Bruno Carotti

Uniformità e autonomia nella sicurezza cibernetica

Abstract: Il settore della sicurezza cibernetica consente prospettive inedite sull'attività amministrativa e sulle formule organizzative. L'analisi qui presentata muove da tre dicotomie che accennano a un movimento tellurico: l'esigenza di assicurare una direzione unitaria preservando l'autonomia dei soggetti coinvolti. Gli spunti presentati inducono a una riflessione su categorie note del diritto amministrativo, quali il coordinamento e l'autonomia nella sua accezione funzionale che, pur conservandosi nella loro essenza, impongono di essere osservate sotto una nuova luce, a testimonianza del modo di costruzione di questa branca del sapere, che deve muovere dal dato reale e non procedere per astrattismi.

Keywords: Cybersecurity, Uniformità, Autonomia, Disciplina istituzionale, Interesse Nazionale.

1. Introduzione

La sicurezza cibernetica contiene una dicotomia: una latente tensione tra uniformità e autonomia. Questa tensione è osservabile in una triplice dimensione: nelle decisioni (centralizzate e singole), nelle funzioni (collaborazione, scambio e unilateralità), nell'organizzazione (centro e periferia). Se ne analizzeranno di seguito tasselli e parti salienti. Questo consentirà di effettuare un primo tentativo ricostruttivo, ricorrendo, in special modo, alle figure del coordinamento e dell'autonomia, nella loro declinazione funzionale e innovativa. Gli equilibri sono altalenanti e mostrano una pittura ancora in corso, in cui alcuni particolari resteranno sfumati, mentre altri saranno definiti con pennellature finali, restituendo un'immagine di competenze e assetti.

Sarà necessaria una premessa, ricordando un interesse che permea l'intera disciplina e l'attività amministrativa che consegue a determinate scelte di politica settoriale.

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: 10.7413/197054760146

2. L'elemento unificante: l'interesse nazionale

L'interesse nazionale è centrale nell'ambito della sicurezza cibernetica. Il decreto-legge n. 82 del 2021 – tappa importante di un percorso iniziato, a singhiozzo, circa dieci anni prima – è chiarissimo in tal senso: lo pone alla radice dell'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), ne permea il funzionamento e tinge l'intero settore dei suoi pigmenti. Condiziona l'esercizio delle funzioni e funge da parametro di legittimità.

Questo ritorno all'interesse nazionale stupisce, in un contesto come quello attuale. Allo stesso tempo, non sorprende. Esso, infatti, ritorna con un fine specifico e latente: quello di consolidare gli interessi tutelati, intimi alla dimensione statale, e le istituzioni coinvolte nel settore, secondo un disegno che inquadra l'informatica all'interno dei fattori 'ad alta sensibilità' rispetto a funzioni fondamentali. In un contesto in cui gli attacchi sono aumentati vertiginosamente, e continueranno a farlo alla luce di interessi economici e strategici, crescono le preoccupazioni e i tentativi di risposta da parte dei decisori politici, prima ancora che tecnici[1].

Dietro la natura dell'interesse, dunque, si intravede un sostrato politico, sfociato nel tessuto giuridico, nel quale assume valenza e consistenza operativa. L'interesse nazionale giustifica la presenza di funzioni centrali, di capacità pervasive, di segretezza, di criteri unitari, di poteri di indagine e sanzionatori in capo a un apparato nazionale. Esso si correla, inoltre, all'ormai ben noto concetto di "perimetro", andando a costituire un *unicum* concettuale o, quantomeno, una dimensione simbolica, dove ambiti istituzionali diversi diventano attigui e vengono uniti da un collante omogeneo. La costruzione che ne risulta è lo Stato-Nazione, che torna a parlare e a indicare la necessità di agire in modo granitico.

La natura pregnante di tale interesse, comunque, non esaurisce la dimensione assiologica del settore. In un momento in cui la cessione di sovranità è ancora in essere (11 Cost.) e dove l'Unione europea gioca ancora un ruolo primario, non può non considerarsi la dimensione sovranazionale. L'interesse nazionale si piega solo al suo cospetto: le più scottanti innovazioni in materia, del resto, derivano dall'attuazione di atti normativi sovranazionali, a partire dalla direttiva Nis, per arrivare alla sua revisione (Nis 2), passando per il *Cybersecurity Act* e per il recente *Cyber Resilience Act*[2]. Sono atti normativi che raccordano gli Stati membri in un insieme unitario e, nel rispettarne le unicità, le uniscono in modo indelebile.

1 "*Throughout the latter part of 2023 and the initial half of 2024, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences*": ENISA, *Threat Landscape July 2023-July 2024*, September 2024 (su https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024). L'ENISA ha osservato, in un arco temporale annuale, più di undicimila attacchi riguardanti l'Unione europea, che presenta un tasso di rischio maggiore nel contesto globale: *ivi*, p. 11-12.

2 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022*, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2),* e il Regolamento UE n. 2841/2023, del Parlamento europeo e del Consiglio, del 13 dicembre 2023, *che stabilisce misure per un livello comune elevato di cibersi-*

Dunque, sul versante europeo, diviene – paradossalmente – un altro elemento di integrazione, che spinge verso le sue componenti più dure e legate al concetto di sovranità; sul piano nazionale, legandosi alla sicurezza dello Stato, intende colmare un divario storico che ha caratterizzato l'ordinamento nazionale. In via consequenziale, sia nella disciplina interna, sia nella legislazione europea, si osserva la preoccupazione di unire le forze e far fronte a esigenze di sicurezza cibernetica, sia in difesa che in attacco[3]. Il costrutto richiede unità di intenti e condivisione: se ne osserveranno le forme giuridico-istituzionali[4].

La disciplina vigente si inserisce in questo scenario. Un interesse unitario, dentro e oltre lo Stato, indirizza le forme e i modi dell'attività istituzionale. Un contesto innovativo, come quello informatico, si avvicina all'età adulta senza mostrare, però, segni di maturità: dell'informatica sono ormai note non solo le potenzialità, ma anche i rischi e, in particolar modo, gli usi distorti che possono essere realizzati da singoli, organizzazioni sociali, e persino da istituzioni. I diversi utilizzi della tecnica sono essenziali, anche in questo caso, per comprendere le dinamiche sottostanti.

3. La dicotomia decisoria

Concentrandosi sull'ordinamento nazionale, non vi sono dubbi sulla portata centralizzatrice dell'Agenzia per la cybersicurezza nazionale (ACN) sul piano decisorio. La sua posizione istituzionale, seppur complessa e divisa tra apparati tecnici e di sicurezza (anche in senso tradizionale), è chiarissima[5]. Allo stesso tempo, le competenze non sono interamente attratte presso l'ente: la definizione di alcuni aspetti lascia impregiudicate le attività e le scelte delle singole amministrazioni. Essa svolge una funzione di sostanziale standardizzazione, di definizione di livelli comuni da interpretare quali soglie minime di rispetto. Il quadro d'insieme è com-

curezza nelle istituzioni, negli organi e negli organismi dell'Unione; Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, *relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013* ('regolamento sulla cibersicurezza'); Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, *sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011*.

3 Decreto-legge 14 giugno 2021, n. 82, recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, convertito, con modificazioni, nella legge 4 agosto 2021, n. 109, art. 7.

4 Si veda il *considerando* 3 del citato Regolamento n. 2841/2023: "gli ambienti tecnologici dei soggetti dell'Unione sono interdipendenti, utilizzano flussi di dati integrati e sono caratterizzati da una stretta collaborazione fra i loro utenti. Tale interconnessione significa che qualsiasi perturbazione, anche se inizialmente limitata a un solo soggetto dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata su altri soggetti dell'Unione" (con enfasi sugli aspetti di interconnessione e sulla interdipendenza reciproca, sia in casi fisiologici che patologici).

5 Sul rapporto tra funzione di sicurezza come parte centrale nella costruzione dello Stato e suo sviluppo in ambito informatico, si veda Ursi 2025.

plesso e piuttosto articolato, probabilmente anche a causa della 'giovane età' delle funzioni esercitate dall'agenzia.

Alcuni aspetti consentono di intuire il concreto modo di operare di questo sistema. Il primo è costituito dalle azioni comuni che, per disposizione normativa, sono dirette a realizzare gli ampi obiettivi affidati all'agenzia, in termini di sicurezza e resilienza (ancorate allo sviluppo della digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e, quindi, del "sistema" Paese).

Le azioni comuni integrano linee di indirizzo che dovranno essere seguite da parte di tutti i soggetti che, a vario titolo, partecipano al (e possono causare alterazioni nel) sistema della sicurezza cibernetica[6]. Ciò che desta interesse è che tali linee muovono da una certa altitudine, ma possono scendere di quota e diventare vere e proprie determinazioni concrete. Dallo schema normativo non traspare il punto di caduta: segno dell'ampio raggio che si può percorrere nel momento applicativo. Le azioni comuni, in questo senso, mostrano un assetto particolare all'interno del panorama decisorio settoriale: svelano l'esigenza di agire in modo coerente e non frammentato, richiedono il riconoscimento di un soggetto qualificato che possa contribuire all'unità, impongono il rispetto delle indicazioni (pena la frustrazione degli obiettivi e la comminazione di sanzioni)[7]. Il dato normativo è sintetico, ma dalla sua lettura scaturisce un evidente grado aumentato di articolazione. Il significato complessivo appare quello di conseguire un obiettivo di unità complessiva in modo calibrato, che non tralasci le singole istanze, ma realizzi un dosaggio composto di interventi[8].

Un altro esempio di oscillazioni si rinviene nella prassi amministrativa e nei documenti dell'Agenzia. All'interno dei *Key performance indicators* sono stabiliti gli obiettivi, indicati i metodi di attuazione, illustrati gli incontri istituzionali. Questa breve trilogia rivela una presenza forte dell'ACN dinanzi altre amministrazioni, chiamate a seguire le indicazioni della prima e a conformare – in via tendenziale – la propria attività, al fine di assicurare misure di contrasto ai rischi informatici[9].

In modo più pregnante opera, invece, l'attività di certificazione di componenti e prodotti, che possono entrare a far parte del patrimonio *hardware* delle amministrazioni solo se ritenute privi di pericolo insiti, vale a dire derivanti da modalità di costruzione, *backdoor*, assenza di falle, resistenza a eventuali attacchi malevoli. La certificazione agisce sul sistema degli appalti e consiste, per quanto qui di inte-

6 In altre parole, tutti i soggetti che utilizzano o erogano sistemi informativi e servizi informatici che possono avere un impatto rilevante sull'interesse nazionale.

7 Matassa 2025.

8 Si veda l'art. 7, comma 1, *lett. a)*, del d.l. n. 82 del 2021, in base al quale l'ACN "promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore".

9 Si veda il documento dell'ACN denominato *Manuale operativo. Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026*, del dicembre 2022, disponibile all'indirizzo https://www.acn.gov.it/portale/documents/20119/87708/ACN+Manuale+Operativo+implementazione+misura-82.pdf/ba48be5f-1e69-6b15-8fb9-2d48e52d0d74?t=1704460313679.

resse, nel livellamento delle decisioni su eventuali acquisti, anche in relazione alla possibile inclusione dei prodotti in listini stilati dalle centrali di committenza. In una dichiarazione del G7 le attività di certificazione sono state definite espressamente come uno dei perni del sistema-Paese[10].

Questa funzione, aderente al concetto di perimetro nazionale[11], si pone al confine tra funzione di collaborazione e controllo, tra sostegno e imposizione. La stessa struttura organizzativa, divisa tra centri e laboratori[12], rivela una tendenza all'uniformità, senza che però si comprima del tutto l'autonomia dei singoli centri decisionali. L'interesse nazionale, già richiamato, presidia i rapporti tra differenti strutture e li unisce idealmente.

Non può sottacersi, infine, la strategia nazionale per il *cloud computing*, che ha dato vita al Polo strategico nazionale (PSN), quale infrastruttura tecnologica ormai centrale nel settore pubblico, sulla quale la migrazione dei servizi delle amministrazioni sta crescendo in maniera esponenziale[13]. Una simile strategia mostra, infatti,

10 Il gruppo, si legge nel documento di maggio 2024, "ha discusso di come operare per favorire insieme agli operatori delle infrastrutture critiche la sicurezza dell'intera catena di approvvigionamento, per ridurre fortemente il rischio che componenti tecnologiche possano diventare veicolo per la diffusione di un attacco alle reti infrastrutturali. Un settore in cui è importante applicare il principio di security-by-design attraverso l'acquisizione di componenti che rispondano ad alti standard di sicurezza". Gli stati membri hanno affermato che "[c] oopereremo sempre meglio e ci consulteremo tutte le volte che ne avremo la necessità. Questo è l'impegno che abbiamo assunto insieme. Scambieremo informazioni sulle principali minacce cyber che riguardano le infrastrutture critiche, sugli incidenti, nonché sulle misure di sicurezza che possono essere adottate dagli operatori critici per farvi fronte. Crediamo tutti molto nel coordinamento con il settore privato. In questo senso la nostra Agenzia, forte dell'esperienza della Legge Perimetro ha una naturale propensione a sviluppare l'interazione con il mondo delle imprese e quello della ricerca".

11 Buoso 2025; consentendo il rimando, Carotti 2020.

12 In particolare, il Centro di valutazione e certificazione nazionale (CVCN) è stato istituito dal decreto-legge 21 settembre 2019, n. 105, recante recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, convertito, con modificazioni, nella legge 18 novembre 2019, n. 133. Si veda, in materia, anche il d.P.R. 5 febbraio 2021, n. 54, recante *Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*. Sui poteri dell'Agenzia in materia, si può fare riferimento all'art. 7, comma 1, *lett. e)*, d.l. n. 82 del 2021. Il CVCN, inizialmente istituito presso l'allora Ministero dello Sviluppo economico, è poi transitato nelle strutture dell'ACN; si coordina con i Centri di Valutazione (CV) istituiti presso i Ministeri della Difesa e dell'Interno e può avvalersi del supporto di una rete di Laboratori accreditati di prova (LAP), così realizzando un modello di collaborazione pubblico-privato. Si v. Previti 2024.

13 Come noto, si tratta di una infrastruttura informatica destinata a ospitare sistemi e servizi forniti dalla pubblica amministrazione mediante un *cloud* nazionale e centralizzato, che risponda alle maggiori garanzie di affidabilità, resilienza e indipendenza. Ricompreso tra le missioni del Piano nazionale di ripresa e resilienza (PNRR), quale obiettivo strategico di utilizzo alle tecnologie del *cloud computing*, il PSN ha visto la luce nel 2021, con la definizione del modello e l'affidamento a un partenariato che ne ha consentito la realizzazione effettiva. La vicenda è finita dinanzi agli organi di giustizia amministrativa: Consiglio di Stato, sez. V, 24 ottobre 2023, n. 9219, che ha determinato l'illegittimità della procedura di scelta, senza però poter determinare il subentro nel contratto, in ragione delle disposizioni sugli

una funzione di decisa preminenza dell'ACN, che vincola le scelte delle singole amministrazioni mediante un preventivo controllo. Rileva, da un lato, l'attività di qualificazione di dati e servizi della pubblica amministrazione (necessaria a comprenderne la natura e la portata, per poi poterne definire la destinazione e il livello di sicurezza all'interno del PSN), così come la qualificazione dei servizi in *cloud* offerti alle amministrazioni da parte di terzi (al fine di rivolgersi solo a soggetti qualificati e in grado di offrire idonee garanzie). Queste funzioni sono transitate dall'Agenzia per l'Italia digitale (AGID) all'ACN, ormai *pivot* del processo che, nel quadro della costruzione dell'infrastruttura nazionale, analizza e classifica i sistemi informatici delle singole amministrazioni. L'ACN condiziona amministrazioni e mercato, in quanto la qualificazione dei servizi offerti ha puntuali effetti sulle scelte delle singole istituzioni e sul novero dei soggetti abilitati a offrire determinati servizi in ambito pubblico[14].

L'ambito decisorio, in sintesi, determina effetti innegabili sulla sicurezza cibernetica. I relativi compiti sono diversi e articolati. Alcuni di essi spettano agli apparati centrali, altri sono lasciati alle singole istituzioni[15]. Il loro esercizio denota un assetto complessivo in costante movimento, nella ricerca di una soluzione ottimale, che non è statica e si rivela complessa e difficile da raggiungere.

4. La dicotomia funzionale

Un equilibrio oscillante, ancora incerto, e forse necessariamente destinato a rimanere tale, caratterizza l'esercizio delle funzioni in materia di cibersicurezza.

affidamenti operanti nel quadro del Pnrr (in particolare, l'art. 48, comma 4, del decreto-legge 31 maggio 2021, n. 77, recante *Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*, convertito, con modificazioni, con legge 29 luglio 2021, n. 108, che richiama l'art. 125 del *Codice del processo amministrativo*). Sul piano normativo, si veda, originariamente, l'art. 33-*septies* del decreto-legge 18 ottobre 2012, n. 179, recante *Ulteriori misure urgenti per la crescita del Paese*, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221. A ottobre 2024, la migrazione al PSN è stata effettuata da quattromila amministrazioni (fonte: https://www.polostrategiconazionale.it/media/stampa/comunicato-obiettivi-pnrr-2024-oltre-100-amministrazioni/).

14 Il regime di qualificazione dei servizi offerti alla pubblica amministrazione è ora definitivamente acquisito tra le competenze dell'ACN: da ultimo, si v. il regolamento adottato con decreto direttoriale 27 giugno 2024, n. 21007, in vigore dal 1° agosto 2024.

15 Rilevante, a questo riguardo, la proposta di legge attualmente in discussione presso la Regione Toscana, che nel quadro della ormai consolidata innovazione digitale, si occupa di sicurezza, intelligenza artificiale e tutela dei singoli, ricercando anche una migliore postura dei dispositivi utilizzati. La Regione ha introdotto anche un proprio CSIRT, quale ulteriore nodo di una complessa rete istituzionale. Si tratta della "*Proposta di Legge n. 272 – Modifica della deliberazione di Giunta regionale che ha approvato la proposta di legge n. 1/2024 (Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla L.R. 54 del 2009)*", del 29 luglio 2024, approvata il successivo 27 novembre (https://iterlegis.consiglio.regione.toscana.it/#/atto/66b5cb6ad56f26046a7eff9f/).

In merito, rilevano tre aspetti: un primo ambito fa emergere lo scambio di informazioni e la cooperazione (termine conservato volutamente, sebbene l'ambito semantico, come si osserverà in chiusura, rinvia a un orizzonte concettuale noto, ma da tenere sotto osservazione); un secondo concerne la definizione di obiettivi comuni, che orientano l'esplicarsi delle funzioni stesse; un terzo riguarda la presenza e l'esercizio dei poteri unilaterali.

Innanzi tutto, l'impianto normativo, anche nei testi più recenti, conferma il ruolo centrale dello scambio di informazioni, vitale per la sicurezza informatica all'interno dell'Unione e degli Stati membri[16]. Si tratta di un riflesso della polimorfia istituzionale e dell'essere la sicurezza cibernetica una materia 'giovane'. Da un lato, infatti, la presenza di numerosi soggetti istituzionali impone di raccordarne le funzioni per assicurare, mediante l'apporto di ciascuno, un effetto su vasta scala; un metodo che appare preferibile rispetto a un'imposizione centralizzata. Dall'altro lato, poiché si richiedono ancora tempo ed esperienza per irrobustire gli ambienti informatici, appare maggiormente congeniale la condivisione del 'sapere' da parte dei soggetti con maggiori risorse; questo avviene, tipicamente, con il consolidamento di apparati centrali, ma il diffondersi di conoscenza e capacità potrà determinare un riequilibrio, assicurando la compartecipazione dei diversi nodi esistenti, in un complesso sistema reticolare fondato sullo scambio (sia biunivoco, sia multilaterale).

Questo duplice orientamento si nota anche nelle formule normative. La rete chiamata a risolvere gli incidenti informatici (*CSIRT Network*) deve informare le istituzioni preposte, attuare una "risposta coordinata" e assicurare agli Stati membri un'adeguata assistenza, qualora emerga una rilevanza transfrontaliera degli incidenti. Simili funzioni si traducono in forme morbide di coordinamento, in cui si sfrutta la presenza dei nodi della rete – presenti all'interno degli Stati membri – per conseguire una reazione più efficace, basata sull'apporto di ciascuno.

Specifici aspetti, peraltro, meritano attenzione. Ad esempio, sempre in riferimento alla rete degli CSIRT, il *considerando* n. 47 e l'art. 15 della direttiva NIS 2 recano il termine *cooperazione operativa*[17]. L'aggettivo utilizzato sembra far compiere un passo ulteriore rispetto alle attività condotte e sembra indicare l'obiettivo – stabilito in via legislativa – di rendere effettiva l'attività di scambio e collaborazione svolta tra amministrazioni interessate. Un passaggio che denota il superamento del mero aspetto formale o burocratico, per andare a toccare il mondo complesso

16 Si veda, in questo senso, il citato Regolamento n. 2023/2841, il cui *considerando* n. 4 ritiene "necessario che i soggetti dell'Unione raggiungano un livello comune elevato di cibersicurezza attraverso l'attuazione di misure di gestione dei rischi di cibersicurezza commisurate ai rischi per la cibersicurezza individuati, lo scambio di informazioni e la collaborazione". Questo aspetto è in perfetta continuità con il settore delle comunicazioni elettroniche, in cui peraltro affondano le radici dell'ENISA. Sulla collaborazione in questo settore, Carotti 2011.

17 *Considerando* n. 47: "[l]a rete di CSIRT dovrebbe continuare a contribuire al rafforzamento della fiducia e a promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri". La dizione si trova quindi ai paragrafi 1, 2, *lettere j*), *k)* e *p)*, e 4, dell'art. 15 citato nel testo.

dell'effettività[18]. Si è al confine della teoria della norma: non bastano più i caratteri formali, mentre occorre la produzione di effetti nel mondo reale, quasi secondo un avvicinamento alla dimensione extragiuridica. La concretezza dei sistemi informatici, del resto, richiede un approccio realistico.

La cooperazione, confermandosi essenziale, vede allargarsi il suo campo di applicazione, a testimonianza della orizzontalità necessaria in questo ambito e della "convivenza funzionale" tra le istituzioni poste in posizioni centrale e quelle laterali (competenti su ambiti territoriali definiti o su materie più ristrette), che si possono considerare come poste alla 'periferia' del sistema[19]. La necessità di una complessiva convivenza delle funzioni nei vari ambiti, mediante un raccordo, testimonia la tensione tra la ricerca di orientamenti uniformi e la conservazione di margini di apprezzamento da delle singole amministrazioni. Un vero e proprio coacervo, che mostra la difficoltà di ricondurre a sistema un ambito di per sé molto complesso, ancora non idoneo a esprimere una sostanziale unità, nemmeno sotto il profilo funzionale.

Questo assetto risponde, in ogni caso, all'unitarietà di interessi e obiettivi sottesi alla normativa. Un unitario interesse di fondo, collegato a una dimensione non solo nazionale, ma europea permea la cooperazione e lo scambio di informazioni. Emerge, al riguardo, una tenenza ben precisa, che cerca di superare la difficoltà di compiti già affidati a soggetti esistenti e, senza comprimerli o eliminarli, li riconduce a una dimensione unitaria. Ciò avviene – è il secondo aspetto annunciato in apertura – mediante la definizione di obiettivi, livelli e soglie di protezione comuni, la cui assicurazione condiziona le forme di "collegamento" tra istituzioni, centri e relative articolazioni. La dinamica del sistema è instabile e produce formule sperimentali: ad esempio, il gruppo di collaborazione istituito in ambito europeo ha, tra gli altri, l'obiettivo di esaminare le attività dei singoli componenti in ordine alle misure di gestione e di segnalazione dei rischi, secondo un metodo di verifica che si svolge tra pari[20].

Infine, con riferimento ai poteri unilaterali, dalla relazione annuale dell'Agenzia[21] emergono attività diverse, dal supporto nell'esercizio di compiti tecnici all'accesso ai locali, secondo un quadro complessivo di attuazione concentrata nelle

18 Falzea 1965.

19 Si veda l'art. 13, par. 4, della Direttiva NIS 2: "[a]l fine di garantire l'efficace adempimento dei compiti e degli obblighi delle autorità competenti, dei punti di contatto unici e dei CSIRT, gli Stati membri, nella misura del possibile, provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra i suddetti organismi e le autorità di contrasto, le autorità di protezione dei dati, le autorità nazionali ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139, gli organismi di vigilanza a norma del regolamento (UE) n. 910/2014, le autorità competenti a norma del regolamento (UE) 2022/2554, le autorità nazionali di regolamentazione a norma della direttiva (UE) 2018/1972, le autorità competenti a norma della direttiva (UE) 2022/2557, nonché le autorità competenti ai sensi di altri atti giuridici settoriali dell'Unione".

20 Si tratta del "gruppo di cooperazione" di cui all'art. 14 della Direttiva NIS 2, il quale, in base all'art. 19, par. 2, svolge la revisione tra pari del gruppo assicurando, tra le altre cose, "il livello di attuazione delle misure di gestione e delle prescrizioni in materia di segnalazione dei rischi di cibersicurezza […]"; dunque, è in grado di incidere piuttosto a fondo sulle singole istituzioni, raccordandole agli obiettivi unitari e al centro costituito per la loro cura.

21 Relazione annuale per l'anno 2023 presentata dall'ACN, disponibile su https://www.acn.gov.it/portale/documents/20119/446882/ACN_Relazione_2023.pdf.

mani dell'ente centrale, sempre più perno del sistema, ma pronto ad aprirsi alla voce e alla collaborazione di quelli periferici.

5. La dicotomia organizzativa

Esiste un'uniformità organizzativa in materia? Vi è una distinzione tra centro e periferia?

L'impianto organizzativo, che costituisce una ricaduta di quello funzionale[22], testimonia una chiara tendenza alla centralizzazione (come emerge dalla presenza necessaria dell'ACN, dalla sua funzione di raccordo con gli altri soggetti dell'Unione europea, dalla sua preminenza nell'assicurare il più volte richiamato interesse nazionale)[23]. L'innegabile tendenza all'unità non implica una sovra-ordinazione gerarchica, ma un esercizio di funzioni in modo accentrato. È qui che risiede la terza dicotomia che, insieme alle altre due, svela la tensione latente dell'intero impianto.

Secondo il dettato normativo, l'ACN promuove competenze, risponde a crisi, definisce livelli comuni e standard di protezione, creando un minimo comun denominatore che opera anche per i soggetti privati: non si determina, però, un'integrazione strutturale. In ambito organizzativo, infatti, si osservano due fenomeni: la fuga dalla sovra-ordinazione gerarchica e la rispondenza delle strutture a soglie di protezione comuni e ai controlli conseguenti.

Evidente, in merito, quanto avviene all'interno dell'Unione europea. Si prenda il caso del Comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board* – IICB), che attraverso i rappresentanti istituzionali si inscrive all'interno della rete delle agenzie dell'Unione europea (*EU Agencies Network* – EUAN)[24]. Esso assicura l'attuazione delle disposizioni e l'osservanza degli indirizzi impartiti da parte dei "soggetti dell'Unione"[25]; svolge funzioni di monitoraggio e

22 Nigro 1967; Giannini 1993.

23 Si v. l'art. 7, comma 1, *lettera d*), d.l. n. 82 del 2021, ai sensi del quale l'ACN è "l'autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento". La disposizione si può leggere in coordinamento con l'art. 8, par. 4, della direttiva NIS 2, in base al quale "[o]gni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonchéé per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro". Da notare che, ai sensi del successivo art. 9, par. 2, laddove "uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche ai sensi del paragrafo 1, esso indica chiaramente quale di tali autorità deve fungere da coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala".

24 Ai sensi dell'articolo 10, paragrafo 3, del Regolamento, siedono all'interno l'IICB rappresentanti designati da diversi soggetti dell'Unione europea (dal Parlamento alla Corte di giustizia, dal Comitato economico e sociale al Garante europeo per la protezione dei dati, per un totale di diciotto rappresentanti).

25 Art. 12, par. 1, Regolamento n. 2023/1248: "controlla efficacemente che i soggetti dell'Unione attuino il presente regolamento e gli indirizzi, le raccomandazioni e gli inviti a intervenire da loro adottati".

verifica, intervenendo in caso di mancata rispondenza agli atti adottati in base al nuovo quadro normativo, secondo un sistema di risposte 'in progressione' (che possono arrivare al distacco dei sistemi di comunicazione da parte dei soggetti che non mitigano il rischio e mettono in pericolo gli altri, nonché a segnalazioni volte a verificare il corretto uso delle risorse finanziarie messe a disposizione in caso di inosservanza)[26].

L'IICB opera "al fine di contribuire all'instaurarsi di un livello comune elevato di cibersicurezza tra i soggetti dell'Unione". L'espressione "livello comune" suscita interesse: lascia intendere che il comitato fissa condizioni minime di protezione, rimettendo la scelta delle singole misure – e la loro profondità – ai centri decisionali coinvolti. Gli aspetti organizzativi non sono estranei allo svolgimento di tali compiti: sono necessari a perfezionare e a rendere possibile questo *modus operandi*, così come il controllo "tra pari" circa l'adeguatezza delle scelte[27]. Al posto di un'organizzazione uniformata (e uniformante) si perseguono forme più labili e indefinite. Queste ultime consentono di raggiungere un'unità di intenti senza l'irrigidimento di un'organizzazione centrale o relazioni gerarchiche.

Va aggiunto che, mentre in ambito nazionale l'interesse è unidirezionale, in quello europeo si rispetta l'autonomia degli Stati: al fondo, permane l'idea di un rapporto dialettico tra i singoli nodi della rete, dislocati negli ordinamenti nazionali. L'ordinamento europeo raccorda le diverse strutture, senza comprimerle[28]. La tecnica utilizzata è, dunque, quella di 'centralizzare uniformando', con la conseguenza di incidere solo su alcuni aspetti, lasciandone aperti altri: una tendenza calibrata all'unità, 'senza esagerare', che potrebbe definirsi 'centralizzazione gentile'[29].

È qui che, come si vedrà a breve, si innesta l'importanza del coordinamento: una conseguenza logica, che si incastona all'interno del disegno complessivo, e che è destinato a divenire un perno dei rapporti tra strutture (oltre a consentire una prima riconduzione a categorie generali).

26 Art. 12, par. 1, *lett. f)*, Direttiva NIS 2.

27 Ai sensi dell'art. 11, par. 1, *lett. d)*, reg. n. 2023/2847, il comitato "stabilisce la metodologia e gli aspetti organizzativi per lo svolgimento di riesami *inter pares* volontari da parte di soggetti dell'Unione".

28 Questo vale anche sul piano funzionale: si consideri l'art. 9 par. 4, della Direttiva NIS 2, rubricato "*Incidenti e crisi su vasta scala*", in base al quale sono definite dallo Stato "le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale generale di gestione delle crisi e i canali di scambio di informazioni". In una sola disposizione emerge una progressiva integrazione, attraverso le attività delle amministrazioni dei singoli stati che confluiscono in un alveo comune sul piano funzionale, mentre dell'osservanza del tessuto normativo rispondono anche gli Stati, con un gioco di equilibri che spinge al rispetto del quadro adottato.

29 Si veda, da questo punto di vista, l'art. 32 della direttiva NIS 2, rubricato "*Misure di vigilanza e di esecuzione relative a soggetti essenziali*". Gli Stati membri provvedono affinché "le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso" (ai sensi del par. 1) e "le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporrei" i soggetti interessati "come minimo" a ispezioni, *audit*, scansioni, ecc. (in base al par. 2).

In modo connesso, emerge *a latere* il rapporto tra centro e periferia: inteso in modo non formalistico, esso si manifesta *in nuce*, con gradi di intensità non assoluti. Questo aspetto sembra rispondere a una diversa sfida, di natura politica ed economica, più che giuridica: concerne l'assetto generale, per ora incontrastato, dell'oligopolio tecnico operante su scala internazionale, caratterizzato dalla concentrazione in poche mani dell'uniformità delle tecnologie e dei processi di raccolta dei dati[30]. Il rafforzamento delle strutture e l'unione delle loro forze, in un insieme diversificato ma coerente, sono il modo per fronteggiare in modo unitario le capacità di soggetti che hanno acquisito un potere enorme e ancora incontrastato, al fine di mitigare gli effetti sfavorevoli o nocivi dello stato attuale dell'informatica e dei suoi rapporti con il potere. I poteri tecnici si accompagnano necessariamente al potere politico, che li usa a proprio vantaggio a diversi fini: dalla politica interna a quella estera. Un maggiore rafforzamento delle 'periferie' statali in un quadro unitario sembra orientata, dunque, a creare e contrapporre una propria voce a potenze economiche dominanti. Resta aperto il problema di quanto sia possibile fare contro gli stessi poteri pubblici, come i governi che usano gli apparati tecnologici per fini non compatibili con un assetto democratico. Una risposta adeguata ed efficace appare, a oggi, ancora inevasa[31].

6. Possibili ricostruzioni

Dalla pur breve disamina effettuata, in cui si è cercato di cogliere indizi e tratti generali, si affaccia l'accennata tensione tra le esigenze di uniformità e autonomia. La ricerca di soluzioni comuni e unitarie è funzionale a garantire una postura di maggiore sicurezza di fronte a scenari critici; l'ambito riservato all'autonomia è necessario a fronte della impossibilità di esercitare le competenze in modo univoco, per tutti i soggetti coinvolti. Questa tensione non è risolta in modo rigido, ma elastico. Salve future evoluzioni, che dipendono anche dallo scenario internazionale – cui la sicurezza cibernetica è intrinsecamente connessa – questo assetto è destinato a perdurare in un mutevole e delicato equilibrio.

Le dinamiche sottese, pur movimentate, consentono di delineare alcuni aspetti ricostruttivi.

Innanzi tutto, è in corso una ridefinizione dei poteri decisori di maggior impatto sulla sicurezza cibernetica a parziale vantaggio del centro. Questa tendenza è, allo stato, prevalente e la forza centripeta aumenta di intensità: da un lato, gli enti centrali dello Stato (l'ACN) e dell'Unione si stanno consolidando; dall'altro lato, l'elasticità non scompare affatto, e limita l'attrazione della componente decisoria. Quest'ultima non si presenta ancora a tutto tondo, ossia in grado di com-

30 Su tutti, Wu 2020.

31 Il caso della Corte costituzionale romena, che ha annullato le recenti elezioni presidenziali, ne costituisce un esempio lampante. Primi riferimenti possono essere trovati in questo commento di Selejen-Gutan 2024. La sentenza è comunque oggetto di diverse e contrastanti letture.

prendere ogni aspetto connesso alla sicurezza cibernetica: tuttavia alcuni profili, connessi alla definizione di livelli minimi di tutela e degli obiettivi da perseguire, sono attratti al centro (è quanto avviene con la certificazione). Il fine è quello di assicurare una maggiore uniformità, a sua volta funzionale ad aumentare l'efficacia della protezione.

In secondo luogo, il piano funzionale denota un'oscillazione tra uniformità e autonomia più evidente: le funzioni presentano un maggior tasso di distribuzione; il consolidamento avviene senza elidere la componente pluralistica, ma riconoscendo l'apporto di tutti i soggetti competenti. Le istanze unitarie, quindi, sono limitate al raggiungimento di una coerenza complessiva.

In terzo luogo, il piano organizzativo mostra una tendenza biunivoca ancor più bilanciata. La centralizzazione si nota in figure istituzionali di carattere forte, come l'ACN. I centri organizzativi di raccordo, di converso, assumono una forma ibrida, fungendo da snodo per interessi non solo periferici, ma anche centrali, mettendo in comunicazione istanze nazionali e sovranazionali (come avviene con gli apparati preposti alla sicurezza interna ed esterna).

Queste tre dicotomie, che possono orientare la lettura della disciplina della cibersicurezza, spingono a interrogarsi sulle categorie generali: non intravedendosi terre sconosciute – o rare, per restare nel mondo della tecnologia – è comunque possibile ravvivarne l'interpretazione e attualizzarle. Le categorie utilizzabili si stagliano attorno a due picchi: il coordinamento e l'autonomia funzionale.

Il primo, come noto, delinea un *modus agendi* idoneo a collegare soggetti privi di una relazione gerarchica, al fine di assicurare l'uniformità dell'attività. Storicamente, sia nella prassi amministrativa che nella ricostruzione della letteratura, il coordinamento si consolida nel momento in cui viene superato l'assetto monista degli interessi e, dunque, con l'affermarsi dello Stato pluriclasse; mostra, quindi, una sostanziale variazione nell'esercizio delle funzioni, mutando le modalità del momento decisorio[32]. La coesistenza di vari interessi, l'assenza di sovra-ordinazione (quantomeno parziale), la necessità di ascoltare più voci lo hanno reso un cardine nella ricostruzione delle forme di esercizio dell'attività amministrativa; rivela la ricerca di una forma sostanziale di collegamento, che preservi le prerogative dei singoli soggetti istituzionali e apra un metodo aperto, salvaguardando al tempo stesso pluralità, unitarietà e autonomi[33], secondo lo spirito repubblicano che promana dalla Costituzione[34]. Questi caratteri distinguono il coordinamento, pur con sfumature notevoli[35], sia dalla collaborazione, che opera sotto il diverso profilo dell'articolazione gerarchica degli interessi tutelati, sia dalla cooperazione che, invece, agisce a livello europeo.

Il coordinamento, dal solo versante organizzativo, è divenuto uno strumento funzionale. In questa accezione, integra una modalità di raccordo coerente con la realtà in costante evoluzione della sicurezza cibernetica, secondo un orizzonte

32 Bachelet 1957; Orlando 1974; Giannini 1958.
33 In merito alla difficile coesistenza tra autonomia e spinte unitarie, Police 2024: 24.
34 Antonelli, De Martin, Mattarella 2024, D'Angelo 2022.
35 Morana 2024.

concettuale aperto a innovazioni, adattamenti e commistioni. Proprio in quest'ottica non può sottacersi il ruolo dell'interesse nazionale, più volte ricordato, che produce una rottura nella linearità complessiva del coordinamento, riportando in auge elementi che, in precedenza, potevano apparire superati. Ne consegue quella "*sovrana incertezza*"[36] che lo caratterizza e che ne fa ripensare, ancora oggi, la figura: di fronte alla compresenza di più interessi, l'interesse nazionale sembra in grado di spostare l'assetto in essere, modificandone il fuoco e l'ellissi. Non si assiste a un cambio radicale della figura del coordinamento, ma a una sua rilettura, in accordo con la tendenza centralizzatrice di funzioni e strutture.

È di ausilio, a tal fine, considerare sia che il coordinamento esprime una idea di "crisi" (termine tutt'altro che indifferente al settore in esame!)[37], sia che i suoi contorni sono sfumati e privi di coerenza e razionalità granitica. Interstizi e margini di intervento sono utili, del resto, a contrastare eventuali '*moloch*', evitando (o cercando di evitare) contrasti con la protezione di interessi, valori e diritti fondamentali, essenziali alla tenuta di uno stato democratico. Può ricordarsi, in merito, che, "il 'coordinare' è in certo senso manifestazione tipica di una società democratica e pluralistica, che intende ottenere l'armonico orientamento di individui, gruppi, istituzioni verso fini determinati, senza però annullare la libertà o l'iniziativa di tali individui, gruppi o istituzioni"[38].

Dunque, la ricerca di una clausola di salvaguardia, o di una valvola di sfogo, è ancora viva: e questo anche in un contesto, come quello attuale, in cui l'autoritatività sembra prendere il sopravvento, o quantomeno proporsi in modo sbilanciato[39]. È da richiamare, allora, quanto affermato in altri contesti e momenti, ricercando anche nel settore della sicurezza cibernetica un "coordinamento non unilaterale e gerarchico, ma condiviso"[40]; solo esso, infatti, "tende a garantire contemporaneamente la autonomia dei singoli organismi coordinati e insieme la possibilità di un loro indirizzo unitario a determinati fini comuni"[41].

Il ragionamento, probabilmente, va effettuato in termini meno deontici e maggiormente orientato alla sua dimensione effettiva, vale a dire all'effetto che è in grado di produrre[42]. Il cambio del *modus agendi* cerca di orientare l'attività a un determinato obiettivo, forzandola; non devono essere consentiti, però, strappi irreparabili, o stravolgimenti senza rimedio dell'assetto esistente. È l'effetto concreto

36 Cortese 2012.
37 Berti 1982: 31.
38 Bachelet 1962. Sull'incidenza delle attività di cibersicurezza sui diritti, Manjikian 2023.
39 Rossa 2023.
40 Così Merloni 2008: 22. Questo il passo complessivo, analizzato in un contesto istituzionale molto differente, che pur indica somiglianze e punti di continuità: "[u]n definitivo assetto dell'attuale soggetto statale, il CNIPA, potrebbe essere trovato in una amministrazione, con forti tratti di autonomia organizzativa e di indipendenza dei componenti degli organi, largamente partecipata dalle diverse amministrazioni; un'amministrazione di livello nazionale, ma "repubblicana" (rappresentativa dei soggetti costituenti la Repubblica, secondo l'art. 114 Cost.) che contribuisce a un coordinamento non unilaterale e gerarchico, ma condiviso".
41 Bachelet 1962.
42 Cassese 1982: 20.

e la dimensione del reale a contare, e non la ricostruzione idealistica dell'istituto. Una prospettiva che si accorda perfettamente, come anticipato, alla natura decisamente concreta dell'informatica.

Vi è un altro orizzonte concettuale che sembra rispondere alle dinamiche profonde dell'assetto istituzionale di settore: quello dell'autonomia funzionale. L'autonomia deve essere intesa come categoria aperta e, dunque, rispondente a un ordine concettuale magmatico. Non è limitata alla sola capacità di porre regole, ma di decidere e agire secondo criteri non unitari[43], ricercando un equilibrio tra i soggetti che permeano il settore e che già dispongono di competenze consolidate.

Questa forma elastica non consegue allo sfaldamento dello stato unitario, cui l'autonomia è tradizionalmente collegata[44]: il sistema in costruzione, anzi, lo presuppone, per tutelare meglio l'interesse nazionale a esso connaturato (che è l'interesse e da cui si sono prese le mosse in questo scritto). La formula sembra paradossalmente assicurare, dunque, la convivenza di tendenze unitarie e pluralistiche, preservando margini di autonomia. L'autonomia funzionale va ricondotta, in questo senso, al *modus operandi* delle amministrazioni, riconoscendo un *agere* specifico che mira agli obiettivi stabiliti senza implicare un modello organizzativo definito. Si è a metà del guado, con la riva del modello istituzionale ancora da raggiungere.

Nell'insieme, non vi sono risposte certe. Anche il dato normativo non è univoco e sul piano terminologico si nota un utilizzo non sempre coerente, in cui vengono affiancati tecniche e concetti in modo non perfettamente lineare. Soprattutto in ambito dell'Unione europea, i riferimenti a forme di coordinamento, cooperazione e collaborazione non sono ben distinti**.** Il piano semantico non sembra rispondere a un ordine concettuale granitico. Probabilmente anche il tessuto normativo riflette la difficoltà di consolidare uno stato magmatico come quello in cui si trova il settore in esame, dove anche le istituzioni devono ancora assestarsi.

A questo stato si collega un elemento ulteriore di valutazione: un diffuso grado di informalità, che sfrutta le pieghe di una costruzione realizzata per tappe per consentire la convivenza delle istanze autonome con il centro. L'informalità costituisce un collante, in grado di avvicinare i diversi soggetti coinvolti, nel tentativo di ricondurli a unità ed evitare conflitti o contraddizioni. Leggendola a fondo, essa rappresenta un sostrato su cui costruire, in un secondo momento, uno strato più solido di uniformità: i legami teleologici si formano con la prima, proiettandola verso la seconda.

43 Va prestata attenzione poi agli ambiti semantici (che, in tempi di LLM, sono attualissimi): l'autonomia, infatti, è una risposta specifica in ambito internazionale e geopolitico, viene usata e declinata come autonomia tecnologica – in alcuni casi contrapponendosi al concetto di sovranità digitale: Cerra e Crespi 2021. In altri casi richiama il tentativo (per ora ancora tale e piuttosto indefinito) di avvicinarsi a concetti filosofici e ontologici, come avviene con l'uso della dizione "autonomia dell'uomo" contenuta art. 3, par. 2, del disegno di legge governativo in materia di intelligenza artificiale.

44 Merloni 1990.

Non si può prescindere, infine, dalla componente politica. Questo elemento chiude il discorso in modo circolare e ricorsivo. La politica fonda l'ordinamento settoriale della sicurezza cibernetica e appare in costante ascesa: indica la presenza di interessi latenti, primari e coessenziali alla vita stessa dello Stato. Anche limitandosi a osservare la direttiva NIS 2[45], simili interessi si riflettono in modo evidente e convergono verso un punto specifico: la dimensione diplomatica, tipica espressione della compagine statale. Le forme di cooperazione già esistenti vengono qui cristallizzate in uno schema istituzionale dai contorni più precisi, funzionale all'intero disegno della sicurezza cibernetica. È una dimensione che sfugge sia alla tecnica, sia alle funzioni regolatorie e di controllo[46]. La latenza di questo genere di interessi rappresenta una chiave di volta del settore, e ne consente la lettura profonda.

7. Conclusioni

Il settore della sicurezza cibernetica è in costante movimento e in cerca della propria identità. Di questo percorso risentono le istituzioni che lo governano. I tratti sono labili e i confini mutevoli: il tempo consoliderà l'assetto in essere, raffredderà le tensioni e lasciando un precipitato maggiormente visibile. Come si è avuto modo di osservare, è possibile riconoscere qualche carattere generale, ricondursi ad attività storicamente consolidate, tentare un primo approccio di massima. Qualche considerazione generale, in questo senso, può essere tratteggiata, ma non completata.

Nell'insieme, la dimensione normativa e istituzionale cammina di fianco a quella tecnica. Lo si osserva nel caso problematico degli attacchi *zero-days* – ossia di vulnerabilità sconosciute, per le quali non si dispone di un rimedio. Essi costituiscono una base conoscitiva di grande spessore: questi attacchi nascono da vulnerabilità conosciute e taciute per esigenze strategiche. Il problema posto alla loro base, dunque, non concerne tanto la tecnica, ma la loro genesi: un *a priori* composto da esigenze politiche e istituzionali crea una sinergia rischiosa, che può rivelarsi anche controproducente, ritorcendosi contro le esigenze di difesa cui si anela[47].

Svelare e comprendere determinate logiche può contribuire a un rafforzamento complessivo del mondo digitale, ripartendo dalle basi: forse occorre tornare a un 'grado zero della sicurezza' volto al ripensamento delle infrastrutture e alla riscrit-

45 Art. 16, par. 3, *lett. d*), direttiva NIS 2, che prescrive di coordinare la gestione degli incidenti e delle crisi di cibersicurezza su vasta scala e "sostenere il processo decisionale a livello politico" in ordine a questi eventi.

46 Nella direttiva NIS 2, viene affermato al *considerando* n. 71 che "EU-CyCLONe dovrebbe fungere da intermediario tra il livello tecnico e politico durante gli incidenti e le crisi di cibersicurezza su vasta scala e dovrebbe rafforzare la cooperazione a livello operativo e sostenere il processo decisionale a livello politico. In cooperazione con la Commissione, tenuto conto della competenza di quest'ultima nel settore della gestione delle crisi, EU-CyCLONe dovrebbe basarsi sui risultati della rete di CSIRT e utilizzare le proprie capacità per elaborare analisi d'impatto di incidenti e crisi di cibersicurezza su vasta scala".

47 N. Pelroth 2021.

tura delle tecnologie da cui oggi dipendiamo. Si tratta di un tema più generale, a cui si può solo accennarsi: va affrontata in modo sistematico la debolezza di alcuni dei protocolli maggiormente utilizzati, a partire da quelli su cui poggia l'infrastruttura tecnologica dominante, ossia *Internet*. Le vulnerabilità che ne sono alla base indicano momenti primordiali, falle emerse o facilmente prevedibili, cui sarebbe necessario ovviare. La futura sicurezza cibernetica dovrebbe partire da un assunto diverso e ben scandito: la protezione dei singoli individui, e non solo quella degli apparati o dei soggetti con maggiori capacità tecniche e peso economico[48].

È muovendo da queste conoscenze, imprescindibili per capire a fondo il settore, che si potrà rifondare un sostrato giuridico e istituzionale in grado di assolvere al proprio compito: per proteggere la persona e favorirne lo sviluppo, anche in un mondo complesso gli Stati devono dialogare nei consessi internazionali, assolvendo al primario compito di ricercare il bene comune, correggendo le distonie che generano l'attuale situazione di crisi dei diritti e, per quanto di interesse in questo scritto, di 'insicurezza informatica'.

Bibliografia

Antonelli V., De Martin G.C., Mattarella B.G. (a cura di) 2024, *Il coordinamento amministrativo dopo Vittorio Bachelet*, Roma: Luiss University Press.

Bachelet V. 1957, *L'attività di coordinamento nell'amministrazione pubblica dell'economica*, Milano: Giuffrè.

Bachelet V. 1962, "Coordinamento", in *Enciclopedia del diritto*, Milano: Giuffrè, X, *ad vocem*.

Berti G. 1982, "Il coordinamento: parola-simbolo tra gerarchia ed equiordinazione", in Amato G., Marongiu G. (a cura di), *L'amministrazione nella società complessa. In ricordo di Vittorio Bachelet*, Bologna: Il Mulino: 31.

Buoso E., 2025, "Ritorno al futuro: il perimetro di cybersicurezza nazionale", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 33 ss.

Carotti B. 2011, *La collaborazione tra autorità europee delle telecomunicazioni*, London: EPLO.

Carotti B. 2020, "Sicurezza cibernetica e Stato-Nazione", in *Giornale di diritto amministrativo:* 629-641.

Cassese S. 1982, "Il coordinamento prima e dopo Bachelet", in Amato G., Marongiu G. (a cura di), *L'amministrazione nella società complessa. In ricordo di Vittorio Bachelet*, Bologna: Il Mulino: 20.

Cerra R., Crespi F. 2021, *Sovranità tecnologica*, Roma: Centro per l'economia digitale (CED), 50.

Cortese F. 2012, *Il coordinamento amministrativo. Dinamiche e interpretazioni*, Milano: Franco Angeli, 5 ss.

48 Egloff 2022; Ishikawa, Yarik 2023.

D'Alberti, M. 1982, "Coordinamento amministrativo: immagini per la ricerca di un concetto", in Amato G., Marongiu G. (a cura di), *L'amministrazione nella società complessa. In ricordo di Vittorio Bachelet*, Bologna: Il Mulino: 55-64.

D'Angelo F. 2022, *Pluralismo degli enti pubblici e collaborazione procedimentale. Per una rilettura delle relazioni organizzative nell'amministrazione complessa*, Torino: Giappichelli.

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

Falzea A. 1965, "Efficacia giuridica", in *Enciclopedia del diritto*, Milano: Giuffrè, Vol. XIV.

Giannini M.S., 1958, "Il decentramento nel sistema amministrativo", in AA. VV., *Problemi della pubblica amministrazione*, Vol. I, Ciclo di conferenze promosso dalla Scuola nell'anno accademico 1956-57, Bologna: Zanichelli.

Giannini M.S. 1993, *Diritto amministrativo*, Milano: Giuffrè, Voll. I-II.

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

Orlando L. 1974, *Contributo allo studio del coordinamento amministrativo*, Milano: Giuffrè.

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

Matassa M. 2025, "Sicurezza cibernetica e nazionale nell'ordinamento multilivello: quale possibile convivenza?", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 75 ss.

Merloni F. 1990, *Autonomie e libertà nel sistema della ricerca scientifica*, Milano: Giuffrè.

Merloni F. 2008, "Coordinamento e governo dei dati nel pluralismo amministrativo", in Ponti B. (a cura di), *Il regime dei dati pubblici*, Rimini: Maggioli: 1-25.

Morana D. 2024, "Il coordinamento nella trama costituzionale: spunti di riflessione", in Antonelli V., De Martin G.C., Mattarella B.G. (a cura di), 2024, *Il coordinamento amministrativo dopo Vittorio Bachelet*, Roma: Luiss University Press.

Nigro M. 1966, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano: Giuffrè.

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

Police A. 2024, "La nozione di coordinamento nell'amministrazione dell'Unione europea e dei suoi Stati membri: una nuova declinazione della lezione di Vittorio Bachelet", in Antonelli V., De Martin G.C., Mattarella B.G. (a cura di), *Il coordinamento amministrativo dopo Vittorio Bachelet*, Roma: Luiss University Press, 24 ss.

Previti L. 2025, "Convergenze e deviazioni in materia di cybersicurezza: implicazioni sistematiche e nuovi interrogativi", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 109 ss.

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

Selejen-Gutan B. 2024, "The Second Round that Wasn't. Why The Romanian Constitutional Court Annulled the Presidential Elections", in *Verfassungsblog*, 7 dicembre (https://verfassungsblog.de/the-second-round-that-wasnt/).

Ursi R. 2025, "Introduzione. La sicurezza cibernetica come funzione pubblica", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 7 ss.

Wu T. 2020, *The Curse of Bigness. Antitrust in the New Gilded Age*, New York: Penguin.