 2017).
69 Franchini e Vesperini 2012: 86.
70 Franchini – Della Cananea 2010: 163 s.
71 Parona 2021: 6.
72 Si veda la ricostruzione di Serini 2021: 251.
73 Con il d.l. n. 82 del 2021.
74 Raccomandazione (UE) 2017/1584 (c.d. *Blueprint*).

Parimenti valorizzato, pur con le specificità che sempre ne caratterizzano l'impiego all'interno degli ordinamenti statali[75], è il modulo della rete: sia sul piano strettamente operativo, in connessione con l'impianto strategico dell'intero sistema[76] e con l'inedito strumentario collaborativo del 'perimetro nazionale', sia su quello burocratico, da ultimo con l'introduzione di un referente per la cybersicurezza nelle singole amministrazioni[77].

La distanza con gli analoghi sistemi sovranazionali è piuttosto da ricercarsi al cuore degli attributi della sovranità, nella (formale) imputazione e nel (concreto) esercizio dei poteri di decisione politico-amministrativa dello Stato. In questo senso permane, ed è anzi costantemente affinata da un legislatore che persegue la "maggiore concentrazione delle funzioni e delle azioni finalizzate alla prevenzione e al contrasto" delle minacce informatiche[78], la subordinazione dell'intero complesso istituzionale all'"alta direzione" e "responsabilità generale" del Presidente del Consiglio, che la esercita in via diretta o per mezzo di un'agenzia *sui iuris*[79] (ACN) sottoposta a penetranti poteri di controllo[80].

Se alla Presidenza[81], in veste di "super-ministero"[82], sono intestate rilevanti competenze strategiche e un'estesa potestà normativa[83], la cui *ratio* va ricercata nel ruolo di *sedes* istituzionale per l'armonizzazione delle politiche di sicurezza all'indirizzo governativo, l'Agenzia per la cybersicurezza costituisce la vera e propria 'centrale operativa' del sistema, garantendone il quotidiano funzionamento. "Autorità nazionale competente" e "punto di contatto unico" per le finalità di cui alla normativa europea[84], ACN assomma, talora inglobando strutture previgenti[85], le principali funzioni di regolazione, vigilanza, coordinamento operativo e certificazione, beneficiando di un generoso regime di autonomia e di poteri autoritativi corrispondenti a precisi obblighi informativi e di conformazione in capo ai destinatari[86].

L'assetto capillare del sistema viene in tal modo 'ricomposto' e razionalizzato attorno ad un'amministrazione di vertice, la quale unisce ad una costante opera di monitoraggio le concrete capacità per adottare tempestive misure di manutenzione preventiva o risposta difensiva. Ne risulta un'incrementata efficienza decisionale cui, nondimeno, fanno da contraltare criticità di rilievo: da un punto di vista

75 Ielo 2003: 376.
76 Su cui v. Ridolfi 2023.
77 Art. 8 l.n. 90 del 2024 su cui Longo 2024, Pietrangelo 2024.
78 Previti 2022: 92.
79 Ennesimo caso di 'fuga dal modello' normativo di agenzia (Merloni 2005).
80 Art. 2 d.l. n. 82 del 2021.
81 Nonché ai comitati in essa incardinati, ovvero il Comitato interministeriale per la cybersicurezza (CIC) e il Comitato interministeriale per la sicurezza della Repubblica (CISR).
82 Lauro 2021: 545.
83 Su cui Parona 2021.
84 Direttiva (UE) 2022/2555 (NIS 2) e Reg. (UE) 2019/881.
85 È il caso del nucleo per la cybersicurezza (NCS) e del CSIRT Italia, ora ricollocati in seno all'Agenzia.
86 *Ex multis*, Rossa 2023a, Forgione 2022, Golisano 2022, Parona 2021.

operativo, la 'burocratizzazione' dell'impianto sembra progredire a discapito di più agili corpi tecnici[87], mentre la perdurante impostazione securitaria della disciplina solleva questioni di legittimazione democratica ed equilibrio costituzionale. La completa avocazione del settore da parte dell'Esecutivo si risolve nella marginalizzazione *de facto* non solo delle minoranze parlamentari[88], bensì degli stessi operatori, pubblici e privati, che 'collaborano' con l'Agenzia da una posizione di sostanziale (e sanzionata) soggezione[89].

6. Alcune conclusioni. Concorrenza tra modelli, pianificazione strategica e amministrazione integrata

Da una pur sommaria ricostruzione dei suoi assetti strutturali, l'intero processo di emersione dell'ordinamento della cybersicurezza sembra potersi descrivere nei termini di un precario equilibrio tra modelli di regolazione antagonisti, o perlomeno concorrenti, di cui resta traccia nella fondamentale ambiguità delle relative scelte normative[90]: un modello reticolare-cooperativo, facente leva per lo più su soluzioni tecniche e connessioni informali tra strutture prettamente operative, e uno autoritario-accentrato, sulla falsariga degli organi statali investiti di funzioni afferenti alla sicurezza nazionale in senso lato. Le opposte matrici (*rationales*) dei due paradigmi si legano a più radicali concezioni della *governance* digitale, trasponendole nella prassi amministrativa. Si tratta, pertanto, in ultima istanza, di risposte di sistema a fronte delle sfide imposte a caratteri e funzioni della statualità classica[91].

Assodato che "*there is nothing fixed about internet governance arrangements in the same way there is nothing fixed about internet architecture*"[92], e che lo statuto del cyberspazio è ben soggetto ad opzioni ideologiche di fondo[93], il dibattito[94] ha prodotto, da un lato, l'idea di una *governance* distribuita a trazione privata e, dall'altro, la concezione securitaria di una sovranità statale proiettata nel digitale; la prima, fondata su postulati libertari[95], è poi evoluta in un approccio *multi-stakeholder* per la gestione condivisa di problemi globali, mentre la seconda, cercando di circoscrivere uno specifico dominio *cyber* statale e prediligendo il dialogo multilaterale tra i Governi, è parsa contribuire al più complesso fenome-

87 Ruohonen – Hyrynsalmi – Leppänen 2016: 750 ss. Indicativo, in questo senso, è lo *status* dei CSIRT regionali, tuttora di incerta natura e collocazione all'interno dell'architettura nazionale disegnata *ex lege*.

88 Caramaschi 2022, Lauro 2021: *passim.*

89 V. anche i dubbi di Longo 2024, Pietrangelo 2024.

90 Parona 2021: 9.

91 Pohle – Thiel 2020 e Mueller – Schmidt – Kuerbis 2013.

92 Denardis – Goldstein – Gross 2016: 20.

93 Il tema è il qualche misura presente già in Wu 1997.

94 Sul tema v. Natale 2022, Pohle – Thiel 2020, Odermatt 2018, Denardis, – Goldstein – Gross 2016, Liaropoulos 2016.

95 Celeberrima, in tal senso, è la sedicente Dichiarazione di indipendenza del Cyberspazio stesa da Barlow.

no di balcanizzazione della Rete[96]. Posteriore alla prima, la fortuna di quest'ultima prospettiva parte dalla lucida constatazione che "*the necessary authority and relevant resources to manage and regulate a wide range of activities in cyberspace reside largely in certain stakeholders—the states*"[97] e dal concreto assurgere del cyberspazio (comprensivo delle sue fondamentali infrastrutture fisiche) a nuova "dimensione della conflittualità"[98], il cui controllo alimenta tensioni geopolitiche facendone l'ultima frontiera del potere pubblico[99].

È uno sviluppo che ben si comprende alla luce di quel *mix* di conflittualità strategiche, crisi economiche e altri *shock* esogeni che, nell'ultimo quindicennio, ha via via condotto vari settori dell'attività amministrativa a teorizzare, o invocare, il ritorno dello Stato come attore primario della vita economica e sociale: un intervento la cui necessità, nell'ambito della cybersicurezza, non sembra potersi mettere in discussione, rivestendo una vitale funzione di presidio dei diritti dei cittadini-utenti, ma di cui vanno invece discusse le modalità. Si impone infatti l'esigenza irrinunciabile di conciliare con alcune garanzie fondamentali i nuovi paradigmi della sovranità digitale, la cui capacità di condizionare le stesse infrastrutture dell'esistenza sociale li rende potenzialmente più invasivi rispetto alle forme classiche del controllo statale[100]. In questo senso, il (parziale) divorzio della cybersicurezza nazionale dal regime dei servizi d'*intelligence* (che appare non solo incompatibile, ma del tutto antitetico rispetto alle esigenze di pubblicità e diffusione di quella)[101] ha certamente giovato ad una più radicata legittimazione del suo ruolo, ma restano da valutarne la capacità di aggiornamento e di coinvolgimento degli operatori privati[102] che, in un settore ad altissima obsolescenza tecnologica, costituiscono il più sicuro innesto di un'amministrazione efficace.

Traduzione, sul piano operativo, di una connotazione teleologica dell'impianto normativo, che assuma cioè le proprie finalità quale "più intimo significato" delle norme stesse[103], è l'orientamento strategico della conseguente azione amministrativa (come testimoniano i principali documenti d'indirizzo nell'ambito della transizione digitale)[104], fondata, nel caso della cyber-resilienza, sulla difesa dinamica di un ""fortino" degli interessi pubblici rilevanti attraverso un'interrelazione di soggetti preposti"[105] ai diversi livelli di intervento. In questo senso, il ritorno, nel cyberspazio, della politica degli Stati può rendersi un'occasione di sviluppo sinergico per il settore, archiviando il 'falso dilemma' che contrappone

96 Hill 2012.
97 Liaropoulos 2016.
98 Martino 2018.
99 Natale 2022, Denardis – Goldstein – Gross 2016.
100 È l'ammonimento di Pohle – Thiel 2020.
101 Sul tema Previti 2022: 81 ss., Sola 2022: 399 ss., Parona 2021: 8 s.
102 Longo 2024, Poletti 2023, Lauro 2021, Romano 2021.
103 Di Gaspare 1995.
104 Così, tra i molti esempi le citate strategie europee e nazionali per la cybersicurezza, ma anche la recentissima *Strategia italiana per l'intelligenza artificiale 2024-2026*.
105 Forgione 2022.

amministrazione aperta ed efficienza degli apparati[106]; a fronte di un cronico analfabetismo digitale, principale falla di qualsiasi sistema di cybersicurezza[107], la partecipazione amministrativa garantisce la diffusione circolare di cultura informatica a beneficio di tutti i soggetti coinvolti, siano essi funzionari pubblici, operatori economici, o cittadini-utenti.

A tal fine la "poliarchia"[108], che si realizza nella dispersione della funzione tra livelli e settori concorrenti all'interno di ordinamenti plurali, chiama in causa la capacità ordinante dell'organizzazione quale principio relazionale: "*un principe qui maintienne la distinction, mais qui essaie d'établir la relation*"[109], mappando l'attribuzione di un potere diffuso e ricomponendo l'amministrazione in funzione della collettività[110], con la doverosa consapevolezza "*que l'ordre ne signifie pas seulement les lois, mais aussi les stabilités, les régularités, les cycles organisateurs, et que le désordre n'est pas seulement la dispersion, la désintégration, ce peut être aussi le tamponnement, les collisions, les irrégularités*"[111]. Dalla risultante aggregazione dipenderà una più chiara definizione dell'ambito funzionale (nonché della relativa finalità), ma soprattutto l'effettiva possibilità del suo corretto perseguimento, assurgendo il modello organizzativo a componente essenziale dell'azione stessa di cybersicurezza nazionale: una funzione finalizzata al consolidamento della sovranità digitale, che, promuovendo l'adesione di cittadini e imprese agli obiettivi di sicurezza condivisa, ne assicuri al contempo una tutela diffusa.

Bibliografia

Bachelet, V. 1965, *Profili giuridici dell'organizzazione amministrativa*, Milano: Giuffrè.

Backman, S. 2023, "Risk vs. threat-based cybersecurity: the case of the EU", *European Security*, 32 (1): 85-103.

Battini, S. 2008, "Le due anime del diritto amministrativo globale", in AA. VV., *Il diritto amministrativo globale oltre i confini*, Milano: Giuffrè.

Battini S. 2016, "I due grandi dualismi alla prova del diritto (amministrativo) globale", in G. A. Benacchio – M. Graziadei, *Il declino della distinzione tra diritto pubblico e diritto privato*, Napoli: Editoriale Scientifica: 101-131.

Berti, G. 1968, *La pubblica amministrazione come organizzazione*, Padova: CEDAM.

Bower, J. L. – C. M. Christensen 1995 "Disruptive Technologies: Catching the Wave.", *Harvard Business Review*, 73 (1): 43-53.

Caramaschi, O. 2022, "La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari", *Osservatorio costituzionale*, 4: 69 ss.

Carbone, A. 2024, "Considerazioni generali sull'organizzazione amministrativa", *Federalismi.it*, 17: 25-63.

106 Come avviene in altri settori: Galli 2023.
107 Longo 2024, Rossa 2023b, Romano 2021, Montessoro 2019.
108 Dahl 1971.
109 Morin 2005: 4.
110 Franchini e Vesperini 2012.
111 Morin 2005: 4.

Cassese, S. 2001, "Le reti come figura organizzativa della collaborazione", in A. Predieri – M. Morisi (a cura di), *L'Europa delle reti*, Torino: Giappichelli: 43-48.
Cassese, S. 2002, "La signoria comunitaria sul diritto amministrativo", *Rivista italiana di diritto pubblico comunitario*, 2-3: 291-301.
Cassese, S. 2005, "Il diritto amministrativo globale. Una introduzione", *Rivista trimestrale di diritto pubblico*, 2: 331-357.
Chiara, p. G. 2023, "Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", *Rivista italiana di informatica e diritto*, 1: 143 ss.
Chiti, E. 2002, *Le agenzie europee. Unità e decentramento nelle amministrazioni comunitarie*, Padova: Cedam.
Chiti, E. 2016, "Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia e di difesa", *Diritto amministrativo*: 511 ss.
Chiti, E. 2021, "The Agencification Process and the Evolution of the EU Administrative System", in p. Craig – G. de Búrca (eds.), *The Evolution of EU Law*, Oxford: Oxford University Press: 123-155.
Chiti, M. p. , 2007, "L'organizzazione amministrativa comunitaria", in AA. VV. *Trattato di diritto amministrativo europeo*, Milano: Giuffrè: 415-466.
Contaldo, A. – F. Peluso 2018, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa: Pacini Giuridica.
D'Alberti, M. 2013, *Lezioni di diritto amministrativo*, Torino: Giappichelli.
Dahl, R. 1971, *Polyarchy: participation and opposition*, New Haven: Yale University Press.
Della Cananea, G. 2009, *Al di là dei confini statuali. Principi generali del diritto pubblico globale*, Bologna: Il Mulino.
Denardis, L. – Goldstein, G. – Gross, D. A. 2016, "The Rising Geopolitics of Internet Governance. Cyber Sovereignty V. Distributed Governance", Tech & Policy Initiative, Columbia SIPA.
Di Gaspare, G. 1995, voce "Organizzazione amministrativa", *Dig. disc. Pubbl*, X, Torino: Utet giuridica: 513 ss.
Eckhardt, Ph – Kotovskaia, A. 2023, "The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive", *International Cybersecurity Law Review*, 4: 147 ss.
Forgione, I. 2022, "Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", *Diritto amministrativo*, 4: 1113 ss.
Franchini, C. e Della Cananea, G. 2010, *I principi dell'amministrazione europea*, Torino: Giappichelli.
Franchini, C. e Vesperini, G. 2012, "L'organizzazione", in S. Cassese, (a cura di), *Istituzioni di diritto amministrativo*, Milano: Giuffrè: 73-130.
Frediani, E. 2010*, La produzione normativa nella sovranità "orizzontale"*, Pisa: ETS.
Galli, F. 2023, "Ambiente, amministrazione e democrazia. Sulla nuova relazione pubblico-privato nel sistema di diritto ambientale, tra etica partecipativa ed esercizio di sovranità", *Rivista Quadrimestrale di Diritto dell'Ambiente*, 3: 4-36.
Gasparri, W. 2024, *Lezioni di diritto amministrativo*, II, Torino: Giappichelli.
Giannini, M. S. 1957, "In principio sono le funzioni", *Amministrazione civile*, 1, 11 ss..
Giannini, M. S. 1986, *Il potere pubblico. Stati e amministrazioni pubbliche*, Bologna: Il Mulino.
Golisano, L. 2022, "Il governo del digitale: strutture di governo e innovazione digitale", *Giornale di diritto amministrativo*, 6: 824 ss.

Guarino, G. 1970, "Sulla utilizzazione di modelli differenziati nella organizzazione pubblica", in Id., *Scritti di diritto pubblico dell'economia*, Milano: Giuffrè.
Guarino, G. 1977, *L'organizzazione pubblica*, Milano: Giuffrè.
Hart, H. L. A. 1958, "Positivism and the Separation of Law and Morals", *Harvard Law Review*, 71: 593-629.
Hill, J. F. 2012, "A Balkanized Internet?: The Uncertain Future of Global Internet Standards", *Georgetown Journal of International Affairs*, 49-58.
Honneth, A. 2002 (1992), *La lotta per il riconoscimento*, Milano: Il Saggiatore.

Ielo, D. 2003, "Amministrazioni a rete e reti di amministrazione: nuovi paradigmi della "global governance"", *Amministrare*, 3: 373-403.
Irti, N. 1968, voce "Rilevanza giuridica", *Noviss. Dig. It*, XV, Torino: Utet: 1094 ss.
Lamberti L. – G. A. Primerano, 2016, "Il principio di efficienza ed i modelli organizzativi: le agenzie amministrative" in R. Cavallo Perin – A. Police – F. Saitta, *L'organizzazione delle pubbliche amministrazioni tra Stato nazionale e integrazione europea*, Firenze: University Press: 283 ss.
Lauro, A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", *Rivista Gruppo di Pisa*, 3: 529-545.
Liaropoulos, A. 2016, "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics", *Journal of Information Warfare*, 4: 14 ss.
Lippi, A. 2001, "Il policy making europeo come "rete"", in A. Predieri – M. Morisi (a cura di), *L'Europa delle reti*, Torino: Giappichelli: 1 ss.
Longo, E. 2024, "Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)", *Rivista italiana di informatica e diritto*, 1: 65-70.
Martino, L. 2018, "La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale", *Politica & Società*, 1: 61-76.
Matassa, M. 2022, "Una strategia nazionale a difesa del Cyberspazio", *p. A. Persona e Amministrazione*, 2: 625-653.
Merloni, F. 2005, "Le agenzie a cinque anni dal d.lgs. n. 300: l'abbandono del modello generale?", in G. Vesperini (a cura di), *La riforma dell'amministrazione centrale*, Milano: Giuffrè: 21 ss.
Merloni, F., "Organizzazione amministrativa e garanzie dell'imparzialità", *Diritto Pubblico*, 1: 57-100
Montessoro, p. L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", *Istituzioni del federalismo*, 3: 783 ss.
Morin, E. 2005, "Complexité restreinte, complexité générale", Colloque "Intelligence de la complexité: épistémologie et pragmatique" (Cerisy-La-Salle).
Mueller, M. – A. Schmidt – B. Kuerbis 2013, "Internet security and networked governance in international relations", *International Studies Review*, 15(1): 86-104.
Natale, G. 2022, "La cybersicurezza nazionale: la nuova frontiera della difesa dello Stato", *Rassegna Avvocatura dello Stato*, 1.
Nigro, M. 1966, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano: Giuffrè.
Nigro, M. 1988, voce "Amministrazione pubblica (Organizzazione giuridica dell')", *Enciclopedia Giuridica*, II, Roma: Treccani.

Odermatt, J. 2018, "The European Union as a Cybersecurity Actor", in: S. Blockmans – p. Koutrakos, (eds.), *Research Handbook on EU Common Foreign and Security Policy*, Cheltenham: Edward Elgar: 354-373.
OECD 2002, *Distributed Public Governance: Agencies, Authorities and other Government Bodies*, Paris: OECD Publishing, disponibile a https://doi.org/10.1787/9789264177420-en
Paleologo, G. 1981, voce "Organizzazione amministrativa", *Enciclopedia del diritto*, XXXI, Milano: Giuffrè: 135-151.
Parona, L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", *Giornale di diritto amministrativo*, 6: 709 ss.
Pauri, E. 2017, "Agency Reform in the time of Cybersecurity Governance: ENISA", *Luiss Law Review*, 2: 95 ss.
Perulli, p. 1998, "Forma Stato e forma rete", in Id., *Neoregionalismo. L'economia arcipelago*, Torino: Bollati Boringhieri.
Pietrangelo, M. 2024, "Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa", *Rivista italiana di informatica e diritto*, 1: 25-29.
Pohle, J. – T. Thiel 2020, "Digital sovereignty", *Internet Policy Review*, 9 (4).
Poletti, S. 2023, "La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica", *Media Laws*, 2: 398-410.
Previti, L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *Federalismi.it*: 65 ss.
Radoniewicz, F. 2022, "Cybersecurity in the European Union Law", in K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, (eds) *Cybersecurity in Poland*, Cham: Springer: 73-92.
Ridolfi, M. 2023, "Servizi di informazione e cybersicurezza", *Giornale di diritto amministrativo*, 2: 207 ss.
Romano, B. N., 2021, "Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"", *Amministrativamente*, 3: 545-594.
Romano, S. 1909, *Lo stato moderno e la sua crisi*, Pisa: Vannucchi.
Rossa, S. 2022, "Administrative Law Reflections on Cybersecurity, and on its Institutional Actors, in the European Union and Italy", *Italian Journal of Public Law*, 14 (2): 426-450.
Rossa, S. 2023a, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale Scientifica.
Rossa, S. 2023b, "Cyber attacchi e incidenti nella pubblica amministrazione, fra organizzazione amministrativa e condotta del funzionario", *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio III*, 17: 161-175.
Rossi, G. 2005, *Diritto Amministrativo*, I, Milano: Giuffrè.
Ruohonen, J. – S. Hyrynsalmi – V. Leppänen, 2016, "An outlook on the institutional evolution of the European Union cyber security apparatus", *Government Information Quarterly*, 33 (4): 746-756.
Serini, F. 2021, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", *Federalismi.it*, 12: 241 ss.
Slack, C. 2016, "Wired yet disconnected: the governance of international cyber relations", *Global Policy*, 7 (1): 69-78.
Sola, A. 2022, "Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale", *MediaLaws*, 3: 386 ss.
Wu, T. S. 1997, "Cyberspace Sovereignty? – The Internet and The International System", *Harvard Journal of Law & Technology*, 3: 647 ss.