RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0234 • articolo sottoposto a peer review • pubblicato in anteprima il 1 ago. 2025

Giovanni Barozzi Reggiani

La *race for the cyberspace* degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance

Il contributo intende compiere una riflessione concernente il tema della dialettica tra forme di *governance* e tradizionali strumenti di *government* attraverso l'angolo di osservazione della proiezione della sovranità degli Stati sul cyberspazio e delle questioni che afferiscono (in via diretta o indiretta) alla cybersicurezza. Dalla disamina e dal raffronto dei quadri giuridici europeo e nazionale in materia, e dall'esame delle caratteristiche delle "architetture" e degli assetti organizzativi che tali quadri giudici disegnano, emerge una rinnovata centralità della sovranità, elemento caratterizzante il Leviatano hobbesiano, e dunque lo Stato nazionale, il quale, pur dovendosi oggi confrontare con le sfide complesse (e in parte inedite) che le peculiarità del cyberspazio (e le esigenze connesse agli obiettivi di cybersicurezza) pongono allo stesso, appare, nel perseguimento delle sue finalità di fondo (garantire la propria sicurezza e il proprio funzionamento e salvaguardare diritti e libertà fondamentali) tutt'altro che in crisi, ed anzi pervaso da una rinvigorita vitalità.

Cybersicurezza – Sovranità – Cyberspazio – Governance – Government

Cybersecurity in the context of the race for the cyberspace: reflections on state sovereignty in the digital world

The paper aims to investigate the relationship between governance and government in connection with the ongoing race for the cyberspace, driven by nation-states, and the issues related to cybersecurity. Starting with an overview of both the European and the Italian legal frameworks, the paper will focus on the centrality of state sovereignty in the global context. Due to the unique characteristics of the cyberspace, states today face significant challenges in protecting citizen's fundamental rights and freedoms from threats emerging from the digital realm. These challenges compel states to cooperate and develop innovative solutions. At the same time, they highlight that the traditional concept of sovereignty is not in crisis, but is instead increasingly central to the network of geopolitical relationships between States and the governance of cyberspace.

Cybersecurity – Sovereignty – Cyberspace – Governance – Government

L'Autore è ricercatore di Diritto costituzionale e pubblico presso il Dipartimento di Giurisprudenza dell'Università di Sassari

Questo contributo è stato elaborato nell'ambito del progetto di ricerca *Il ruolo della governance nei processi decisionali delle democrazie pluralistiche*, finanziato ai sensi del bando Progetti di ricerca interdisciplinare - d.m. 737/2021, risorse 2021-2022

1. Considerazioni introduttive

Come è stato osservato, non è dato rinvenire alcuna "porzione di terra emersa che non appartenga al territorio di un'entità statale" (se si esclude l'Antartide)[1].

La sovranità degli Stati[2] – che si riferisce ai territori – si estende poi anche a talune zone marine (il c.d. mare territoriale) e allo spazio aereo sovrastante i territori medesimi (quantomeno fino a una certa altitudine); altre "porzioni di globo", che non cadono sotto la sovranità di alcun ordinamento statuale (si pensi alle acque internazionali), sono invece assoggettate a regole, di matrice prevalentemente convenzionale, che ne disciplinano la natura giuridica e il modo in cui gli ordinamenti si rapportano ad esse.

La descritta situazione risponde a quello che potremmo definire "principio dell'*horror vacui* geopolitico", compendiabile nella massima secondo cui se esiste uno spazio occupabile, prima o poi il medesimo verrà effettivamente occupato, fisicamente o "giuridicamente".

La propensione alla "occupazione di territorio", del resto, da sempre caratterizza gli Stati, in quanto espressione di quella volontà di potenza che, secondo i postulati del c.d. realismo geopolitico, spinge i medesimi a tentare di aumentare costantemente la propria influenza sullo scacchiere mondiale, e che risulta pienamente "coerente con le concezioni classiche del diritto pubblico statale, evocando l'idea dello Stato come entità sovrana autofondata e *superiorem non recognoscens*"[3], costituendo dunque un atto materiale – cui si riconnettono tuttavia

1. Così Chessa 2019, p. 12.
2. Non è certo questa la sede per disquisire sul concetto di sovranità; ciò che maggiormente interessa è chiarire quale sia l'accezione nella quale, nel presente scritto, detto termine verrà utilizzato. In questo senso, sovranità verrà qui intesa e usata come sostanziale sinonimo del concetto di *government*. Quest'ultimo, a sua volta, verrà considerato in una precisa declinazione, ovvero come riferito ai modelli di regolazione e governo di specifici fenomeni delineati dagli architravi costituzionali dei diversi ordinamenti, e quindi (e proprio per ciò, ancorché con un'opera di semplificazione) quale sostanziale sinonimo di sovranità, o comunque termine a quest'ultima riconducibile in quanto espressione della stessa. Trattasi di utilizzo del termine che, ancorché con le menzionate semplificazioni, appare ammissibile, ai fini del presente lavoro; nello stesso volume di Chessa 2019 si rinvengono espressioni che sembrano confermare la "legittimità" di detto utilizzo, laddove l'Autore parla di *government* come di "potere rappresentativo lato sensu […] che ricomprende l'intero apparato degli organi costituzionali, lo Stato-persona (o Stato soggetto, Stato-governo, Stato-apparato)" (p. 325) ovvero di "dispositivi tradizionali di government statale" (p. 336) o ancora utilizza uno accanto all'altro i termini government e sovranità statale (p. 332).
3. In questo senso Chessa 2025, p. 86.

anche effetti giuridici[4] – che esprime concretamente la sovranità.

In questo senso, ancorché si discuta da tempo (secoli, invero) circa l'ampiezza del novero delle potestà pubbliche riconducibili alla sovranità (senza che si sia addivenuti ad una sistematizzazione condivisa[5]), è difficilmente revocabile in dubbio che a quest'ultima afferisca quella che Jean Bodin definiva attività di "dichiarare la guerra e concludere la pace", che consiste (anche) nell'occupazione di territori[6].

Si tratta, peraltro, di aspirazione e prerogativa tutt'altro che "dormiente": come è stato infatti notato, attualmente si sta assistendo ad un rinvigorirsi delle "pretese territoriali" degli Stati[7], oltre che ad una progressiva corsa al riarmo pressoché in ogni parte del globo[8].

Si potrebbe dire: nulla di nuovo; gli Stati fanno ciò che fanno da sempre, e che è nella loro natura fare. Tuttavia, nel mondo moderno alcune delle ambizioni di espansione degli Stati riguardano un "territorio" che presenta caratteristiche affatto particolari.

Stiamo parlando del cyberspazio, che è stato qualificato (a partire dai primi anni del XXI secolo) in termini di "quinto dominio" (accanto a terra, acqua, aria e spazio), oggetto in quanto tale di potenziali conquiste e – conseguentemente – conflitti tra gli Stati[9].

Questi ultimi possono, su tale "dominio", proiettare la propria volontà di potenza, che si declina quale ambizione all'occupazione di "territorio" o alla regolazione di fenomeni o condotte di soggetti o attività che per il medesimo transitano (in numero sempre crescente[10]) e, specularmente, alla difesa e alla salvaguardia di dette attività nonché

4. E difatti, come è stato osservato, quella concernente l'occupazione di terra costituisce la "decisione veramente fondamentale, creativa di nuovi ordinamenti" (così ancora Chessa 2025, p. 72).
5. Ciò risulta vero al punto che autorevolissima dottrina ha affermato come appaia "preferibile rinunciare alla ricerca di itinerari che portino a trovare le 'essenze' della sovranità, e tornare alla vecchia opinione, che questa è costituita dalle somme potestà dell'ordinamento statale" (così Giannini 1990, p. 227).
6. Bodin 1576/1964, p. 495.
7. Constatazione riportata da ultimo da Cassese 2025.
8. Nel marzo 2025 la Commissione europea ha presentato il *ReArm Europe Plan/ Readiness 2030*, che prevede investimenti nel settore della difesa e del riarmo per circa 800 miliardi di euro. Nello stesso mese, la Commissione e l'Alto Rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza hanno presentato il Libro Bianco *for European Defence Readiness 2030* (doc. JOIN(2025) 120, del 19 marzo 2025), nel quale, in uno dei diversi passaggi significativi, viene affermato: "the moment has come for Europe to re-arm. To develop the necessary capabilities and military readiness to credibly deter armed aggression and secure our own future, a massive increase in European defence spending is needed. This needs to be coordinated and directed more effectively than ever between Member States, reflecting our collective strengths and addressing the weaknesses that come from uncoordinated action".
9. La definizione del cyberspazio quale "*quinto dominio della conflittualità*" si deve a William J. Lynn III, allora vice-Segretario alla Difesa degli Stati Uniti (cfr. in particolare Lynn iii 2010, p. 97). Il riconoscimento ufficiale del cyberspazio quale quinto dominio operativo si ebbe poi all'esito del Summit NATO di Varsavia del 2016. Sul fronte dell'ordinamento nazionale, una interessante epifania normativa è rappresentata dalle modifiche che l'art. 51, comma 8, lett. e) del d.l. 17 maggio 2002, n. 50 (convertito, con modificazioni, dalla legge 15 luglio 2022, n. 91) ha apportato all'art. 88 del Codice militare (decreto legislativo 15 marzo 2010, n. 66) il cui novellato comma 1 stabilisce che "lo strumento militare è volto a consentire la permanente disponibilità di strutture di comando e controllo di Forza armata e interforze, facilmente integrabili in complessi multinazionali, e di unità terrestri, navali, aeree, cibernetiche e aero-spaziali di intervento rapido, preposte alla difesa del territorio nazionale, delle vie di comunicazione marittime e aeree, delle infrastrutture spaziali e dello spazio cibernetico in ambito militare; è finalizzato, altresì, alla partecipazione a missioni anche multinazionali per interventi a supporto della pace".
10. In effetti, come è stato condivisibilmente sostenuto, a seguito del progressivo affermarsi della società dell'informazione, il cyberspazio è "diventato un elemento cruciale per le dinamiche politiche, sociali, finanziarie e umane del XXI secolo" (così Martino 2018, p. 62).

delle strutture che sorreggono il cyberspazio e ne garantiscono il funzionamento.

In effetti, è in corso una vera e propria "*race for the cyberspace*", che ha una proiezione tanto attivo-offensiva (concernente la conquista di sempre maggiori "spazi" e "territori") che passivo-difensiva (relativa alla protezione di componenti, dati, strutture) e che non appare confinata solo alla dimensione economica e commerciale dei rapporti tra gli Stati: in questo senso, costituisce un dato ormai acquisito che nel cyberspazio possono venir condotte anche operazioni militari[11], e che anzi all'attualità non è dato rinvenire un'operazione di tale natura (condotta secondo le metodologie tradizionali e in uno degli altri "dominii") che non sia preceduta o accompagnata da attività di *cyberwarfare*[12].

Come appare evidente, rispetto al quadro descritto vengono in rilievo esigenze che attengono alla stessa sicurezza dello Stato – sia sul fronte interno che su quello esterno[13] – e in specie all'interesse di quest'ultimo alla "propria integrità territoriale, indipendenza e – al limite – alla stessa sua sopravvivenza", interesse che risulta "preminente su ogni altro in tutti gli ordinamenti statali, quale ne sia il regime politico"[14].

Rispetto alla descritta prospettiva, appare certo da condividersi l'osservazione secondo la quale "l'insicurezza del cyberspazio non minaccia solo l'economia, ma addirittura il funzionamento delle nostre democrazie e i valori su cui si fonda la società [dato che] le politiche interne degli Stati che riguardano l'ordine pubblico, la sicurezza nazionale e la stessa protezione delle libertà devono fare i conti con le minacce che provengono o si consumano nel cyberspazio"[15].

Se la garanzia della sicurezza dello Stato è funzionale (anche) alla salvaguardia del

11. Emblematica in questo senso l'affermazione concernente l'invocabilità dell'art. 5 del Trattato NATO (relativo alla reciproca difesa, da parte dei membri dell'alleanza) anche in riferimento agli attacchi cibernetici (in tema cfr., da ultimo, le conclusioni della riunione dei Capi di Stato e di Governo tenuta a Vilnius l'11 luglio 2023, par. 66).
12. Particolarmente indicativo, sul punto, quanto si legge nel citato Libro Bianco *for European Defence Readiness* (al par. 8), circa il fatto che "both defensive and offensive cyber capabilities are needed to ensure the protection and freedom of manoeuvre in cyberspace. There is a need to develop together with Member States a voluntary support scheme for offensive cyber capabilities as credible deterrence". In tema, v. anche quanto osservato da De Felice 2012, p. 76, circa il fatto che "l'ampia gamma di azioni ostili può andare dallo spionaggio agli attacchi veri e propri, con finalità ibride, all'alterare o addirittura distruggere dati, hardware, reti o eventuali servizi e sistemi ad essi connessi. Generalmente possono essere rivolte ad assetti governativi, economico-finanziari, imprese, infrastrutture critiche o servizi dedicati alla società civile. I possibili effetti da essi generati possono facilmente divenire strategicamente rilevanti oppure influenzare comportamenti, azioni e documentazione collegati anche ad operazioni militari in corso".
13. Come è stato rilevato, "diversamente dal concetto di sicurezza 'reale', la cybersicurezza pone particolare rilevanza non solo verso il profilo esterno, ma anche verso quello della gestione del rischio endogeno che, nel caso specifico, ricomprende gli incidenti di sicurezza dovuti a condotte dolose di soggetti interni ad amministrazioni, organi dello Stato o dipendenti di organizzazioni private, perpetrate con o senza l'ausilio di strumenti informatici; e gli eventi riconducibili al c.d. fattore umano, ossia incidenti dovuti alla mera inconsapevolezza degli utenti circa il rispetto di buone pratiche di sicurezza informatica (best practices) o sulle tecniche di prevenzione da attacchi di ingegneria sociale" (così Serini 2022, p. 271).
14. Sentenza n. 82 del 1976, punto 5 Cons. in Dir. Nello stesso senso si sono espresse le sentenze n. 86 del 1977 (punto 5 Cons. in Dir.); n. 106 del 2009 (punto 3 Cons. in Dir.); n. 40 2012 (punto 4 Cons. in Dir.); n. 24 del 2014 (punto 5 Cons. in Dir.).
15. Longo 2024-a, p. 314. In senso analogo cfr. Pietrangelo 2024, p. 17, la quale osserva che "nelle politiche e pratiche della transizione digitale la cybersicurezza è oggettivamente una condizione di esistenza: rendere più sicuri reti, sistemi e dati vuole dire giocoforza rendere più sicuri gli Stati e i loro apparati, le persone e le loro vite. Una specie di protezione delle protezioni, una sicurezza maxima da cui dipendono le sorti delle Nazioni come degli individui, tutti inesorabilmente immersi nella dimensione digitale". Il concetto in esame mi pare peraltro

funzionamento delle democrazie, e più ampiamente dell'ordinamento costituzionale, e se il cyberspazio è un dominio nell'ambito del quale tale sicurezza può venir messa in discussione, ne consegue, per semplice sillogismo, che gli Stati devono farsi carico di garantire specifiche istanze di sicurezza concernenti il cyberspazio anche nell'ottica di salvaguardare i diritti e le libertà fondamentali degli individui (che vengono garantiti dall'ordinamento costituzionale ed anzi, come autorevolmente sostenuto, sono la causa e il fondamento delle Costituzioni[16]).

L'obiettivo della protezione di diritti e libertà amplia peraltro l'ambito di operatività delle istanze difensive e di sicurezza che riguardano il cyberspace; detti diritti e libertà, infatti, possono venir minacciati non solo da attività ostili provenienti da altre entità statuali o da gruppi terroristici, ma anche da soggetti che svolgono nello spazio virtuale attività illecite (come il furto dei dati o le truffe)[17] o semplicemente dalla commissione, anche in buona fede o per semplice ingenuità, di errori.

In questo senso, dalla cyber-difesa (attività, di natura prevalentemente militare, che concerne principalmente il tema del contrasto al *cyberwarfare*, e quindi delle azioni ostili provenienti da Stati o comunque agli stessi riconducibili) si passa al più ampio concetto di cybersicurezza, del quale si rinvengono anche definizioni normative, tra cui quella posta dal Regolamento (UE) 2019/881[18], che definisce il termine quale "insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche", o quella che si rinviene nel d.l. n. 82 del 2021, il cui art. 1, al comma 1, lett. a), descrive il concetto come "l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"[19].

Da entrambe le definizioni – con la seconda che chiaramente rende l'idea della complementarietà tra cybersicurezza e attività di *intelligence* – emerge l'immagine della cybersicurezza quale complesso di

ben reso dalla definizione di "resilienza nazionale nello spazio cibernetico", posta dall'art. 1, comma 1, lett. b) del d.l. 14 giugno 2021, n. 82 – che ha tra le altre cose istituito e disciplinato l'Agenzia Nazionale (italiana) per la Cybersicurezza – che qualifica il concetto come l'insieme delle "attività volte a prevenire un pregiudizio per la sicurezza nazionale" che possa comportare un "danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici militari, economici scientifici e industriali dell'Italia, conseguentemente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale […]".

16. Quella così sintetizzata (e si spera non banalizzata) è la tesi di fondo del lavoro di Chessa 2002.
17. La strumentalità della messa in sicurezza del *cyberspace* a garantire diritti e libertà fondamentali dei singoli è sottolineata anche dalla Direttiva del 1° agosto 2015 della Presidenza del Consiglio dei Ministri (che ha imposto alle pubbliche amministrazioni l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici). Come è stato sottolineato, "si tratta di un passaggio di grande significato politico, ma anche giuridico: viene riconosciuto che il tema della cyber security non è solo questione di 'difesa nazionale', ma è di garanzia per i diritti fondamentali degli individui, quelli, cioè, costituzionalmente protetti" (così Bruno 2020, p. 16).
18. Regolamento (UE) 2019/881 del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013.
19. È un concetto, quello del rapporto tra attività di cyber-difesa e attività di cyber-sicurezza, che si rinviene ben compendiato nella *Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità* della IV Commissione permanente del Senato (di cui il 2 aprile 2025 è stato approvato il documento conclusivo) laddove si legge (p. 75) che "la difesa cibernetica si sostanzia in uno spettro di competenze dello Stato di natura prettamente militare, da inquadrare in una più ampia strategia nazionale per la sicurezza cibernetica, la cui architettura si è andata componendo grazie a una serie di interventi normativi".

attività (che dunque costituiscono un insieme, non necessariamente omogeneo[20]) strumentali alla protezione di alcuni beni – che sussistono o trovano inedite modalità di estrinsecazione nel cyberspazio – da "minacce informatiche", concetto, quest'ultimo, che ha un notevole ambito di estensione, essendo stato definito (sempre dal Regolamento europeo 2019/881) come "qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone" (art. 2, punto 8).

Le minacce informatiche[21], se efficacemente attuate, possono poi determinare il verificarsi di un incidente, come tale qualificato – in particolare dall'art. 6, n. 6, della Direttiva (UE) 2022/2555 (c.d. Direttiva NIS II[22], che ha abrogato la Direttiva (UE) 2016/1148, c.d. NIS I) – qualsiasi "evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi"[23].

Sono dunque tali minacce, e per esse gli incidenti informatici, a costituire il fattore cui le attività di cybersicurezza (e di *cyber-defence*) devono prestare la principale attenzione, posto che è da tali attività che può derivare la reale lesione o anche solo la semplice messa in pericolo dei beni giuridici e degli interessi alla cui salvaguardia la cybersicurezza è preposta[24].

Tale conclusione pone il tema di come tali minacce possano venire efficacemente contrastate.

Nell'ottica di fornire risposta al quesito – e prima di interrogarci su quali siano i "modelli regolatori" più adatti allo scopo (specie a riguardo della dialettica *governance* – *government*[25])

20. Al concetto di cybersicurezza, secondo le definizioni richiamate, sarebbe riconducibile un triplice ordine di attività: "da un lato la protezione dei contenuti, dei dati, delle informazioni, un secondo relativo alla protezione hardware (quindi gli elementi fisici dei dispositivi quali PC, Smartphone, Mainframe, Server ecc.); una terza protezione relativa agli aspetti software intesi quali programmi, reti, database, archivi digitali ed altre impostazioni tecnologiche militari" (così Contaldo–Salandri 2020, p. 2).
21. Per un inquadramento delle principali minacce informatiche v., nel sito ENISA, *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*
22. Il termine "NIS" è acronimo di *Network and Information Security*.
23. Anche rispetto alla definizione in parola si evidenzia il focus peculiare sui dati, specie se tale definizione viene raffrontata a quella posta dalla Direttiva NIS I, che definiva l'incidente (all'art. 4, n. 7) come "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi" (senza quindi un esplicito riferimento ai dati). La Direttiva NIS II contiene peraltro una definizione anche del concetto di "incidente di cibersicurezza su vasta scala", definito quale "incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri" (art. 6, n. 7).
24. Si tratta di insieme di beni e interessi ad ampio spettro, che comprende tanto interessi strategici dello Stato quanto "l'incolumità del tessuto produttivo, con un focus particolare sulle vulnerabilità che interessano le amministrazioni, da un lato, e le piccole e medie imprese, dall'altro" (così Longo 2024-b, p. 67).
25. Il tema del rapporto tra *government* e *governance* ha fatto versare alla dottrina i proverbiali fiumi di inchiostro. Per una bibliografia minima si rimanda a quella riportata da Chessa 2019, p. 331, nt. 15 (oltre che alle osservazioni dello stesso Chessa al Capitolo Quindicesimo della sua corposa monografia). Ai fini del presente scritto, e rinviando a quanto esposto in precedenza sul *government* (cfr. nt. 2), si rileva che del concetto di *governance* non si rinviene una definizione condivisa. In dottrina, è stato affermato che detto termine "signifies a change in the meaning of government, referring to a new process of governing; or a changed condition of ordered rule; or the new method by which society is governed" (così Rhodes 1996, p. 653) ovvero che il medesimo indica "un nuovo stile di governo, distinto dal modello del controllo gerarchico e caratterizzato da un maggior grado di cooperazione e dall'interazione tra lo Stato e attori non-statuali all'interno di reti decisionali miste pubblico/private" (così Mayntz 1999, p. s.). La *governance* concernerebbe dunque un modo di governare, e quindi regolare, un determinato fenomeno, ma secondo schemi e modalità diversi da quelli riferibili al *government*; più nello specifico, come è stato osservato, entrambi i termini "refer to purposive behavior, to goal oriented

– appare indispensabile effettuare qualche considerazione sulla natura e sulle caratteristiche del cyberspazio, che configura un luogo (un territorio, un dominio) diverso da tutti gli altri, e che proprio in ragione di tale diversità richiede di declinare in senso particolare l'ambizione all'occupazione di territorio e la volontà di potenza degli Stati.

2. Le caratteristiche del cyberspazio (luogo fisico e virtuale) e le questioni afferenti alla costruzione di architetture di cybersicurezza

È noto che la coniatura del termine "cyberspazio" si deve ad uno scrittore di fantascienza, William Gibson, che lo utilizzò dapprima nel racconto *Burning Chrome*, pubblicato nel 1982, e successivamente nel romanzo *Neuromante* (che ha visto le stampe nel 1984), considerato una delle pietre miliari del genere letterario *cyberpunk*.

Se il termine è divenuto ormai di largo utilizzo, non vi è però certezza e condivisione sul suo esatto significato.

Nel *Glossario* della *Guide for Conducting Risk Assessments* redatta dal *National Institute of Standards and Technology* del *Department of Commerce* statunitense, il cyberspazio è definito come "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[26].

Si tratta, invero, di una definizione che non può oggi considerarsi pienamente appagante ed esaustiva, nella misura in cui pone un'eccessiva (ed anzi esclusiva) enfasi sugli elementi "fisici" che connotato il cyberspazio, il quale è invece caratterizzato dal fatto che "alla sua formazione concorrono sia elementi naturali che virtuali"[27].

---

activities, to system of rule; but government suggests activities that are backed by formal authority, by police powers to ensure the implementation of duly constituted policies whereas governance refers to activities backed by shared goals that may or may not derive from legal and formally prescribed responsibilities and that do not necessarily rely on police powers to overcome defiance and attain compliance" (così Rosenau–Czempiel 1992, p. 4, i quali aggiungono poi che il concetto di *governance* "embraces governamental institutions but it also subsumes informal, non-governamental mechanisms whereby those persons and organizations within its purview move ahead, satisfy their needs and fulfill their wants"). Nei modelli di *governance*, in particolare, l'elemento della decisione autoritativa risulterebbe più affievolito, venendo in rilievo un modo di governare i fenomeni e assumere decisioni di carattere più "orizzontale e diffuso" che "verticale e decifrabile" (il quale ultimo caratterizza invece – cfr. D'Orsogna 2024, pp. 923 ss., nt. 83 – i modelli di *government*), cui prenderebbe parte una pluralità di attori e nel quale un ruolo di primo rilievo verrebbero a giocare soggetti dotati di particolare *expertise* tecnica, nella logica dell'effettuazione di scelte regolatorie basate su criteri obiettivi (in quanto aventi matrice tecnico-scientifica) che si imporrebbero (anche al decisore politico) proprio in ragione della loro "oggettività". A fronte di ciò, resta il tema della difficile inquadrabilità del concetto di *governance*; osserva in questo senso Barletta 2019, che il termine sarebbe suscettibile di "ricomprendere ipotesi di governo complesso nel quale interagiscono diversi attori con differenti provenienze istituzionali", venendo utilizzato in svariate accezioni, che vanno "da governance intesa come processo sino a governance intesa come governo della cosa pubblica o gestione di società commerciali". Ciò detto, si osserva che l'affermazione di modelli di *governance* a scapito della tradizionale rappresentanza/decisione politica sarebbe da ascriversi alla ormai acclarata incapacità del *government* di intercettare e regolare efficacemente diversi fenomeni della contemporaneità e di rispondere a istanze sociali (in tema, tra gli altri, Negri 2011, p. 206) e produrrebbe la conseguenza che "in ambiti sempre più vasti non c'è più la deliberazione politica degli organi rappresentativi e di governo, non c'è più la scelta unilaterale di indirizzo politico e la sua immediata traduzione in atti normativi e attività amministrative, secondo i tradizionali moduli gerarchici" dato che "alla direzione politica si sostituiscono la valutazione tecnica e l'accordo informale guidato da criteri che si rappresentano come scientificamente obiettivi e quindi a-politici" (Chessa 2019, p. 333).

26. National Institute of Standards and Technology – U.S. Department of Commerce, *Guide for Conducting Risk Assessments*, Special Publication 800-30, September 2012, p. B-3.

27. Martino 2018, p. 64.

In questo senso, appaiono più corrette definizioni come quella proposta da Ottis e Lorents, secondo la quale "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems"[28], o quella avanzata da Khuel, che ne parla in termini di "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies"[29].

La rilevanza (e la "maggior correttezza") di definizioni come quelle da ultimo richiamate è data dalla loro idoneità a dare conto del carattere polistrutturato e polimorfo del cyberspazio, che è composto da elementi materiali e immateriali, strutture, software ma, anche, esseri umani, che si muovono e agiscono al suo interno contribuendo, mediante i dati e le informazioni che fanno circolare e rendono disponibili, a farlo crescere e funzionare.

Ed invero, secondo le ricostruzioni più comuni e accettate il cyberspazio si strutturerebbe su tre distinti (ma interconnessi) *layers*, denominati "fisico", "logico" e "sociale"[30].

Sul piano "fisico" si collocherebbero le infrastrutture e, in generale, le componenti hardware indispensabili a consentire la circolazione dei dati (cavi sottomarini, antenne, computer, e così via[31]).

Il piano "logico" è invece quello nel quale si rinvengono i software e i codici che consentono a macchine (gli hardware) di dialogare tra loro, definendo le regole del funzionamento del cyberspazio[32].

Infine, il piano sociale (detto anche della "*cyber-persona*") è formato dalle interazioni che possono verificarsi fra persone fisiche o, come ormai sempre più spesso accade, tra persone e macchine o tra macchine e macchine.

Considerate le descritte caratteristiche, è certo da accogliere la posizione di chi si riferisce al cyberspazio come a un concetto atto a "identificare un'area/spazio (virtuale) in cui coesistono e funzionano in modo coordinato reti di computer, web semantico, social media e altre tecnologie dell'informazione e della comunicazione (ICT)"[33], e in cui operano persone; tali "componenti" (persone incluse) "risiedono, simultaneamente, nello spazio fisico e nello spazio virtuale, così come all'interno e all'esterno dei confini geografici"[34].

La base del cyberspazio è dunque certo fisica (esso funziona su e per il tramite di strutture o elementi reali e aventi una concreta dimensione nella realtà), ma il medesimo configura un luogo, o un insieme di luoghi, che, a differenza di tutti gli altri, prescinde dal requisito della territorialità[35], oltre a non avere una sua struttura fissa e definita, essendo dinamico (in quanto basato sulle continue relazioni

28. Ottis–Lorents 2010, p. 268.

29. Khuel 2009, p. 28.

30. In alcuni lavori, si rinviene una terminologia parzialmente diversa, senza che si riscontrino però sostanziali differenze circa il contenuto dei termini. Si veda ad esempio Libicki 2009, p. 12 ss., che parla di livelli fisico, sintattico e semantico.

31. Secondo alcuni Autori, il *layer* "fisico" sarebbe scomponibile in due sotto-livelli, quello geografico e quello fisico-infrastrutturale; in tema, tra gli altri, v. Pătrașcu 2019, p. 53, il quale rileva che "the geographic component has the role of hosting cyber infrastructures in its specific environments (soil, water, air and space), while the physical network component is made up of cyber infrastructures that are supported by connectors for the physical network which are a combination of wired and wireless links and satellites".

32. Sul punto è stato osservato che "the logical layer is where cyber terrain exists, and the primary cyberspace terrain feature is the network, a collection of devices that implement applications, services, and data stores" (così McCroskey–Mock 2017, p. 44).

33. Matassa 2023, p. 25.

34. Ursi 2023, p. 8.

35. In questo senso, se è vero che "the physical layer is the hardware, located in the physical domain, on which the other two layers exist" il medesimo "is not cyberspace terrain itself" (McCroskey–Mock 2017, p. 44).

che gli utenti instaurano tra loro) e pertanto definibile in termini di "spazio-movimento"[36].

Da tali caratteristiche discende la "irrelevance of geographic boundaries", dal momento che "cyberspace is about cross-border electronic communications"[37], costituendo un "virtual medium, one far less tangible than ground, water, air, or even space and the RF spectrum"[38].

Piuttosto, l'elemento che si configura come realmente costitutivo e caratterizzante il cyberspazio (o quantomeno essenziale per il suo funzionamento) è rappresentato dai dati[39].

La centralità di questi ultimi per il funzionamento del cyberspazio (ed anzi per la comprensione della natura profonda dello stesso) emerge in modo chiaro in alcune delle più recenti definizioni (sempre di cyberspazio)[40].

Negli anni, la mole di dati che circolano nel *cyberspace* è cresciuta esponenzialmente e, con essa, il numero di attività – fondate sui dati o aventi questi ultimi quale oggetto specifico – che nel medesimo vengono svolte; le applicazioni dell'intelligenza artificiale, divenute sempre più efficienti e precise grazie alla raffinazione dei processi di *machine learning* e il ricorso ai c.d. *big data*, hanno offerto una gamma via via maggiore di servizi, con la conseguenza che all'attualità il cyberspazio costituisce un luogo nel quale vengono svolte molte delle attività che caratterizzano la quotidianità (economica e sociale) dei singoli[41], comprese alcune riconducibili a servizi essenziali (aventi, in quanto tali, un rilievo pubblicistico) o a prestazioni rese dalle pubbliche amministrazioni, sempre più digitalizzate e in grado di dialogare con i cittadini/utenti mediante modalità telematiche e digitali (SPID, carta d'identità elettronica, e così via).

Ne consegue che le istanze concernenti la protezione dei dati e delle modalità con le quali i medesimi circolano assumono un primario rilievo, a riguardo della cybersicurezza e del contrasto alle minacce informatiche[42].

36. "Chi si avventura nel cyberspace vaga senza fine tra reti di comunicazione, inventando nuovi spazi e nuove velocità. È per così dire inafferrabile, giacché il suo spazio non è mai strutturato a priori, non è fisico, bensì dinamico, è cioè spazio-movimento" (così Amato Mangiameli 2000, p. 7).
37. Così Longworth 2000, p. 14.
38. Libicki 2009, p. 12.
39. Ed infatti, il cyberspazio configura una realtà "fatta di 'cose' che si vedono e si sentono, ma che non sono oggetti fisici né, necessariamente, rappresentazioni di oggetti fisici, bensì costrutti di dati" (così Tagliagambe 1997, p. 39). È stato in questo senso altresì osservato che "la produzione, l'immagazzinamento, la diffusione dei dati sono i motivi principali che spingono allo sviluppo del cyberspace" (così Mirti 2021, p. 42).
40. Si veda in questo senso quella che si rinviene nel *Glossary of Terms and Definitions* NATO (AAP-06 Edition 2018), che lo qualifica come "the global domain consisting of all interconnected communication, information technology, and other electronic systems, networks, and their data, including those which are separated or independent, which process, store, or transmit data". In termini analoghi si esprimono le Linee Guida ISO/IEC 2018, che definiscono il cyberspace come un "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".
41. È in questo senso stato correttamente rilevato che "cyberspace is where we create and use the digital information that fuels the global economy. Every day, the global business community exchanges trillions of dollars via cyberspace, transactions in which not a single dime or euro of hard currency is moved" (così Khuel 2009, p. 29).
42. Alla cybersicurezza può dunque ricondursi il tema della protezione dei dati degli individui (o delle imprese o delle amministrazioni) rispetto a tentativi di furto, appropriazione o danneggiamento da parte dei terzi: del resto, alcune delle tradizionali minacce informatiche (si pensi al *phishing*) hanno proprio ad oggetto la sottrazione di dati; tuttavia, le connessioni tra cybersicurezza e tutela dei dati personali (disciplina che concerne specificamente le modalità di trattamento, conservazione ed eventuale diffusione o comunicazione degli stessi, anche per fini economico-commerciali) non si esauriscono a temi legati al contrasto a episodi di *data breach* o altri fenomeni di furto o sottrazione dei dati. Nell'impossibilità di approfondire in questa sede tali connessioni si rinvia, sul tema, a Ponti 2024, p. 58 ss. Più ampiamente sul tema della regolazione dei dati nell'ambito della

Da ultimo, deve darsi conto di un ulteriore fattore caratterizzante il cyberspazio, rappresentato dal fatto che nessuna delle componenti del medesimo costituisce una monade isolata e indipendente, configurando piuttosto una parte del tutto (a questo, e alle altre componenti dello stesso, connessa)[43].

Una caratteristica, quella della interconnessione/interdipendenza – che emerge anche da alcune definizioni di cyberspazio contenute in documenti diffusi a livello internazionale[44] – che si traduce nell'idea secondo la quale la garanzia dell'integrità e della capacità di operare correttamente ed efficientemente delle singole componenti del cyberspazio può configurare un elemento atto ad assicurare il funzionamento e la sicurezza del medesimo (complessivamente inteso): come è stato infatti osservato, in certe circostanze anche una piccola vulnerabilità dei sistemi informativi, delle reti o dei dati può determinare incidenti e danni a parti più o meno vaste del cyberspazio[45].

Ne discende, da un lato, che le singole componenti di quest'ultimo, o quantomeno alcune di esse, nella prospettiva della cybersicurezza assumono una rilevanza e un valore che risulta molto maggiore di quello che esse avrebbero se considerate isolatamente e in sé; dall'altro, che gli Stati non possono limitarsi a garantire e proteggere esclusivamente quelle componenti che cadono sotto il proprio dominio (la propria sovranità), dovendosi preoccupare anche delle scelte e delle condotte degli altri Stati.

Ne dovrebbe conseguire una "comune e globale" tensione di tutti gli Stati verso il conseguimento dell'obiettivo del raggiungimento di un elevato livello di sicurezza dei sistemi informatici e di rete, dei dati e in generale delle componenti che regolano il funzionamento del cyberspazio.

Le cose, tuttavia, non stanno sempre in questi termini, e talvolta la realtà offre scenari ben diversi.

Ciò si deve al fatto che alcuni Stati possono non aver alcun desiderio di garantire la sicurezza e il buon funzionamento delle strutture che si collocano nell'ambito della sfera della propria sovranità, o potrebbero addirittura voler sfruttare tale circostanza per ottenere vantaggi sul piano geopolitico e delle relazioni internazionali.

A ciò aggiungasi che alcuni Stati, ancorché "volenterosi", potrebbero non essere in grado di garantire adeguati livelli di cybersicurezza per carenza di risorse o di capacità tecniche.

Ecco perché pensare che possa conseguirsi un adeguato livello di sicurezza del cyberspazio (e di una o più delle attività che nel medesimo vengono svolte) mediante le attività di cybersicurezza o cyberdifesa che gli Stati *spontaneamente*, vale a dire in assenza di obblighi vincolanti, pongono in essere, rappresenta un'illusione, e dunque un presupposto errato da cui muovere.

Occorre piuttosto ragionare di una regolazione del cyberspazio[46] (e della costruzione di

società digitale v. Iannuzzi 2024, p. 107 ss.; Calzolaio 2023, p. 13 ss.; Colapietro 2023, p. 151 ss.; Colapietro 2021, p. 831 ss.

43. Sul tema del rapporto tra interconnessione e sicurezza (del cyberspazio) v. Djurdjevic–Stevanovic 2016, p. 15 ss.
44. Si veda ad esempio quella che si rinviene nel Volume 2 del documento NISTIR 8074, redatto dall'*International Cybersecurity Standardization Working Group del National Security Council's Cyber Interagency Policy Committee* statunitense, che lo descrive come un "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it" (International Cybersecurity Standardization Working Group of the National Security Council's Cyber Interagency Policy Committee, NISTIR 8074, Volume 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, December, 2015).
45. Salvaggio 2023, p. 140: "Although the application of adequate software engineering processes can reduce the probability of exploitable weaknesses and mitigate their severity, even a small mistake on the part of one of the many members of a developing chain can remain unnoticed for long while fully compromising the security of the systems overall".
46. Abbandonando così definitivamente l'approccio basato sulla affermata necessità di "lasciare libera" la rete, approccio i cui principi ispiratori sono compendiati nella nota *Declaration of the Independence of Cyberspace* di J.P. Barlow del 1996.

architetture organizzative e istituzionali di cybersicurezza) effettuata a mezzo degli strumenti del diritto internazionale, con la definizione di regole accettate da un numero il più possibile elevato di Stati, che contemperi le esigenze della (preservazione) della sovranità dei medesimi con quelle connesse alla cybersicurezza e alla garanzia del buon funzionamento dei sistemi e delle reti (e conseguente salvaguardia delle attività e dei diritti che tramite le stesse vengono esercitate)[47].

Non potendo in questa sede approfondire il tema di quale debba considerarsi, fra quelli proposti, il modello più efficace e realizzabile di regolazione globale del cyberspazio, ci si limiterà a ragionare sul se e su quali limitazioni alla sovranità degli Stati imponga la costruzione di architetture di cybersicurezza che prevedano obblighi specifici per gli Stati medesimi, e se tale costruzione imponga, in ragione delle caratteristiche del cyberspazio, un'erosione del *government* in favore di modelli di *governance* ovvero se il primo conservi una sua primarietà nelle questioni concernenti la cybersicurezza.

Procedendo sul tema, si osserva che ai singoli Stati potrebbe venir richiesta una limitazione di sovranità che potrebbe afferire ad esigenze di "protezione fisica" di una o più infrastrutture, ovvero l'accettazione di regole (tecniche e non) concernenti la realizzazione e il successivo mantenimento in funzione delle infrastrutture stesse o la garanzia delle attività che si svolgono nel cyberspazio.

La prima tipologia di richiesta è naturalmente difficilmente "digeribile", per gli Stati, specie laddove la medesima dovesse prevedere la presenza "sul territorio" di elementi (strutture, veicoli, tecnici o addirittura soldati) riferibili a realtà statuali straniere.

È invece più probabile che questi ultimi accettino la definizione di regole e standard concernenti il funzionamento e la sicurezza di uno o più aspetti del cyberspazio (comprese le infrastrutture)[48] ovvero di entrare a far parte di un circuito di cooperazione e gestione in qualche modo "condivisa" (anche per il mezzo di network di enti o organismi) di eventuali minacce e incidenti: si tratta indubbiamente anche in questo caso di cessioni di sovranità – sul piano della potestà legislativa, e quindi della produzione di regole, o dell'organizzazione amministrativa o di altro ancora – ma alle quali diversi Stati, in molti altri ambiti (la storia dell'ordinamento dell'Unione europea ne fornisce la più evidente conferma), hanno acconsentito.

Rispetto, dunque, al descritto profilo, appare del tutto possibile che gli Stati accettino limitazioni alla propria sovranità, limitazioni che, a ben vedere, rispondono agli interessi degli Stati stessi, i quali (unitamente al "popolo" agli stessi riferibile) oltre a poter trarre vantaggio da un cyberspazio "ben funzionante" potrebbero ottenere benefici da risorse (economiche e tecniche) loro assegnate quale contropartita all'assunzione di obblighi volti alla costruzione di un determinato modello di *governance* della cybersicurezza e a garanzia dell'efficace adempimento degli stessi.

Si è utilizzato appositamente il termine *governance* in ragione delle caratteristiche che possiedono alcuni dei modelli di architetture di cybersecurity che sono stati storicamente definiti (in particolare negli Stati Uniti d'America e nell'ordinamento dell'Unione europea), caratteristiche che *apparentemente* collocano i medesimi in una posizione distante dai tradizionali modelli di *government*.

Un'importante presenza di regole e standard a forte contenuto tecnico – elaborate nell'ambito di

47. In effetti, molte voci si sono espresse in tal senso, senza che tuttavia sia emersa una soluzione condivisa circa il modello regolatorio da considerarsi più adatto e le modalità di ripartizione degli obblighi tra i singoli Stati; come è stato infatti rilevato in dottrina, "mentre alcuni esperti, come evidenziato nello studio 'Cyber Governance: Balancing Sovereignty and Global Cooperation' (Oxford Journal of Cyber Policy, 2023), sostengono che il cyberspazio debba essere considerato un bene comune globale, altri, come riportato nel 'NATO Cyber Defence Policy Framework' (2024), enfatizzano la necessità di una regolamentazione sovrana che permetta agli stati di controllare e proteggere i propri asset digitali" (così Calabrese, 2025).

48. Come è stato osservato, "establishment and use of international cybersecurity standards are essential for: ensuring the integrity and reliable operation of critical infrastructure, improving trust in online transactions, mitigating the effects of cyber incidents (e.g., crime), and ensuring secure interoperability among trade, law enforcement, and military partners, thereby facilitating increased efficiencies in the global economy" (Nistir, Volume 2, cit., p. 2).

processi decisionali sostanzialmente cooperativi e ai quali partecipano diversi attori (statali e non) –, la prevista istituzione di Autorità e organismi a loro volta dotati di ampia *expertise*, una (almeno apparente) compressione della discrezionalità politico-amministrativa degli Stati e incentivi all'attivazione di forme di partenariato pubblico privato costituiscono elementi che sembrano ricondurre le architetture istituzionali e normative di cybersecurity che si rinvengono in alcune importanti realtà alla vasta ed eterogenea (e invero forse indefinita) costellazione dei modelli di *governance*, e che parrebbero collocare in una posizione di secondo piano i "dispositivi tradizionali di government statale"[49].

Si tratta tuttavia di una conclusione solo apparentemente corretta, come emergerà dalla disamina di uno specifico quadro normativo-istituzionale concernente la cybersicurezza (quello europeo) e dal suo raffronto con quello riconducibile ad uno Stato membro dell'Unione (l'Italia), disamina che – si ritiene – mostrerà come in materia di cybersicurezza appaia corretto parlare, più che di crisi della sovranità, di compenetrazione e complementarietà fra *governance* e *government*, con il secondo a costituire il reale fondamento della prima (alle condizioni dallo stesso poste).

3. I quadri giuridico-normativi in materia di cybersecurity degli ordinamenti europeo e italiano

In riferimento al contesto europeo (e limitando l'analisi alle iniziative e agli atti concernenti in via diretta la cybersicurezza[50]) un primo atto che può menzionarsi è la comunicazione congiunta della Commissione europea e dell'Alto Rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza del 7 febbraio 2013, dal titolo *Strategia dell'Unione europea per la cybersicurezza: un ciberspazio aperto e sicuro*[51].

In essa emergeva la consapevolezza delle istituzioni dell'Unione circa l'importanza del cyberspazio e della necessità di una sua regolazione al fine di tutelare diritti, beni e valori di sicuro rilievo per l'ordinamento europeo (quali "i diritti fondamentali, la democrazia e lo Stato di diritto") rispetto al rischio del verificarsi di "incidenti, attività dolose e abusi"[52].

Inoltre, la Strategia metteva bene in luce la pluralità di soggetti (pubblici e privati) dai quali dipendono l'organizzazione e il funzionamento del cyberspazio, pluralità che doveva venir prioritariamente considerata nella definizione dei modelli di *governance* (così espressamente denominati) di quest'ultimo[53].

49. Quella riportata è una citazione tratta dal volume di Chessa 2019.
50. Ed infatti, è opportuno precisare che le iniziative dell'Unione europea "hanno riguardato l'ambito trasversale a diverse politiche dell'Ue della sicurezza delle reti e sicurezza dell'informazione" (così Marrani 2021, p. 80). Proprio la "trasversalità" della "materia" cybersicurezza ha imposto all'Unione di prevedere, in tutti gli atti afferenti al tema, disposizioni concernenti il raccordo con altre politiche settoriali e con discipline che, regolando attività che si svolgono principalmente per il tramite della rete, intercettano direttamente o indirettamente il tema della cybersicurezza (tra cui il GDPR, il *Digital Markets Act*, il *Digital Services Act*, l'*AI Act*).
51. Doc. JOIN(2013) 1. È tuttavia opportuno precisare che il termine "cybersecurity" era comparso già nella relazione sull'implementazione della Strategia europea in materia di sicurezza del 2003, pubblicata nel 2008 (Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 dicembre 2008), ma "è il 2013 a costituire l'anno spartiacque in termini di avanzamento cibernetico a livello comunitario" (Borriello–Fristachi 2022, p. 162). Per una ricostruzione di atti e politiche europee latamente riconducibili alla cybersicurezza adottate in epoca antecedente al 2013 si rimanda alla ricostruzione di Longo 2024-c, p. 209 ss.
52. Per entrambi i riferimenti v. il § *1.1. Contesto*.
53. Al § 1.2. *Principi della cibersicurezza*, si legge che "il mondo digitale non è controllato da un'entità singola: attualmente sono parecchi i soggetti interessati, tra cui entità commerciali e non governative, implicati nella gestione quotidiana delle risorse, dei protocolli e delle norme di internet e nel futuro sviluppo della rete. L'Ue ribadisce l'importanza di ciascun soggetto interessato nell'attuale modello di governance e appoggia questo approccio partecipativo alla governance di internet" e che "la crescente dipendenza dalle tecnologie dell'informazione e delle comunicazioni in tutti i campi della vita umana ha creato vulnerabilità che è necessario definire

Nel sottolineare la centralità degli Stati nella definizione delle politiche e delle azioni in materia di cybersicurezza, la *Strategia* indicava alcuni interventi specifici volti a "rafforzare l'efficienza complessiva dell'Ue" (in materia), con particolare riferimento allo sviluppo della cyber-resilienza – tesa "a contrastare i rischi e le minacce cibernetiche aventi dimensione transfrontaliera e a preparare a una risposta coordinata in situazioni di emergenza" – e della cybersicurezza (nell'Unione europea), quest'ultima intesa come funzionale ad "aumentare la resilienza dei sistemi informativi e di comunicazione che supportano gli interessi della difesa e della sicurezza nazionale degli Stati membri"; rispetto alle azioni e alle direttrici indicate, un ruolo di primario rilievo veniva attribuito all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), che era stata istituita nel 2004[54].

Sulla Strategia il Parlamento adottò una apposita Risoluzione (il 12 settembre 2013), che – nel condividere nel complesso il contenuto della Strategia medesima e nel formulare ulteriori indicazioni e indirizzi – pose particolare enfasi sulla necessità dell'adozione (o dell'aggiornamento) di *Strategie nazionali per la cybersicurezza* da parte degli Stati membri, volte a disciplinare "gli aspetti tecnici e quelli relativi al coordinamento, alle risorse umane e alla dotazione finanziaria" e recanti "regole specifiche sui benefici e le responsabilità del settore privato, al fine di garantire la partecipazione di quest'ultimo, nonché a prevedere procedure complete per la gestione del rischio e a salvaguardare il quadro normativo" (punto 5).

L'adozione di Strategie nazionali (in materia di sicurezza delle reti e dei sistemi informativi) venne ad assumere carattere obbligatorio a fronte dell'entrata in vigore della Direttiva NIS, la quale "rappresenta la prima disciplina UE introdotta con l'intento di innalzare la protezione della rete e dei sistemi informativi degli Stati membri dell'Unione attraverso un approccio orizzontale"[55].

Oltre a rendere obbligatoria la definizione di Strategie nazionali, la Direttiva NIS definì (in un'ottica di armonizzazione) i contenuti minimi obbligatori delle Strategie, che dovevano individuare (art. 1, par. 1), oltre a obiettivi e priorità, il "quadro della governance" ("inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti") per il conseguimento degli stessi, le misure di preparazione, risposta e recupero, "inclusa la collaborazione tra settore pubblico e settore privato", programmi di formazione, sensibilizzazione e istruzione e piani di ricerca e sviluppo, oltre a un piano di valutazione dei rischi e "un elenco dei vari attori coinvolti nell'attuazione della strategia"[56].

Inoltre, la Direttiva previde (all'art. 8) l'obbligo, per gli Stati, di istituire "Autorità competenti in materia di sicurezza delle reti e dei sistemi informativi" e un "Punto di Contatto Unico in materia di sicurezza delle reti e dei sistemi informativi" (che poteva coincidere con l'Autorità), dotati (l'una e l'altro) "di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della […] direttiva" (così l'art. 8, al par. 5).

Gli Stati erano poi tenuti a designare "Gruppi di intervento per la sicurezza informatica in caso di incidente" (CSIRT), destinati a essere inseriti in una rete europea (art. 12), e a stilare elenchi di operatori di servizi essenziali e digitali, chiamati ad adottare una serie di misure (di prevenzione e gestione dei rischi) e a notificare all'Autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi prestati.

Di fondamentale rilievo risultavano, altresì, i previsti obblighi di sicurezza e di notifica per gli

adeguatamente, analizzare in profondità, riparare o ridurre. Tutti gli attori implicati, siano essi autorità pubbliche, settore privato o singoli cittadini, devono riconoscere questa responsabilità condivisa, attivarsi per proteggersi e se necessario assicurare una risposta coordinata per rafforzare la cibersicurezza".

54. Ad opera del Regolamento (CE) 2004/460 del 10 marzo 2004.

55. Matassa 2023, p. 29.

56. L'imposizione agli Stati membri dell'Unione di adottare strategie nazionali era funzionale a garantire che i medesimi fossero in condizione di "reagire – attraverso il recupero dei servizi – a potenziali attacchi cibernetici distruttivi" (Borriello–Fristachi 2022, p. 162).

"operatori di servizi essenziali" e per i "fornitori di servizi digitali"[57].

Per entrambe le categorie di fornitori di servizi (pur con qualche differenza) la Direttiva prevedeva che gli Stati membri definissero obblighi di adozione di misure tecnico-organizzative (adeguate a gestire i rischi e a minimizzare l'impatto di incidenti[58]) e di notifica di incidenti aventi un impatto rilevante sulla continuità dell'erogazione dei servizi medesimi (anche nell'ottica di ricevere il supporto dell'Autorità nazionale competente e del CSIRT).

Nel 2017 è stata adottata la seconda *Strategia* in materia di cybersicurezza, imperniata sui tre concetti fondamentali di resilienza, deterrenza e difesa, che prefigurava la necessità della riforma dell'ENISA, riforma operata concretamente dal citato Regolamento (UE) 2019/881, che ha ridefinito poteri e funzioni dell'Agenzia (peraltro ridenominandola Agenzia dell'Unione europea per la cybersicurezza) e ha delineato un quadro comune europeo per la certificazione della sicurezza di prodotti e servizi ICT[59].

I poteri che il Regolamento attribuisce all'ENISA (di cui vengono sottolineate "l'indipendenza e la particolare 'capacità tecnica'") sono ampi, e volti, fondamentalmente, a fornire supporto alla Commissione e agli Stati membri "nell'elaborazione e nell'attuazione di politiche dell'Unione relative alla cybersicurezza, ivi comprese le politiche settoriali in materia di cybersicurezza" (art. 4, par. 2) e nello sviluppo delle capacità di prevenzione, rilevazione e analisi delle minacce informatiche e degli incidenti (art. 6), oltre che a rafforzare la cooperazione fra gli Stati e fra questi e l'Unione[60].

Del dicembre 2020 è invece la *EU's Cybersecurity Strategy for the Digital Decade*[61], avente quale elemento cardine "l'istituzione di un'unità congiunta per il ciberspazio (nota come Joint Cyber Unit o

57. Trattasi di categorie di fornitori di servizi considerati di particolare rilievo per il funzionamento delle società moderne (e del mercato interno). Gli operatori di servizi essenziali dovevano essere identificati (e inseriti in apposito elenco) dagli Stati membri sulla base di criteri definiti (invero in modo ampio e generico) dalla Direttiva e laddove tali operatori operino in un dei settori qualificato come essenziale dalla Direttiva medesima (all'Allegato II); i fornitori di servizi digitali venivano invece circoscritti a tre tipologie, identificate nell'Allegato III alla Direttiva, che richiamava i seguenti servizi: Mercato *online*; Motore di ricerca *online*; Servizi nella nuova (*cloud computing*).
58. La Direttiva non indicava direttamente la metodologia da utilizzare per la definizione delle misure di sicurezza, riconoscendo in questo senso ampia discrezionalità agli Stati. All'inevitabile rischio di frammentazione connesso a tale situazione ha fornito parziale di rimedio il gruppo di cooperazione dei CSIRT, che ha definito indicazioni e orientamenti (v. in particolare il *Reference document on security measures for Operators of Essential Services*, CG Publication 01/2018).
59. Tra gli obiettivi del Regolamento (secondo quanto previsto dall'art. 1, par. 1, del medesimo) vi era quello di definire "un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione". A tal fine il Regolamento dispone l'istituzione di un Quadro europeo di certificazione della cibersicurezza (il quale, secondo quanto previsto dall'art. 46, par. 2, "prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita") oltre che il varo, da parte della Commissione, di un "programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza" (art. 47).
60. L'attribuzione all'ENISA di compiti sostanzialmente consultivi è stata fatta oggetto di critiche, da parte della dottrina, che ha sottolineato come, a livello europeo, "sarebbe stato preferibile attribuire all'Agenzia funzioni maggiormente incisive, in considerazione della rilevanza del bene giuridico tutelato e della crescente esigenza di sicurezza informatica all'interno del mercato unico digitale" (così Previti 2022, p. 74).
61. Doc. JOIN(2020) 18.

JCU) come piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cybersicurezza all'interno dell'Ue, ciò con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera"[62].

Con la Direttiva NIS II si è poi inteso innalzare ulteriormente il livello della cybersicurezza europea (anche alla luce delle emerse lacune della Direttiva NIS I), principalmente mediante ampliamento del novero dei fornitori di servizi (con il venir meno della distinzione tra fornitori di servizi essenziali e fornitori di servizi digitali) soggetti agli obblighi e agli adempimenti previsti dalla Direttiva stessa e, ciò che forse costituisce la novità più rilevante, tramite definizione di criteri più dettagliati per l'individuazione degli stessi, con correlativa diminuzione degli spazi di discrezionalità degli Stati membri. Inoltre, la Direttiva ha inteso procedere nel senso dell'implementazione di una politica di "coordinated vulnerability disclosure" prevedendo (all'art. 12) l'istituzione di una banca dati europea delle vulnerabilità e che i singoli Stati adottino proprie regolazioni concernenti le modalità di rilevamento delle vulnerabilità dei sistemi informatici[63].

Del 2024 è il *Cyber Resilience Act* (Regolamento (UE) 2024/2847), relativo ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali[64] mentre, da ultimo, occorre menzionare il *Cyber Solidarity Act* (Regolamento (UE) 2025/38), che contiene disposizioni atte a declinare il contrasto alla cybersicurezza in una logica sempre più "comunitaria", definendo un sistema "integrato" tra gli Stati membri atto a garantire la sicurezza informatica.

La prospettiva dalla quale il Regolamento ora citato prende le mosse è rappresentata dalla "necessità di rafforzare rilevamento e conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione e intensificare la solidarietà migliorando la preparazione e la capacità degli Stati membri e dell'Unione di prevenire gli incidenti di cybersicurezza significativi e gli incidenti di cybersicurezza su vasta scala e di rispondervi" (così il considerando n. 7).

In tale ottica, il Regolamento prevede l'istituzione di una rete paneuropea di Poli informatici (denominata *Sistema europeo di allerta per la cybersicurezza*) e di un "meccanismo per le emergenze di cybersicurezza", al fine in particolare di "sostenere gli Stati membri, su loro richiesta, nella preparazione e nella risposta agli incidenti di cybersicurezza significativi e agli incidenti di cybersicurezza su vasta scala, nell'attenuarne l'effetto e nell'avviare la ripresa dagli stessi" (così sempre il considerando n. 7).

La disamina dell'architettura e dell'insieme dei soggetti chiamati a realizzare gli obiettivi di cybersicurezza definiti dal Regolamento in parola offre spunti di sicuro interesse.

Il Regolamento, come accennato, prevede l'istituzione di un *Sistema europeo di allerta per la cybersicurezza* costituito da una "rete paneuropea di Poli informatici", la cui *mission* è costituita dallo sviluppo e dal potenziamento di "capacità coordinate in materia di rilevamento e capacità comuni in materia di conoscenza situazionale" (a fini di cybersecurity), e di cui fanno parte tanto Poli informatici nazionali quanto Poli informatici transfrontalieri.

I Poli informatici nazionali sono posti e agiscono "sotto l'autorità di uno Stato membro" (così come espressamente riconosciuto dall'art. 4, par. 2), e per quanto concerne la natura giuridica, la struttura e l'organizzazione dei medesimi il Regolamento lascia agli Stati ampia discrezionalità[65], ponendo requisiti invece più stringenti in riferimento a capacità funzionali e prestazionali[66].

62. Matassa 2023, p. 28 ss.

63. In tema Ricotta 2024, p. 82 ss.

64. Per approfondimenti si rimanda a Chiara 2023, p. 143 ss.

65. Ai sensi dell'art. 4, par. 2 del Regolamento, infatti, "può trattarsi di un CSIRT o, se del caso, di un'autorità nazionale di gestione delle crisi informatiche o di un'altra autorità competente designata o istituita a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, o di un altro soggetto".

66. Più nello specifico, il Regolamento prevede che ciascun Polo informatico nazionale debba possedere la capacità "di fungere da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello

Da un lato, dunque, il Regolamento riconosce ampia discrezionalità agli Stati membri per quanto concerne l'istituzione e la definizione delle caratteristiche dei Poli informatici nazionali, dall'altro, prevedendo i menzionati requisiti di capacità e prestazionali, pone "limiti esterni" a detta discrezionalità, richiedendo agli Stati membri di garantire l'idoneità dei propri Poli nazionali a rispettare gli standard e a conseguire gli obiettivi dallo stesso individuati.

Gli Stati possono poi scegliere di far aderire un proprio Polo informatico ad un Polo informatico transfrontaliero, organismo, quest'ultimo, definito come "una piattaforma multinazionale, istituita mediante un accordo di consorzio scritto, che riunisce in una struttura di rete coordinata i poli informatici nazionali di almeno tre Stati membri e che è concepita per migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche, per impedire gli incidenti informatici e per favorire l'elaborazione di analisi delle minacce informatiche, in particolare mediante lo scambio di dati e informazioni pertinenti, se del caso anonimizzati, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia" (art. 2, n. 1).

L'adesione di un Polo nazionale ad un Polo transfrontaliero (adesione che, lo si ribadisce, ha natura volontaria) implica l'impegno da parte del primo ad aderire ad un accordo di consorzio che prevede, fra le altre cose, lo scambio di rilevanti informazioni[67] e il perseguimento di determinati obiettivi di "sviluppo di strumenti e tecnologie avanzati, quali gli strumenti di intelligenza artificiale e di analisi dei dati" (art. 6, par. 2, lett. c)[68].

Oltre al descritto *Sistema europeo di allerta per la cybersicurezza*, il Regolamento prevede poi l'istituzione di un *Meccanismo per le emergenze informatiche* e di un *Meccanismo di riesame degli incidenti di cybersicurezza*.

Il primo persegue gli obiettivi di sostenere le azioni di preparazione di soggetti operanti in settori cruciali per la società, al fine di sondarne le capacità di resistenza nei confronti di eventuali minacce e creare una riserva dell'Ue per la cybersicurezza concernente servizi pronti per essere erogati su richiesta di Stati membri o istituzioni per aiutare i medesimi a gestire gli incidenti di cybersicurezza significativi o su vasta scala, ovvero garantire assistenza a uno Stato membro che stia a sua volta assistendo un altro Stato membro interessato da un incidente di cybersicurezza; il *Meccanismo di riesame degli incidenti di cybersicurezza* è invece volto a consentire agli organismi ed alle istituzioni dell'Unione e degli Stati membri di trarre insegnamenti dagli incidenti nell'ottica di migliorare le risposte agli incidenti medesimi.

Questi gli elementi più rilevanti del Regolamento (UE) 2025/38. L'analisi degli stessi, ma invero del complessivo quadro giuridico europeo in materia di cybersicurezza, consente di effettuare alcune considerazioni sul tema del rapporto tra *government* e *governance*, e di chiedersi se uno dei due (e nel caso quale) debba considerarsi prevalente rispetto all'altro, o comunque caratterizzante il sistema.

Nel rispondere positivamente, verrebbe quasi istintivo indicare, quale istituto caratterizzante la regolazione della cybersecurity, la *governance* (termine al quale, peraltro, molti degli atti esaminati fanno espresso richiamo), ma un'analisi più cauta

nazionale per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti informatici e per contribuire a un polo informatico transfrontaliero" (art. 4, par. 2, lett. a) ed essere in grado "di rilevare, aggregare e analizzare dati e informazioni relativi alle minacce e agli incidenti informatici, come le analisi sulle minacce informatiche, utilizzando in particolare tecnologie all'avanguardia, al fine di prevenire gli incidenti" (art. 4, par. 2, lett. b).

67. Tra le informazioni da porre ad oggetto di condivisione, secondo quanto disposto dall'art. 6, par. 1, quelle relative a "minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di cybersicurezza e raccomandazioni relative alla configurazione degli strumenti di cybersicurezza per rilevare gli attacchi informatici, tra loro all'interno del polo informatico transfrontaliero".

68. In conclusione di questa assai sintetica disamina del Sistema europeo di allerta per la cybersicurezza delineato dal Regolamento (UE) 2025/38, si osserva poi che gli Stati che intendano aderire al medesimo sono tenuti a farsi carico di obblighi concernenti la garanzia di "un elevato livello di cybersicurezza" (secondo quanto previsto dall'art. 8) e il finanziamento del sistema e delle attività allo stesso riconducibili.

e meditata consente di delineare un quadro ben diverso, che restituisce una piena centralità al *government*, e dunque alla sovranità, degli Stati.

Ed infatti, in tutti gli atti (normativi e non) che compongono il quadro giuridico concernente la cybersicurezza europea viene affermato e ribadito, a riguardo di molti ambiti e profili, il rispetto, da parte dell'ordinamento unionale, della sovranità e della "discrezionalità politica" dei singoli Stati, cui è riconosciuta ampia autonomia nell'adozione delle misure ritenute necessarie a proteggere beni e valori essenziali – quali la sicurezza, l'ordine pubblico, il perseguimento di reati[69] – e nella definizione in concreto delle proprie Strategie nazionali, oltre che nella definizione dell'organizzazione amministrativa preposta a tale fine[70].

Rispetto, in particolare, all'ultimo profilo menzionato, si rileva che l'organismo europeo che occupa una posizione di centrale rilievo nell'ambito dell'architettura della cybersicurezza, l'ENISA, risulta essere titolare più di funzioni di supporto e cooperazione con le Autorità e gli organismi degli Stati membri che di prerogative e poteri suscettibili di vincolare unilateralmente (sul piano normativo o amministrativo) questi ultimi[71].

Per quanto concerne le Autorità nazionali competenti (la cui istituzione è stata prevista a partire dalla Direttiva NIS I), giova osservare che la normativa unionale lascia agli Stati grande libertà nel definirne natura e organizzazione: non a caso, nel panorama dei diversi ordinamenti degli Stati membri si rinvengono attribuzioni di funzioni di Autorità nazionali competenti tanto ad Autorità indipendenti quanto a enti governativi (Ministeri, Capi di Governo) o comunque in varia misura dipendenti dai governi[72].

69. In questo senso vanno, ad esempio, l'art. 1, par. 6, della Direttiva NIS I – il quale stabilisce che "la presente direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati" (v. anche il considerando n. 8) – o i paragrafi 4 e 5 dell'art. 1 del Regolamento (UE) 2025/38 che prevedono, rispettivamente, che "le azioni intraprese a norma del presente regolamento sono realizzate nel debito rispetto delle competenze degli Stati membri e integrano le attività svolte dalla rete di CSIRT, da EU-CyCLONe e dal gruppo di cooperazione NIS" e che "il presente regolamento lascia impregiudicate le funzioni statali essenziali degli Stati membri, tra cui la garanzia dell'integrità territoriale dello Stato, il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza nazionale. In particolare, la sicurezza nazionale resta una competenza esclusiva di ciascuno Stato membro".

70. Trattasi invero di approccio che appare (ed è forse l'unico possibile, in questo senso) conforme all'art. 4, par. 2, del Trattato sull'Unione europea, il quale stabilisce che l'Unione "rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro".

71. Ed infatti, "l'attività principale dell'ENISA è quella di coordinare l'operato degli stati membri e favorire il dialogo intra-europeo, attraverso l'elaborazione di linee guida e l'individuazione di best practices. A questo scopo, l'agenzia pubblica molti documenti, disponibili online e liberamente consultabili, per cercare di tenere aggiornato lo stato dell'arte della cybersecurity in Europa e stimolare il confronto tra i vari stati, nell'intento che si affermino le pratiche più avanzate" (così Cencetti 2014, p. 26). In questo senso v. anche Bruno 2020, p. 13 s., che sottolinea come spia dell'approccio "rispettoso delle prerogative degli Stati membri in materia di disciplina delle attività di sicurezza sia rappresentata anche dalla configurazione dell'ENISA quale 'organo tecnico di assistenza alla Commissione europea ed agli Stati membri'".

72. Sono scelte riconducibili a quel fenomeno che è stato descritto in termini di "verticalizzazione della leadership in campo cyber a favore dei capi di governo, incentivata dalla necessità di evitare la frammentazione del potere in questi ambiti" (cfr. Longo 2024-a, p. 328). Si tratta di un processo che è stato commentato anche criticamente da quella parte di dottrina che vede con preoccupazione il protagonismo degli apparati governativi e spazi limitati per il controllo parlamentare e la partecipazione dei cittadini (su queste posizioni, tra gli altri, Pietrangelo 2024, p. 14 s. e Moroni 2024, *passim*).

Le scelte dell'ultimo tipo mostrano la volontà degli Stati di prevedere l'inserimento delle Autorità di cybersicurezza nel circuito governativo, e di fare delle stesse (anche) strumento di definizione e attuazione di politiche, facendo risultare l'aspetto politico-decisionale predominante su quello tecnico (che sarebbe invece risultato prevalente a fronte della individuazione di Autorità amministrative indipendenti).

Dunque, se da un lato l'istituzione di un apposito ente (e più in generale di un apparato amministrativo), attività che rientra nel novero dei metodi di risposta degli Stati "alle tradizionali minacce sperimentate nell'arena materiale di espressione della [propria] sovranità"[73], ha in questo caso una provenienza esogena rispetto ai meccanismi politico-decisionali degli Stati, l'esatta collocazione di tale ente (apparato) nel quadro costituzionale e dell'organizzazione amministrativa dello specifico ordinamento considerato risulta essere di esclusivo appannaggio degli Stati.

A fronte delle riportate considerazioni, mi pare che da un'analisi dell'evoluzione che il quadro normativo europeo in materia di cybersicurezza ha conosciuto negli anni emerga chiaramente come quelli che pure possono essere qualificati quali modelli di *governance* – nelle loro varie possibili declinazioni – mostrino la piena centralità del *government* per quanto concerne la regolazione del cyberspazio.

Ed infatti, se appare lecito parlare eventualmente di quella che è stata definita "sleeping sovereignity, che si desta solo quando essa stessa valuta opportuno destarsi"[74], e/o di un (volontario e deliberato) arretramento della decisione politica in favore di una regolazione avente un indubitabile contenuto tecnico (e il cui sviluppo richiede un necessario – ma comunque voluto, dalla parte pubblica-statuale – coinvolgimento di attori privati) resta il fatto che la costruzione dell'architettura della cybersicurezza unionale non prescinde affatto dal *government* dei singoli Stati e, anzi, ne conferma la piena presenza, quale espressione di quella "sovranità digitale" che si concretizza nella capacità di questi ultimi (e di riflesso della stessa Unione europea) "to act independently in the digital world", anche in riferimento alle questioni concernenti la regolazione e la gestione del cyberspazio[75].

L'affermazione della effettività della sovranità digitale impone di tener conto delle caratteristiche del cyberspazio e del tema della interconnessione/interdipendenza in materia di cybersicurezza – e quindi di strutturare un'architettura normativo-organizzativa che preveda anche forme di cooperazione con Enti e organismi di altri ordinamenti e di scambio di buone pratiche e informazioni – senza che ciò si traduca nello slittamento del *government* in forme di *governance* (le quali, come detto, prevedono processi decisionali aventi carattere prevalentemente orizzontale e condiviso, e in cui le decisioni politiche dei singoli Stati assumono carattere recessivo, venendo condizionate al punto da perdere il proprio contenuto e le proprie caratteristiche connotative).

Ulteriori conferme a tale conclusione provengono da alcune scelte normativo-regolatorie effettuate dall'ordinamento italiano, nell'ambito del quale si è venuto a definire un quadro giuridico del quale possono individuarsi alcuni elementi caratterizzanti.

Un primo elemento è costituito dalla centralità del ruolo assunto dal Presidente del Consiglio dei Ministri, centralità che si rinviene fin dalle prime disposizioni riferibili al tema (ed in specie quelle concernenti il "Sistema di informazione per la sicurezza della Repubblica", disegnato dalla legge 3 agosto 2007, n. 124[76]) e che risulta successivamente confermata da quelle attuative degli atti normativi

73. Così Giupponi 2024, p. 277.

74. Così Chessa 2019, p. 328.

75. La citazione è tratta dal documento dell'European Parliamentary Research Service *Digital sovereignty for Europe* del luglio 2020 (p. 1). Osservano in tema Sorrentino–Spagnuolo 2024, p. 689, che il concetto di sovranità digitale indica "la capacità di un Paese di esercitare autorità all'interno del cyberspazio, garantendo l'indipendenza tecnologica e il controllo sui dati personali". Sul concetto di sovranità digitale e sulle questioni regolatorie concernenti il web v. anche Bertola 2022, p. 39 ss. e Santaniello 2022, p. 47 ss.

76. Ai sensi della legge in parola, al Presidente del Consiglio dei Ministri spetta tra le altre cose "l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento" (così l'art. 1, comma 1,

europei (o che con questi ultimi erano comunque tenute a fare i conti).

Senza ripercorrere l'articolata evoluzione del quadro normativo, e soffermandoci esclusivamente sulle disposizioni vigenti, si rileva che il d.l. n. 82/2021 assegna al Presidente del Consiglio un complesso di compiti e funzioni che fanno del medesimo la figura cardine nella definizione delle politiche di cybersicurezza e delle misure di direttiva e indirizzo ai fini dell'attuazione delle stesse.

Ai sensi dell'art. 2, comma 1, del decreto-legge in parola, spettano in particolare al Presidente del Consiglio dei Ministri "a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza; b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) […]; c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale […] previa deliberazione del Consiglio dei ministri".

Numerose e rilevanti funzioni sono poi attribuite al Presidente del Consiglio dei Ministri dal c.d. Decreto *perimetro* (d.l. 21 settembre 2019, n. 105, recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*), specie a riguardo dell'individuazione dei soggetti e degli enti da includersi nel "perimetro di sicurezza nazionale cibernetica", in quanto tali tenuti al rispetto delle misure e degli obblighi previsti dal medesimo decreto, nonché dagli atti di recepimento delle Direttive europee NIS I e NIS II

lett. a), il coordinamento delle politiche dell'informazione per la sicurezza (e l'adozione, a tale fine, di apposite direttive sentito il Comitato interministeriale per la sicurezza della Repubblica) e un potere di carattere residuale funzionale all'emanazione di "ogni disposizione necessaria per l'organizzazione e il funzionamento del Sistema di informazione per la sicurezza della Repubblica" (per tutte le funzioni da ultime citata v. l'art. 1, comma 3, della legge in esame). Ai sensi del comma 3-*bis* dell'art. 1 della l. n. 124 del 2007 (inserito dall'articolo 1, comma 1, della l. 7 agosto 2012, n. 133) "il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali". Per quanto concerne il tema del raccordo tra l'azione del Presidente del Consiglio e il Parlamento, l'art. 38, comma 1-*bis*, della legge n. 124 prevede che il Governo alleghi alla relazione sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, che è tenuto a presentare annualmente al Parlamento, "un documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché' alla protezione cibernetica e alla sicurezza informatica". In attuazione del citato comma 3-*bis*, con d.P.C.M. 19 marzo 2013, n. 66, è stata adottata un'apposita Direttiva "recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", avente il fine specifico di definire, a legislazione vigente, un quadro strategico nazionale, "con la specificazione dei ruoli che le diverse componenti istituzionali devono esercitare per assicurare la sicurezza cibernetica del Paese e la predisposizione di meccanismi e procedure di azione secondo un approccio interdisciplinare e coordinato, su più livelli, che coinvolga tutti gli attori pubblici, ferme restando le attribuzioni previste dalla normativa vigente per ciascuno di essi, nonché gli operatori privati interessati" (così il Preambolo). La Direttiva, in tale ottica, delineava un'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, articolata su tre distinti livelli d'intervento, di cui il primo di indirizzo politico e coordinamento strategico (teso all'individuazione degli obiettivi anche attraverso l'elaborazione di un Piano nazionale per la sicurezza dello spazio cibernetico), il secondo "di supporto" e di attuazione di quanto definito al primo livello (in particolare nell'ambito della pianificazione), il terzo di gestione delle crisi, con il compito di curare e coordinare le attività di risposta e di ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate. Alla Direttiva del 2013 ha fatto poi seguito quella del 2015, in precedenza citata. L'architettura originariamente disegnata dal d.P.C.M. del 2013 è stata poi successivamente modificata ad opera del d.P.C.M. 17 febbraio 2017, n. 85, che ha ampliato le funzioni del Presidente del Consiglio dei Ministri, introdotto le definizioni di operatori di servizi essenziali e di fornitori di servizi digitali e previsto, in un apposito articolo (il 6) specifiche linee di azione per la sicurezza cibernetica.

(rispettivamente d.l. 18 maggio 2018, n. 65 e 4 settembre 2024, n. 138, con quest'ultimo che ha abrogato il primo).

Come è stato osservato, dal complesso dei menzionati atti normativi emerge con chiarezza una "notevole scelta accentratrice in materia di cybersicurezza", tesa "ad evitare che tendenze centrifughe – sia interne allo Stato sia esterne ad esso – possano compromettere lo svolgimento di quelle funzioni essenziali della Nazione che si realizzano mediante l'uso di reti e sistemi informatici"[77].

Il carattere "accentrato" (e "incentrato" sul Governo e sul Presidente del Consiglio) dell'architettura della cybersecurity nazionale è confermato dalle scelte concernenti la struttura e la natura delle Autorità e dei diversi organismi previsti dalle disposizioni europee e facenti parte (a vario titolo) dell'architettura della cybersicurezza.

Per quanto concerne "l'Autorità nazionale competente", il nostro Legislatore non ha optato per il modello dell'Autorità indipendente, bensì per quello dell'Agenzia, della quale peraltro il Presidente del Consiglio (o l'Autorità delegata eventualmente istituita) si avvale (secondo quanto espressamente stabilito dall'art. 5, comma 2, del d.l. n. 82/2021)[78].

L'Agenzia per la cybersicurezza nazionale, posta "sotto la guida politica del Presidente del Consiglio dei Ministri"[79], svolge peraltro anche funzioni di Punto di contatto unico NIS, di Gruppo nazionale di risposta agli incidenti di sicurezza informatica (il CSIRT, ovvero l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informativa per i settori, i sottosettori e le tipologie di soggetti individuati e definiti dal d.lgs n. 138/2024, e in specie dall'art. 15 del medesimo), di Autorità nazionale di gestione delle crisi informatiche, di Autorità nazionale di certificazione della cybersicurezza – ai sensi dell'articolo 58 del regolamento (UE) 2019/881 – e di Autorità competente per l'esecuzione dei compiti previsti dal regolamento delegato (UE) 2024/1366 della Commissione.

Si tratta, in larga misura, di funzioni di natura tecnica, che l'Agenzia è chiamata a svolgere anche in cooperazione con le altre Autorità nazionali e gli altri organismi previsti a livello europeo, nonché di funzioni di supporto all'autorità governativa, e in specie al Presidente del Consiglio dei Ministri, cui, a riguardo di molti profili, spetta l'assunzione delle decisioni "finali", che hanno ovviamente natura politico-amministrativa (natura che prevale su quella tecnica, pur presente[80]).

77. Longo 2024-a, p. 337.

78. L'Agenzia gode di alcune forme di autonomia, ad essa specificamente riconosciute dalla legge. In particolare, ai sensi dell'art. 5, comma 2, del d.l. n. 82 del 2021, la medesima "è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria", ancorché nei limiti previsti dal medesimo decreto; ciò farebbe dell'ACN un'Agenzia caratterizzata da "una più marcata autonomia rispetto ad altre agenzie", tale da collocarla "al di fuori del modello di agenzia creato dal d.lgs. n. 300/1999" (cfr. il dossier del Servizio Studi di Camera e Senato - A.C. 3161, Dossier su "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", 23 luglio 2021, p. 19 ss.). La sussistenza dei descritti ambiti di autonomia non è in ogni caso sufficiente a colmare lo spazio che separata il modello delle Agenzie da quello delle Autorità indipendenti (in questo senso cfr. Calzolaio 2024, p. 102), e a ricondurre dunque l'ACN a questo secondo novero.

79. Forgione 2022, p. 1120.

80. Ai sensi dell'art. 7 del d.l. n. 82 del 2021, l'Agenzia, tra le altre cose, predispone (lett. b) la Strategia nazionale di cybersicurezza, che viene poi adottata dal Presidente del Consiglio, sentito il Comitato interministeriale per la cybersicurezza, e svolge (lett. c) "ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza" – il quale, a sua volta, ai sensi dell'art. 8, comma 1, del medesimo decreto, svolge funzioni di "supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento" – oltre a supportare "il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro" (lett. i). A ciò aggiungasi che, secondo quanto stabilito dall'art. 6 della l. 28 giugno 2024, n. 90, il Presidente del Consiglio dei Ministri, sentiti il direttore generale del Dipartimento delle informazioni per la sicurezza e il direttore generale dell'Agenzia per la cybersicurezza nazionale, "può disporre il differimento degli obblighi informativi cui è in ogni caso tenuta l'Agenzia ai sensi delle disposizioni vigenti, ivi compresi quelli

4. Osservazioni conclusive

Alla luce di quanto si è illustrato nel corso del presente contributo, mi pare che possa affermarsi con relativa sicurezza che la *race for the cyberspace* vede un chiaro protagonismo degli Stati (e quindi degli ordinamenti statuali), i quali da un po' di tempo a questa parte sembrano aver pienamente compreso l'importanza del cyberspazio e la rilevanza delle minacce e degli incidenti informatici, che possono essere utilizzati anche per finalità geopolitiche (e di *cyberwarfare*).

Minacce e incidenti possono produrre conseguenze di estremo rilievo, pregiudicando l'erogazione di servizi, alterando il funzionamento dei mercati, sottraendo dati rilevanti (e sensibili) per utilizzi anche illeciti e in vari modi incidendo su diritti e libertà fondamentali dei cittadini.

Si tratta, dunque, come in precedenza si accennava, di difendere e salvaguardare valori e beni garantiti dalle Carte costituzionali di gran parte degli ordinamenti giuridici contemporanei: in particolare, oltre ai singoli diritti e alle singole libertà, vengono in rilievo la sicurezza pubblica, la difesa, e invero lo stesso corretto funzionamento dei sistemi democratici (dato che le minacce e gli incidenti informatici possono interferire con le funzioni degli organi costituzionali e a rilevanza costituzionale).

Di qui la sempre più sentita esigenza di costruire architetture organizzative e politiche di cybersicurezza volte a scongiurare minacce o incidenti e/o a minimizzarne l'impatto (ove l'attività di prevenzione risulti inefficace) e, parallelamente, a sviluppare la cyber-resilienza di sistemi e reti informatiche.

La definizione, tuttavia, di architetture di sistemi di cybersicurezza nazionali può produrre riflessi sul funzionamento complessivo del cyberspazio (luogo che, lo si è detto, è oggi insostituibile per lo svolgimento di gran parte delle attività che caratterizzano la quotidianità degli individui e il funzionamento dei mercati), i cui "luoghi" e le cui "componenti" sono, come illustrato, interconnessi a livello globale.

La regolamentazione di un oggetto avente simili caratteristiche, e l'esigenza degli Stati di non spogliarsi di proprie prerogative sovrane (evenienza inaccettabile stante il valore degli interessi in gioco), sembra imporre la definizione di regole condivise, secondo i classici moduli e schemi del diritto internazionale[81].

Non si è tuttavia ancora addivenuti alla definizione di simili regole (essendoci fino ad ora limitati alla sottoscrizione di documenti – come il *Cyber Defence Pledge* firmato al vertice NATO di Varsavia del 2016 – contenenti impegni aventi un'efficacia vincolante relativa) e forse tale obiettivo non verrà mai conseguito: e ciò anche in ragione del fatto che se il cyberspazio ha, come detto, caratteristiche di "luogo", lo stesso non è un territorio (essendo, anzi, connotato da de-territorialità), di talché rispetto ad esso non si tratta tanto di definire regole concernenti il regime giuridico di aree (e la misura della sovranità che i singoli Stati hanno su di essi) quanto piuttosto di regolamentare il funzionamento di attività e servizi e stabilire norme e obblighi atti ad assicurare che lo scambio di dati e informazioni sulle reti avvenga con determinate garanzie di non accadimento di incidenti informatici.

previsti ai sensi dell'articolo 17, commi 4 e 4-*bis*, del decreto-legge n. 82 del 2021, nonché il differimento di una o più delle attività di resilienza di cui all'articolo 7, comma 1, lettere n) e n-*bis*), del medesimo decreto-legge" a fronte di informativa ricevuta dalle Agenzie di informazione e sicurezza esterna e interna (disciplinate rispettivamente dagli articoli 6 e 7 della l. 3 agosto 2007, n. 124) che indichi il differimento come strettamente necessario "per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica". Anche in questo caso, esigenze concernenti la tutela di interessi fondamentali dello Stato, la cui valutazione è affidata al Presidente del Consiglio dei Ministri, sono destinate a prevalere su quelle concernenti l'adempimento, da parte dell'Agenzia nazionale per la cybersicurezza, degli obblighi sulla stessa incombenti.

81. Il parallelismo con la regolamentazione degli spazi marini appare in questo senso calzante. Osserva sul punto Calabrese 2025 che "come le acque internazionali, il cyberspazio è un dominio condiviso, dove diverse entità, siano esse statali o private, operano in uno spazio senza confini fisici definiti. Tuttavia, mentre le acque internazionali sono regolate da convenzioni globali come la Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS), il cyberspazio non dispone ancora di un quadro normativo altrettanto consolidato. Ciò crea un vuoto regolamentare che complica la governance e l'attribuzione delle responsabilità".

Il quadro è reso però complicato dal fatto che i singoli Stati non sempre sono disposti a condividere le informazioni che riguardano la cybersicurezza (con il termine informazione intendiamo qui riferirci tanto ai dati – e agli elementi "di fatto" che risultano rilevanti rispetto ad una determinata fattispecie e a una possibile minaccia – quanto alle conoscenze tecniche necessarie per costruire un sistema di difesa dagli attacchi che risulti efficace ed efficiente), considerato quanto le stesse possono risultare sensibili e rilevanti per la protezione di beni giuridici di rango anche costituzionale; ciò pone un freno allo *sharing* (delle informazioni), il che, a sua volta, limita l'efficacia delle azioni concernenti la cybersicurezza.

In tema, sarà importante osservare l'impatto che avrà il Regolamento (UE) 2025/38, il quale rileva che lo scambio di informazioni costituisce una delle attività che si pongono alla base del funzionamento dei Poli informatici transfrontalieri e che risulta funzionale a consentire ai Poli stessi, e a quelli nazionali, di "migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche", a "impedire gli incidenti informatici" e di "favorire l'elaborazione di analisi delle minacce informatiche" (così l'art. 2, n. 1, recante la definizione di "Polo informatico transfrontaliero", e l'art. 5, par. 4)[82].

Non a caso, il Regolamento contiene specifiche disposizioni atte a favorire – nell'ottica della costituzione del *Sistema europeo di allerta per la cybersicurezza* – la cooperazione e lo scambio di informazioni tra Poli informatici transfrontalieri e Poli informatici nazionali facenti parte di Poli informatici transfrontalieri (così in particolare l'art. 6), oltre che tra Poli informatici transfrontalieri e la rete di CSIRT (così l'art. 7), prevedendo altresì che la scelta degli Stati membri di far aderire a un Polo informatico transfrontaliero un proprio Polo informatico imponga a quest'ultimo di aderire ad un accordo di consorzio che preveda, tra le altre cose, di "mettere in comune i dati e le informazioni pertinenti sulle minacce e sugli incidenti informatici provenienti da varie fonti all'interno dei poli informatici transfrontalieri e condividere informazioni analizzate o aggregate attraverso i poli informatici transfrontalieri, se del caso con la rete di CSIRT" (art. 3, par. 2, lett. b).

Alla base dell'adesione ai Poli informatici transfrontalieri vi è, però, come si precisava in precedenza, una scelta volontaria degli Stati, ai quali peraltro il Regolamento riconosce la possibilità di escludere la comunicazione di informazioni "la cui divulgazione sarebbe contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa" (art. 1, par. 6); ne discende, a riguardo del profilo dello *sharing* delle informazioni, la constatazione che la scelta della definizione delle modalità di "presenza" nel cyberspazio e di contrasto e reazione a minacce e incidenti informatici resti saldamente in capo ai singoli Stati, che possono decidere – con decisione di natura politico-amministrativa – di aprirsi o meno alla cooperazione effettuando un bilanciamento tra la scelta di migliorare l'efficacia e l'efficienza della propria cybersicurezza (cooperando con organismi e Autorità di altri Stati e dell'Ue) e quella di mantenere la segretezza su determinati dati e informazioni.

Anche poi rispetto alla definizione dell'architettura istituzionale-amministrativa della *cybersecurity* si rinvengono elementi che confermano la piena presenza del *government* statale.

Considerato che, come è stato condivisibilmente affermato, l'organizzazione amministrativa (che ha una natura "funzionalizzata" in quanto si definisce in ragione degli obiettivi e delle funzioni da svolgersi per conseguirli[83]) costituisce "il più efficace e potente meccanismo di comando di cui disponga l'autorità, la più vasta e potente articolazione di dominio presente nell'ordinamento"[84], la medesima ha strettamente "a che fare" con la sovranità, la quale si declina, in questo senso, nella possibilità, per gli Stati, di definire la propria

82. Allo scambio di informazioni l'ordinamento unionale ha fin dalle origini riconosciuto un ruolo primario, nella definizione delle politiche (e degli obblighi) in materia di cybersicurezza. La Direttiva NIS I, ad esempio, qualificava detta attività come uno dei principali fattori di rafforzamento della cooperazione strategica fra gli Stati (e proprio con obiettivi di *information sharing* fu istituito il gruppo di cooperazione tra i CSIRT).

83. In questo senso cfr. Allegretti 2000, pp. 403 s., il quale osserva che "l'organizzazione non può non adeguarsi alle necessità della funzione" e che "è la funzione che determina il modo d'essere dell'organo".

84. Perfetti 2019, p. 65.

organizzazione (amministrativa) in modo pieno e in assenza di interferenze "esterne"[85].

Se le cose stanno in questi termini, deve allora concludersi che laddove tale organizzazione, o anche solo una parte di essa, risulti definita secondo modalità non riconducibili alla volontà politica di uno Stato (come concretizzatasi alla luce dei processi e degli schemi individuati dal quadro costituzionale di riferimento), la sovranità di quest'ultimo ne risulta affievolita.

Tale affievolimento può poi risultare da una scelta dello Stato, ovvero da un'imposizione di provenienza esterna allo stesso (e dal medesimo non voluta): solo in tale seconda ipotesi può in ipotesi parlarsi di effettivo "affievolimento", dato che nel primo caso pare più corretto ragionare di limitazione o "cessione" di sovranità (o al più di *sleeping sovereignty*), e dunque, di fatto, di *esercizio* di sovranità (secondo una specifica modalità, quella della auto-limitazione da parte dello Stato).

Ciò detto, giova richiamare che, rispetto al tema in esame, si rinviene un quadro di norme dell'Unione europea che è andato articolandosi e stratificandosi nel tempo, anche in riferimento ai profili della *governance* e dell'organizzazione amministrativa delle funzioni concernenti la cybersicurezza.

A partire in particolare dalla Direttiva NIS I, si è prevista l'istituzione di enti e organismi ascrivibili all'organizzazione amministrativa dei singoli Stati membri, ed in particolare Autorità nazionali competenti, Punti di contatto unici, Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e altri ancora.

A differenza di come ha operato in altri settori (si pensi a quelli dell'energia e del gas), nei quali all'obbligo, per gli Stati membri, di istituzione di enti o autorità pubbliche l'Unione europea ha fatto corrispondere la necessità della previsione, nell'ambito delle rispettive discipline istitutive, di contenuti minimi (atti ad esempio a garantire l'indipendenza e la funzionalità delle autorità), rispetto agli enti e agli organismi concernenti l'ambito della cybersicurezza l'ordinamento europeo riconosce agli Stati una ampia discrezionalità nella definizione della natura, dell'organizzazione e delle modalità di funzionamento degli stessi, non richiedendo la sussistenza della caratteristica dell'indipendenza degli organismi ma imponendo requisiti prestazionali e di idoneità a conseguire gli obiettivi: rispetto a tale quadro appare pienamente condivisibile l'osservazione secondo la quale, rispetto al quadro giuridico in materia di cybersecurity che si rinviene a livello sia europeo che nazionale, "l'autorità può non essere dotata del requisito dell'indipendenza, ma non può perdere quello della specializzazione, spesso della iper-specializzazione, tecnica"[86].

Altri esempi potrebbero poi essere riportati, ma il quadro pare ormai (almeno a chi scrive) sufficiente chiaro.

Dal medesimo, come si è più volte detto e argomentato nel corso del presente contributo, a riguardo del cyberspazio e delle funzioni di cybersicurezza emerge una compenetrazione tra modelli di *governance* e di *government*, con la prima che, lungi dal costituire un fattore di arretramento o "dissolvimento" delle sovranità statuali, pare configurare piuttosto una modalità specifica di esercizio di quest'ultima rispetto ad un oggetto, il cyberspazio, avente caratteristiche particolarissime (la sua natura mista fisico-virtuale, l'alto grado di interconnessione e interdipendenza fra le sue componenti, la sua rilevanza per l'esercizio di diritti e libertà fondamentali degli individui, gli effetti potenzialmente devastanti degli incidenti informatici…).

Nel cyberspazio gli Stati hanno compreso di poter (ambire a) esprimere la propria volontà di potenza, ma al contempo vedono nel medesimo

85. Richiamando le precedenti osservazioni concernenti l'individuazione del novero delle potestà pubbliche che possono ritenersi rientrare nelle prerogative della sovranità, si osserva che l'organizzazione costituisce uno degli elementi costitutivi degli ordinamenti giuridici, si può affermare, con relativa sicurezza, che la potestà di un ordinamento (*rectius*: dei poteri a ciò abilitati dal quadro normativo e costituzionale) di definire liberamente l'organizzazione degli uffici e degli organi titolari di potestà normative e amministrative costituisca una delle potestà direttamente connesse alla sovranità. In altre parole, se è vero (come è vero) che la sovranità implica che lo Stato è "libero di prendere, all'interno delle sue frontiere, tutte le decisioni amministrative e politiche che più gli convengono, fuori da ogni ingerenza da parte di uno Stato straniero" (così Freund 2008, p. 105), nel novero di tali decisioni rientrano indubbiamente quelle concernenti le predette istanze organizzative.

86. Calzolaio 2024, p. 105.

un fronte sterminato e difficilmente controllabile di potenziali attacchi, anche portati da altri Stati sovrani: tali constatazioni non offrono particolari margini allo sviluppo di schemi di *governance* alternativi al *government*, e ritengo non li offriranno mai.

Per tali ragioni, gli Stati tengono "stretta a sé" la cybersicurezza, allocando (non a caso) spesso e volentieri le funzioni alla medesima connesse al livello governativo.

Nel descritto quadro, ogni apertura a modelli di *governance* risponde sempre, in ultima istanza, a obiettivi e interessi dei singoli Stati, che possono rendere *dormiente* la propria sovranità e accettare forme di cooperazione, scambi di informazione o imposizione di regole se ciò consente a tali interessi (abbiano, gli stessi, natura economico-commerciale, (geo)politica, militare, sociale…) di meglio prosperare.

Non a caso, la mancata definizione di regole condivise a livello globale concernenti specificamente il cyberspazio non ha impedito a molti soggetti (compresi organizzazioni internazionali e Stati) di affermare come al cyberspazio medesimo si applichino le norme del diritto internazionale, comprese quelle relative al riconoscimento e al rispetto della sovranità sia interna che esterna degli Stati[87].

Un'applicazione (che invece altri contestano) che in ogni caso non potrà prescindere da qualche "adattamento": lo impone la natura del cyberspazio, il suo essere un luogo-non luogo, che richiede di pensare all'occupazione del territorio non in termini di invasione di aree territoriali (se si esclude il caso estremo dell'occupazione o della distruzione fisica di infrastrutture) bensì quale attività concernente l'acquisizione, senza il consenso dei legittimi titolari, di codici, protocolli e dati, oltre che la capacità di aggirare le difese informatiche di Stati, organizzazioni, imprese e individui.

È a tutto ciò che la definizione di modelli di *governance* è strumentale, non a consentire lo sviluppo di attività, mercati e/o processi decisionali a prescindere (o a scapito) dagli Stati; possiamo allora concludere affermando che il Leviatano è vivo e vegeto – come peraltro indirettamente conferma il *ReArm Europe Plan*, che è piano di riarmo degli Stati, non dell'Ue, e nel quale peraltro il tema della cybersicurezza non trova spazi – e "tenacemente presente" anche nelle datificate contrade della rete, e più in generale in quel "mondo nuovo che molti attendevano all'apparire della globalizzazione e della integrazione economica"[88].

Riferimenti bibliografici

U. Allegretti (2000), *La verità è nell'assunto: Stato e Istituzioni nel pensiero di Feliciano Benvenuti*, in "Jus", 2000, n. 3

A.C. Amato Mangiameli (2000), *Diritto e Cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, 2000

A. Barletta (2019), voce *Governance [dir. Cost.]*, in "Enciclopedia Treccani online", 2019

V. Bertola (2022), *La sovranità digitale e il futuro di Internet*, in "Rivista italiana di informatica e diritto", 2022, n. 1

J. Bodin (1576/1964), *Les six livres de la republique*, Paris, 1576 [trad. it. a cura di M. Isnardi Parente], UTET, I, 1964

G. Borriello, G. Fristachi (2022), *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in "Rivista di Digital Politics", 2022, n. 1-2

B. Bruno (2020), *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in "federalismi.it", 2020, n. 14

87. Per un inquadramento del tema cfr. Zorzi Giustiniani 2021 e Ruotolo 2021, p. 701 ss.

88. Cfr., per entrambe le citazioni, Cassese 2016, p. 45, che sul punto peraltro cita King–Lieberman 2009, p. 550.

D.L. Calabrese (2025), *Chi controlla il cyberspazio? La zona grigia della responsabilità*, in "AgendaDigitale", 12 febbraio 2025

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

S. Calzolaio (2023), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Casarosa, G. Comandé (2024), *Aspettando la NIS2: ovvero il diritto privato della cybersecurity*, in "Il Diritto dell'informazione e dell'informatica", 2024, n. 1

S. Cassese (2025), *L'Europa si difenda*, in "Corriere della Sera", 13 marzo 2025

S. Cassese (2016), *Territori e potere. Un nuovo ruolo per gli Stati*, il Mulino, 2016

C. Cencetti (2014), *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Edizioni Nuova Cultura, 2014

O. Chessa (2025), *Realismo geopolitico e volontà statale*, in "Diritto Costituzionale", 2025, n. 1

O. Chessa (2019), *Dentro il Leviatano. Stato, sovranità e rappresentanza*, Mimesis Edizioni, 2019

O. Chessa (2002), *Libertà fondamentali e teoria costituzionale*, Giuffrè, 2002

P.G. Chiara (2023), *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in "Rivista italiana di informatica e diritto", 2023, n. 1

C. Colapietro (2023), *Gli algoritmi tra trasparenza e protezione dei dati personali*, in "federalismi.it", 2023, n. 5

C. Colapietro (2021), *Circolazione dei dati, automatizzazione e regolazione*, in "Osservatorio sulle fonti", 2021, n. 2

A. Contaldo, L. Salandri (2020), *La disciplina della cybersicurezza nell'Unione Europea*, in A. Contaldo, D. Mula (a cura di), "Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche", Pacini Giuridica, 2020

D. Djurdjevic, M. Stevanovic (2016), *The Value Challenge of Interconnectedness in Cyberspace for National Security*, Sinteza, 2016

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

M. D'Orsogna (2024), *Povertà sanitaria e welfare generativo: nuovi orizzonti e nuove sfide per la tutela della salute*, in "Diritto amministrativo", 2024, n. 4

I. Forgione (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*, in "Diritto amministrativo", 2022, n. 4

J. Freund (2008), *La crisi dello Stato tra decisione e norma*, Guida, 2008

M.S. Giannini (1990), voce *Sovranità*, in "Enciclopedia del Diritto", Giuffrè, 1990

T. Giupponi (2024), *Il governo nazionale della cybersicurezza*, in "Quaderni costituzionali", 2024, n. 2

A. Iannuzzi (2024), *I regolamenti intersettoriali per l'istituzione dei "data spaces": Data Governance Act e Data Act*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

D.T. Khuel (2009), *From Cyberspace to Cyberpower: Defining the Problem*, in F.D. Kramer, S.H. Starr, L.K. Wentz (eds.), "Cyberpower and national security", University of Nebraska Press, 2009

D. King, R.C. Lieberman (2009), *Ironies of State Building: A Comparative Perspective on the American State*, in "World Politics", vol. 61, 2009, n. 3

M.C. Libicki (2009), *Cyberdeterrence and Cyberwar*, Rand Corporation, 2009

E. Longo (2024-a), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna parlamentare", 2024, n. 2

E. Longo (2024-b), *Audizione informale per il disegno di legge in materia di "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717) Camera dei Deputati, Commissioni riunite I e II - Roma, 28 marzo 2024*, in "Rivista italiana di informatica e diritto", 2024, n. 1

E. Longo (2024-c), *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

E. Longworth (2000), *The Possibilities for a Legal Framework for Cyberspace - including a New Zealand Perspective*, in T. Fuentes-Camacho (ed.), "The International Dimensions of Cyberspace Law", Unesco Publishing, 2000

W.J. Lynn III (2010), *Defending a New Domain: the Pentagon's Cyberstrategy*, in "Foreign Affairs", vol. 89, 2010, n, 5

D. Marrani (2021), *Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia*, in "Freedom, Security & Justice: European Legal Studies", 2021, n. 1

L. Martino (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica e società", 2018, n. 1

M. Matassa (2023), *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), "La sicurezza nel cyberspazio", Franco Angeli, 2023

R. Mayntz (1999), *La teoria della governance: sfide e prospettive*, in "Rivista Italiana di Scienza Politica", 1999, n. 1

E.D. McCroskey, C.A. Mock (2017), *Operational Graphics for Cyberspace*, in "Joint Forces Quarterly", vol. 85, 2017

M. Mirti (2021), *Il cyberspace. Caratteri e riflessi sulla Comunità internazionale*, Edizioni Scientifiche Italiane, 2021

L. Moroni (2024), *La governance della cybersicurezza a livello interno ed europeo*, in "federalismi.it", 2024, n. 14

A. Negri (2011), *Sovereignity between government, exception and governance*, in H. Kalmo, Q. Skinner (eds.), "Sovereignty in Fragments. The Past, Present and Future of a Contested Concept", Cambridge University Press, 2011

R. Ottis, P. Lorents (2010), *Cyberspace: Definition and Implications, Proceeding of the International Conference on Information Warfare*, Cooperative Cyber Defense Centre of Excellence, 2010

P. Pătrașcu (2019), *Missions and Actions Specific to Cyberspace Operations*, in "Proceedings of the International Conference *Knowledge-based organization*", vol. 25, 2019, n. 3

L.R. Perfetti (2019), *L'organizzazione amministrativa come funzione della sovranità popolare*, in "Il diritto dell'economia", 2019, n. 1

M. Pietrangelo (2024), *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in "Rivista italiana di informatica e diritto", 2024, n. 2

B. Ponti (2024), *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in "Rivista italiana di informatica e diritto", 2024, n. 2

L. Previti (2022), *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in "federalismi.it", 2022, n. 25

R.A.W. Rhodes (1996), *The New Governance: Governing without government*, in "Political Studies", vol. 44, 1996

F.N. Ricotta (2024), Vulnerability disclosure *e* penetration testing*: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2*, in "Rivista italiana di informatica e diritto", 2024, n. 2

J. Rosenau, E.O. Czempiel (1992), *Governance without Government: Order and Change in World Politics*, Cambridge University Press, 1992

G.M. Ruotolo (2021), *Le fonti dell'ordinamento internazionale e la disciplina della Rete*, in "DPCE online", numero speciale, 2021

S.A. Salvaggio (2023), *The European framework for cybersecurity: strong assets, intricate history*, in "International Cybersecurity Law Review", vol. 4, 2023

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in "Rivista italiana di informatica e diritto", 2022, n. 1

F. Serini (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in "federalismi.it", 2022, n. 12

E. Sorrentino, A.F. Spagnuolo (2024), *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in "Rivista italiana di informatica e diritto", 2024, n. 2

S. Tagliagambe (1997), *Epistemologia del cyberspazio*, Demos, 1997

R. Ursi (2023), *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), "La sicurezza nel cyberspazio", Franco Angeli, 2023

F. Zorzi Giustiniani (2021), *Il* Position Paper *dell'Italia sull'applicabilità del diritto internazionale nel cyberspazio, la sentenza del Tribunale UE nel caso Google Shopping e l'Oxford Statement sulla regolamentazione internazionale degli attacchi* ransomware, in "Nomos. Le attualità del diritto", 2021, n. 3