Massimiliano Malvicini

Appunti sull'evoluzione dell'architettura strategica nazionale in materia di sicurezza cibernetica e sugli spazi di intervento del Parlamento

Abstract: Lo scritto indaga l'evoluzione della governance nazionale della cybersecurity nel contesto giuridico italiano. Nel farlo, il lavoro si concentra sui poteri e le competenze attribuite al Presidente del Consiglio dei Ministri e alle autorità amministrative italiane negli ultimi decenni; successivamente, analizza il controllo parlamentare sui temi della cybersecurity negli anni recenti.

Keywords: Cybersecurity; Presidente del Consiglio dei Ministri; Parlamento; Agenzia per la Cybersicurezza Nazionale; Diritto pubblico italiano.

1. Premessa

La regolamentazione della sicurezza cibernetica è un fenomeno di grande interesse sotto diversi punti di vista[1]. Volendoci limitare all'ambito costituzionalistico, tramite di essa non solo si arricchisce l''intarsio' tra le diverse fonti recanti principi e regole in materia (tra livello nazionale e europeo)[2], ma – inevitabilmente – si altera anche la cornice entro cui si sviluppano i rapporti fra gli organi al vertice dell'ordinamento (la forma di governo) e le relazioni tra questi e i consociati (la forma di Stato, intesa quale declinazione delle interconnessioni tra la sfera dell'autorità e quella della libertà).

Data l'ampiezza del fenomeno in discussione, di seguito si approfondirà, mediante un approccio giuspubblicistico, l'evoluzione dei rapporti fra il nostro Go-

1 Per un inquadramento generale del concetto di cybersecurity ancora molto utile l'analisi di Schatz, Bashroush, Wall 2017. Sulla definizione di sicurezza in prospettiva costituzionalistica v. Giupponi, 2023 e 2022, Ursi, 2022; De Vergottini 2019; Pace, 2014. Sull'inquadramento della cybersecurity nell'ambito delle tradizionali funzioni statali v. Ursi 2023; Vigneri 2023; Scognamillo 2023. In generale, sul rapporto tra cybersecurity e ordinamento giuridico italiano cfr. Rossa 2023: 9-64; Lotta 2024, 173-184; Buoso 2023; Previti 2022; Gaggero, Berruti 2022; Lauro 2021; Renzi 2021; Contaldo, Mula 2020; Montessoro 2019.

2 Su cui, di recente, v. la ricostruzione di Moroni 2024. In generale v. Salvaggio, Gonzales 2023.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760149

verno e il Parlamento in materia di sicurezza cibernetica. In tal senso, il lavoro si soffermerà dapprima sulle coordinate normative che nel nostro ordinamento definiscono poteri, competenze e responsabilità in questa sfera, per poi mettere a fuoco la prassi che negli ultimi anni ha contraddistinto i rapporti fra assise legislativa e organi governativi.

2. Le coordinate istituzionali: l'assetto dei poteri e delle competenze in materia di sicurezza cibernetica

In termini generali, l'attuale quadro ordinamentale in materia di sicurezza cibernetica – ciò a cui ci si riferisce abitualmente come 'l'architettura strategica nazionale' – è il risultato di una stratificazione normativa realizzatasi nel corso di oltre un decennio.

Il primo intervento in materia risale alla legge 7 agosto 2012, n. 133, recante "Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto"[3], la quale intervenne in questo ambito conferendo nuove competenze al Presidente del Consiglio, al Comitato interministeriale per la sicurezza della Repubblica (CISR) e al Dipartimento delle informazioni per la sicurezza (DIS).

In quell'occasione si stabilì che il Presidente del Consiglio dei Ministri[4], sentito il CISR, avrebbe potuto impartire direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale (art. 1). D'altro canto, sulla base delle direttive del Presidente, e in virtù delle informazioni e dei rapporti provenienti dai servizi di intelligence, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati, il DIS avrebbe dovuto coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali (art. 3); infine, il Governo avrebbe avuto l'incarico di allegare alla relazione al Parlamento il "documento di sicurezza nazionale" che avrebbe dovuto contenere non solo un riferimento attività relative alla protezione delle infrastrutture critiche materiali e immateriali ma anche l'indicazione delle azioni volte alla "protezione cibernetica e alla sicurezza informatica" (art. 9).

Di là da questo primo intervento, la definizione delle vere e proprie coordinate istituzionali in materia risale al 24 gennaio 2013, data di approvazione del DPCM recante la direttiva sugli "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" (cd. "decreto Monti").

In termini di politica del diritto, anche allora si scelse di arricchire le competenze del sistema di intelligence, facendo aggio sul compito di salvaguardia del Paese

3 Su cui cfr. Scaccia 2012.

4 Sul ruolo del Presidente del Consiglio dei Ministri nell'ordinamento italiano cfr., da prospettive diverse, Cassese, Melloni, Pajno 2022; Teodoldi 2019; Ciolli 2018.

da pericoli e minacce provenienti sia dall'interno sia dall'esterno, riprendendo il fraseggio della legge 124 del 2007[5].

Così, il DPCM 24 gennaio 2013 individuò nella Presidenza del Consiglio dei Ministri il vertice dell'architettura nazionale in materia di sicurezza cibernetica. Al Presidente del Consiglio fu affidato il potere di adottare: a) il quadro strategico nazionale per la sicurezza dello spazio cibernetico, entro il quale andavano indicati profili e tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, ma anche la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati; b) su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, contenente obiettivi da conseguire e linee di azione da porre in essere per realizzare il quadro strategico nazionale, emana le direttive e gli atti d'indirizzo necessari per la sua attuazione; nella stessa prospettiva, al Presidente era conferito anche il potere di impartire, sentito il CISR, le direttive al DIS e alle Agenzie (*i.e.* l'Agenzia informazioni e sicurezza interna – l'AISI e l'Agenzia informazioni e sicurezza esterna – AISE) ai sensi dell'art. 1, comma 3-bis, della legge n. 124/2007.

Parallelamente, fu potenziato il ruolo del Comitato interministeriale per la sicurezza della Repubblica, affidando a esso alcuni poteri specifici: sorvegliare sull'applicazione del Piano nazionale per la sicurezza dello spazio cibernetico; esprimere pareri sulle direttive del Presidente del Consiglio; approvare specifiche linee d'indirizzo per favorire la collaborazione tra soggetti istituzionali e operatori privati interessati alla sicurezza cibernetica; elaborare indirizzi generali e obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali da perseguire nel quadro della politica dell'informazione per la sicurezza della Repubblica.

Ora, benché, nel disegno di questo DPCM venisse conferita al DIS, all'AISI e all'AISE la funzione di salvaguardare la protezione cibernetica e la sicurezza informatica nazionali tramite l'esercizio di "attività di ricerca e di elaborazione informativa", al cuore del sistema era collocato il Nucleo per la sicurezza cibernetica (NSC), istituito presso il Consigliere militare del Presidente del Consiglio. Presieduto dal Consigliere militare e composto, fra gli altri, dai rappresentanti del DIS, dell'AISE, dell'AISI, del Ministero degli Affari esteri, del Ministero dell'Interno, del Ministero della Difesa, del Ministero dello Sviluppo economico, al Nucleo erano affidate funzioni strumentali a supporto del Presidente del Consiglio in materia di prevenzione e preparazione a situazioni di crisi e per l'attivazione delle procedure di allertamento. Con ciò si costituì altresì il punto di riferimento nazionale per i rapporti con ONU, NATO, UE, altre organizzazioni internazionali e gli altri Stati. Così, al Nucleo fu attribuito il compito di raccordare le varie componenti coinvolte nella salvaguardia della sicurezza cibernetica, ma anche quello di programmare e pianificare le risposte a situazioni di crisi, nonché di promuovere la condivisione di informazioni tra le amministrazioni competenti e tra gli operatori

5 Su cui, cfr. Giupponi 2010; Mosca, Gambacurta, Scandone, Valentini 2008. In prospettiva più ampia si veda altresì Valentini 2017.

privati interessati. Ciò anche al fine della gestione delle crisi e della diffusione di allarmi su eventi cibernetici.

Nel corso degli anni successivi, l'architettura recata dal decreto Monti è stata oggetto di alcuni intenti riformatori. In un primo momento, attraverso l'emanazione del DPCM 1° agosto 2015 (cd. "direttiva Renzi"), venne evidenziata la necessità di consolidare un sistema di reazione efficiente, capace di raccordare le capacità di risposta delle singole Amministrazioni, al fine di assicurare la resilienza dell'infrastruttura informatica nazionale. Per raggiungere questo obiettivo venne indicato come necessario: a) favorire un maggior coordinamento e una più ampia integrazione delle funzioni dei diversi soggetti pubblici, tenendo conto che il quadro di competenze rimane ancora frammentato sotto il profilo legislativo; b) realizzare un maggior sviluppo delle relazioni con il settore privato, mediante un capillare partenariato con tutti gli operatori non pubblici a cui è affidato il controllo di infrastrutture informatiche e telematiche.

Proprio in ottica di coordinamento inter-istituzionale il DPCM evidenziava la necessità che esso si sarebbe dovuto realizzare, a livello centrale, nell'ambito dell'attività degli Organismi di informazione per la sicurezza, ribadendo il ruolo del DIS nell'assicurare la piena unitarietà nella programmazione della ricerca informativa e nel rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Successivamente, la razionalizzazione della governance in materia di cibersicurezza si è perfezionata mediante l'approvazione del Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017 (recante la "Direttiva in materia protezione cibernetica e sicurezza informatica nazionali", il cd. 'Decreto Gentiloni').

In quell'occasione, accanto all'esplicito riconoscimento dell'alta direzione e della responsabilità della politica generale del Governo anche nel campo della cybersecurity, al Presidente del Consiglio vennero attribuite specifiche competenze per far fronte agli scenari di crisi nazionale, sulla scia di quanto disposto dal decreto-legge 30 ottobre 2015, n. 174, in materia di servizi d'intelligence (convertito dalla legge 11 dicembre 2015, n. 198)[6]. Parallelamente, modificando l'impostazione del 'DPCM Monti' accogliendo le linee programmatiche espresse dalla 'direttiva Renzi', si sono potenziate le attribuzioni del DIS, affidando al suo direttore generale il compito di definire le necessarie linee di azione per innalzare i livelli di sicurezza dei sistemi e delle reti (verificandone ed eliminandone le vulnerabilità), ed incardinando al suo interno il Nucleo per la Sicurezza Cibernetica (presieduto da un vicedirettore generale del Dipartimento, su delega del direttore generale) con il compito di elaborare una risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei ministeri competenti in materia.

A un anno di distanza, in attuazione della direttiva (UE) 2016/1148 (c.d. direttiva NIS 1 – Network and Information Security) – il cui obiettivo era stabilire misure per uno standard comune elevato di sicurezza delle reti e dei sistemi informativi

6 Sul punto, volendo, Malvicini 2016.

nell'Unione al fine di aumentare il livello di collaborazione nella prevenzione alle minacce cibernetiche[7] – è intervenuto il decreto legislativo 18 maggio 2018, n. 65 che, fra l'altro, ha attribuito al Presidente del Consiglio la competenza alla definizione della strategia nazionale di sicurezza cibernetica per la tutela delle reti e dei sistemi di interesse nazionale (sentito il CISR).

Un ampliamento delle attribuzioni governative si è inoltre registrato a distanza di qualche mese, a seguito dell'approvazione del decreto-legge 21 settembre 2019, n. 105 (il c.d. 'decreto perimetro')[8]. In particolare, tramite questo atto si è attribuito al Presidente del Consiglio uno specifico potere di ordinanza in materia di cibersicurezza[9]. Nello specifico, in presenza di un "rischio grave e imminente" per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente può disporre, ove indispensabile e per il tempo strettamente necessario all'eliminazione "dello specifico fattore di rischio o alla sua mitigazione", in deroga a ogni disposizione vigente, ma nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, la disattivazione, anche totale, "di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati" (art. 5, c. 1). Entro trenta giorni dall'esercizio di questo potere, il Presidente del Consiglio deve informare il COPASIR delle misure disposte.

Più di recente, anche in attuazione del PNRR[10], l'"architettura italiana" di sicurezza cibernetica è stata oggetto di ulteriori interventi.

In particolare, tramite il d.l. 14 giugno 2021, n. 82 (convertito con modificazioni dalla l. 4 agosto 2021, n. 109)[11] si sono trasposte, coordinandole e razionalizzandole, le innovazioni susseguitesi nel corso dell'ultimo decennio. Nel perfezionare tale passaggio il legislatore ha confermato l'attribuzione al Presidente del Consiglio dei Ministri dell'alta direzione e della responsabilità generale delle politiche di cibersicurezza (art. 2, c. 1), quest'ultima intesa come 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). Così, al Presidente spettano l'adozione della strategia nazionale di cibersicurezza e il potere di impartire le direttive per attuarla; nel contempo, egli emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia (art. 2, c. 2). Nell'esercizio delle sue attribuzioni, egli è ora affiancato dal Comitato Interministeriale per la Cybersicurezza (CIC), che presiede, al quale è conferito il compito di proporre gli indirizzi generali da perseguire nel quadro delle politi-

7 Sulle iniziative europee e il loro intreccio con l'ordinamento italiano cfr. Moroni 2024: 185 ss; Matassa 2023; Contaldo, Salandri 2020; Peluso 2020; Salamo 2017.

8 Su cui v. Calandriello 2023.

9 Sul potere di ordinanza v. ex multis Cavino, 2021.

10 Sul Piano Nazionale di Ripresa e Resilienza italiano cfr., da prospettive diverse, e in termini generali: Bartolucci 2024; De Lungo, Marini 2023; Casalone, Sciortino, Massa Pinto 2023.

11 Su cui cfr. Serini 2022.

che di cibersicurezza nazionale, e di realizzare "l'alta sorveglianza" sull'attuazione della strategia nazionale (art. 5, c. 2). Il CIC è composto dall'Autorità delegata (se istituita), dal ministro degli Affari esteri e della Cooperazione internazionale, dal ministro dell'Interno, dal ministro della Giustizia, dal ministro della Difesa, dal ministro dell'Economia e delle Finanze, dal ministro dello Sviluppo economico, dal ministro della Transizione ecologica, dal ministro dell'Università e della Ricerca, dal ministro delegato per l'Innovazione tecnologica e la Transizione digitale e dal ministro delle Infrastrutture e della Mobilità sostenibili (art. 4, c. 3).

Parallelamente, il legislatore ha istituito un apposito ente con specifiche competenze nell'ambito in esame: l'Agenzia per la cybersicurezza nazionale (ACN)[12]. In particolare, l'ACN, il cui direttore generale è nominato dal Presidente del Consiglio, assicura il coordinamento fra i soggetti pubblici coinvolti in materia di cibersicurezza, promuovendo una maggiore tutela e resilienza rispetto alle minacce cibernetiche, spettando a essa ogni competenza in fatto di già attribuita dalle disposizioni vigenti alle strutture preesistenti (i.e. Ministero dello sviluppo economico, Presidenza del Consiglio dei Ministri; DIS, Agenzia per l'Italia Digitale). In tal senso, l'Agenzia ha il compito di predisporre la strategia nazionale di cybersicurezza, oltre che di determinare i livelli minimi di capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione e di definizione dei parametri di qualità, performance, scalabilità, interoperabilità e portabilità dei servizi cloud per la p. A.

Inoltre, all'ACN spettano altri due compiti cruciali: a) sviluppare le capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire attacchi informatici e incidenti di sicurezza informatica, anche promuovendo iniziative di partenariato pubblico-privato, ma coordinando altresì la cooperazione internazionale in tale materia; b) promuovere la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cibersicurezza, tenendo anche conto di orientamenti e sviluppi in ambito internazionale (a tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari in questa materia).

Coerentemente con tale impostazione, è istituito presso l'Agenzia il Nucleo per la Cybersicurezza (NCS), a supporto del Presidente del Consiglio dei ministri in questo ambito (la cui composizione riprende, pur con qualche variazione, quella dell'originario Nucleo per la Sicurezza Cibernetica istituito nel 2013 e, dal 2017, transitato sotto l'egida del DIS).

Nel complesso, dinanzi agli interventi susseguitisi nel corso di un decennio, è possibile affermare che il legislatore ha optato per la definizione di una *governance* nazionale della cibersicurezza contraddistinta dall'attribuzione di ampi compiti di direzione e coordinamento alle amministrazioni nazionali e, rispetto ad esse, soprattutto alle strutture serventi la Presidenza del Consiglio dei Ministri (con ciò, contribuendo ad un rafforzamento delle attribuzioni di

12 Su cui cfr. Forgione 2023; Cusenza 2023; Parona 2021. Sulla specificità dell'ACN cfr. Rossa 2023: 91 ss., spec. 94-95.

programmazione e alta amministrazione del Governo, attribuendo, al più, alle Camere uno spazio di controllo).

A questo esito ha contribuito senz'altro la natura delle problematiche concernenti la cibersicurezza, anche considerando la sua attitudine ad intrecciarsi profondamente (e immediatamente) anzitutto con la sicurezza nazionale[13], la quale ha influito anche sulla scelta di valorizzare, entro l'ambito governativo, la Presidenza del Consiglio dei ministri (in questa sede ritenuta come legittima). Infatti, come afferma Giupponi:

> alla luce della sua natura strategica e trasversale, non stupisce che la responsabilità politica venga affidata alla Presidenza del Consiglio dei ministri, nell'ambito della sua tradizionale funzione di direzione della politica generale del Governo, *ex* art. 95 Cost. Tuttavia, si tratta di un ambito che richiede elevate competenze di natura tecnica, capacità di coordinamento e rapidità di intervento, anche alla luce dell'aumento esponenziale del rischio delle minacce in ambiente cyber cui si è assistito negli ultimi anni, anche attraverso l'utilizzo di veri e propri strumenti di natura ibrida.[14]

Del pari, proprio in virtù del dato normativo, la Presidenza del Consiglio sembra giocare un ruolo mutevole[15], in alcuni casi inserendosi in schemi procedimentali contraddistinti da una collegialità delle scelte di Governo, altri in cui a risultare predominante è l'assunzione di responsabilità del solo Presidente del Consiglio. Ciò vale non solo nell'assunzione delle scelte di carattere organizzativo o strategico in materia di cibersicurezza, ma anche nell'esercizio dei poteri di normativi e/o amministrativi in casi di emergenza. Al fianco della decretazione d'urgenza (la quale, come noto, presuppone un coinvolgimento del Consiglio e implica il necessario coinvolgimento del Parlamento nella fase di conversione), si sommano gli strumenti previsti più di recente, i quali – pur non occultando del tutto il principio collegiale – fanno aggio sulla capacità decisionale del Premier (ciò vale, in parti-

13 A onor del vero, ci si potrebbe chiedere se questa sfera, radicata nell'area ricompresa, quantomeno, tra l'art. 117, c. 2, lettere 'd' Cost. (difesa e sicurezza dello Stato) e lettera 'h' (ordine pubblico e sicurezza), non rappresenti un esempio, paradigmatico, di materia 'trasversale', in quanto suscettibile di riguardare altre materie e interessi pubblici di spettanza dello Stato (*e.g.* si pensi ai politica estera e rapporti internazionali; all'organizzazione amministrativa dello Stato e degli enti pubblici nazionali; alla cittadinanza e le anagrafi) e delle Regioni (per limitarci agli ambiti di competenza concorrente, si pensi alla ricerca scientifica e tecnologica; alla tutela della salute; al governo del territorio; alla gestione di porti e aeroporti civili e delle grandi reti di trasporto e di navigazione, ma anche alla produzione, trasporto e distribuzione nazionale dell'energia) e – alla luce di ciò – quali conseguenze ciò comporti rispetto agli spazi di intervento delle altre amministrazioni e soggetti di cui si compone la Repubblica. Un profilo, questo di indubbio interesse, anche considerando i profili di coordinamento inter-istituzionale ad esso connesso (*in primis*, quello dell'eventuale coinvolgimento degli enti regionali e degli altri enti territoriali considerati non solo quali terminali delle scelte compiute dallo Stato in materia di ordine pubblico e sicurezza, ma anche come portatori di interessi che, ancorché non direttamente afferenti alla materia *de qua,* Cost., siano teleologicamente connessi alla competenza esclusiva dello Stato, senza però dimenticare l'importanza degli operatori privati e le istituzioni sovranazionali).

14 Giupponi 2024: 295.

15 Giupponi 2024.

colar modo, per il potere *ex* art. 5 del d.l. 105/2019, la cui competenza spetta al Presidente del Consiglio, previa deliberazione del Comitato interministeriale per la Sicurezza della Repubblica)[16].

3. (segue) I principali interventi del Parlamento

Ora, premesso che l'attuale assetto della *governance* della cybersecurity si caratterizza per una concentrazione di competenze di indirizzo e programmazione in capo al Presidente del Consiglio e all'ACN, è interessante provare a determinare quali sono le principali coordinate entro cui si può sviluppare l'azione del Parlamento.

Ora, posto che il dato normativo sancisce un assetto di competenze per il quale l'indirizzo sulla materia *de quo* è attribuito al Governo e, nello specifico, al Presidente del Consiglio dei ministri (ad esso spetta l'adozione della strategia nazionale di cibersicurezza e il potere di impartire le direttive per attuarla, art. 2, d.l. 82/2021), lo spazio che, attualmente, sembra residuare alle Camere è quello del controllo politico[17]. Per chiarire meglio questo profilo può essere

16 Un profilo di particolare interesse – al quale in questa sede si può solo accennare – riguarda l'opportunità della previsione di uno specifico potere di ordinanza in materia di cibersicurezza a (parziale) integrazione della generale potestà legislativa nella forma della decretazione d'urgenza. Ora, posto che dinanzi ad un "rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi facenti parte del perimetro di sicurezza nazionale" la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati da parte del Presidente del Consiglio sembra iscriversi all'esercizio di un potere riconducibile più alla cura concreta e attuale degli interessi pubblici (il provvedere) che non alla predisposizione di una disciplina generale (il predisporre), il riconoscimento del potere di ordinanza finalizzato a questo scopo non sembra risultare inopportuno (anche considerando come esso rispetti il principio di legalità sostanziale, data la determinazione del contenuto e delle modalità di esercizio – su questi profili v., *ex multis*, Corte cost. sent. 115/2011).

Ciò posto, anche alla luce di quanto appena affermato, va comunque detto che la risposta (in termini giuridico-costituzionali) all'interrogativo di apertura dipende, da un lato, dal tipo di bene/interesse che si vuole proteggere e, dall'altro, dalla minaccia che incombe (del resto, lo stesso potere di ordinanza incontra dei limiti rispetto alle materie coperte da riserva di legge: nei casi di riserva assoluta esso non è ammesso – lasciando così spazio alla sola decretazione d'urgenza –, mentre nel caso della riserva relativa di legge l'attribuzione del potere di ordinanza è ammissibile purché delimitato nel suo esercizio così da orientare, anche in modo non dettagliato, l'adozione dei provvedimenti urgenti; sul punto v. Corte cost. sent. n. 115 del 2011).

17 Dal punto di vista generale, la valorizzazione dei poteri di indirizzo del Governo nei confronti del Parlamento si colloca in linea di continuità rispetto a quanto avvenuto con riguardo ai servizi di intelligence (ma in linea di discontinuità rispetto ad altri ambiti, come evidenziato in Malvicini 2022, 221-261). A questo esito contribuisce, molto probabilmente, non solo la tecnicità della materia e la capacità del solo Governo a tutelare adeguatamente, nei tempi e nei modi, gli interessi preminenti dell'ordinamento, ma anche la cultura organizzativa (e costituzionale) delle varie componenti dell'assise parlamentare, a partire da quelle maggioritarie, dalla quale potrebbe scaturire una preferenza, in termini di politica del diritto, verso opzioni normative volte a istituzionalizzare un assetto di poteri/competenze

utile individuare quali sono le principali figure tramite cui l'assise rappresentativa può esercitare questa attività, intesa quale "riesame compiut[o] da un soggetto od organo (le Camere) nei confronti di un altro soggetto od organo (il Governo) al fine di verificare e garantire la corrispondenza del comportamento del soggetto od organo controllato ai canoni normativi che tale comportamento disciplinano"[18].

Nel fare ciò, occorre considerare almeno due variabili: da un lato, la presenza, in capo agli organi di indirizzo, di un obbligo di ostensione della loro attività alle Camere (o loro organi, anche ausiliari), valutando come tale eventuale onere possa articolarsi nelle sue varie dimensioni. Considerando questa variabile, possiamo analizzare l'ampia ed eterogenea fenomenologia delle figure di verificazione identificando quelle a maggiore istituzionalizzazione, ossia le ipotesi in cui il Governo è tenuto a sottoporre, spesso periodicamente, la propria attività alle Camere, *ex lege* o perché il Parlamento si è dotato di un organo che può far valere una specifica competenza al riguardo, ma anche le fattispecie in cui è il Governo che si induce sua sponte a 'ostendere' la propria attività, su richiesta meramente eventuale del Parlamento.

La seconda variabile è la presenza, in capo alla Camera e/o al Senato, di un onere (reciproco al primo), circa la necessità (o meno) di procedere effettivamente al riesame dell'attività governativa, vuoi per obblighi disposti dall'ordinamento o per accordo interistituzionale.

L'applicazione di questo schema all'ambito della sicurezza cibernetica ci fornisce qualche indicazione di grande interesse.

Anzitutto, l'attuale quadro normativo fornisce una notevole variabilità di strumenti di controllo a disposizione delle Camere, alcuni dei quali prevedono un riesame periodico, ancorché eventuale, dell'attività del Governo, mentre altri sono improntati a una maggiore istituzionalizzazione.

In secondo luogo, anche in virtù dell'impostazione originaria data dal legislatore nel 2013, il controllo del Parlamento sul Governo in questo ambito specifico è rafforzato dalla presenza del Comitato Parlamentare per la Sicurezza della Repub-

volutamente sbilanciato a favore del governo per quanto riguarda la promozione dell'indirizzo politico. Sul ruolo del Governo e il suo rafforzamento nei confronti del Parlamento si vedano i contributi in Musella 2019.

18 Cfr. Chimenti 1974. Come evidenziato in altra sede (Malvicini, 2022, a cui si rinvia per la letteratura sul tema), nella sua accezione ristretta di attività di riscontro-verificazione, il controllo parlamentare si qualifica per tratti tipici: il carattere relazionale, che si presenta anzitutto come alterità tra il soggetto controllante e quello controllato; il suo profilo logicamente accessorio e strumentale; il parametro sulla base del quale avviene l'attività di riesame, costituito, salvo eccezioni, anzitutto, dal programma di governo ma anche da tutti gli atti e documenti idonei ad integrare quest'ultimo; la natura politica del giudizio in cui si concretizza l'attività di verificazione del Parlamento sul Governo; le figure tipiche in cui si articola. Questo *modus operandi* – che si richiama all'impostazione di matrice amministrativista le cui origini risalgono quantomeno alla riflessione di U. Forti degli inizi del Novecento (1915), poi ripresa da autorevolissima dottrina, a partire da M.S. Giannini (1974) – porta a distinguere l'attività di controllo dal mero esercizio di 'influenza' o 'ingerenza' politica delle Camere nei confronti del Governo. Sui controlli si cfr., di recente, D'Alterio 2019: 681 ss.

blica (COPASIR)[19]. A quest'ultimo si riferiscono le principali figure di verifica sui profili organizzativi e funzionali di poteri e strutture competenti in materia[20].

In particolare, l'art. 2, c. 3, del d.l. 82/2021 prevede che il Presidente del Consiglio debba informare periodicamente il Comitato parlamentare, oltre che le commissioni permanenti competenti, sulle nomine del direttore generale e del vicedirettore generale dell'ACN. In aggiunta, ai sensi dell'art. 5, c. 6, del d.l. 82/2021, lo stesso COPASIR può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza (ex art. 31, c. 3, l. 124/2007).

Inoltre, il Comitato parlamentare esprime un parere, fra l'altro, sul regolamento circa l'ordinamento e il reclutamento del personale dell'Agenzia (art. 12, c. 8) e sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi finalizzate alla tutela della cibersicurezza, art. 11, c. 4).

In aggiunta, l'art. 14, comma 1 del d.l. 82/2021 stabilisce che, entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri debba trasmettere al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente in materia di cibersicurezza nazionale; a tale relazione se ne aggiunge un'altra, che va presentata dal Presidente del Consiglio entro il 30 giugno al COPASIR e che verte sulle attività svolte l'anno precedente dall'Agenzia rispetto alle attività di tutela della sicurezza nazionale nello spazio cibernetico.

Accanto a questi istituti si colloca l'onere che grava sul Presidente del Consiglio di informare il Comitato sull'avvenuta disattivazione, anche totale, "di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati", in caso di rischio grave e imminente» per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici (ai sensi di quanto previsto dall'art. 5, c. 1 del d.l. n. 105/2019).

Chiarite le principali figure di controllo delle Camere nei confronti del Governo in materia di cibersicurezza, è di particolare interesse completare l'analisi considerando anche la prassi attuativa (passando in sostanza dal piano delle regole a quello delle regolarità). In tale direzione, nonostante la particolare riservatezza dei lavori parlamentari, emergono numerosi elementi di grande interesse. Nello specifico, emerge che, analogamente ad altri ambiti riconducibili alla sua sfera di attribuzione, il Comitato è stato non solo un organo *reattivo* ma anche *proattivo* nell'esercizio delle sue attribuzioni[21].

19 Sul ruolo e l'attività del Comitato parlamentare per la sicurezza della Repubblica cfr. Perini 2023; Giuffrè 2021; Perrone 2018; Franchini 2014: Nardone 2008; Campanelli, 2008.

Per un'analisi di tipo comparato cfr. Schirripa, 2023; Piciacchia, 2018 e 2017.

Anche in virtù delle competenze ex art. l. 124/2007 il COPASIR viene identificato come un organo attraverso il quale il Parlamento esercita, accanto alla funzione di controllo, quella di garanzia costituzionale. Sulla funzione di garanzia costituzionale nel nostro ordinamento si vedano, quantomeno, Tarchi, 2021; Silvestri, 2009; Galeotti, 1950; 1969. Sull'attività di salvaguardia costituzionale svolta dalle Camere v. Gianniti, Lupo 2023[4]: 194-196; Manzella, 2003[3] e, soprattutto, 1970.

20 Sul punto v. Caramaschi 2022.

21 Sul punto si vedano gli acuti rilievi di Perrone 2018 secondo cui: "il Comitato, nell'effettivo dipanarsi della sua attività, si è rivelato organo di cerniera e cinghia di trasmissione affin-

In tal senso non si può non richiamare come, sin dalla XVI legislatura, il COPASIR sia stato promotore di iniziative di studio e approfondimento sulla sicurezza cibernetica, sotto molteplici punti di vista. Esito di questa attività è stata anzitutto la "Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico" presentata alle Camere il 7 luglio 2010 (Doc. XXXIV, n. 4). In essa si possono trovare riferimenti all'esigenza di pianificare in modo coordinato la difesa dei sistemi strategici nazionali connessi alla rete informatica, oltre che la raccomandazione al Governo di predisporre soluzioni organizzative presso la Presidenza del Consiglio, capaci di assicurare "leadership adeguata", anche tramite l'elaborazione di adeguate "politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati".

A tale documento ha fatto seguito, nella XVII legislatura, la "Relazione sulle procedure e la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni" (Doc. XXXIV, n. 7), dove si trovano numerosi riferimenti all'esigenza di perfezionare alcuni aspetti della governance predisposta dai primi DPCM. Nella XVIII legislatura, anche in reazione ad alcuni attacchi informatici subiti dal nostro Paese, il Comitato ha approfondito alcuni aspetti trattati incidentalmente nel corso degli anni precedenti. Anche grazie a un ciclo di audizioni articolato, che ha coinvolto sia il direttore del DIS sia una pluralità di rappresentanti e autorità militari e civili, ivi incluse aziende strategiche nazionali, il Comitato ha così potuto concentrarsi su alcuni profili specifici circa la sicurezza cibernetica nel Paese (*e.g.* il livello di sicurezza informatica garantito ai cittadini, alle istituzioni, alle infrastrutture critiche e alle imprese di interesse strategico nazionale; il grado di implementazione degli interventi attuativi delle linee di indirizzo strategiche e operative fissate nei documenti di indirizzo approvati). Con ciò il Comitato ha perfezionato specifiche valutazioni e proposte attuative, contenute nella "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale" presentata al Parlamento il 12 dicembre 2019 (Doc. XXXIV, n. 1).

Più di recente, nell'ambito della Relazione sull'attività svolta nella prima parte della XIX legislatura, presentata alle Camere il 17 aprile 2024 (Doc. XXXIV, n. 1), il Comitato si è occupato di sicurezza cibernetica nell'ambito di varie audizioni, riservando specifica attenzione alla trasformazione delle minacce informatiche di conseguenza, ai meccanismi di tutela necessari per salvaguardare il processo di digitalizzazione della pubblica amministrazione, alla luce della Strategia nazionale di cybersicurezza 2022-2026 e dell'annesso Piano di implementazione.

L'intraprendenza del COPASIR, che conferma l'immagine di un Parlamento che esercita un controllo a 'geometria variabile' (di notevole istituzionalizzazio-

ché potesse realizzarsi – nel metodo e nel merito – la mediazione tra le diverse esigenze richiamate; in tale ottica, il Copasir si è presentato come una sede di dialogo e camera di compensazione e di verifica tra il Parlamento legislatore e le richieste dei diversi attori chiamati ad intervenire sul piano della lotta al terrorismo internazionale".

ne nell'ambito della sicurezza nazionale, di minor proiezione su altri campi)[22], è stata massima nella fase crepuscolare della XVIII legislatura. Da un lato, il Comitato ha interloquito con il Governo al fine di modificare l'allora bozza del decreto-legge 14 giugno 2021, n. 82, prevedendo specifici spazi di controllo a disposizione delle Camere rispetto all'azione dell'ACN inizialmente non facenti parte dell'assetto di governance del sistema. Dall'altro, tra il 2021 e il 2022, il Comitato ha provveduto con sollecitudine all'esame e all'espressione del parere sugli schemi previsti per il funzionamento dell'ACN (*i.e*. il regolamento di organizzazione e funzionamento dell'Agenzia, il regolamento del personale, il regolamento di contabilità e quello recante le procedure per la stipula di contratti di appalti di lavoro, servizi e forniture).

Bibliografia

Bartolucci, L. 2024, *Piano nazionale di ripresa e resilienza e forma di governo tra Italia e Unione Europea*, Torino: Giappichelli.

Bassu, C., Pistorio, G. e Sterpa A. (a cura di) 2023, *Diritto pubblico della sicurezza*, Napoli: Editoriale Scientifica: 89-108.

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

Calandriello, L. 2023, "Il perimetro di sicurezza nazionale cibernetica"*,* in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 139-151.

Campanelli, G., 2008, "Il Comitato parlamentare per la sicurezza della Repubblica nella legge 3 agosto 2007 n. 124", in *Quaderni costituzionali*, 2: 372-375.

Caramaschi, O., 2022, "La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari", in *Osservatorio costituzionale AIC*, 4: 69-83.

Cariola, A., Castorina, E. e Ciancio, A. (a cura di) 2010, *Studi in onore di Luigi Arcidiacono*, vol. IV, Torino: Giappichelli.

Casalone, G., Sciortino, A. e Massa Pinto, I. 2023, *Il Piano Nazionale di Ripresa e Resilienza*, Napoli: Editoriale Scientifica.

Cassese, S., Melloni, A. e Pajno A. (a cura di) 2022, *I Presidenti e la Presidenza del Consiglio dei ministri nell'Italia repubblicana: storia, politica, istituzioni*, Bari-Roma: Laterza.

Cavino, M. 2021, *Ordinamento giuridico e sistema delle fonti*, Napoli: Editoriale Scientifica, 361-388.

Chimenti, C. 1974, *Il controllo parlamentare nell'ordinamento italiano*, Milano: Giuffrè.

Ciolli, I. 2018, *La questione del vertice di Palazzo Chigi. Il Presidente del Consiglio nella Costituzione repubblicana,* Napoli: Jovene.

Contaldo, A. e Mula, D. (a cura di) 2020, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche,* Pisa: Pacini Giuridica.

Contaldo, A. e Salandri, L. 2020, "La disciplina della cybersecurity nell'Unione Europea", in A. Contaldo e D. Mula (a cura di) 2020, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: 1-55.

22 Malvicini 2022, 221-261.

Costanzo, p. Magarò, M. e Trucco, L. (a cura di) 2022, *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Atti del Convegno annuale dell'Associazione "Gruppo di Pisa", Genova 18-19 giugno 2021, Napoli: Editoriale Scientifica.
Cusenza, G.G., 2023, "I poteri dell'agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 123-151.
D'Alterio, E. 2019, "La funzione di controllo e l'equilibrio tra i poteri pubblici: 'dove nascono i problemi'", in *Rivista trimestrale di diritto pubblico*, 3: 681 ss.
De Lungo, D. e Marini, F.S. (a cura di) 2023, *Scritti costituzionali sul piano nazionale di ripresa e resilienza*, Torino: Giappichelli.
De Vergottini G. 2019, "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata", in *Rivista AIC*, 4: 65-84.
Dickmann R. e Staiano, S. (a cura di) 2008, *Funzioni parlamentari non legislative e forma di governo. L'esperienza dell'Italia*, Milano: Giuffrè.
Forgione, I. 2023, "Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 95-121.
Forti, U. 1915, "I controlli nell'amministrazione comunale", in *Trattato di diritto amministrativo* diretto da V.E. Orlando, vol. II, parte II, Milano: Giuffrè.
Franchini, M. 2014, "Alcune considerazioni sulle nuove competenze del Comitato Parlamentare per la Sicurezza della Repubblica", in *Rivista AIC*, 1.
Gaggero, F. e Berruti, M. 2022, "I pilastri normativi della sicurezza cibernetica", in p. Costanzo, M. Magarò e L. Trucco (a cura di) 2022, *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Atti del Convegno annuale dell'Associazione "Gruppo di Pisa", Genova 18-19 giugno 2021, Napoli: Editoriale Scientifica.
Galeotti, S., 1950, *La garanzia costituzionale (presupposti e concetto),* Milano: Giuffrè.
Galeotti, S., 1969, "Garanzia costituzionale", *Enciclopedia del diritto*, vol. XVIII, Milano: Giuffrè, 491-511.
Giannini, M.S. 1974, "Controllo: nozione e problemi", in *Rivista trimestrale di diritto pubblico*, 4: 1263-1283.
Gianniti, L. e Lupo, N. 2023, *Corso di diritto parlamentare*, Bologna: il Mulino.
Giuffrè, F., 2021, "I 'Servizi di informazione e sicurezza' della Repubblica nella dialettica tra Governo e Parlamento", in *Percorsi costituzionali*, 3: 757-776.
Giupponi T.F. 2022, "I rapporti tra sicurezza e difesa. Differenze e profili di convergenza", in *Diritto costituzionale. Rivista quadrimestrale*, 1: 21-48.
Giupponi T.F. 2023, "Sicurezza e potere", in *Enciclopedia del diritto. I tematici, Vol. V, Potere e Costituzione*, Milano: Giuffrè: 1165 ss.
Giupponi T.F. 2024, "Il governo nazionale della cybersicurezza", in *Quaderni costituzionali*, 2: 277-303.
Giupponi, T.F. 2010, "Servizi di informazione e segreto di Stato nella legge n. 124/2007", in A. Cariola, E. Castorina e A. Ciancio (a cura di) 2010, *Studi in onore di Luigi Arcidiacono*, vol. IV, Torino: Giappichelli: 1677-1751.
Lauro, A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *La Rivista del Gruppo di Pisa,* fasc. spec. 3: 529-545.
Lotta, C. 2024, *Governance della rete, accesso a internet e cybersicurezza. Profili costituzionali* Napoli, Editoriale Scientifica.
Malvicini, M. 2016, "Sicurezza della Repubblica e forma di governo parlamentare. Il Rapporto tra presidente del Consiglio dei ministri e Copasir alla luce dei più recenti inter-

venti legislativi (legge 11 dicembre 2015, n. 198)", in *Forum Quaderni Costituzionali*, 11 maggio 2016.
Malvicini, M. 2022, *La funzione di controllo del Parlamento nell'ordinamento costituzionale italiano*, Torino: Giappichelli.
Manzella, A. 1970, *I controlli parlamentari*, Milano: Giuffrè.
Manzella, A. 2003, *Il Parlamento*, Bologna: il Mulino.
Manzella, A. 2017, "Il Parlamento come organo costituzionale di controllo", in *Nomos. Le attualità del diritto*, 1.
Matassa, M. 2023, "La regolazione della cybersecurity in Italia", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 21-42.
Montessoro, p. L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Le Istituzioni del Federalismo*, 3.
Moroni, L. 2024, "La governance della cybersicurezza a livello interno ed europeo: un quadro intricato", in *Federalismi.it*, 14: 179-197.
Mosca, C., Gambacurta, S., Scandone, G., e Valentini, M. 2008, *I servizi di informazione e il segreto di stato (Legge 3 agosto 2007, n. 124)*, Milano: Giuffrè.
Musella, F. (a cura di) 2019, *Il governo in Italia. Profili costituzionali e dinamiche politiche*, Bologna: il Mulino.
Nardone, C. 2008, "Il controllo parlamentare sui servizi di informazione", in R. Dickmann e S, Staiano (a cura di) 2008, *Funzioni parlamentari non legislative e forma di governo. L'esperienza dell'Italia*, Milano: Giuffrè: 375-415.
Pace, A. 2014, "La funzione di sicurezza nella legalità costituzionale", *Quaderni costituzionali*, 4: 989-1000.
Peluso, F. 2020, *La disciplina italiana in tema di cybersecurity*, in A. Contaldo e D. Mula (a cura di) 2020, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: 119-144.
Parona, L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale di diritto amministrativo*, 6.
Perini, M. 2023, "Evoluzione della forma di governo alla luce della disciplina e della prassi del COPASIR", in *Rassegna parlamentare*, 1: 19-41.
Perrone, A., 2018, "Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica", in *Federalismi.it,* 11: 1-28.
Piciacchia, p. 2017, *Parlamenti e costituzionalismo contemporaneo. Percorsi e sfide della funzione di controllo*, Napoli: Jovene.
Piciacchia, p. 2018, "La dimensione del controllo parlamentare su segreto di Stato e intelligence alla prova delle crescenti esigenze di sicurezza degli Stati tra problemi aperti e prospettive: le esperienze di Italia, Francia e Belgio", in *Democrazia e sicurezza – Democracy and Security Review*, 1: 37-107.
Previti, L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it,* 25.
Renzi, A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giornale di diritto amministrativo,* 4.
Rossa, S. 2023, *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, Napoli.
Salamo, L.V.M. 2017, "La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione", in *Federalismi.it*, 23.
Salvaggio, S.A. e Gonzales, N. 2023, "The European framework for cybersecurity: strong assets, intricate history", in *International Cybersecurity Law Review*, 4.
Scaccia, G. 2012, "Intelligence e segreto di Stato nella legge n. 133 del 2012", in *Diritto e società*, 3.

Schatz D. Bashroush R. e Wall J. 2017, "Towards a More Representative Definition of Cyber Security", in *Journal of Digital Forensics, Security and Law*, 2: 53-74.
Schirripa, M. 2023, *Il controllo parlamentare sulle attività del Sistema di informazione per la sicurezza nazionale: il ruolo del Copasir ed uno sguardo comparato*, in C. Bassu, G. Pistorio, A. Sterpa (a cura di) 2023, *Diritto pubblico della sicurezza*, Napoli: Editoriale Scientifica: 89-108.
Scognamillo, L. 2023, "Cybersicurezza e sicurezza nazionale", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 71-84.
Serini, F., 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", in *Federalismi.it*, 12: 241-272.
Silvestri, G., 2009, *Le garanzie della Repubblica,* Torino: Giappichelli.
Tarchi, R., 2021, *Democrazia e istituzioni di garanzia*, Napoli: Editoriale Scientifica.
Teodoldi L. (a cura di) 2019, *Il presidente del Consiglio dei ministri dallo Stato liberale all'Unione Europea*, Milano: Biblion Edizioni.
Ursi R. 2022, "La difesa: tradizione e innovazione", in *Diritto costituzionale. Rivista quadrimestrale*, 1: 5-20.
Ursi, R. (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli.
Ursi, R. 2023, "La sicurezza cibernetica come funzione pubblica", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 7-20.
Valentini, M. 2017, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionali*, Napoli: Editoriale Scientifica.
Vigneri, A.F. 2023, "I profili giuridici della sicurezza nazionale. Tra collocazione sistematica e problemi definitori: un'introduzione critica", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 43-69.