ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

12 GIUGNO 2024

La governance della cybersicurezza a livello interno ed europeo: un quadro intricato

di Lorenzo Moroni
Ricercatore di Diritto costituzionale
Università degli Studi di Cagliari

La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*

di Lorenzo Moroni
Ricercatore di Diritto costituzionale
Università degli Studi di Cagliari

Abstract [It]: dopo avere chiarito la portata normativa del termine cybersicurezza, il saggio intende evidenziare le criticità derivanti dall'eterogena attuazione delle direttive europee in materia di governance della cybersicurezza, nonché la necessità che la funzione di garanzia della cybersicurezza sia esercitata dagli Stati attraverso una governance democratica.

Title: Cybersecurity governance at the domestic and European levels: an intricate picture
Abstract [En]: after clarifying the normative scope of the term cybersecurity, the essay aims to highlight the critical issues arising from the heterogeneous implementation of European directives in mate-rials of cybersecurity governance, as well as the need for the cybersecurity assurance function to be exercised by states through democratic governance.

Parole chiave: cybersicurezza; governance; autorità nazionali competenti NIS; tecnocrazia; democrazia
Keywords: cybersecurity; governance; NIS competent national authorities; technocracy; democracy

1. Il ruolo della tecnologia: *servant or master*?

«Technology is a useful servant but a dangerous master». Con queste parole, il politico norvegese Christian Lous Lange, nel discorso di accettazione del premio Nobel per la pace del 13 dicembre 1921, ammonì la comunità internazionale sulle potenzialità, anche distruttive, che la tecnologia poteva assumere nelle mani degli Stati. A distanza di più di un secolo, queste parole risultano essere ancora oggi attuali. Il dirompente progresso tecnologico a cui stiamo assistendo, con l'emersione nel panorama mondiale di tecnologie in grado finanche di auto-implementarsi attraverso meccanismi di *machine learning*[1], forse per la prima volta nella storia dell'umanità consentono di immaginare con meno fantasia un futuro distopico in cui il rapporto tra uomo e macchina si possa invertire. Un futuro in cui la tecnologia, da *useful servant*, possa diventare *a dangerous master*.

* Articolo sottoposto a referaggio.
[1] Basti pensare alla rapidissima diffusione nell'ultimo anno di sistemi di intelligenza artificiale, come i chatbot. Tra le varie applicazioni dell'intelligenza artificiale si pensi al Natural Language Processing (NLP), al Computer Vision, all'Intelligent Data Processing (IDP), al Recommendation System, senza contare poi le soluzioni fisiche, come i veicoli autonomi, gli Autonomous Robot e gli Intelligent Object.

Non solo l'universo tecnologico è in frenetica evoluzione, ma tanto più è veloce il progresso tecnologico quanto maggiori sono i rischi legati a un suo utilizzo dannoso. A tale proposito, l'ultimo rapporto dell'Associazione Italiana per la Sicurezza Informatica (CLUSIT) mette in evidenzia che tra il 2022 e il 2023 i cyberattacchi sono aumenti a livello mondiale del 12%, mentre in Italia, nello stesso periodo, sono aumentati del 65%[2]. Peraltro, nonostante l'Italia rappresenti solamente il 2% del PIL mondiale e lo 0,7% della popolazione globale, nel 2023 è stato rilevato che ben l'11,2% dei cyberattacchi avvenuti a livello mondiale ha riguardato bersagli italiani[3]. Inoltre, si tratta di attacchi non solo quantitativamente numerosi ma qualitativamente anche molto pericolosi, tanto è vero che nel 2023 gli attacchi con severity-grade "critical" e "high" hanno rappresentato l'81% del totale[4]. Senza contare, poi, i gravi danni che i cyberattacchi provocano all'economia mondiale, basti pensare che secondo le proiezioni del "Cybersecurity Ventures" il costo del *cyberscrime* raggiungerà i 10,5 trilioni di dollari annui entro il 2025[5].

A quanto detto, dobbiamo aggiungere che oramai il cyberspazio[6] e la sua accessibilità da parte degli utenti rappresenta la precondizione per il pieno godimento di molti dei diritti fondamentali dell'uomo: dalla libertà di manifestazione del pensiero al diritto all'immagine, dall'identità personale alla riservatezza e alla libertà del voto[7]. Dunque, tutelare la sicurezza nel cyberspazio è oramai indispensabile per garantire il pieno godimento dei diritti fondamentali nella realtà virtuale[8].

Ragion per cui, il tema sul come gli Stati debbano regolare il cyberspazio e, in particolare, sul come debbano garantire la sicurezza all'interno dello spazio virtuale è diventato centrale, tanto più oggi giorno che la c.d. cybersicurezza non riguarda più una circoscritta nicchia di utenti per alcune specifiche attività, bensì l'intera collettività nello svolgimento della vita di tutti i giorni.

---

[2] CLUSIT, *Rapporto 2024 sulla sicurezza ICT in Italia*, Milano, 2024, p. 34.
[3] *Ivi*, p. 35.
[4] *Ivi*, p. 24.
[5] S. MORGAN, *Cybercrime To Cost The World 9.5 Trillion USD Annually In 2024*, in *cybercrime magazine*, oct. 25, 2023.
[6] Il termine divenne famoso grazie all'utilizzo che ne fece W. GIBSON, *Neuromancer*, New York, 1984, a mente del quale «Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts (…) A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding». Una definizione del termine più pragmatica è quella fornita da U.S. JOINT CHIEFS OF STAFF, *Cyberspace*, in *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Washington, DC, 2011, "[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 controller».
[7] Con riguardo alle minacce che subiscono le libertà fondamentali come, ad esempio, quella di espressione o di voto, si v. M. BETZU, *I baroni del digitale*, Napoli, 2022, p. 83 ss.; con riguardo alle implicazioni rispetto, ad esempio, al giusto processo, si v. E. LONGO, *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, Milano, 2023. Più in generale, sull'impatto dei sistemi automatizzati regolati da algoritmi sulle libertà, si v. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1, 2019, p. 63 ss.
[8] Per il collegamento tra la sicurezza e la garanzia dei diritti fondamentali, si v. T. GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali*, in *Forum di Quaderni Costituzionali*, 2008, p. 6 ss.

2. La cybersicurezza

Prima di interrogarsi sul come debba essere organizzata la *governance* della cybersicurezza, è necessario interrogarsi sul concetto stesso di cybersicurezza.

Prendendo le mosse dal testo della Costituzione italiana, si possono effettuare fin da subito due constatazioni: la prima è che nel testo della Carta non compare alcun riferimento esplicito alla cybersicurezza; la seconda è che i Costituenti hanno voluto attribuire in via esclusiva allo Stato il compito di garantire la sicurezza della Repubblica[9]. A tale ultimo proposito, l'art. 117, c. 2, lett. d), Cost., con riferimento alla sicurezza *esterna*, ossia nei confronti degli altri Stati, dispone la potestà legislativa esclusiva dello Stato in materia di «difesa e Forze armate; sicurezza dello Stato». Mentre, con riferimento alla sicurezza *interna* al territorio repubblicano, l'art. 117, c. 2, lett. h), Cost., sancisce la potestà esclusiva dello Stato in materia di «ordine pubblico e sicurezza»[10].

La competenza dello Stato in materia di sicurezza *esterna* e *interna*, inoltre, è confermata a livello europeo dall'art. 4, par. 2, del Trattato dell'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»[11].

Tuttavia, se da una parte è chiara la ripartizione delle competenze in materia di sicurezza tra gli enti territoriali della Repubblica e tra l'Unione Europa e i suoi Stati membri, dall'altra parte è sicuramente meno chiaro il significato proprio di "sicurezza"[12]. Proprio col fine di individuare il significato del termine "sicurezza" e, di conseguenza, di circoscrivere la portata normativa delle disposizioni che la riguardano, è necessario avvalersi della giurisprudenza della Corte costituzionale.

---

[9] G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4, 2019, p. 67 ss.

[10] Ove, con ordine pubblico deve intendersi «il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale», così Corte cost., sent. n. 118 del 2013, punto 5 del *Considerato in diritto*; sulla stessa linea, *ex plurimis*, Corte cost., sentt. n. 35 del 2011 e n. 226 del 2010. Per mese esigenze di completezza, si noti che il termine "sicurezza" ricorre dieci volte nel testo della Costituzione e, in particolare, negli artt. 13, c. 3; 16, c. 1; 17, c. 3; 25, c. 3; 41, c. 2; 117, c. 2, lett. d; 117, c. 2, lett. h); 117, c. 3; 120, c. 2; 126, c. 1.

[11] Nonostante non sia presente alcuna definizione di "sicurezza", poiché la Commissione aveva ritenuto che l'individuazione del suo significato fosse di competenza degli Stati nazionali, tuttavia la giurisprudenza della Corte di Lussemburgo ha chiarito che essa esercita un sindacato sugli effetti che la regolamentazione nazionale ha sui valori essenziali così come sanciti dall'art. 2 del Trattato sull'Unione Europea e dalla Carta dei diritti fondamentali, i quali possono essere limitati per ragioni di sicurezza ma mai "azzerati". Sul punto, in giurisprudenza si v., da ultimo, con particolare riferimento al diritto alla privacy, ECJ, Grand Chambre, sentenza del 5 aprile 2022, causa C-140/20, *G.D. c. Commissioner of An Harda Sìochàna*. In dottrina, si v., da ultimo, G. SALVI, Intelligence *e potere*, in *Enciclopedia del diritto. I tematici*, vol. V, *Potere e costituzione*, Milano, 2023, p. 258 ss.

[12] Sui diversi significati di «sicurezza» in Costituzione, con riguardo alla dottrina si veda, tra i tanti, M. DOGLIANI, *Il volto costituzionale della sicurezza*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012, p. 1 ss.; T. GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali*, cit., p. 1 ss.; ID., *Sicurezza e potere*, in *Enciclopedia del diritto. I tematici*, vol. V, *Potere e costituzione*, Milano, 2023, p. 1165 ss.; M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 1980, p. 17 ss.

La Consulta, infatti, a partire dall'analisi del rapporto tra terrorismo e ricorso al segreto di Stato, è giunta fin dalla seconda metà degli anni '70 ad affermare che tanto nel versante *esterno* quanto in quello *interno*, «la sicurezza dello Stato costituisce interesse essenziale, insopprimibile della collettività, con palese carattere di assoluta preminenza su ogni altro, in quanto tocca (…) la esistenza stessa dello Stato»[13].

In altre parole, la sicurezza è una *funzione* dello Stato[14] ed è essenziale nell'ordinamento costituzionale, poiché consente l'esistenza dello Stato democratico a cui è affidato il compito di garantire il pieno godimento dei diritti fondamentali.

Se non che, oggi, accanto alle forme classiche di minaccia della sicurezza esterna e interna, come quelle rappresentate dagli attacchi armati provenienti da Stati terzi o da gruppi di persone presenti nel territorio, se ne sommano di ulteriori che tendono a sfumare i tentativi di classificazione che sono stati fatti dalla giurisprudenza e dalla dottrina[15]. In particolare, ci si riferisce a tutte quelle forme di minaccia della sicurezza che si muovono non più sul classico piano della realtà fisica, bensì su quello della realtà virtuale[16].

---

[13] Si v. Corte cost., sent. n. 86 del 1977, punto 5 del *Considerato in diritto*. Sulla stessa linea Corte cost., sentt. n. 82 del 1976; n. 110 del 1998; n. 106 del 2009; n. 40 del 2012. Sempre Corte cost., sent. n. 86 del 1977, è giunta a specificare, con particolare riferimento alla sicurezza *esterna* – il cui riferimento normativo è da rinvenirsi «nella formula solenne dell'art. 52, che afferma essere sacro dovere del cittadino la difesa della Patria» –, che essa «involge lo Stato nella sua personalità internazionale, cioè nell'interesse dello Stato-comunità alla propria integrità territoriale, alla propria indipendenza e, al limite, alla stessa sua sopravvivenza». Con riguardo al concetto di «difesa della patria», la Corte afferma che esso «può avere una accezione molto larga ed abbracciare anche aspetti che vanno al di là di quel che in effetti merita di trovare una protezione che valga a superare (come si vedrà in prosieguo) altri principi che pur sono ritenuti essenziali nel nostro ordinamento costituzionale. Ma si può osservare che in altre disposizioni il concetto di difesa assume un significato più specifico, come nell'art. 87 Cost. che prevede un organo ad hoc denominato Consiglio supremo di difesa e che certamente, anche nel silenzio della norma, ha compiti attinenti in maniera rigorosa ai problemi concernenti la difesa militare e, pertanto, la sicurezza dello Stato» (punto 5 del *Considerato in diritto*).

[14] A. PACE, *La funzione di sicurezza nella legalità costituzionale*, in *Quaderni costituzionali*, n. 4, 2014, p. 989 ss.; A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, in M. PALMA, S. ANASTASIA (a cura di), *La bilancia e la misura*, Milano, 2001, p. 19. Sempre sulla qualificazione della "sicurezza" in termini diversi dal diritto e, più precisamente, in termini di valore costituzionale, si v.; M. RUOTOLO, *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e sicurezza*, n. 2, 2013, p. 1 ss.; T.F. GIUPPONI, *Contro il "diritto alla sicurezza". Immigrazione, sicurezza e autonomie territoriali nella più recente giurisprudenza della Corte costituzionale*, in AA.VV., *Studi in onore di Giuseppe De Vergottini*, vol. I, Padova, 2015, p. 719 ss.; ID., *Sicurezza e potere*, cit., p. 1165 ss.; D. PULITANÒ, *Sicurezza e diritti. Quale ruolo per il diritto penale?* in *Diritto penale e processo*, n. 11, 2019, p. 1542 ss.; L. RISICATO, *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Torino, 2019; G. TROMBETTA, *Diritto alla sicurezza o sicurezza dei diritti? Brevi riflessioni intorno a una recente proposta di legge costituzionale*, in *Forum di Quaderni Costituzionali*, n. 4, 2021, p. 159 ss. *Contra*, a favore, quindi, della qualificazione della "sicurezza" in termini di diritto, si v. T.E. FROSINI, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni costituzionali*, p. 1 ss.; P. TORRETTA, *"Diritto alla sicurezza" e (altri) diritti di libertà della persona: un complesso bilanciamento costituzionale*, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, 2003, p. 451 ss.; C. MOSCA, *La sicurezza- Valori, modelli e prassi istituzionali*, Napoli, 2021, p. 89 ss.; S. RAIMONDI, *Per l'affermazione della sicurezza pubblica come diritto*, in *Diritto amministrativo*, n. 4, 2006, p. 747 ss.; G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, cit., p. 73 ss.; N. ZANON, *Un diritto fondamentale alla sicurezza?*, in *Diritto penale e processo*, n. 11, 2019, pp. 1555 ss. V. PAPAKONSTANTINOU, *Cybersecurity as* praxis *and as a* state*: The Eu law path towards acknowledgement of a new right to cybersecurity?*, in *Computer Law & Security Review*, n. 44, 2022, p. 7; S. FREDMAN, *The Positive Right to Security*, in B.J. GOOLD, L. LAZARUS (eds.), *Security and Human Rights*, London, 2007, p. 307 ss.

[15] A tale proposito, si v. A. PANSA, *La sicurezza nazionale. Innovazione e nuovi limiti*, in *Rivista italiana di Intelligence*, n. 1, 2019, p. 25.

[16] S.A. SALVAGGIO, N. GONZÀLEZ, *The European framework for cybersecurity: strong assets, intricate history*, in *International Cybersecurity Law Review*, n. 4, 2023, p. 142, affermano «The realms of cybersecurity and traditional security have been

Si tratta di forme di minaccia particolarmente insidiose. Il cyberspazio, infatti, non è diviso in territori in cui ciascuno Stato esercita una propria giurisdizione esclusiva. Inoltre, nel cyberspazio le fonti di pericolo si moltiplicano in modo incalcolabile dal momento che, potenzialmente, può rappresentare un'insidia per la sicurezza di uno Stato chiunque sia dotato di un computer e delle capacità per utilizzarlo, indipendentemente dal fatto che si tratti di un Paese terzo, di una società o di una persona fisica residente fisicamente nel territorio nazionale o fuori da esso.

Dinanzi a questo nuovo contesto virtuale e a queste nuove forme di pericolo per la sicurezza, però, "il Re non è nudo"[17], il diritto non perde la sua validità. In opposizione al tema del fondamento tellurico di legittimità del diritto, che porterebbe a concludere per l'invalidità del diritto nella realtà virtuale[18], risulta condivisibile l'impostazione di Hans Kelsen, secondo il quale i luoghi sono semplici campi di vigenza delle norme, le quali rinvengono il proprio fondamento di validità nella *Grundnorm*, ossia nelle Costituzioni[19]. Pertanto, si deve concludere che la Costituzione è valida ed esercita la propria funzione normativa anche nel cyberspazio, senza che, peraltro, sia necessario intervenire sul suo testo col fine di assicurare la sicurezza nel mondo virtuale. La Costituzione, infatti, dovendo essere «intesa e interpretata, in tutte le sue parti *magis ut valeat*»[20], quando la struttura delle specifiche disposizioni lo consentono[21], è in grado di dispiegare effetti anche alle fattispecie che riguardano la realtà virtuale attraverso la semplice attività interpretativa, senza che sia necessario, quindi, procedere a una sua revisione. Infatti, attraverso un processo interpretativo logico che si sostanzia in una sineddoche, ove è letteralmente previsto il termine "sicurezza" è necessario che si legga, di conseguenza, anche il correlato termine "cybersicurezza",

merged into one». Sulla stessa linea S. SAVAŞ, S. KARATAŞ, *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance*, in *International Cybersecurity Law Review*, n. 3, 2022, p. 11. Sul problema dello spazio, si v., tra i tanti, D.R. JOHNSON, D. POST, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, n. 5, 1996, p. 1371 ss.; D.J. SVANTESSON, *Solving the Internet Jurisdiction Puzzle*, Oxford, 2017; U. KOHL, *Jurisdiction and the Internet*, Cambridge, 2009; M. BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Rivista di diritto dei media*, n. 2, 2021, p. 43 ss.; O. POLLICINO, M. BASSINI, *The Law of the Internet between Globalization and Localization*, in M. MADURO, K. TUORI, S. SANKARI (a cura di), *Transnational Law. Rethnking Law and Legal Thinking*, Cambridge, 2014, p. 346 ss.; L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, n. 2, 1999, p. 501 ss.

17 La locuzione trae origine da «il Re è nudo», espressione utilizzata nella favola di H.C. ANDERSEN, *I vestiti nuovi dell'imperatore*, in *Fiabe*, trad. it. di A. CAMBIERI, Milano, 2004.

18 Infatti, se, come notoriamente sostenuto da C. SCHMITT, *Il nomos della terra*, Milano, 1991, p. 54 ss., il fondamento costitutivo del diritto fosse il *nomos* della terra, ossia la presa di possesso spaziale, allora si dovrebbe concludere che nel cyberspazio il diritto sarebbe invalido a causa dell'assenza di una dimensione fisica e di una sua divisibilità in spazi delimitabili.

19 Sul rapporto tra spazio e tempo nella validità delle norme, si v. H. KELSEN, *Il problema della sovranità e la teoria del diritto internazionale*, 1920, trad. it. di A. CARRINO, Milano, 1989, p. 105 ss.; ID., *Teoria generale delle norme*, in M.G. LOSANO (a cura di), trad. it. di M. TORRE, Torino, 1985, p. 225 ss. Sul punto, si v. N. IRTI, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2001, p. 41.

20 V. CRISAFULLI, *La costituzione e le sue disposizioni di principio*, Milano, 1952, p. 11. Con le parole di M. DOGLIANI, *Interpretazioni della Costituzione*, Milano, 1982, p. 44, l'interprete deve «estrarre dalla norma scritta tutti i significati che in base alle regole della logica costituiscono suoi sviluppo e specificazioni».

21 Sui confini tra interpretazione evolutiva e sovra-interpretazione, con particolare riferimento al cyberspazio, si v. M. BETZU, *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista AIC*, n. 4, 2012, p. 1 ss.

esattamente intendendo il tutto per la parte. Quindi, giusto per fare un esempio, ove la Costituzione stabilisce che compete esclusivamente allo Stato la potestà legislativa in materia di «sicurezza» (*ex* art. 117, c. 2, lett. *h*, Cost.), è necessario che l'interprete riconduca al medesimo alveo di competenza anche la materia «cybersicurezza».

Preso atto della capacità della Costituzione di dispiegare i propri effetti nella «quinta dimensione della conflittualità»[22] (dopo terra, aria, acqua e spazio extra-atmosferico), tuttavia rimane ancora in piedi il quesito su cosa si intenda precisamente col termine cybersicurezza.

Concentrando l'attenzione sulla sola accezione giuridica, il decreto legge 14 giugno 2021, n. 82, così come convertito dalla l. 4 agosto 2021, n. 109, stabilisce che per cybersicurezza deve intendersi «l'insieme delle attività (…) 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» (art. 1, c. 1, lett. *a*).

In altre parole, la disciplina nazionale ci restituisce un significato di cybersicurezza particolarmente generale che riguarda qualunque tipo di attività necessaria per proteggere i sistemi di hardware e di software dalle minacce informatiche, indipendentemente dal soggetto da cui provengono, sia quando la finalità è quella di tutelare la loro integrità sia quando la finalità è, invece, quella di tutelare anche la sicurezza nazionale e l'interesse nazionale attraverso la garanzia dell'integrità dei sistemi informatici.

Volgendo lo sguardo alla dimensione sovranazionale[23], la scelta definitoria del termine cybersicurezza compiuta a livello europeo non risulta del tutto diversa. In particolare, per "cybersecurity" dobbiamo intendere «the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats» (art. 2, (1), regolamento UE 2019/881)[24]. Ove, per "network and information system", ai sensi dell'art. 4, par. 1, del regolamento UE 2022/2555 (NIS II) si intende,

---

[22] Con queste parole L. MARTINO, *L quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, n. 1, 2018, p. 61 ss.

[23] Oltre a quella vigente sul piano dell'Unione Europea, vi sono anche altre definizioni, come per esempio quella adottata dalla Recommendation ITU-T X.1205 in accordance with UN resolution 181 (Guadalajara, 2010), secondo la quale «Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality».

[24] Sul concetto di cybersecurity come *praxis* («activities and measures to accomplish cybersecurity's aims and objectives») o come *state* («the condition that is achieved once cybersecurity as praxis has succeeded»), nonché sull'ipotesi di una cybersecurity come diritti fondamentale nell'UE, si v. V. PAPAKONSTANTINOU, *Cybersecurity as* praxis *and as a* state*: The Eu law path towards acknowledgement of a new right to cybersecurity?*, cit., p. 1 ss.

secondo tre accezioni di significato diverse ma complementari: a) reti di comunicazione elettronica[25]; b) uno o più dispositivi che attraverso un programma compiono un trattamento automatico dei dati digitali; c) i dati digitali che sono stati oggetto del funzionamento dei dispositivi digitali, quindi quelli trasmessi, estratti, conservati ecc.

A parte alcune differenze, ad esempio il d.l. n. 82 del 2021 richiama tra le finalità di tutela della sicurezza nel cyberspazio anche la sicurezza nazionale e l'interesse nazionale, mentre la definizione fornita a livello europeo sintetizza il complesso di sistemi informatici e dei dati trasmessi nella locuzione "network and information system", tuttavia, come preannunciato, le definizioni non sono dissimili tra loro. In particolare, in entrambi i livelli di governo la cybersicurezza implica la difesa delle infrastrutture del cyberspazio – hardware e software – e dei suoi utenti dalle minacce esterne provenienti da qualsivoglia soggetto, sia esso pubblico, come uno Stato terzo, o privato, come una persona fisica o una società.

3. La governance europea della cybersicurezza e la sua eterogenea attuazione a livello statale

La cybersecurity richiede la predisposizione di un'organizzazione istituzionale adeguata ad affrontare le sfide e le minacce che sempre più spesso provengono dal mondo digitale. Sicuramente i principali protagonisti di questa stagione di nuova regolamentazione devono essere gli Stati. Non vi sono dubbi, infatti, che contro le degenerazioni anti-libertarie che potrebbero venire a crearsi nel cyberspazio l'antidoto non è il predominio della libertà assoluta, come ha sostenuto J.P. Barlow nella sua Dichiarazione di Indipendenza del Cyberspazio[26], ma sono gli Stati democratici nei limiti e nelle forme previste dalle Costituzioni. Tuttavia, difficilmente ciascuno Stato isolato e da solo è in grado di garantire concretamente la "sicurezza dei diritti" nel cyberspazio[27], dal momento che la realtà virtuale, a differenza

[25] Ai sensi dell'art. 2, par. 1, direttiva (UE) 2018/1972, con "reti di comunicazione elettronica" (più note in inglese con la locuzione "electronic communications network") deve intendersi «i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata, e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva, e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato».

[26] Si v. J.P. BARLOW, *A Declaration of the Independence of Cyberspace*, 1996, il quale esordisce affermando «Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather». A favore dell'autoregolamentazione del cyberspazio, si v. D.R. JOHNSON, D. POST, *Law and Borders: The Rise of Law in Cyberspace*, cit., p. 1371 ss. *Contra*, a favore, quindi, di una condivisibile regolamentazione statale del cyberspazio, si v. J.L. GOLDSMITH, *Against Cyberanarchy*, in *University of Chicago Law Review*, n. 4, 1998, p. 1199 ss.

[27] L'espressione si riferisce all'evoluzione della funzione del potere statale rispetto alla tutela dei diritti. In particolare, secondo la tradizione liberale, era sufficiente un *non agere* dello Stato se non in chiave repressiva della violazione dei diritti, mentre, con l'affermazione del costituzionalismo liberaldemocratico, allo Stato è richiesto anche un *agere* volto, in chiave preventiva, a promuovere positivamente la garanzia e il godimento dei diritti della persona. Sicché, trasposto tale concetto sul piano della sicurezza, con le parole di T. GIUPPONI, *Sicurezza e potere*, cit., p. 1161, il compito dello Stato «non è tanto garantire un preteso "diritto alla sicurezza" dei singoli individui, quanto la complessiva "sicurezza dei diritti"

di quella materiale, non è suscettibile di divisione in confini. Ragione per cui, proprio per rendere effettiva la sicurezza nel cyberspazio e, di conseguenza, possibile la tutela dei diritti fondamentali nella dimensione virtuale, è essenziale stabilire forme di cooperazione a livello sovrastatale.

A tale proposito, quindi, ci si deve interrogare sul *come* l'Unione Europea e i suoi Stati membri si stanno organizzando per predisporre una adeguata governance della *cybersecurity*[28].

La necessità di garantire la sicurezza delle infrastrutture e degli utenti del cyberspazio e di coordinare le regolazioni statali in materia di cybersicurezza ha portato l'Unione Europea ad adottare numerosi atti che incidono sulla regolazione del cyberspazio[29]. Tra questi, però, risultano particolarmente determinanti ai fini della costruzione di una governance della cybersicurezza la direttiva UE 2016/1148, Network and Information System (NIS I), recepita dagli Stati membri[30], successivamente abrogata dalla più recente direttiva UE 2022/2555 (NIS II), la quale dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024.[31].

La vigente direttiva NIS II[32] assolve il compito di aumentare la "cyber-resilienza" dell'Unione Europea attraverso il rafforzamento della cybersicurezza dell'UE e la riduzione delle minacce ai sistemi informatici

dei cittadini». Sul punto, con prospettive diverse tra loro, si v. A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, cit.; L. RISICATO, *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, cit.

[28] Sull'analisi, anche diacronica, della regolazione europea in molteplici settori che riguardano la cybersicurezza si v. Z. BEDERNA, Z. RAJNAI, *Analysis of the cybersecurity ecosystem in the European Union*, in *International Cybersecurity Law Review*, n. 2, 2022, p. 35 ss.

[29] Gli atti europei che, in modo più o meno diretto, incidono sulla regolazione della cybersicurezza sono molteplici e abbracciano un arco temporale di oramai 20 anni. Limitando l'attenzione agli atti più rilevanti non citati nel testo centrale, si va dal regolamento che ha istituito la European Network and Information Security Agency (UE/2004/460), passando per il General Data Protection Regulation (GDPR - regolamento UE 2016/679), il Cybersecurity Act (regolamento UE/2019/881) e il regolamento UE 2023/2841 sull'high common level of cybersecurity, per giungere poi all'Artificial Intelligent Act (COM(2021)206; approvato in dal Parlamento UE il 13/03/24), al Cyber Resilience Act (COM(2022)454), e al Cyber Solidarity Act (COM(2023)209), gli ultimi due in corso di approvazione. Per maggiori approfondimenti sul rapporto tra Artificial Intelligence Act e il Cyber Resilience Act, con particolare riferimento alla regolazione dei *regulatory sandbox*, si v. F. BAGNI, *The Regulatory Sandbox and the Cybersecurity Challange: from the Artificial Intelligence Act to the Cyber Resilience Act*, in *Rivista italiana di informatica e diritto*, n. 2, 2023, p. 1 ss. Per maggiori approfondimenti sul rapporto tra il Cyber Resilience Act e gli altri Atti riguardanti la cybersicurezza si v. P.G. CHIARA, *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction*, in *International Cybersecurity Law Review*, n. 3, 2022, p. 255 ss. Con riguardo, invece, alla giurisprudenza, con particolare riferimento al rapporto tra la tutela della riservatezza dei dati personali e la cybersicurezza si v., *ex plurimis*, ECJ, sentenza del 10 ottobre 2016, C-582/14, *Breyer c. Bundesrepublik Deutschland*; ECJ, Grand Chambre, sentenza del 26 dicembre 2016, C-2013/15 e C-698/15, *Tele2 Sverige AB c. Post-och telestyrelsen*, ECJ, Grand Chambre, sentenza del 6 ottobre 2020, C-623/17, *Privacy International c Secretary of State for Foreign and Commonwealth Affairs et al.*

[30] Con riguardo all'Italia, si v. d.lgs. del 18/05/2018, n. 65, rubricato "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione".

[31] Sul punto, si v. F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 12, 2022, p. 241 ss.

[32] Per maggiori approfondimenti sul sistema previsto dalla direttiva NIS I, si v., tra i tanti, S. SCHMITZ-BERNDT, P.G. CHIARA, *One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS 2 directive*, in *International Cybersecurity Law Review*, n. 3, 2022, p. 289 ss.

e di rete dei servizi classificati come "essenziali" (es. energia, trasporti, sanità e finanza) e "importanti" (es. alimentare, manifatturiero, pubblica amministrazione, chimico, postale, corriere, ecc.)[33].

Tra le diverse modalità attraverso le quali la direttiva NIS II mira a rafforzare la cyber-resilienza dell'Unione Europea, sicuramente una delle principali è quella di provvedere al potenziamento dell'articolato sistema di governance in materia di cybersicurezza previsto dalla direttiva NIS I, il quale, secondo uno schema ricorrente, vede al suo vertice un'autorità europea e, sotto di essa, una costellazione di autorità e organismi degli Stati membri.

L'autorità europea è la preesistente *European Union Agency for Cybersecurity* (ENISA), a cui il regolamento UE/2019/881 attribuisce compiti di assistenza e consulenza per lo sviluppo e l'armonizzazione delle politiche e delle regolazioni degli Stati membri in materia di cybersicurezza[34].

Accanto all'ENISA, la direttiva NIS II ha previsto l'istituzione di tutta una serie di organi indicati nell'art. 1 e, per ciò che in questa sede rileva, al par. 2, lett. a), è stata confermata l'istituzione delle autorità nazionali in materia di cybersicurezza (c.d. autorità nazionali competenti NIS)[35]. Queste, coadiuvate dai *Computer Security Incident Response Teams* – CSIRTs[36], svolgono le cruciali funzioni di implementazione e attuazione delle disposizioni contenute all'interno della direttiva NIS II, nonché di vigilanza della loro corretta applicazione[37]. Proprio per il proficuo perseguimento di tali fini, la direttiva NIS II ha previsto l'attribuzione di importanti poteri alle autorità nazionali competenti NIS, come, ad esempio, quelli di «ispezioni in loco e vigilanza a distanza» (art. 32, par. 2, lett. a, NIS II), «audit ad hoc» (lett. c), «richieste

[33] In particolare, la NIS II ha esteso l'ambito di applicazione della NIS I che era limitata ai soli "operatori di servizi essenziali" e ai "fornitori di servizi digitali", si v. artt. 1 ss., direttiva UE 2016/1148. Con riguardo ai servizi essenziali e importanti si v. artt. 1-3 e all. 1 e 2, direttiva UE 2022/2555 (NIS II). Per maggiori approfondimenti, anche critici, sulla base giuridica di cui all'art. 114 TFUE, "internal market hamonization", sulla base della quale sono state emanate le direttive NIS si v. S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *AISDUE*, n. 5, 2021, p. 69 ss. A proposito dell'art. 114 TFUE, B. DE WITTE, *Exclusive Member States competences: is there such a thing?*, in I. GOVAERE, S. GARBEN (eds.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford, 2017, p. 59, afferma che «is the most powerful tool for the expansion of the EU legislative activity».

[34] Si v. artt. 3 ss. del regolamento UE 2019/881. Con riguardo al contesto normativo, invece, il regolamento UE/2019/881 ha proceduto ad abrogare il regolamento UE/526/2013, il quale, a sua volta, aveva proceduto ad abrogare il regolamento CE/460/2004 (e sue modificazioni CE/1007/2008 e 580/2011) con il quale si era proceduto a istituire l'ENISA.

[35] L'istituzione delle autorità nazionali competenti NIS era già prevista dall'art. 8 della direttiva NIS I.

[36] Si v. art. 1, c. 1, lett. a), e artt. 10 ss., direttiva UE 2022/2555 (NIS II).

[37] Più precisamente, l'art. 1 della direttiva UE 2022/2555 (NIS II) prevede: «1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno. 2. A tale fine, la presente direttiva stabilisce: a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT); b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557; c) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza; d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri». L'art. 8, par. 2, della direttiva NIS II prevede che le autorità nazionali competenti NIS «controllano l'attuazione della presente direttiva a livello nazionale».

di accesso a dati, documenti e alter informazioni» (lett. f); ovvero, poteri di ordinare ai soggetti interessati «di porre termine al comportamento che viola la presente direttiva e di astenersi dal ripeterlo» (art. 32, par. 4, lett. c), «di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole» (lett. f), «di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata» (h).

L'importanza dei poteri di cui le autorità nazionali competenti NIS saranno titolari, che negli Stati democratici sono attribuiti di regola alle autorità di pubblica sicurezza, unita alla crucialità del ruolo che esse svolgono nella buona riuscita delle strategie europee di cybersicurezza, suggeriscono un'applicazione quanto più omogenea possibile delle direttive NIS, almeno sotto il punto di vista dell'istituzione delle autorità nazionali competenti NIS[38]. Ma così, fino a oggi, non è stato.

Complice, infatti, la trasversalità delle politiche di cybersecurity, che oramai riguardano quasi tutti gli aspetti della vita quotidiana che hanno un risvolto in rete – per intenderci, dall'acquisto di un prodotto nell'e-commerce, alla richiesta online di un documento alla pubblica amministrazione, per giungere alla ricerca di una parola su Google –, unita all'ampio margine di discrezionalità che lo strumento giuridico delle direttive europee solitamente concede a ciascuno Stato membro in ordine al risultato da raggiungere, si è giunti ad avere un'applicazione della direttiva NIS I particolarmente eterogenea tra gli Stati membri. Tale eterogeneità si è riflettuta anche sulle autorità nazionali competenti NIS, le quali hanno conosciuto modalità di istituzione diverse negli Stati europei[39].

Un primo gruppo di Stati ha deciso di affidare il ruolo di autorità nazionale competente NIS a molteplici autorità amministrative indipendenti o a organi tecnici di regolamentazione[40]. Tra questi, ad esempio, il Lussemburgo ha assegnato le funzioni di cybersecurity ad autorità indipendenti come l'*Institut Luxembourgeois de Régulation* e la *Commission de Surveillance du Secteur Financier*, a seconda delle aree di competenza[41].

---

[38] Sulla capacità dell'armonizzazione della regolazione in materia di cybersecurity a livello europeo per incrementare l'efficienza della cyber resilienza, si veda S. SCHMITZ-BERNDT, P.G. CHIARA, *One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS 2 directive*, cit., p. 307 ss. Evidenziano la frammentazione della regolazione europea in materia di cybersecurity P. ECKHARDT, A. KOTOVSKAIA, *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*, in *International Cybersecurity Law Review*, n. 4, 2023, p. 150 ss.

[39] Con riguardo alla classificazione in tre gruppi, si v. A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *La Rivista Gruppo di Pisa*, 3, 2021, p. 532 ss.

[40] Rientra in questo gruppo di Stati membri anche Cipro.

[41] L'*Institut Luxembourgeois de Régulation* si occupa di molteplici aree di competenze, dal trasporto all'energia, passando per il sistema sanitario e il sistema idrico. La *Commission de Surveillance du Secteur Financier*, invece, si occupa delle infrastrutture del mercato bancario e finanziario. Sul punto, si v. art. 3, commi 1 e 2, A372 Loi du 28 mai 2019, a mente dei quali «La Commission de surveillance du secteur financier, ci-après «la CSSF», est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des établissements de crédit et des infrastructures de marchés financiers tels que définis aux points 3 et 4 de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF.

Un secondo gruppo di Stati, invece, ha affidato il ruolo di autorità nazionale competente NIS a Ministeri o a organismi da essi dipendenti[42]. In Irlanda, ad esempio, le funzioni di autorità nazionale competente NIS sono state incardinate nel *Department of Communications, Climate Action and Environment*[43], mentre in Germania sono state attribuite all'Ufficio federale per la sicurezza informatica (*Bundesamt für Sicherheit in der Informationstechnik*), incardinato presso il Ministero Federale dell'Interno[44].

Un terzo gruppo di Stati, infine, ha deciso di attribuire il ruolo di autorità nazionale competente NIS direttamente al capo del Governo o a un'agenzia governativa da esso dipendente[45]. Si pensi, ad esempio, alla Francia e all'Italia, le cui autorità nazionali competenti NIS, rispettivamente la *Agence nationale de la sécurité des systèmes d'information* e la *Agenzia per la cybersicurezza nazionale*, svolgono le loro funzioni sotto l'influenza del Primo ministro francese e del Presidente del Consiglio dei Ministri italiano.

Di fronte alla molteplicità di soluzioni adottate dagli Stati membri, sorge spontaneo chiedersi quale dei diversi modi di organizzazione della governance in materia di cybersicurezza deve considerarsi preferibile. Si tratta di una domanda a cui è impossibile dare una risposta univoca, dal momento che molto dipende dal concreto funzionamento della forma di governo di ciascuno Stato. Tuttavia, adottando come prospettiva di osservazione la forma di Stato, per due ragioni si può ritenere che in una democrazia le autorità nazionali competenti NIS andrebbero incardinate presso organismi costituzionali dotati di rappresentanza politica, quindi il Parlamento o il Governo.

La prima ragione è riconducibile al fatto che le autorità nazionali competenti NIS – come già si è avuto modo di vedere –, una volta data attuazione alla direttiva NIS II, saranno destinate ad esercitare delle funzioni amministrative, come quelle di ispezione, audit, richiesta di accesso a dati, documenti e informazioni, che nella realtà materiale sono tradizionalmente di competenza dello Stato e sono esercitate da autorità di pubblica sicurezza direttamente dipendenti dai Ministeri del Governo, come il Ministero dell'Interno, della Giustizia o della Difesa[46].

La seconda ragione è che le autorità nazionali competenti NIS coadiuvano gli Stati membri nell'attività *politica* di cybersecurity. Si pensi, ad esempio, alla definizione della "Strategia nazionale per la cibersicurezza", attraverso la quale si stabiliscono le politiche, e le relative risorse economiche, che dovranno essere attuate da ciascuno Stato in materia di sicurezza nel cyberspazio. Sul punto, l'art. 7 della

L'Institut luxembourgeois de régulation, ci-après «l'ILR», est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente».

[42] Rientrano in questo gruppo di Stati membri: Spagna; Danimarca; Malta; Polonia; Lettonia; Paesi Bassi; Finlandia; Svezia; Slovenia; Bulgaria; Grecia; Croazia; Lituania, Estonia.

[43] S.I. no. 360/2018.

[44] Si veda Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40, ausgegeben zu Bonn am 29. Juni 2017, p. 1885 ss.

[45] Rientrano in questo gruppo di Stati membri: Belgio; Slovacchia; Romania; Portogallo; Austria.

[46] Si v., ad esempio, art. 32 direttiva NIS II.

Direttiva NIS II si limita a prevedere in modo generico che tali strategie nazionali devono essere adottate da «ogni Stato membro» (art. 7, par. 1). In questo modo, la direttiva NIS II sembrerebbe aprire all'ipotesi che tali politiche in materia di cybersicurezza possano essere adottate tanto dal Governo o dal Parlamento, quanto da autorità amministrative che agiscono in modo indipendente dagli organi costituzionali dotati di rappresentanti politica, come teoricamente può essere un'autorità nazionale competente NIS. Ma anche volendo ammettere che la Strategia nazionale possa essere adottata solo dal Governo o dal Parlamento, comunque le autorità nazionali competenti NIS partecipano spesso in modo determinante nella redazione di queste politiche. È emblematico il caso dell'Italia, ove la "Strategia nazionale di cybersicurezza" è adottata dal Presidente del Consiglio dei ministri (sentito il comitato interministeriale per la cybersicurezza)[47], ma è predisposta dall'Agenzia per la cybersicurezza nazionale, ossia l'autorità nazionale competente NIS italiana[48].

Per tali ragioni, riconducibili all'esercizio di funzioni amministrative tradizionalmente di competenza degli Stati e alla partecipazione all'attività di natura politica in materia di cybersicurezza, si ritiene che le autorità nazionali competenti NIS dovrebbero essere incardinate presso il Governo o il Parlamento. Di conseguenza, invece, suscita perplessità l'attribuzione delle funzioni di autorità nazionali competenti NIS a organismi che svolgono la loro attività in modo indipendente dagli organi costituzionali dotati di rappresentanza politica, come le autorità amministrative indipendenti. Infatti, è sicuramente vero che le autorità amministrative indipendenti hanno contribuito a evolvere i sistemi di governance nella direzione di una maggiore efficienza, anche attraverso la rivalutazione del rapporto tra pubblico e privato, consentendo di risolvere importanti problemi di funzionamento delle democrazie moderne[49]. È altrettanto vero, però, che le autorità amministrative indipendenti, operando slegate dal circuito della legittimazione democratica (a favore, invece, di quella tecnocratica)[50], non prevengono il rischio che esse, un domani, possano arrivare a ritagliarsi un alveo di esercizio del potere pubblico in materia di cybersicurezza non adeguatamente controbilanciato da un pieno ed effettivo controllo democratico da parte del Parlamento.

---

[47] Si v. art. 4, d.l. n. 82 del 2021.

[48] Si v., rispettivamente, art. 2, c. 1, lett. b), e art. 7, c. 1, lett. b), d.l. n. 82/2021.

[49] Si v. G. GIRAUDI, S. RIGHETTINI, *Le autorità amministrative indipendenti. Dalla democrazia della rappresentanza alla democrazia dell'efficienza*, Roma-Bari, 2002, p. 202 ss.

[50] F. DONATI, *Democrazia pluralista e potestà normativa delle autorità indipendenti*, in *Osservatorio sulle fonti*, n. 3, 2017, p. 2. Sempre sul tema della legittimazione delle autorità amministrative indipendenti si v., tra i tanti, G. AMATO, *Autorità semi-indipendenti e autorità di garanzia*, in *Rivista trimestrale di diritto pubblico*, 1997, p. 645 ss.; A. PAJNO, *L'esercizio di attività in forme contenziose*, in S. CASSESE, C. FRANCHINI (a cura di), *I garanti delle regole*, Bologna, 1996, p. 109; E. CHELI, *Le autorità amministrative indipendenti nella forma di governo*, in *Associazione per gli studi e le ricerche parlamentari*, n. 11, Torino, 2000, p. 130; D. CORLETTO, *Autorità indipendenti e giudice amministrativo*, in P. CAVALIERI, G. DELLE VEDOVE, P. DURET, *Autorità indipendenti e agenzie*, Padova, 2003, p. 114; A. RIVIEZZO, *Autorità amministrative indipendenti e ordinamento costituzionale*, in *Quaderni costituzionali*, n. 2, 2005, p. 338, nonché, più di recente, M. MANETTI, *Poteri e garanzie (Autorità indipendenti)*, in *Enciclopedia del diritto. I tematici*, vol. V, *Potere e costituzione*, Milano, 2023, p. 782 ss.

4. La governance italiana della cybersicurezza: il ruolo del Governo e del Parlamento

Le autorità nazionali competenti NIS, come visto, una volta data attuazione alla direttiva NIS II, non solo saranno chiamate a esercitare funzioni di tradizionale competenza dello Stato, come quelle di vigilanza, implementazione e soprattutto esecuzione delle direttive NIS, ma già tutt'ora partecipano all'esercizio della funzione di indirizzo politico, ad esempio coadiuvando in modo determinante i decisori politici nella redazione delle "Strategie nazionali per la cybersicurezza". Senza contare, poi, che oggi il cyberspazio rappresenta il contesto principale per l'esercizio di molti dei diritti fondamentali, sicché, tutelarne la sicurezza, non significa più solamente proteggere lo Stato da aggressioni interne o esterne, ma anche garantire ai propri cittadini l'esercizio dei diritti fondamentali.

Proprio per la pervasività che assume il tema della cybersicurezza, risulta necessario che vi siano forme di controllo da parte del Parlamento sull'attività delle autorità nazionali competenti NIS e, inoltre, che sia assicurata la trasparenza del loro operato. Ciò vale, in particolare, quando queste autorità sono incardinate presso il Governo o, ancor di più, quando sono autorità amministrative indipendenti.

A tale proposito, risulta particolarmente interessante il caso italiano, in cui le funzioni di autorità nazionale competente NIS sono state attribuite dal decreto-legge n. 82 del 2021 all'Agenzia per la cybersicurezza nazionale (ACN)[51]. Si tratta di un'agenzia governativa d'intelligence che, sebbene dotata di alcuni margini di indipendenza[52], svolge le sue funzioni sotto l'influenza del Presidente del Consiglio dei ministri. Al Presidente del Consiglio, infatti, è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza e, inoltre, ha il potere di nominare e revocare il Direttore e il Vicedirettore dell'Agenzia[53]. Se da una parte è palese la volontà del legislatore di concentrare il potere in materia di cybersicurezza in capo al Governo, dall'altra parte è altrettanto evidente il tentativo di rinforzare la funzione parlamentare di controllo del potere esecutivo.

L'organo rappresentativo del corpo elettorale, infatti, oltre ad avere a sua disposizione gli istituti classici del controllo parlamentare del Governo[54], esercita specifiche funzioni di controllo sull'attività del Presidente del Consiglio e dell'Agenzia nazionale per la cybersicurezza. In particolare, il d.l. n. 82 del 2021

[51] Art. 5, d.l. n. 82 del 2021. Per quanto riguarda le specifiche funzioni svolte dall'ACN si v. art. 7, d.l. n. 82 del 2021.

[52] Ai sensi dell'art. 5, d.l. n. 82 del 2021, presenta autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti del decreto stesso.

[53] Art. 2, c. 1, d.l. 14 giugno 2021, n. 82, così come convertito dalla legge 4 agosto 2021, n. 109. Per esigenze di completezza è necessario sottolineare che presso l'ACN è istituito, in via permanente, il Nucleo per la cybersicurezza. Si tratta di un organo che svolge la funzione di supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione, preparazione di situazioni di crisi e attivazione di procedure di allertamento in materia di cybersicurezza, ed è composto dal Direttore generale dell'ACN, che lo presiede, da un consigliere militare del Presidente del Consiglio, da un rappresentante del Dipartimento delle informazioni per la sicurezza (DIS), da un rappresentante del Dipartimento della protezione civile della Presidenza del Consiglio e, per la trattazione di informazioni classificate, anche da un rappresentante dell'Ufficio centrale per la segretezza (si v. art. 8, d.l. n. 82 del 2021).

[54] Inchieste, indagini conoscitive, audizioni, interrogazioni, interpellanze e mozioni.

ha individuato nel Comitato parlamentare per la sicurezza della Repubblica (c.d. COPASIR) l'organo con cui il Parlamento può svolgere la sua funzione di controllo sull'attività d'indirizzo politico in materia di cybersicurezza[55]. Tale funzione, in particolare, è svolta dal COPASIR attraverso molteplici attribuzioni, come il potere di chiedere l'audizione del Presidente dell'ACN (art. 5, c. 6, d.l. n. 82 del 2021) e il potere di esprimere pareri preventivi sull'adozione dei regolamenti che definiscono: a) l'organizzazione e il funzionamento dell'ACN (art. 6, c. 3); b) lo stanziamento delle somme annuali necessarie al funzionamento dell'ACN (art. 11, c. 3); c) le procedure di stipulazione dei contratti pubblici dell'ACN (art. 11, c. 4); d) il rapporto di lavoro coi dipendenti dell'ACN (art. 12, c. 8). Inoltre, sempre col fine di rendere edotto il Parlamento sulle attività dell'ACN, è previsto che ogni anno, entro il 30 giugno, il Primo ministro debba trasmettere sia al Parlamento sia al COPASIR una relazione annuale sull'attività svolta dall'ACN nell'anno precedente (art. 14)[56].

Nel sistema italiano, quindi, non si può certo dire che il Parlamento sia escluso dal controllo del Governo nell'esercizio della funzione di indirizzo politico in materia di cybersicurezza. Tuttavia, a fronte di tale aspetto positivo, il sistema previsto in Italia comunque presenta talune criticità.

Infatti, a fronte della pervasività della cybersicurezza e della trasversalità delle materie da essa riguardate, per due principali ragioni il ruolo e il funzionamento del COPASIR appare, invece, non del tutto adeguato a garantire un sufficiente livello di trasparenza dell'attività di controllo dell'indirizzo politico in materia di cybersicurezza[57].

La prima ragione, specifica sull'organo in sé, è riconducibile al fatto che il COPASIR, nascendo col compito di verificare che l'attività di *intelligence* del Sistema di informazione per la sicurezza della Repubblica[58] si svolga nel rispetto della Costituzione, delle leggi e dell'esclusivo interesse e per la difesa della Repubblica, è pensato per svolgere le sue funzioni con un elevato livello di riservatezza. Basti pensare, ad esempio, alla sua composizione, limitata a soli 5 deputati e 5 senatori più i due Presidenti della Camera e del Senato[59], o all'obbligo del segreto, anche dopo la cessazione della carica, a cui sono tenuti

[55] Le funzioni del COPASIR specificamente previste con riguardo all'attività del Governo in materia di cybersicurezza si sommano alle funzioni utili allo svolgimento del controllo parlamentare che sono attribuite dalla l. n. 124 del 2007, artt. 30 ss.

[56] Sul punto, si v. anche A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., p. 541.

[57] *Ivi,* p. 542, definisce il ruolo del COPASIR «*limitante* rispetto alla vastità di ambiti cui ormai presiede e *limitato* tanto nella composizione che nelle forme di pubblicità».

[58] Composto, ai sensi dell'art. 2, c. 1, della l. n. 124 del 2007, dal Presidente del Consiglio, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità delegata di cui all'art. 3 ove istituita, dal Dipartimento delle informazioni per la sicurezza (DIS), dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI).

[59] Art. 30, legge n. 124 del 2007.

tutti coloro che hanno acquisito nell'esercizio delle proprie funzioni informazioni relative all'attività del COPASIR[60].

La seconda ragione, di tipo sistematico, concerne il fatto che dall'istituzione dell'autorità NIS presso la Presidenza del Consiglio dei ministri e dall'attribuzione del ruolo di vigilanza parlamentare del Governo principalmente al COPASIR deriva una eccessiva concentrazione di potere in capo al vertice del Governo. Sicché, anche in materia di cybersicurezza, è riscontrabile quel tendenziale spostamento di equilibrio dall'organo legislativo a quello esecutivo che la dottrina ha registrato già da tempo anche in altri settori[61]. Difatti, il Presidente del Consiglio svolge un ruolo pivotale non soltanto all'interno del Sistema di informazione per la sicurezza e in materia di segreto di Stato[62], ma, com'è noto, anche all'interno dello stesso COPASIR. A tale ultimo proposito, basti pensare che, ad esempio, il COPASIR, per ottenere informazioni e copie di atti o documenti a cui sia stato opposta la "riservatezza" in ragione del pericolo che essi possono procurare alla sicurezza della Repubblica, deve necessariamente avere il consenso del Presidente del Consiglio[63].

Il COPASIR, insomma, a causa della particolare riservatezza dell'operato e della "confidenzialità" con cui lavora abitualmente a stretto contatto col vertice del Governo, non risulta essere un organo del tutto adeguato a garantire un sufficiente livello di trasparenza anche al di fuori del Parlamento[64], come invece lo sarebbero la Camera e il Senato se fossero coinvolte maggiormente. In una prospettiva *de iure condendo*, quindi, sono molteplici gli interventi che il legislatore italiano potrebbe attuare per coinvolgere in maggior

[60] Art. 36, legge n. 124 del 2007.

[61] A tale proposito, tra i tanti, si vedano i contributi presenti nel volume M. SICLARI (a cura di), *I mutamenti della forma di governo. Tra modificazioni tacite e progetti di riforma*, Roma, 2008, nonché, di recente, con particolare riferimento alle fonti, A. CARDONE, *Sistema delle fonti e forma di governo. La produzione normativa della Repubblica tra modello costituzionale, trasformazioni e riforme (1948-2023)*, Bologna, 2023. Sempre a proposito di spostamento di equilibrio in materia di governance della cybersicurezza, A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., p. 542, constata la progressiva tendenza emarginare le sedi principali dei poteri riguardati (ad es. il Parlamento) a favore delle sedi ristrette e distaccate (ad es. apposite Commissioni parlamentari).

[62] In particolare, se già nel previgente assetto delineato dalla legge n. 801 del 1977 il Presidente del Consiglio ricopriva un ruolo pivotale in materia di servizi d'informazione, tale funzione così centrale è stata ulteriormente rafforzata con la riforma dell'organizzazione dell'attività d'*intelligence* operata con la legge n. 124 del 2007, sul punto si v., su tutti, T. GIUPPONI, *Servizi di informazione e segreto di Stato nella legge n. 124/2007*, in *Forum di Quaderni costituzionali*, 2010, p. 1 ss., nonché ID., *Segreto di Stato (diritto costituzionale)*, in *Enciclopedia del diritto*, Annali X, Milano, 2017, p. 856 ss.

[63] Art. 31, cc. 7 e 8, l. n. 124 del 2007. Ulteriori esempi da cui si trae l'importanza del ruolo del Presidente del Consiglio rispetto al COPASIR sono desumibili, ad esempio, dall'art. 31, c. 2, l. n. 124 del 2007, in forza del quale è necessario che il COPASIR ottenga il consenso del Presidente del Consiglio per audire un dipendente del Sistema di informazione per la sicurezza, ovvero dall'art. 31, cc. 14 e 15, l. n. 124 del 2007, il quale stabilisce che il COPASIR può disporre accessi e sopralluoghi negli uffici del Sistema di informazione per la sicurezza solo una volta data preventiva comunicazione al Presidente del Consiglio, il quale può differirne l'esecuzione in caso di pericolo di interferenza con operazioni in corso.

[64] Peraltro, non vi sono pochi ostacoli al disvelamento del segreto in sede parlamentare e, inoltre, non è così agevole far valere la responsabilità politica e giuridica del Governo. Sul punto, si v. R. BIFULCO, *Segreto e potere politico*, in *Enciclopedia del diritto*, Annali X, Milano, 2017, p. 1115 ss.; M. LUCIANI, *Il segreto di Stato nell'ordinamento nazionale*, in *Gnosis. Rivista italiana di intelligence*, n. 2, 2013, p. 22 ss.

misura le aule parlamentari[65]. Si pensi, ad esempio, alla previsione di audizioni parlamentari pubbliche semestrali o quadrimestrali dell'ACN, oppure all'istituzione di nuova commissione parlamentare bicamerale *ad hoc* di controllo sull'attività del Governo, la cui maggiore rappresentatività della composizione e pubblicità dei lavori garantiscano una adeguata conoscenza delle decisioni assunte in materia di cybersicurezza. Non si deve dimenticare, infatti, che «l'apparato della democrazia ha per regola la trasparenza, ed il segreto costituisce una eccezione»[66], e ciò vale a maggiore ragione per la sicurezza nel cyberspazio, la quale, come più volte è stato ricordato, oramai interseca tutti i campi della vita quotidiana.

5. Gli Stati democratici garanti della tecnologia come *useful servant*

La funzione di garanzia della sicurezza all'interno del cyberspazio è necessario che venga esercitata dagli Stati nel rispetto dei propri valori e dei principi supremi[67], i quali, in Europa e in Italia, trovano una sintesi nel concetto di democrazia. Conformemente all'art. 2 del Trattato sull'Unione Europea e all'art. 1 della Costituzione italiana, infatti, è necessario che la cybersicurezza sia esercitata attraverso una governance che possa dirsi *democratica*. Ciò, in particolare, si realizza quando vi è un adeguato coinvolgimento del Parlamento e del Governo nel circuito decisione, esecuzione e vigilanza relativo alle politiche di cybersicurezza.

Non si tratta di un obiettivo semplice da raggiungere. Da una parte, la necessità di una repentina reazione alle minacce cibernetiche sicuramente non trova la risposta più efficiente nel coinvolgimento delle assemblee parlamentari. Dall'altra parte, però, il compito di protegge la collettività da un utilizzo criminoso della tecnologia è rimesso agli Stati democratici, nei limiti e nelle forme previste dalle Costituzioni. Si badi bene, proprio il coinvolgimento delle istituzioni democratiche e rappresentative della popolazione assolve all'obiettivo non solo di garantire il godimento e la tutela dei diritti fondamentali nel cyberspazio da eventuali minacce esterne o interne rispetto al Paese, ma anche all'ulteriore obiettivo di prevenire l'ipotesi che tali minacce possano derivare dalla stessa autorità statale, la quale, abusando delle esigenze di sicurezza nazionale, possa giungere a violare gli stessi diritti fondamentali che intende tutelare.

---

[65] Sul piano degli strumenti di controllo parlamentare, A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., p. 542, propone lo svolgimento di sedute annuali di effettivo controllo e discussione sulle tematiche della difesa e della cybersicurezza, le quali, quindi, vadano oltre «la mera presa d'atto delle Relazioni trasmesse dalle istanze competenti».

[66] P. BARILE, *Democrazia e segreto*, in *Quaderni costituzionali*, n. 1, 1987, p. 29; N. BOBBIO, *La democrazia e il potere invisibile* (1980), in ID., *Il futuro della democrazia*, Torino, 1991, pp. 106 e 88; A. ANZON, *Segreto di Stato e Costituzione*, in *Giurisprudenza costituzionale*, 1976, p. 1761; R. BIFULCO, *Segreto e potere politico*, cit., p. 1101 ss.

[67] Ancora una volta, quindi, risultano sbagliate le idee di coloro i quali prevedevano la fine degli Stati, come A.J. NOCK, *Our Enemy, The State*, New York, 1935; E. MAESTRI, *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars interpretandi*, 1, 2017, p, 19. Sul punto, si v. P. CIARLO, *Un'idea sbagliata: la fine dello Stato*, in *AIC, Costituzionalismo e Costituzione nella vicenda unitaria italiana. Atti del XXVI convegno annuale*. Torino, 27-29 ottobre 2011, Napoli, 2014. M. BETZU, *I baroni del digitale*, cit., p. 19 ss.

In risposta a coloro i quali ritengono, irenicamente[68], che l'abuso dell'autorità pubblica sia oramai una degenerazione sepolta nel passato, è bene ricordare, in modo polemico[69], che le violazioni delle libertà fondamentali perpetrate sulla base della tutela della sicurezza nazionale possono avvenire tutt'oggi anche negli Stati democratici più avanzati. Oltre Oceano[70], la stessa U.S. Court of Appeals for the Third Circuit, in occasione della decisione del caso *Hassan v. City of New York* (14-1688), nell'accertare l'illegittimità per violazione della c.d. *equal protection clause*[71] del programma del *New York Police Department* volto a sorvegliare i fedeli di religione musulmana per prevenire eventuali attacchi terroristici, ha ricordato che le forme illegittime di sorveglianza delle minoranze da parte delle autorità statunitensi non sono certo una novità nella storia americana[72]. In Europa, non è passato molto tempo dal c.d. caso *Datagate*, ossia da quando la Corte EDU, nella sentenza *Big Brother watch ed altri c. Regno Unito* del 13 settembre 2018, ha accertato che le leggi in vigore nel Regno Unito sulla sorveglianza di massa davano vita a un sistema di intercettazioni che violavano il diritto alla riservatezza e la libertà di espressione[73]. Di tempo ne è passato ancora meno se si considerano le violazioni delle libertà fondamentali, che talvolta sono state perpetrare sull'altare della sicurezza dalle più evolute democrazie moderne durante la pandemia da COVID-19[74].

Proprio alla ricerca del giusto equilibrio tra efficienza dei meccanismi di reazione alle minacce cibernetiche e coinvolgimento delle istituzioni statali democratiche, ben vengano soluzioni di compromesso che

---

68 M. LUCIANI, *Costituzionalismo irenico e costituzionalismo polemico*, in Giurisprudenza costituzionale, 2, 2006, p. 1643 ss.

69 *Ibidem*.

70 Oltre al caso citato nel testo centrale, si v., con riferimento al Giappone, NGO SHADOW REPORT-ATTORNEY TEAM FOR VICTIMS OF ILLEGAL INVESTIGATION AGAINST MUSLIMS, *Extensive and Systematic Surveillance and Profiling of Muslims: Japan's Violation of the International Covenant on Civil and Political Rights*, 2014, p. 1 ss.

71 XIV emendamento della Costituzione degli Stati Uniti d'America.

72 United States Court of Appeals for the Third Circuit, caso *Hassan v. City of New York* (no. 14-1688), 13 ottobre 2015, con queste parole «What occurs here in one guise is not new. We have been down similar roads before. Jewish-Americans during the Red Scare, African Americans during the Civil Rights Movement, and Japanese-Americans during World War II are examples that readily spring to mind. We are left to wonder why we cannot see with foresight what we see so clearly with hindsight—that "[l]oyalty is a matter of the heart and mind [,] not race, creed, or color". *Ex parte Mitsuye Endo*, 323 U.S. 283, 302 (1944)». Sulla stessa linea U.S. District Court Eastern District of New York, case *Raza v. City of New York*, no. 13-3448, 28 ottobre 2015. Per maggiori approfondimenti, si v. P. ANNICCHINO, *Sicurezza nazionale e diritto di libertà religiosa*, in *Stato, Chiese e pluralismo confessionale*, 2017, p. 1 ss.; M.A. WASSERMAN, *First Amendment Limitations on Police Surveillance: The Case of the Muslim Suveillance Programme*, in *New York university Law Review*, 2015, p. 1786 ss.

73 Rispettivamente artt. 8 e 10 CEDU. Sul punto, si v. G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, cit., p. 83. Si v. anche, L.P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the EU and US constitutional system*, in L. VIOLINI, A. BARAGGIA (a cura di), *The fragmented landscape of fundamental rights protection in Europe: the role of judicial and non-judicial actors*, Cheltenham, 2018. Sempre della Corte EDU si v., *ex plurimis*, sentenza del 12 gennaio 2016, *Szabò e Vissy c. Ungheria* (ricorso 37138/14); sentenza del 4 dicembre 2016, *Zakharov c. Russia* (ricorso 47143/06). Invece, con riguardo alle decisioni della Corte di Giustizia in materia di sorveglianza di massa di v., *ex plurimis*, ECJ, sentenza del 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd*, sul punto si v. O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, n. 3, 2014; F. FABBRINI, *The European Court of Justice ruling the Data retention and its lessons for privacy and surveillance in the US*, in *Harvard Human Rights Journal*, n. 28, 2015, p. 65 ss.; M.P. GRANGER, K. IRON, *The Court of Justice and the Data retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching lessons in privacy and data protection*, in *European Law Review*, 39(6), 2014, p. 835 ss.

74 M. BETZU, P. CIARLO, *Epidemia e Mezzogiorno: la differenziazione necessaria*, in *Diritti regionali. Rivista di diritto delle autonomie territoriali*, 2020, p. 582 ss.

vedono, ad esempio, le autorità nazionali competenti NIS incardinate presso i Ministeri o il Primo Ministro, ma che consentano, allo stesso tempo, alle assemblee parlamentari di esercitare la loro funzione di controllo sul potere esecutivo. Al contrario, invece, suscitano perplessità le soluzioni che attribuiscono i poteri di autorità nazionali competenti NIS ad autorità indipendenti, le quali, se da un punto di vista dell'efficienza nell'attuazione della cybersicurezza sicuramente non conoscono pari, dal punto di vista del controllo democratico dell'esercizio dei poteri loro attribuiti, invece, non forniscono adeguate garanzie.

In questo periodo caratterizzato da frenetiche e travolgenti innovazioni tecnologiche è oramai chiaro ed evidente che la convivenza tra democrazia e tecnica sia fisiologica[75]. Gli Stati, infatti, non possono certo rinunciare all'apporto fornito dai tecnici per adempiere ai propri tradizionali doveri, come quello di garantire la cybersicurezza ai propri cittadini. Tuttavia, è proprio nei momenti come questi, di grande bisogno dei tecnici, che si rischia di invertire il rapporto tra tecnica e democrazia. La tecnica deve rimanere in una posizione di supporto rispetto alle scelte di indirizzo assunte dagli organi dotati di legittimazione popolare, come il Parlamento e il Governo. Quando, invece, sull'onda dell'eccesso di fiducia nei confronti dei tecnici o della insidiosa difficoltà di comprenderne il linguaggio, la politica abdica alla tecnica, allora quest'ultima si trasforma in "tecnocrazia"[76]. In questo modo la tecnologia diventa da *useful servant* a *dangerous master*. Tuttavia, come già ricordava Norberto Bobbio, tecnocrazia e democrazia sono antitetiche tra loro, poiché se la prima si regge sulle scelte assunte da pochi "esperti", la seconda, invece, nasce per assicurare che tutti possano decidere tutto, indipendentemente dalle condizioni economiche e sociali di ciascuno[77]. Per tali ragioni, oggi più che mai è necessario che gli Stati democratici si impegnino a garantire il controllo costituzionale di qualunque forma di potere, sia esso politico, economico o, come nel nostro

[75] M. VOLPI, *Tecnocrazia e crisi della democrazia*, in ID. (a cura di), *Governi tecnici e tecnici al Governo*, Torino, 2017, p. 2.

[76] Per D. FISICHELLA, *L'altro potere. Tecnocrazia e gruppi di pressione*, Roma-Bari, 1997, p. 54, si può parlare di regime tecnocratico quanto è il tecnocrate a stabilire, sulla base della competenza, i mezzi e i fini dell'azione sociale. Per A. RAYMOND, *Che cosa è la tecnocrazia?,* Milano, 1933, p. 5, la tecnocrazia è un nuovo sistema e filosofia di governo; per C. SCHMITT, *Il custode della costituzione* (1931), Milano, 1981, p. 215, si tratta di una nuova forma di Stato "neutrale" governata da esperti e specialisti. Sul rapporto tra tecnica e politica, v. J. HABERMAS, *Nella spirale tecnocratica. Un'arringa per la solidarietà europea*, Roma-Bari, 2014, p. 5 ss.; V. SCHMIDT, *Can Technocratic Government Be Democratic?*, Telos, 23, 2011; N. IRTI, *Del salire in politica. Il problema della tecnocrazia*, Torino, 2014; C. DE FIORES, *Tendenze sistemiche e aporie costituzionali dei governi tecnocratici in Italia*, in *Costituzionalismo.it*, n. 2, 2021, p. 36 ss.; F. FISCHER, *Democracy and Expertise*, Oxford, 2009; A. ESMARK, *The New Technocracy,* Bristol, 2020, p. 76 ss.

[77] N. BOBBIO, *Il futuro della democrazia*, Torino, 1984, p. 23.

caso, tecnologico[78], perché solo in questo modo è possibile scongiurare l'avvento della schmittiana «epoca delle neutralizzazioni e delle spoliticizzazioni»[79].

[78] G. AZZARITI, *Tecnica, politica, Costituzione. Perché non solo la politica, ma anche la tecnica deve essere limitata dalla Costituzione*, in G. GRASSO (a cura di), *Il Governo tra tecnica e politica*, Napoli, 2016, p. 115 ss. Sul potere digitale, di recente si v. O. POLLICINO, *Potere digitale*, in *Enciclopedia del diritto. I tematici*, vol. V, *Potere e costituzione*, Milano, 2023, p. 410 ss. Sui poteri privati nello spazio digitale si v., tra i tanti, M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, n. 3, 2021, p. 739 ss., nonché ID., *I baroni del digitale*, cit., p. 15 ss.; F. PARUZZO, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Napoli, 2023; E. CREMONA, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023. Sul c.d. totalitarismo cibernetico determinato dal "dataismo", nonché sull'impatto del digitale sul diritto costituzionale, si v. di recente E. LONGO, *La ricerca di un'antropologia costituzionale della società digitale*, in *Rivista italiana di informatica e diritto*, 2, 2023, p. 151 ss, nonché i contributi contenuti in S. CALZOLAIO (a cura di), *La fine di internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, sezione monografica della *Rivista italiana di informatica e diritto*, 2023.

[79] C. SCHMITT, *L'epoca delle neutralizzazioni e delle spoliticizzazioni*, 1929, in ID., *Le categorie del 'politico'*, Bologna, 1972, p. 167 ss.