Manfredi Matassa

Sicurezza cibernetica e nazionale nell'ordinamento multilivello: quale possibile convivenza?

Abstract: Il paper si concentra sul rapporto tra cybersecurity e sicurezza nazionale da una prospettiva funzionale, con l'obiettivo principale di individuare le problematiche della coesistenza di queste funzioni nel sistema multilivello. In particolare, dopo un inquadramento generale volto ad affrontare alcune questioni definitorie centrali ritenute indispensabili ai fini dell'analisi, l'elaborato intende evidenziare le ricadute del mutevole rapporto tra i concetti in esame. L'analisi mira ad approfondire il tema sia con riferimento alla distribuzione delle competenze tra Unione Europea e Stati membri (sul versante verticale) sia tra gli attori pubblici e privati coinvolti (sul versante orizzontale).

Keywords: Cybersecurity; Sicurezza nazionale; ENISA; Agenzia per la Cybersicurezza Nazionale; ACN.

1. Inquadramento del campo di indagine

Nel corso degli ultimi anni la sicurezza cibernetica[1] ha assunto una crescente centralità all'interno del dibattito giuspubblicistico fino al punto di assumere i caratteri di una inedita funzione pubblica distinta rispetto alle tradizionali funzioni di sicurezza. Partendo dal presupposto per cui l'esponenziale aumento delle capacità lesive degli attacchi informatici abbia elevato la cibersicurezza a prerequisito essenziale per la sopravvivenza di qualsiasi organizzazione complessa, la materia in oggetto si è ormai imposta al centro delle agende di ogni legislatore.

1 Al fine di prevenire equivoci di tipo terminologico si precisa che nel presente scritto le espressioni 'sicurezza cibernetica', 'sicurezza informatica' e 'cibersicurezza' – anche nella sua versione anglofona '*cybersecurity*' – saranno impiegati come sinonimi. Ritenendo condivisibili i rilievi mossi dall'Accademia della Crusca in tal senso, si è ritenuto opportuno non utilizzare la dicitura ibrida 'cybersicurezza' al momento preferita dal legislatore italiano. Per un inquadramento di ampio respiro sul tema si rinvia, tra gli altri, a Giupponi 2024: 277-303, Longo 2024: 313-347, Buoso 2023; Rossa 2023; Carotti 2020: 629-641; Serini 2022: 241-272; Ursi 2023: 7-20 e Matassa 2023: 21-42.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760161

L'Unione europea non è stata di certo tra le prime istituzioni ad acquisire una piena consapevolezza circa la necessità di adottare in tempi rapidi dei modelli regolatori capaci di affrontare al meglio le future sfide di sicurezza cibernetica[2]. Nonostante la *cybersecurity* si sia affermata come componente indispensabile soltanto in anni recenti, oggi non sorprende notare tra le prime venti posizioni del *Global Cybersecurity Index* la presenza di ben undici Paesi europei[3]. Ebbene, senza voler sminuire gli sforzi individuali compiuti dagli Stati tradizionalmente più attenti al tema della sicurezza informatica[4], i meriti riconosciuti a tali Paesi devono ritenersi in larga parte connessi ai recenti interventi europei che hanno permesso la realizzazione di un'infrastruttura comune di sicurezza cibernetica all'avanguardia.

Cionondimeno, il percorso che ha portato alla creazione dell'attuale architettura di difesa cibernetica europea è stato tutt'altro che lineare. La *cybersecurity* è stata catalogata nel novero degli '*important issues*' europei già in una raccomandazione del 2000, ma – stante l'istituzione nel 2004 di un'Agenzia temporanea preposta alla sicurezza della rete e delle informazioni (ENISA) e di altri interventi settoriali non particolarmente incisivi – il tema non è stato oggetto di vere e proprie iniziative regolamentari fino all'adozione della *Network and Information Security directive* ('direttiva NIS') del 2016. La pubblicazione di tale direttiva non è stato un punto di arrivo delle politiche europee di cibersicurezza, ma ha segnato l'inizio di una fase di iperproduzione normativa – ancora oggi *in itinere* – che ha dato vita a una disciplina straordinariamente complessa e intricata. Infatti, tra le fonti primarie a livello euro-unionale in materia di sicurezza cibernetica più rilevanti, oggi in vigore è possibile ricordare il regolamento 881/2019 ('cybersecurity Act'), il regolamento 2554/2022 ('regolamento DORA') e la direttiva 2555/2022 ('direttiva NIS II'). Inoltre, tale pacchetto normativo è destinato a essere ampliato nel prossimo futuro da due ulteriori pilastri regolatori, volti da un lato ad aggiornare il sistema di certificazioni di cibersicurezza ('Cyber Resilience Act') e, dall'altro, a istituire uno scudo di difesa europea basato su meccanismi solidali e incentivanti ('Cyber Solidarity Act').

L'approccio italiano alla sicurezza cibernetica si è distinto da quello degli altri Paesi europei per la sua struttura innovativa e articolata. Negli ultimi anni l'Italia

2 Ad esempio, gli Stati Uniti hanno inserito la *cybersecurity* tra le priorità del governo federale già nel 1997, dimostrando già allora consapevolezza circa l'importanza che avrebbe avuto il tema nel determinare i futuri equilibri tra Stati (mentre, come si avrà modo di evidenziare *infra*, la prima disciplina organica dell'Unione europea risale al 2016).

3 ITU, Global Cybersecurity Index (GCI) 2020, 25, reperibile su www.itu.int (visitato il 18 luglio 2024). Segnatamente, all'interno del '*global score and rank*' si segnalano, in ordine di apparizione: Estonia (3°), Spagna (4°), Lituania (6°), Francia (9°), Lussemburgo e Germania (13°), Portogallo (14°), Lettonia (15°), Olanda (16°), Belgio 19° e Italia (20°).

4 Tra gli esempi più virtuosi non possono che segnalarsi i differenti modelli di difesa cibernetica elaborati da Francia e Germania: la prima ha creato un'agenzia destinata alla sicurezza cibernetica (ANSSI) già nel 2008 durante la presidenza di Sarkozy; la seconda ha fondato nel 1991 (dunque ancor prima della stessa diffusione commerciale di Internet) il *Bundesamt für Sicherheit in der Informationstechnik* come autorità dedicato all'ufficio federale della sicurezza informatica.

ha intrapreso significativi passi avanti nel rafforzare le proprie capacità di difesa e risposta agli attacchi informatici attraverso l'elaborazione *ad hoc* di strumenti e apparati inediti volti a far fronte alle nuove sfide imposte dalla cibersicurezza. L'assoluta priorità acquisita dalla sicurezza cibernetica nell'agenda degli ultimi governi non è determinata esclusivamente dai nascenti obblighi di matrice euro-unitari, ma è stata stimolata anche (forse soprattutto) da fattori esogeni. Basti pensare che, dal primo semestre del 2018 al secondo semestre del 2023, è stato rilevato un aumento dell'86% degli attacchi informatici e nello stesso periodo la media di attacchi gravi per mese è passata da 124 a 230 (arrivando così a quasi otto per giorno)[5].

Nel conteso descritto, preso atto della circostanza per cui le organizzazioni pubbliche e private italiane fossero maggiormente esposte agli attacchi informatici rispetto alla media europea, il legislatore nazionale è stato chiamato ad affrontare il tema della sicurezza cibernetica attraverso l'elaborazione di soluzioni spesso originali. In particolare, come si avrà modo di approfondire *infra*, se in un primo momento il decisore politico italiano si è limitato a una mera attuazione delle misure contenute all'interno della direttiva NIS, dopo appena un anno l'architettura normativa nazionale si è distinta (in positivo) per aver introdotto uno strumento di sicurezza informatica all'avanguardia, ossia il Perimetro di Sicurezza Nazionale Cibernetica (d'ora in avanti 'PSNC' o 'Perimetro'). Peraltro, al di là degli obiettivi fissati dalla strategia quinquennale in materia di sicurezza cibernetica 2022-2026 e dal piano triennale per l'informatica della pubblica amministrazione 2024-2026, negli ultimi anni si è realizzato un complessivo ripensamento dell'intera infrastruttura di sicurezza cibernetica trainato soprattutto dall'istituzione dell'Agenzia per la Cybersicurezza Nazionale (d'ora in avanti 'ACN' o 'Agenzia'). In ultimo, oltre alla recentissima approvazione della l. 28 giugno 2024, n. 90 (dapprima noto come 'd.d.l. cyber'), il quadro normativo nazionale è destinato ad arricchirsi ulteriormente con la necessaria e attuazione della direttiva NIS2[6].

A un primo sguardo la componente nazionale di sicurezza cibernetica sembra collegata con quella europea fino al punto da risultare non tanto complementare, quanto piuttosto ricollegata a una medesima e inedita funzione dal carattere autonomo (ossia la sicurezza cibernetica). Cionondimeno, osservando con maggiore accortezza la disciplina descritta è possibile notare delle distinzioni profonde al punto da mettere in dubbio qualsiasi tentativo di *reductio ad unum* della materia. Nonostante sul piano concreto le 'dimensioni' della cibersicurezza tendano in larga parte a coincidere, occorre notare, come sul piano teorico, le stesse perseguano tra loro finalità ben distinte: il livello europeo della sicurezza cibernetica è volto

5 Clusit, *Rapporto 2024 sulla Sicurezza ICT in Italia*, 15 reperibile su https://clusit.it/rapporto-clusit (visitato il 12 ottobre 2024). Più nel dettaglio, i dati indicati nel rapporto mettono in evidenza come – al di là degli 'attacchi multipli' (19,4%) – il settore più colpito da tali attacchi è il settore sanitario con una percentuale che si assesta sul 14,3%, seguito da quello governativo e militare che si assesta sull'11,7%.

6 La direttiva NIS2 è stata da ultimo recepita nell'ordinamento italiano con il d.lgs. 4 settembre 2024, n. 138.

alla tutela del mercato interno dell'Unione, mentre quello italiano è indirizzato alla tutela della sicurezza nazionale.

Oltre a mettere in discussione qualsiasi lettura volta ad attribuire alla sicurezza cibernetica il carattere di funzione autonoma e unitaria, la distinzione in esame porta con sé delle conseguenze di ordine pratico. La scelta del legislatore italiano di ricondurre la *cybersecurity* nell'alveo della sicurezza nazionale permette di esercitare sulla parte della materia la 'riserva di Stato' di cui all'art. 4, par. 2, del Trattato sull'Unione europea (TUE), il quale, dopo aver individuato le 'funzioni essenziali dello Stato', precisa che "[…] la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro". Su tali presupposti, comprendere la relazione tra le funzioni di tutela del mercato e quelle di sicurezza nazionale si rivela essenziale per approfondire *in primis* i rapporti tra il versante nazionale ed europeo della materia e, *in secundis*, come immediata ricaduta, il grado di cedevolezza delle tutele dei privati rispetto all'interesse 'superiore' (supremo?) alla sicurezza. Cionondimeno, lo studio non potrebbe raggiungere gli obiettivi prefissati senza aver prima fornito alcune definizioni volte a permettere un corretto inquadramento generale della materia.

2. Alcuni necessari chiarimenti sul versante definitorio

Una delle principali cause che ha rallentato lo sviluppo di studi in campo pubblicistico volti ad approfondire il tema in oggetto può ricondursi alla possibilità di considerare ambedue le componenti essenziali poste alla base della nozione di *cybersecurity* (ossia la sicurezza e la cibernetica) dei 'concetti giuridici indeterminati'.

Nel diritto pubblico, così come nel linguaggio comune, la nozione di sicurezza può essere osservata soltanto dopo aver collocato il concetto in un determinato "paradigma"[7] o "dimensione"[8]. Così, partendo dall'assunto per cui la sicurezza è "un concetto generico e vuoto, che se non è specificato o riempito non significa nulla" (Bobbio 1976, 322), la scienza giuridica ha sviluppato dei metodi di indagine 'relazionali' utili ai fini dell'individuazione di nuovi significati della nozione. Tra questi è possibile distinguere gli approcci basati su una prospettiva relazionale 'in positivo' (volti cioè a ricercare il contenuto del termine mediante un raffronto con profili di valutazione di tipo oggettivo e soggettivo) dagli approcci volti a ricostruire il significato di sicurezza 'in negativo' (partendo dall'individuazione del rischio quale elemento speculare al concetto di sicurezza). Cionondimeno, poiché nella materia in esame la nozione di 'sicurezza' entra in contatto con un altro concetto giuridico indeterminato (la cibernetica), comprendere l'esatto significato del termine 'cibersicurezza' si dimostra un compito tutt'altro che agevole.

7 Per un approfondimento sull'evoluzione dei "paradigmi giuridici della sicurezza" in Italia si rimanda all'analisi di Ursi 2022: 15-46.

8 Sul punto si rimanda in generale al lavoro di Giupponi 2008: *passim*.

Poiché considerazioni in larga parte analoghe possono estendersi al concetto di 'sicurezza nazionale', considerato "giuridicamente evanescente" (Monti 2020, 75) nonché riconducibile alla sfera del "pre-, extra-, o meta-giuridico" (Barberis 2017, 97), in un simile scenario chiunque intenda approfondire la relazione tra le nozioni di sicurezza cibernetica e sicurezza nazionale è chiamato a misurarsi con ostacoli posti su più livelli. Non potendo in questa sede soffermarsi sui numerosi problemi di natura definitoria messi a fuoco dalla dottrina d'oltreoceano nel corso dell'ultimo ventennio, si ritiene opportuno evidenziare che, allo stato dell'arte, è possibile ricavare dalla normativa vigente una definizione di 'sicurezza cibernetica' ma non di 'sicurezza nazionale'.

Segnatamente, prendendo atto della coesistenza di almeno diciotto definizioni diverse di *cybersecurity* (Fuster e Jasmontaite 2020: 105-106), il legislatore europeo ha definito all'art. 2, comma 1, del regolamento 881/2019 la 'cibersicurezza' come "l'insieme delle attività necessarie per proteggere la rete e i servizi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche". Tale definizione è stata successivamente sviluppata nel diritto nazionale dall'art. 1, comma 1, lett. a) del d.l. 14 giugno 2021, n. 82, come "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"[9]. Ebbene, le modifiche apportate dal legislatore italiano alla definizione di cibersicurezza possono essere comprese soltanto se lette in combinato disposto con la nozione di 'resilienza nazionale nello spazio cibernetico', introdotta nella successiva lett. b), ossia "quel complesso di attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'art. 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131"[10].

Se sul versante formale la distinzione tra 'cybersicurezza' e 'resilienza nazionale nello spazio cibernetico' sembra collocare tali concetti in una relazione da genere a specie, non può ignorarsi come – in una prospettiva sostanziale (e più approfondita) – la normativa di riferimento si presti anche a interpretazioni differenti.

9 Ragioni di completezza di analisi suggeriscono di riportare per intero il contenuto del citato art. 1, comma 1, lett. a), d.l. 82/2021: "[ai fini del presente decreto si intende per 'cybersicurezza'] 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".

10 Art. 1, comma 1, lett. f), DPCM 30 luglio 2020, n. 131: "[ai fini del presente decreto si intende per 'pregiudizio per la sicurezza nazionale'] 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 gli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale […]".

Difatti, inquadrando i concetti presi in esame in chiave formalistica, la sicurezza cibernetica potrebbe essere rappresentata come una nozione ampia al punto da ricomprendere al suo interno tutte quelle attività volte non solo ad assicurare la riservatezza, l'integrità e la disponibilità dei dati (la Triade nota come RID o CIA), ma anche la "sicurezza nazionale nello spazio cibernetico". Diversamente, la resilienza nazionale nel ciberspazio è un concetto legato a doppio filo con quello della tutela della sicurezza nazionale (e dunque riferito a una componente speciale di 'resilienza'). Una simile chiave di lettura potrebbe essere utilizzata quale fondamento teorico generale per individuare con sufficiente determinatezza un criterio distintivo tra le competenze in materia di sicurezza cibernetica, in astratto attribuibili all'Unione europea, e quelle necessariamente riservate agli Stati membri in forza dei limiti stabiliti dall'art. 4, par. 2, TUE.

Tuttavia, un'analisi più puntuale del quadro normativo nazionale permette di mettere in dubbio la possibilità di distinguere in modo chiaro questi concetti. Del resto, è sufficiente esaminare il contenuto del citato art. 1, comma 1, lett. f) del DPCM 131/2020 per notare come la nozione di 'sicurezza nazionale' non si presti a essere agevolmente contenuta all'interno di un perimetro circoscritto. Infatti, come già messo in evidenza *supra*, quest'ultimo termine è stato descritto dal legislatore in modo talmente ampio da ricomprendere non solo qualsiasi "danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche", ma anche qualsiasi pericolo ricollegato agli "interessi politici, militari, economici, scientifici e industriali dell'Italia". Ebbene, figurando la tutela della riservatezza, integrità e disponibilità dei dati tra gli 'interessi nazionali' politici ed economici, una lettura estensiva del combinato disposto permette di ricavare un significato del concetto di sicurezza cibernetica più ampio rispetto a quello attribuito alla sicurezza nazionale. Così, a seconda dell'angolo visuale, ognuno dei due concetti finisce per diventare allo stesso tempo sia contenuto, sia contenitore dell'altro.

Su tali premesse la scelta del legislatore nazionale di introdurre una (quantomeno equivoca) distinzione tra i concetti di 'sicurezza' e 'resilienza' cibernetica può ritenersi tutt'altro che casuale. *A contrario*, considerata anche la limitata utilità pratica della distinzione presa in esame, il parziale distacco rispetto alla definizione elaborata dal reg. (UE) 881/2019 può ritenersi frutto della volontà del decisore nazionale di mantenere intatti i benefici concessi dall'ambiguità del rapporto tra sicurezza cibernetica e sicurezza nazionale. Tale meccanismo permette alle istituzioni nazionali di valutare la medesima funzione talvolta come attività condivisa con l'Unione, consentendo così di beneficiare dei meccanismi di solidarietà europea (si pensi alla condivisione di informazioni e alla distribuzione di risorse vincolate al miglioramento dell'infrastruttura di difesa cibernetica nazionale), talvolta come attività strettamente correlata alla sicurezza nazionale. Ed infatti, il parallelismo tra sicurezza cibernetica e nazionale attribuisce alla Presidenza del Consiglio dei ministri – e all'ACN – poteri capaci di incidere sensibilmente sui diritti di libera iniziativa economica dei privati[11].

11 Assumono particolare rilievo in tal senso i poteri in materia di Perimetro Nazionale

3. La cibersicurezza come funzione tra sicurezza nazionale ed esigenze di tutela del mercato dell'Unione

Sulla base degli elementi fin qui tratteggiati la sicurezza cibernetica può essere rappresentata, almeno in una prima approssimazione, come una funzione pubblica complessa, multilivello, dal carattere composito e che coinvolge al suo interno due distinti gruppi di funzioni: uno strettamente collegato al paradigma securitario della materia (difesa, sicurezza pubblica, sicurezza nazionale e – più di recente – difesa attiva[12]) e un secondo a funzioni dal carattere spesso eterogeneo elaborate *ad hoc* per far fronte alle minacce cibernetiche, ossia quelle connesse alla tutela della 'Triade'(riservatezza, l'integrità e la disponibilità dei dati). Tuttavia, la relazione tra questi due gruppi di funzioni è cambiata radicalmente nel corso degli ultimi anni seguendo l'evoluzione del rapporto tra l'infrastruttura nazionale ed europea in materia di sicurezza cibernetica.

In una prima fase (2013-2021) il rapporto tra le esigenze di tutela del mercato interno e quelle della sicurezza nazionale si poteva inquadrare in un'ottica di completamento della disciplina nazionale rispetto a quella dell'Unione. Sul fronte europeo, la direttiva NIS si era occupata di disegnare una prima linea di difesa volta a offrire un livello di tutela al mercato interno dell'Unione (lasciando fuori dal campo di applicazione alcuni settori essenziali tra cui – oltre alla Pubblica Amministrazione – il settore nucleare e spaziale). Sul fronte nazionale, invece, la disciplina del 'decreto Perimetro' ha inteso dotare l'Italia di uno strumento diretto alla protezione in via autonoma di infrastrutture ritenute rilevanti per la sicurezza nazionale del Paese. Così, partendo dall'idea per cui nelle materie di 'sicurezza' il titolare di una funzione è il soggetto preposto a valutare il livello di rischio o di pericolo (lasciando l'individuazione del rischio o del pericolo in sé al decisore politico), fino al 2021 era possibile distinguere, almeno tendenzialmente, le funzioni esclusivamente statali volte a garantire la sicurezza nazionale da quelle condivise con l'Unione europea, nell'esercizio delle quali l'amministrazione nazionale agiva soprattutto 'in funzione comunitaria'[13]. Lo scenario fin qui descritto è mutato ra-

di Sicurezza Cibernetica (PSNC) originariamente attribuiti dal d.l. 105/2019 alla Presidenza del Consiglio dei ministri (successivamente trasferiti in capo all'ACN dal d.l. 82/2021). Posto che l'attuale disciplina preclude ai privati di conoscere le ragioni poste a fondamento della decisione della Presidenza del Consiglio, rendendo di fatto i 'soggetti inclusi' all'interno del Perimetro sprovvisti degli strumenti necessari per sindacare la loro inclusione all'interno del PNSC dinanzi a qualsiasi giudice, va segnalato che i gravosi obblighi attribuiti ai 'soggetti inclusi' sono oggi posti interamente a carico di quest'ultimi. Dunque, come si avrà modo di notare più avanti, l'attuale quadro normativo impone ai privati di sostenere dei costi ingenti a fronte di benefici che risultano a beneficio di tutta la collettività.

12 Si fa riferimento, in particolare, alla previsione contenuto all'interno del 'decreto aiuti *bis*' che ha attribuito al Presidente del Consiglio dei ministri il potere di adottare, una volta acquisito il parere del CISR e del COPASIR, "disposizioni per l'adozione di misure di *intelligence* di contrasto in ambito cibernetico" in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza.

13 Sull'argomento si rinvia, *ex multis*, al lavoro di Saltari 2007.

dicalmente con l'avvio di una seconda fase di politiche in materia di cibersicurezza tra cui si ricorda, a livello eurounitario, la direttiva NIS II, i regolamenti CER e DORA, le proposte note come 'Cyber Solidarity Act' e 'Cyber Resilience Act' e, sul versante nazionale, la l. 90/2024 (che in questo nuovo ciclo di politiche non può annoverarsi tra gli interventi più felici)[14].

Per quel che qui interessa, il nuovo quadro complessivo delineato dalla direttiva NIS2 ha causato un'evidente crisi del rapporto tra sicurezza nazionale e cibernetica. Crisi, quest'ultima, che può essere ricondotta alla scelta del legislatore europeo di tutelare il mercato interno attraverso n complesso di regole più incisive – tanto per ampiezza, quanto per profondità – rispetto a quelle utilizzate dagli Stati membri per garantire la sicurezza nazionale.

La complessità del quadro giuridico che caratterizza l'ordinamento multilivello di sicurezza cibernetica può cogliersi in modo plastico mettendo a confronto le sanzioni previste dal decreto istitutivo del Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[15] con quelle proprie della Direttiva NIS2[16]. La violazione degli obblighi di segnalazione e condivisione delle informazioni contenute nella disciplina NIS2 comporta la momentanea sospensione dei certificati di cibersicurezza eventualmente rilasciati, la momentanea sospensione dei dirigenti dal loro incarico e una sanzione del 2% del fatturato globale (per un minimo di dieci milioni di euro) nel caso dei soggetti essenziali[17], o dell'1,4% nel caso soggetti importanti[18].

14 Le principali perplessità vanno ricollegate alla circostanza per cui, stante l'imminente scadenza del termine per il recepimento della direttiva NIS2, il legislatore nazionale abbia introdotto misure inedite volte ad aumentare il livello di cibersicurezza del Paese senza al contempo dare neppure un'attuazione parziale alla 'nuova' direttiva (la quale, come detto, è stata recepita successivamente con il d.lgs. 4 settembre 2024, n. 138).

15 D.l. 23 luglio 2019, n. 105, convertito con modificazioni dalla l. 16 settembre 2019, n. 126, recante "misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19 e per l'esercizio in sicurezza di attività sociali ed economiche".

16 Si rimanda, in particolare, al contenuto degli artt. 34-36 dir. (UE) 2022/2555. Vale la pena precisare che le disposizioni in esame hanno natura *self-executing* in funzione di quanto indicato dall'art. 34, par. 8, dir. (UE) 2022/2555, secondo il quale "[s]e l'ordinamento giuridico di uno Stato membro non prevede sanzioni amministrative pecuniarie, lo Stato membro in questione provvede affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti".

17 Art. 34, par. 4, dir. (UE) 2022/2555. I 'soggetti essenziali' sono stati identificati dall'art. 3, par. 1, dir. (UE) 2022/25555 come quei soggetti la cui interruzione di servizio avrebbe un impatto diretto e immediato sul funzionamento della società e dell'economia (imprese pubbliche o private operanti nel settore dell'energia, dei trasporti, della salute e della fornitura di acqua, ma anche tutte le amministrazioni centrali dei Paesi membri).

18 Art. 34, par. 5, dir. (UE) 2022/2555. I 'soggetti importanti sono stati individuati dall'art. 3, par. 2, dir. (UE) 2022/25555 come quei soggetti titolari di funzioni di rilievo all'interno dell'economia digitale e sociale (includendo servizi digitali come motori di ricerca, *cloud computing* e piattaforme *online*) meritevoli di tutela benché non critici allo stesso livello dei 'soggetti essenziali'.

Diversamente, le sanzioni individuate dal decreto Perimetro vanno da un minimo di duecento mila euro a un massimo di poco meno di due milioni, pari a circa un ventesimo delle sanzioni previste dalla direttiva NIS II[19].

Quanto fin qui messo in evidenza permette di comprendere come, allo stato dell'arte, il rapporto tra sicurezza cibernetica e nazionale non si presti a una lettura statica e uniforme. Sul versante formale, la presenza della 'riserva di Stato' in materia di sicurezza nazionale stabilita dall'art. 4, par. 2, TUE si impone quale rigida e insuperabile linea capace di regolare i confini tra la dimensione europea e la dimensione nazionale della materia. Tuttavia, osservando il quadro normativo multilivello in materia di cibersicurezza in una prospettiva sostanziale, il descritto limite non ha permesso la creazione di un vero e proprio 'nucleo duro' di funzioni di prerogativa statale volte a introdurre delle misure più stringenti (in ragione della particolare rilevanza degli interessi nazionali in gioco). Così, in nome della tutela del mercato interno dell'UE, nell'introdurre misure più dissuasive rispetto a quelle utilizzate dagli Stati membri per la tutela della sicurezza nazionale, la nuova fase di politiche di *cybersecurity* ha determinato una crisi del rapporto tra le categorie prese in esame e – come immediata ricaduta – un cortocircuito nella distribuzione di competenze a livello verticale.

4. Considerazioni conclusive sul futuro prossimo della sicurezza cibernetica

L'impossibilità di offrire una lettura univoca del rapporto tra sicurezza nazionale e sicurezza cibernetica richiede ulteriori considerazioni sul futuro prossimo della sicurezza cibernetica.

Anzitutto, l'impossibilità di individuare dei confini certi all'interno della materia rispetto alla componente assimilabile alla 'sicurezza nazionale' crea dei problemi piuttosto evidenti con riferimento al ruolo '*whole of society*' attribuito ai privati dalla Strategia Nazionale[20]. Difatti, a meno di accettare la configurabilità in astratto di un esercizio privato di funzioni pubbliche in tale materia, fissare uno spazio all'interno della *cybersecurity* riservato alla 'sicurezza nazionale' equivale a individuare un'area in cui è precluso l'intervento di attori estranei al 'comparto sicurezza'. In tal senso, i sostenitori delle capacità dello 'Stato innovatore'[21] potrebbero obiettare che lo stesso sviluppo della tecnologia internet sia stato in qualche modo frutto di un'attività di esternalizzazione della sicurezza nazionale[22], ma questa posizione può essere avallata

19 Art. 1, comma 9, lett. b), d.l. 105/2019 secondo cui "il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera a), nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000".

20 ACN, *Strategia Nazionale di Cybersicurezza*, 2022, 8, ove precisa che "la presente strategia è ispirata ad un approccio "*whole-of-society*", che vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza".

21 Il riferimento non può che essere al noto lavoro di Mazzuccato 2018 [2014].

22 Come è noto, la rete oggi conosciuta come Internet è nata all'inizio degli anni Sessanta nell'ambito di un progetto militare in cui, almeno in una prima fase, gli Stati Uniti d'America si

solo tenendo in considerazione la circostanza per cui proprio lo Stato innovatore sia finito per attribuire – seppur per un periodo ben circoscritto – a un singolo individuo il controllo esclusivo di una delle tecnologie più rivoluzionarie della storia[23]. Ciò non significa necessariamente opporsi a un maggiore coinvolgimento dei privati in questioni di sicurezza nazionale in senso ampio. Infatti, l'assenza di competenze specialistiche nel settore pubblico rende difficili gli sforzi delle amministrazioni di fronteggiare le sfide sempre più complesse poste dalla cibersicurezza.

Nonostante questa esigenza di competenze, è fondamentale definire una chiara linea di demarcazione tra pubblico e privato, capace di prevenire il ripetersi di errori del passato, come l'attribuzione incontrollata di funzioni strategiche a soggetti privati. La definizione di tali confini – è bene specificarlo – non deve però essere vista come una limitazione alla collaborazione tra pubblico e privato, bensì come uno strumento di garanzia per entrambe le parti, volto a proteggere gli interessi nazionali senza sacrificare l'innovazione o la flessibilità. La chiave sta nel costruire un quadro normativo che sia sufficientemente solido da garantire la sicurezza, ma al tempo stesso abbastanza flessibile da permettere un adattamento continuo alle innovazioni tecnologiche. Solo in questo modo sarà possibile costruire una governance della cibersicurezza capace di rispondere efficacemente alle sfide moderne, evitando sia l'eccessiva regolamentazione che la deregulation indiscriminata, e preservando così settori vitali per la sicurezza del Paese.

In secondo luogo, il contesto fin qui descritto richiede di interrogarsi circa l'opportunità di mantenere intatto il PSNC così come disegnato dal d.l. 105/2019 o se, invece, propendere verso un maggiore avvicinamento tra la dimensione nazionale e quella europea di sicurezza cibernetica. A tal proposito, se è vero che il legislatore del 'decreto Perimetro' ha elaborato tale meccanismo allo scopo di fornire un livello di tutela adeguato a quei soggetti pubblici e privati la cui attività è stata ritenuta essenziale ai fini della salvaguardia della 'sicurezza nazionale', va ricordato che il Perimetro è stato introdotto in un contesto emergenziale per porre rimedio ad alcune gravi lacune della direttiva NIS del 2016. Difatti, in una prima fase delle politiche in materia di cibersicurezza, il PSNC ha assunto un ruolo di indiscuti-

sono limitati ad essere 'promotori' dello sviluppo della tecnologia (finanziando e vigilando sul lavoro svolto da numerosi soggetti privati distribuiti in tutto lo Stato). In un secondo momento, nondimeno, le 'antiche sovranità' e i 'padri della rete' sono entrati in conflitto nel momento di stabilire quale soggetto dovesse mantenere il controllo della rete.

23 Il riferimento è agli eventi degli anni Novanta che videro protagonista uno tra i fondatori della rete, Jon Postel, ritenuto da alcuni niente di meno che "il Dio dell'Internet" [Goldsmith e Wu 2006: 29-46]. A fronte della pretesa degli Stati uniti di acquisire un maggiore controllo sulla rete, Postel decise di sfidare l'amministrazione americana con l'obiettivo di dimostrare che il ruolo dei 'fondatori' non potesse essere sostituito dagli strumenti tradizionali in possesso delle antiche sovranità. Così, attraverso una semplice email destinata a dodici operatori sparsi in tutto il mondo, un solo individuo ottenne il controllo – *rectius*, il potere di 'nominare e numerare' (la '*root authority*') – di una delle tecnologie più rivoluzionarie della storia dell'umanità. Sebbene Postel abbia 'volontariamente' rinunciato a tali poteri dopo circa una settimana, la vicenda che lo vede coinvolto merita di essere tenuta in adeguata considerazione nel dibattito sull'esternalizzazione. Per uno studio di ampio respiro sul tema dell'*internet governance* non può che rinviarsi a Carotti 2016.

bile centralità nell'infrastruttura legislativa multilivello, in quanto ha permesso di estendere alcuni obblighi di notifica degli incidenti e di certificazione anche agli 'illustri esclusi' dalla prima direttiva europea (la quale, come già ricordato, non includeva neppure le pubbliche amministrazioni).

Cionondimeno, nell'attuale quadro normativo – in cui le misure poste a tutela della sicurezza nazionale risultano meno incisive rispetto a quelle introdotte per proteggere il mercato interno dell'Unione – non risulta affatto complicato contestare la ragion d'esistere del Perimetro di sicurezza nazionale cibernetica. Difatti, nell'attesa di comprendere le modalità di attuazione a livello nazionale delle principali novità introdotte dalla direttiva NIS II, non si può fare a meno di notare come allo stato dell'arte il Perimetro produca una duplicazione degli oneri posti in capo ai soggetti 'perimetrati' (e sottoposti parallelamente al regime NIS) difficilmente giustificabile alla luce della più ampia portata delle nuove disposizioni europee. Nel contesto descritto, le entità sottoposte contestualmente alle misure nazionali ed europee sono soggetti a una gravosa duplicazione degli oneri di *compliance* e di notifica (il cui costo ricade interamente sugli stessi).

Tale circostanza dà luogo a due ordini di problemi tra loro strettamente collegati. In primo luogo, lungi dal ridurre lo sforzo richiesto ai privati per sostenere la sicurezza cibernetica italiana ed europea, il quadro normativo vigente chiede a quest'ultimi maggiori sacrifici individuali volti al raggiungimento di un'utilità diffusa (orientando il complesso di politiche italiane verso una direzione contraria rispetto alle ambizioni dell'Unione). In secondo luogo, spostando l'attenzione sui soggetti pubblici 'perimetrati', la duplicazione degli oneri aumenta ulteriormente il divario tra il grado di conoscenza richiesta alla pubblica amministrazione e la realtà del pubblico impiego italiano, il quale – oltre a non possedere una cultura informatica elementare – si dimostra oggi incapace di assorbire le competenze specialistiche richieste per far fronte alle sfide del nuovo millennio. Quest'ultima circostanza si traduce in una generale tendenza delle amministrazioni sottoposte agli obblighi PSNC e NIS a una significativa esternalizzazione degli oneri richiesti in favore di soggetti privati specializzati, il che dà luogo a un rapporto di forte dipendenza dell'apparato pubblico rispetto a un *know how* destinato a rimanere in buona parte prerogativa dei privati (strategia che nel lungo termine non può che dimostrarsi perdente)[24].

Per concludere è possibile evidenziare come, allo stato dell'arte, non sia possibile offrire una rappresentazione del rapporto tra la sicurezza cibernetica e nazionale capace di offrire una visione statica e ordinata della disciplina multilivello della cibersicurezza. Ad oggi i due concetti sono avvicinati da una forza centripeta frutto, sul piano nazionale, del progressivo allontanamento della materia dal Sistema di Informazione per la Sicurezza della Repubblica (SISR)[25] e, sul versante euro-unita-

24 Per un'analisi volta a rappresentare le sfide della collaborazione pubblico-privato nel settore della cibersicurezza si rimanda, tra gli altri, a Previti 2022: 65-93.

25 Il Sistema di Informazione per la Sicurezza della Repubblica (SISR) è l'infrastruttura disegnata dalla legge l. 3 agosto 2007, n. 124 allo scopo di riorganizzare l'assetto del 'comparto *intelligence*' italiano che, fino a quel momento, aveva operato sotto la vigenza l. 24 ottobre 1977, n. 801.

rio, dal contestuale indebolimento (superamento?) del dogma della 'prerogativa di Stato' in materia di sicurezza nazionale di cui all'art. 4, par. 2, TUE[26].

Le peculiarità che caratterizzano lo stato dell'arte della disciplina in commento non devono tuttavia disincentivare ulteriori studi volti ad approfondire la relazione in oggetto. Non solo, come messo in evidenza *supra*, le modalità con cui tale rapporto viene declinato hanno delle conseguenze profonde a livello pratico ricollegate soprattutto alla distribuzione di competenze verticali (tra Unione europea e Stati membri) e orizzontali (tra pubblico e privato) e assumono grande rilievo anche sul versante teorico generale. Del resto, se è vero che le istituzioni nazionali ed europee si occupano di definire soltanto la nozione di 'sicurezza cibernetica', è evidente che la codificazione di questa nuova 'dimensione' della sicurezza rappresenta uno dei principali stimoli – insieme alla disciplina dei *golden powers*[27] – della nuova fase di giuridicizzazione della *national security*.

Bibliografia

Barberis M. 2017, *Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, Bologna: Il Mulino.

Bobbio N. 1976, "Eguaglianza ed egualitarismo", *Rivista internazionale di filosofia*, Vol. 53 (n. 3): 321-330.

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

Carotti B. 2016, "Il sistema di Governo di Internet", Giuffrè: Milano.

Carotti B. 2020, "Sicurezza cibernetica e Stato-nazione", *Giornale diritto amministrativo*, (5): 629-641.

De Nitto S. 2022, "Il golden power nei settori rilevanti della difesa e della sicurezza nazionale: alla ricerca di un delicato equilibrio", *Diritto amministrativo*, (2): 553-587.

Fuster G.G., Jasmontaite GG. 2020, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights", in M. Christen, B. Gordijn and M. Loi (eds.), *The Etics of Cybersecurity*, Cham: Springer.

Giupponi T.F. 2008, *Le dimensioni costituzionali della sicurezza*, Bologna: Libreria Bonomo.

Giupponi T.F. 2024, "Il governo nazionale della cybersicurezza", *Quaderni costituzionali*, n. 2: 277-303.

Goldsmith J. and Wu T. 2006, *Tho controls the internet? Illusion of a Borderless World*, Oxford: Oxford University Press.

Longo E. 2024, "Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere", *Rassegna Parlamentare*, n. 2: 313-347.

Matassa M. 2023, "La regolazione della cybersecurity in Italia", in R. Ursi (ed.), *La sicurezza nel cyberspazio*, Milano: Franco Angeli: 21-42.

26 Cfr. Zalnieriute 2022: 198-218.

27 In estrema sintesi *golden powers* possono essere inquadrati come quei poteri speciali previsti dal d.l. 15 marzo 2012, n. 21 volti ad attribuire al Governo italiano il potere di dettare specifiche condizioni all'acquisto di partecipazioni, di porre veto all'adozione di determinate delibere societarie e di opporsi all'acquisto di partecipazioni (oggi disciplinati al livello europeo dal regolamento 2019/452). Per un approfondimento sull'esercizio dei poteri speciali nei settori della difesa e della sicurezza nazionale si rimanda a De Nitto 2022: 553-587 e Matassa 2024: 325-352.

Matassa M. 2024, "I golden powers italiani nel settore della difesa e sicurezza nazionale", *Il diritto dell'economia*, Vol. 113 (1): 325-352.
Mazzuccato M. 2018 [2014], *Lo Stato innovatore*, Roma-Bari: Laterza.
Monti A. 2020, "Internet e ordine pubblico", in G. Cassano, S. Previti (eds.), *Il diritto di internet nell'era digitale*, Milano: Giuffré Francis Lefebvre: 51-80.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *federalismi.it*, (25): 65-93.
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica.
Saltari L. 2007, *Amministrazioni nazionali in funzioni comunitarie*, Milano: Giuffrè.
Serini F. 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto legge n. 82 del 2021", *federalismi.it*, (12): 241-272.
Ursi R. 2022, *La sicurezza pubblica*, Bologna.
Ursi R. 2023, "La sicurezza cibernetica come funzione pubblica", in R. Ursi (ed.), *La sicurezza nel cyberspazio*, Milano: Franco Angeli: 7-20.
Zalnieriute M. 2022, "A struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union", *Modern Law Review*, Vol. 85 (n. 1): 198-218.