AIC
Associazione Italiana dei Costituzionalisti
Osservatorio costituzionale

OSSERVATORIO COSTITUZIONALE
Codice ISSN: 2283-7515
Fasc. 4/2022
Data: 2 agosto 2022

La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari[*]

di **Omar Caramaschi** – *Dottore di ricerca in Diritto (curriculum: Diritto costituzionale interno, comparato ed europeo) nell'Università degli Studi di Genova*

TITLE: National cybersecurity at the time of the cyber war: the role of parliamentary bodies

ABSTRACT: Il contributo affronta il tema della sicurezza nazionale dalla peculiare prospettiva della sicurezza informatica o "cybersicurezza", specialmente nel contesto dei recenti eventi bellici (in particolare nello spazio cibernetico) e della nuova "architettura" istituzionale e normativa del sistema italiano di cybersicurezza. Alla luce di tale quadro di riferimento ci si sofferma sul ruolo di controllo in materia svolto dagli organi parlamentari.

The paper deals with the issue of national security from the point of view of cybersecurity, particularly in the context of recent war events (especially in cyberspace) and within the framework of the new institutional and normative "architecture" of Italian national cybersecurity, with special regard to the role of parliamentary bodies.

KEYWORDS: Cybersicurezza; architettura normativa; guerra cibernetica; organi parlamentari; funzione di controllo parlamentare; cybersecurity; regulatory architecture; cyber war; parliamentary bodies; parliamentary control function.

[*] Lavoro sottoposto a referaggio secondo le linee guida della Rivista.

SOMMARIO: 1. Premessa. – 2. L'architettura normativa della cybersicurezza in Italia. – 3. Il ruolo del Parlamento e del COPASIR. – 4. Cenni conclusivi: la cybersicurezza nazionale di fronte alle attuali sfide "belliche".

1. Premessa

I recenti attacchi informatici che hanno riguardato il nostro Paese – da ultimo quello del 31 maggio scorso ad opera di hacker russi nei confronti, tra gli altri, dell'Agenzia per la cybersicurezza nazionale – nel contesto del conflitto in territorio ucraino[1] e, più in generale, di crescenti fenomeni quali i cd. *cyberwar* e *cybercrime*, hanno riportato all'attenzione dell'opinione pubblica e delle istituzioni repubblicane il tema della cybersicurezza nazionale[2], inquadrabile nel più ampio contesto della sicurezza pubblica dello Stato italiano[3], pur senza delinearsi un eventuale e autonomo diritto

[1] Su cui v. almeno, da una prospettiva costituzionalistica, M. BENVENUTI, *Le conseguenze costituzionali della guerra russo-ucraina. Prime considerazioni*, in *Osservatorio AIC*, 3/2022, 20-46.

[2] Quanto alla "cybersicurezza" o "*cybersecurity*" v. *ex multis* V. DE LUCA, G. TERZI DI SANT'AGATA, F. VOCE (a cura di), *Il ruolo dell'Italia nella sicurezza cibernetica. Minacce, sfide e opportunità*, Milano, Franco Angeli, 2018; F. VOCE, *Lo stato dell'arte della cyber security italiana*, ivi, 22-26; A. CONTALDO, D. MULA (a cura di), *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, Pacini Giuridica, 2020; A. CONTALDO, L. SALANDRI, *La nuova disciplina giuridica c.d. "orizzontale" della Cybersicurezza per le infrastrutture in un'ottica di sviluppo dei sistemi informativi*, in *Rivista amministrativa della Repubblica Italiana*, 11-12/2016, 567-595; U. GORI, *Interesse nazionale, intelligence e strategie nell'era cibernetica*, in *Gnosis*, 2/2016, 87-93; R. BRIGHI, P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 21/2021, 18-42; B. BRUNO, *"Cybersecurity" tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, ivi, 14/2020, 11-45; P.L. MONTESSORO, *"Cybersecurity": conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *Istituzioni del Federalismo*, 3/2019, 783-800.

[3] Sul concetto generale di sicurezza pubblica nell'ordinamento costituzionale v. almeno T.F. GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali*, in *Forum di Quaderni Costituzionali*, 2008, spec. 16 ss. (anche in S. VIDA (a cura di), *Diritti umani: trasformazioni e reazioni*, Bologna, Bononia University Press, 2008, 275-301; ID., *Le dimensioni costituzionali della sicurezza*, Bologna, Bononia University Press, 2008; M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Atti del Convegno Milano 4 giugno 2009, Milano, Giuffrè, 2012, 17-80; A. PACE, *Il concetto di ordine pubblico nella Costituzione italiana*, cit.; ID., *Libertà e sicurezza Cinquant'anni dopo*, in *Diritto e Società*, 2/2013, 177-205. Sulla "sicurezza della Repubblica" e al ruolo del Comitato parlamentare per la sicurezza della Repubblica (COPASIR) v. tra gli altri M. VALENTINI, *L'ordinamento del sistema politico dell'informazione per la sicurezza*, in S. GAMBACURTA, C. MOSCA, G. SCANDONE, M. VALENTINI, *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)*, Milano, Giuffrè, 2008, 23-94; ID., *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Napoli, Editoriale Scientifica, 2017; T.F. GIUPPONI, *Servizi di informazione e segreto di Stato nella legge n. 124/2007*, in A. CARIOLA, E. CASTORINA, A. CIANCIO (a cura di), *Studi in onore di Luigi Arcidiacono*, vol. IV, Torino, Giappichelli, 2010, 1677-1751; C. NARDONE, *L'evoluzione del controllo parlamentare sulla politica di informazione per la sicurezza*, in *Parlamento della Repubblica: organi, procedure, apparati*, Camera dei deputati, 2013, vol. I, spec. 25 ss.; M. FRANCHINI, *Alcune considerazioni sulle nuove competenze del Comitato parlamentare per la sicurezza della Repubblica*, in *Rivista AIC*, 2014; E. RINALDI, *Arcana Imperii. Il segreto di Stato nella forma di governo italiana*,

costituzionale alla sicurezza, anche nella sua potenziale declinazione cibernetica o, che dir si voglia, informatica[4].

Ora prima di addentarsi nel tema specifico di questo contributo, avente ad oggetto in particolare il ruolo degli organi istituzionali, in specie quelli parlamentari, con riguardo alla cybersicurezza nazionale, pare opportuno delineare (brevemente) il quadro normativo, soprattutto con riferimento a quello nazionale, su cui si fonda la sicurezza cibernetica[5], vale a dire quell'insieme di misure che possono adottarsi al fine di proteggere i sistemi informatici da attacchi esterni che ne determinerebbero la compromissione del funzionamento.

Napoli, Jovene, 2016, spec. 164 ss.; A. PERRONE, *Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica*, in *Federalismi.it*, 11/2018, 1-28.

[4] La dottrina si interroga da tempo sulla possibilità di individuare un diritto costituzionale alla sicurezza, all'interno del quale sarebbe da ricomprendersi anche una dimensione "cibernetica" della stessa; in senso favorevole ad un tale diritto v. in particolare, G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, 1/2008, 31-44, spec. 34-35; T.E. FROSINI, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali*, 2006; S. RAIMONDI, *Per l'affermazione della sicurezza pubblica come diritto*, in *Dir. amm.*, 4/2006, 747-758, spec. 753-754; P. TORRETTA, *"Diritto alla sicurezza" e (altri) diritti di libertà della persona: un complesso bilanciamento costituzionale*, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, Giuffrè, 2003, 451-484; C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche di sicurezza*, Padova, Cedam, 2012; A. D'ALOIA, *La sicurezza* tra *i diritti*, in AA. VV., *Studi in onore di Franco Modugno*, vol. II, Napoli, Editoriale Scientifica, 2011, 1091-1115; G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4/2019, 65-84, spec. 73 ss.; N. ZANON, *Un diritto fondamentale alla sicurezza?*, in *Diritto penale e processo*, 11/2019, 1555-1557. In senso contrario v. invece A. PACE, *Libertà e sicurezza. Cinquant'anni dopo*, in *Dem. soc.*, 2/2013, 177-205; G. TROMBETTA, *Diritto alla sicurezza o sicurezza dei diritti? Brevi riflessioni intorno a una recente proposta di legge costituzionale*, in *Forum di Quaderni Costituzionali*, 4/2021, 159-180; M. RUOTOLO, *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e sicurezza*, 2/2013, 1-12; ID., *La sicurezza nel gioco del bilanciamento*, cit.; M. DOGLIANI, *Il volto costituzionale della sicurezza*, in *Astrid Rassegna*, 22/2010, 1-9; A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, in S. ANASTASIA, M. PALMA (a cura di), *La bilancia e la misura. Giustizia sicurezza riforme*, Milano, Franco Angeli, 2001, 19-36, spec. 21, secondo il quale la configurazione di un tale diritto fondamentale alla sicurezza non sarebbe «altro che il risultato di una costruzione costituzionale falsa o perversa»; infatti, essa risulta «superflua» se assume il significato di «legittima domanda di sicurezza di tutti i diritti da parte di tutti i soggetti», dovendosi, tra l'altro, parlare non già di diritto alla sicurezza, quanto di «sicurezza dei diritti» ovvero di «diritto ai diritti».

[5] Sul punto v. *amplius* per tutti F. GAGGERO, M. BERRUTI, *I pilastri normativi della sicurezza cibernetica*, in P. COSTANZO, M. MAGARÒ, L. TRUCCO (a cura di), *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, 2022, 375-398.

2. L'architettura normativa della cybersicurezza in Italia

Come conseguenza di una cospicua adozione di atti normativi dell'Unione europea in materia di sicurezza informatica[6], negli ultimi anni anche il nostro ordinamento ha provveduto a dotarsi di numerosi atti normativi e legislativi in tema, di cui si ripercorrono ora i più rilevanti.

Con la legge 7 agosto del 2012, n. 133 è stata modificata la legge 3 agosto 2007, n. 124 recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", in particolare introducendo per la prima volta alcune competenze circa la sicurezza informatica agli organi già preposti a garantire la sicurezza nazionale, ossia insistendo in particolare sul Presidente del Consiglio dei ministri il quale, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza (DIS) e ai Servizi di informazione per la sicurezza (AISE e AISI) direttive al fine di «rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali» (art. 1, comma 3-bis); sulla base delle indicazioni derivanti dalla Presidenza del Consiglio e dei dati acquisiti dai servizi di informazione per la sicurezza, il Dipartimento delle informazioni per la sicurezza «coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali» (art. 4, comma 3, lett. d-bis)[7].

Di qualche tempo successiva è stata l'adozione del d. lgs. 18 maggio 2018, n. 65 recante "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio

[6] Anzitutto si pensi al Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), con il compito di sostenere Commissione europea e Stati membri nell'assicurare un alto livello di sicurezza delle reti informatiche. Successivamente troviamo invece la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; si tratta della cd. Direttiva NIS (Network and Information Security), recepita dal nostro ordinamento con il d. lgs. 18 maggio 2018, n. 65 (*v. infra*), che rappresenta un tentativo iniziale di armonizzazione dei livelli di sicurezza delle reti e dei sistemi informativi attraverso un coordinamento europeo con l'individuazione delle autorità nazionali NIS, dei punti di contatto unico nazionali e dei gruppi di intervento per la sicurezza informatica in caso di incidenti (CSIRT). Più di recente, infine, vi è il cd. *Cybersecurity Act*, ossia il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA (Agenzia dell'Unione europea per la cybersicurezza) e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) 2013/526; con tale atto non solo si stabilizza la presenza dell'agenzia (già istituita con il Regolamento (CE) 2004/460 e prorogata dal Regolamento (UE) 2013/526), ma si introduce un quadro europeo per la certificazione della cybersicurezza, il cui scopo è quello di favorire la circolazione europea dei servizi informatici nell'ottica del mercato unico, anche attraverso l'armonizzazione degli standard di sicurezza nazionali.

[7] In dottrina v. almeno G. SCACCIA, *Intelligence e segreto di Stato nella legge n. 133 del 2012*, in *Diritto e società*, 3/2012, 585-599.

2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", vale a dire il cd. decreto legislativo NIS. Con tale atto normativo – sulle cui modifiche successive si tornerà a breve – è stato previsto che il Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, adotti la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale (art. 6); si sono individuati quali Autorità NIS i Ministeri dello sviluppo economico, delle infrastrutture e dei trasporti (ora infrastrutture e mobilità sostenibili), dell'economia e delle finanze, della salute, dell'ambiente (ora della transizione ecologica), per i settori specificamente indicati (energia e trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), designando inoltre come «punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi» il Dipartimento delle informazioni per la sicurezza istituito presso la Presidenza del Consiglio dei ministri, al fine di coordinare la sicurezza delle reti e la cooperazione transfrontaliera a livello europeo (art. 7); inoltre si è istituito presso la Presidenza del Consiglio il cd. CSIRT italiano, ossia il gruppo di intervento per la sicurezza informatica in caso di incidente, il quale definisce le procedure per la prevenzione e la gestione dei rischi e degli incidenti informatici (art. 8).

A questo primo intervento – di sostanziale recepimento della normativa europea – ne è seguito un altro, vale a dire il d. l. 21 settembre 2019, n. 105 recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica", convertivo con modificazioni dalla legge 18 novembre 2019, n. 133. Tale decreto – cd. decreto-legge perimetro[8] – ha istituito il cd. perimetro di sicurezza nazionale cibernetica al fine di

[8] In attuazione del decreto-legge n. 105 del 2019 sono stati adottati alcuni provvedimenti: il D.P.R. 5 febbraio 2021, n. 54 ("Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133"), che ha definito procedure e modalità di valutazione delle acquisizioni da parte dei soggetti inclusi nel perimetro di sicurezza cibernetica, nonché le procedure delle attività di verifica e ispezione; il D.P.R. 14 aprile 2021, n. 81 ("Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza"); il D.P.C.M. 30 luglio 2020, n. 131 ("Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133"), il quale stabilisce i criteri per individuare i soggetti inclusi nel perimetro summenzionato, nonché specifica i settori nei quali operano i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica (governativo, interno, difesa, tecnologia critiche, spazio e aerospazio, trasporti, enti previdenziali e lavoro, telecomunicazioni, economia e finanza, energia, servizi digitali; il D.P.C.M. 15 giugno 2021 ("Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di

tutelare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, ovvero degli enti e degli operatori pubblici e privati nazionali da quali dipendono funzioni e servizi essenziali per attività civili, sociali o economiche di assoluto rilievo per gli interessi dello Stato, «dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale» (art. 1, comma 1). Con tale atto normativo sono stati definiti inoltre criteri e modalità per l'individuazione di amministrazioni pubbliche, enti e operatori nazionali (pubblici e privati) da includersi nel perimetro di sicurezza nazionale cibernetica sulla base della loro essenzialità per gli interessi nazionali, in particolare in quei settori più soggetti ad attacchi informatici (sempre più frequenti) quali la difesa, i trasporti, le telecomunicazioni o i sistemi bancari e finanziari. È rilevante osservare come l'elencazione di tali soggetti sia contenuta in un atto amministrativo adottato dal Presidente del Consiglio dei ministri, su proposta del Comitato interministeriale per la cybersicurezza (CIC), caratterizzato dall'essere escluso – ovviamente a tutela della sicurezza nazionale – dal diritto di accesso ovvero dagli obblighi di trasparenza e pubblicazione, risultando noto, oltre agli stessi soggetti coinvolti (ciascuno con riguardo soltanto alla propria inclusione), all'Agenzia per la cybersicurezza nazionale (*v. infra*), al Dipartimento delle informazioni per la sicurezza (DIS), all'Agenzia informazioni e sicurezza esterna (AISE) e all'Agenzia informazioni e sicurezza interna (AISI), all'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (art. 1, comma 2-bis), nonché al Comitato parlamentare per la sicurezza della Repubblica (art. 1, comma 4-bis)[9].

Infine, troviamo il d.l. 4 giugno 2021, n. 82 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la

sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133").

[9] Così l'art. 1 d.l. n. 105 del 2019 come modificato dal successivo d.l. 30 dicembre 2019, n. 162 "Disposizioni urgenti in materia di proroga di termini legislativi, di organizzazione delle pubbliche amministrazioni, nonché di innovazione tecnologica" e convertito con modificazioni in legge 28 febbraio 2020, n. 8, nonché da ultimo dal d.l. 4 giugno 2021, n. 82 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", convertito con modificazioni in legge 4 agosto 2021, n. 109.

In attuazione di tale disposizione il Governo ha adottato il DPCM 30 luglio 2020, n. 131 "Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133", con cui ha definito modalità e criteri procedurali per l'individuazione concreta dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) da includere nel perimetro di sicurezza nazionale cibernetica.

cybersicurezza nazionale", convertito con modificazioni in legge 4 agosto 2021, n. 109. Si tratta del cd. decreto-legge cybersicurezza[10], con cui si è intervenuti radicalmente sull'architettura ordinamentale relativa alla sicurezza informatica, prevedendo anche nel nostro ordinamento – sui modelli di Francia e Germania, sebbene con un notevole ritardo, e in gran parte in ragione degli interventi adottati nel contesto del PNRR[11] – un'unica autorità nazionale competente in materia che viene individuata nell'Agenzia per la cybersicurezza nazionale[12]. A questa e al nuovo Comitato interministeriale per la cybersicurezza[13] vengono di fatto trasferite tutte le competenze, in materia di

[10] In dottrina v. almeno F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 12/2022, 241-272.

[11] La sicurezza cibernetica costituisce uno degli svariati interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021; in particolare la sicurezza cibernetica è uno dei principali investimenti nell'ambito della digitalizzazione della pubblica amministrazione, in particolare della Componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" ricompresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo". In particolare, l'intervento prevede quattro aree principali: il rafforzamento dei presidi di *front-line* per la gestione degli eventi a rischio verso la PA e le imprese di interesse nazionale; il consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'*hardware* e del *software*; il potenziamento del personale delle forze di polizia dedicate alla prevenzione e investigazione del crimine informatico; l'implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

[12] Il d.l. n. 82/2021 istituisce l'Agenzia per la cybersicurezza nazionale avente personalità giuridica di diritto pubblico e autonomia regolamentare, amministrativa, organizzativa, contabile e finanziaria (art. 5); il direttore generale e il vicedirettore generale dell'Agenzia sono nominati (e revocabili) dal Presidente del Consiglio, previa deliberazione del Consiglio dei ministri e dopo aver informato il Comitato parlamentare per la sicurezza della Repubblica e le commissioni parlamentari competenti (art. 2); tale Agenzia, in quanto Autorità nazionale per la cybersicurezza, svolge alcune rilevanti funzioni: assicura il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni; è punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi; è Autorità nazionale di certificazione della cybersicurezza; esercita le competenze riguardo al perimetro di sicurezza nazionale cibernetica attribuite alla Presidenza del Consiglio dei ministri e assume le funzioni demandate dal decreto-legge perimetro al Dipartimento delle informazioni per la sicurezza (art. 7).

Al d.l. n. 82 del 2021 è stata data attuazione con tre decreti del Presidente del Consiglio che disciplinano vari aspetti dell'Agenzia per la cybersicurezza nazionale: D.P.C.M. 9 dicembre 2021, n. 222 ("Regolamento di contabilità dell'Agenzia per la cybersicurezza nazionale"); D.P.C.M. 9 dicembre 2021, n. 223 ("Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale"); D.P.C.M. 9 dicembre 2021, n. 224 ("Regolamento del personale dell'Agenzia per la cybersicurezza nazionale").

[13] Previsto dall'art. 4 del d.l. n. 82 del 2021 «con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza» (comma 1). Il Comitato infatti «a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza; d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale» (comma 2). Il Comitato è istituito presso la Presidenza del Consiglio dei ministri, presieduto dal Presidente del Consiglio dei ministri e composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal

cybersicurezza, prima assegnate rispettivamente al Dipartimento delle informazioni per la sicurezza (DIS) e al Comitato interministeriale per la sicurezza della Repubblica (CISR). L'Agenzia, infatti, costituisce il nuovo punto di contatto unico NIS, sicché essa svolgerà le funzioni di coordinamento con le autorità NIS degli altri Stati membri europei, con il gruppo di cooperazione e con l'Autorità garante per la protezione dei dati personali. Invariate restano invece le competenze della Presidenza del Consiglio dei ministri cui spetta in via esclusiva l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, l'adozione della strategia nazionale di cybersicurezza[14], sentito il Comitato interministeriale per la cybersicurezza, la nomina e la revoca del direttore e del vicedirettore generali dell'Agenzia per la cybersicurezza (art. 2).

3. Il ruolo del Parlamento e del COPASIR

Dalla normativa appena ripercorsa emerge nitidamente come l'intero impianto della *governance* della cybersicurezza ruoti sostanzialmente attorno all'esecutivo (analogamente a quanto accade per la cd. sicurezza della Repubblica, come delineata dalla già citata legge n. 124 del 2007) in specie alla Presidenza del Consiglio dei ministri laddove si incardinano i vari organismi poc'anzi brevemente osservati. A fronte di un tale accentramento al vertice dell'Esecutivo dovrebbe corrispondere un adeguato consolidamento del ruolo del Parlamento sul piano del controllo e della garanzia costituzionali. Il Parlamento risulta infatti dotato di una minore consistenza "decisionale" nel settore della sicurezza informatica, sebbene, a ben vedere, esso benefici di alcune rilevanti prerogative nell'ambito della considerevole funzione di controllo che gli è propria. L'ambito

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 (comma 3).

[14] Per quanto riguarda l'adozione della Strategia nazionale di cybersicurezza – la cui predisposizione risulta però affidata all'Agenzia per la cybersicurezza nazionale come da art. 7, comma 1, lett. b) – oltre a una mera differenza terminologica (il termine "sicurezza cibernetica" è infatti stato sostituito con il termine "cybersicurezza" con una infelice crasi tra il termine inglese e quello italiano), risulta rilevante il fatto che il piano non debba essere più trasmesso direttamente dalla Presidenza del Consiglio alla Commissione europea, in quanto provvederà a ciò direttamente l'Agenzia, determinando una semplificazione dei rapporti nell'ambito dell'ordinamento eurounitario.

In particolare, il 18 maggio 2022 il Comitato Interministeriale per la Cybersicurezza (CIC), presieduto dal Presidente del Consiglio dei ministri, ha approvato la Strategia nazionale di cybersicurezza (2022-2026) e il relativo Piano di implementazione; attraverso questi due documenti, il Governo si propone di rispondere a diverse sfide e problematiche attuali e future come il rafforzamento della resilienza nella transizione digitale del sistema Paese, la gestione delle crisi cibernetiche, il raggiungimento dell'autonomia strategica nella dimensione cibernetica.

concernente i servizi e la sicurezza della Repubblica è infatti uno dei molti in cui si estrinseca la relazione istituzionale e dialettica tra Governo e Parlamento[15]. Essendo l'Esecutivo responsabile degli apparati preposti alla sicurezza nazionale nei confronti delle Camere, queste ultime possono disporre dei poteri di indirizzo, controllo e informazione che si manifestano attraverso gli appositi strumenti previsti dai regolamenti parlamentari, vale a dire sia gli istituti di natura eminentemente conoscitiva quali l'inchiesta parlamentare, l'audizione e l'indagine conoscitiva, sia quelli del sindacato ispettivo (ossia quelli più legati al controllo politico dell'Esecutivo)[16], i quali sono finalizzati in particolare «ad accertare, ed eventualmente correggere, la rispondenza degli atti governativi agli indirizzi politici di maggioranza»[17].

Inoltre, alle ordinarie prerogative, specialmente di controllo parlamentare, in capo alle Camere, si affiancano quelle specificamente attribuite all'organo parlamentare che più di tutti si occupa, per sua natura, di tutto ciò che attiene alla sicurezza nazionale, vale a dire il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) [18].

---

[15] Cfr. G. ROMANO, *Parlamento e servizi di informazione e sicurezza: riflessioni per una riforma attesa da venti anni*, cit., il quale osserva che «i rapporti tra Parlamento ed organismi informativi non sembrano riconducibili *sic et simpliciter* allo schema generale che connota le relazioni intercorrenti tra Parlamento e Governo. La ragione di un interesse specifico per il tema in questione nasce infatti dalle particolari modalità operative che caratterizzano l'azione dei servizi di informazione e sicurezza, conformate per loro stessa natura ad un principio generale di riservatezza che si pone in quanto tale in conflitto con il generale canone della trasparenza e della pubblicità dell'azione delle amministrazioni pubbliche». Pertanto, in questo specifico ambito, «le Camere si trovano a dover fare dunque i conti con un complesso di esigenze, formali e sostanziali, che non si pongono invece in alcun modo all'atto di acquisire elementi di conoscenza in ordine, ad esempio, al funzionamento di uno determinato ministero, alla trattazione di una questione burocratica, ovvero ai risultati conseguiti in esito ad uno specifico programma di interventi la cui attuazione sia demandata ad organi, enti o istituti ricadenti nell'ambito della sfera di competenza dell'Esecutivo».

Quanto al rapporto tra Parlamento e Governo nell'ambito del sistema della sicurezza della Repubblica la dottrina appare piuttosto limitata e risalente nel tempo; v. S. LABRIOLA, *Le informazioni per la sicurezza dello Stato*, Milano, Giuffrè, 1978, spec. 211 ss.; G. ARENA, *Le attribuzioni del Parlamento in materia di servizi per le informazioni e la sicurezza in Italia e negli Stati Uniti*, in *Rivista trimestrale di diritto pubblico*, 1/1978, 485 ss.; C. TROISIO, *Controllo parlamentare e servizi di sicurezza nell'ordinamento italiano*, Roma, Marves, 1981; G. DE LUTIIS, *Controllo e servizi segreti: una comparazione*, in *Democrazia e diritto*, 1/1986, 47 ss. Più di recente v. i già citati G. ROMANO, *Parlamento e servizi di informazione e sicurezza: riflessioni per una riforma attesa da venti anni*, cit.; A. PERRONE, *Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica*, cit.

[16] Cfr. G. ROMANO, *Parlamento e servizi di informazione e sicurezza: riflessioni per una riforma attesa da venti anni*, in *Per Aspera Ad Veritatem*, 21, 3/2001 (*Il Parlamento della Repubblica*, Roma, Camera dei deputati, vol. 11).

[17] R. MORETTI, *Attività informative, di ispezione, di indirizzo e di controllo*, in T. MARTINES, G. SILVESTRI, C. DECARO, V. LIPPOLIS, R. MORETTI, *Diritto parlamentare*, Milano, Giuffrè, 2011, 2° ed., 335-380, spec. 336.

[18] Un apposito organo parlamentare è previsto anche in altri ordinamenti europei. In Francia il controllo parlamentare sull'attività dei servizi è garantito dalla *Délégation parlementaire au renseignement*, vale a dire un organo parlamentare bicamerale previsto dalla Loi n. 2007-1443 du 9 octobre 2007 e composto da quattro deputati e quattro senatori (tra questi vi sono quattro membri di diritto – vale a dire i Presidenti delle commissioni parlamentari permanenti dell'Assemblea nazionale e del Senato in tema di difesa e sicurezza interna, rispettivamente la *Commission de la Défense* e la *Commission de Lois* – e quattro membri invece nominati dai Presidenti delle due assemblee in maniera tale da assicurare una rappresentanza equilibrata e pluralista tra maggioranza e opposizione; inoltre, la

Innanzitutto, la legge n. 124 del 2007 stabilisce che alla Relazione sulla politica dell'informazione per la sicurezza – trasmessa annualmente dal Governo alle Camere – sia allegato altresì il Documento di sicurezza nazionale «concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica» (art. 38, comma 1-bis)[19].

Inoltre, con particolare riguardo alla cybersicurezza[20], il Presidente del Consiglio trasmette una relazione annuale, circa l'attività svolta dall'Agenzia per la cybersicurezza nell'anno precedente in

presidenza dell'organo è affidata a turno a uno dei membri di diritto (un anno al Presidente della *Commission de la Défense* e uno a quello della *Commission de Lois*). Tra le prerogative della *Délégation* troviamo, in particolare quanto alla funzione di controllo, la possibilità di udire il Primo ministro, i Ministri e il Segretario generale della difesa nazionale, nonché i direttori dei servizi di *intelligence*; inoltre essa gode della possibilità di inviare al Presidente della Repubblica e al Primo Ministro raccomandazioni ovvero osservazioni (che vengono trasmessi anche ai Presidenti di assemblea) ed è tenuta a presentare annualmente un Rapporto pubblico sulla propria attività (omettendo, tuttavia, i dati protetti dal segreto della difesa nazionale).

Analogamente, anche in Germania i Servizi federali di informazione e sicurezza – in quanto organo afferente al potere esecutivo – sono sottoposti al controllo parlamentare, svolto in particolare dal Comitato per il controllo parlamentare dell'attività di *intelligence* della Federazione (*Parlamentarisches Kontrollgremium - PKGr*), istituito con la riforma costituzionale del 17 luglio 1999 (che vi ha fatto confluire il precedente organo di controllo, vale a dire la *Parlamentarische Kontrollkommission* ossia la Commissione parlamentare di controllo) e disciplinato dalla "Legge sul controllo parlamentare delle attività di *intelligence* della Federazione" (*Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes - Kontrollgremiumgesetz - PKGrG*) del 29 luglio 2009. Il numero dei membri e le regole di funzionamento del Comitato sono scelti dal *Bundestag* all'inizio di ogni legislatura, i componenti sono eletti tra i deputati a maggioranza assoluta dallo stesso *Bundestag*, mentre la presidenza del Comitato ha durata annuale e prevede l'alternanza tra maggioranza e opposizione; attualmente il Comitato è comporto da 13 deputati (4 SPD, 3 CDU/CSU, 2 Verdi, 2 FDP, 1 *Die Linke*, 1 AfD) e la presidenza è di maggioranza (Verdi). Quanto alle prerogative del Comitato esso viene informato dal Governo federale circa le attività dei Servizi di *intelligence* e i relativi eventi di particolare interesse, può udire i membri dei Servizi e avere accesso alla loro documentazione, così come esso è tenuto a presentare due relazioni al *Bundestag* (rispettivamente a metà e a fine legislatura).

Sul punto cfr. almeno CAMERA DEI DEPUTATI, *La disciplina dei servizi di informazione in Francia, Germania, Regno Unito e Spagna*, in *I servizi di intelligence in Europa*, 08 marzo 2018, in camera.it.

[19] L'art. 16, comma 2, del d.l. n. 82 del 2021, aveva disposto l'abrogazione del comma 1-bis a far data dal 15 giugno 2021, mentre in sede di conversione, con modificazioni, la l. n. 109 del 2021 ha disposto la proroga dell'abrogazione di tale comma al giorno 1° gennaio 2023; per cui la Relazione sulla politica dell'informazione per la sicurezza relativa all'anno 2021 presentata al Parlamento il 28 febbraio 2022 sarà presumibilmente l'ultima a contenere tale Documento di sicurezza nazionale.

[20] Il d.l. n. 105 del 2019 prevede diverse disposizioni in tema. Si segnala che spetta al Presidente del Consiglio dei ministri coordinare la coerente attuazione delle disposizioni del presente decreto che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del Dipartimento delle informazioni per la sicurezza, che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni di cui al presente decreto e con i soggetti di cui al comma 1 del presente articolo. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui al comma 6, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attività svolte (art. 1, comma 19-bis).

Inoltre il d.l. 105/2019 prevede l'ipotesi che si verifichi una crisi di natura cibernetica: «in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici», il Presidente del Consiglio dei ministri, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, «può comunque disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o

materia di cybersicurezza nazionale, entro il 30 aprile al Parlamento[21] ed entro il 30 giugno al Comitato parlamentare per la sicurezza della Repubblica «negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato» (art. 14, d.l. n. 82 del 2021).

Con specifico riferimento all'Agenzia, diversi sono gli ambiti e le attività ad essa relativi sottoposti al controllo parlamentare del COPASIR, ai sensi del d.l. n. 82 del 2021: l'obbligo del Presidente del Consiglio di informare preventivamente il Comitato parlamentare per la sicurezza della Repubblica, nonché le commissioni parlamentari competenti, circa la nomina e la revoca del direttore generale e del vicedirettore generale dell'Agenzia per la cybersicurezza (art. 2, comma 3); la possibilità per il COPASIR di chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza, ai sensi dell'articolo 31, comma 3, della legge n. 124 del 2007 (art. 5, comma 6); il parere positivo richiesto da parte delle Commissioni parlamentari competenti per materia e, circa i profili di competenza, del Comitato parlamentare per la sicurezza della Repubblica e del CIC, quanto al decreto del Presidente del Consiglio dei ministri con cui è adottato il regolamento sull'organizzazione e sul funzionamento dell'Agenzia (art. 6, comma 3); la comunicazione al COPASIR dello stanziamento annuale di risorse assegnate all'Agenzia con legge di bilancio, sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri (art. 11, comma 1); il parere positivo del COPASIR quanto all'adozione del regolamento di contabilità dell'Agenzia, di concerto con il Ministro dell'economia e delle finanze, su proposta del direttore generale dell'Agenzia (art. 11, comma 3); la trasmissione al COPASIR del bilancio consuntivo dell'Agenzia e della relativa relazione della Corte dei conti (art. 11, comma 3, lett. a)); il parere positivo del COPASIR quanto al regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta del direttore generale dell'Agenzia, con cui sono definite le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico (art. 11, comma 4); l'obbligo di tempestiva e motivata comunicazione alle Commissioni parlamentari

più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati»; delle misure adottate in questi casi il Presidente del Consiglio informa entro trenta giorni il Comitato parlamentare per la sicurezza della Repubblica (art. 5).

[21] L'art. 10-bis del d.l. n. 82 del 2021 ha previsto che, in sede di prima applicazione del decreto, la prima relazione al Parlamento venga trasmessa entro il 30 novembre 2022, così come che entro il 31 ottobre 2022 il Presidente del Consiglio dei ministri è tenuto a trasmettere al Parlamento una relazione che dia conto dell'attuazione al 30 settembre 2022 delle disposizioni di cui al decreto-legge in parola, anche al fine di formulare eventuali proposte in merito.

competenti e al COPASIR, dei provvedimenti adottati in materia di dotazione organica dell'Agenzia (art. 12, comma 5); il previo parere delle Commissioni parlamentari competenti e del COPASIR circa l'adozione del regolamento sull'ordinamento e il reclutamento del personale dell'Agenzia, e il relativo trattamento economico e previdenziale (art. 12, comma 8).

4. Cenni conclusivi: la cybersicurezza nazionale di fronte alle attuali sfide "belliche"

Le funzioni di controllo e consultive del COPASIR non si sostanziano soltanto in obblighi di informazione e di pareri, previsti, come poc'anzi osservato, con stretto riguardo all'Agenzia per la cybersicurezza nazionale, ma trovano margine per assumere anche una forma più ampia. Infatti, con riguardo alla sicurezza informatica e cibernetica in senso lato, il Comitato trova tra le sue prerogative, specialmente in merito alla funzione di controllo, quella di svolgere audizioni del Presidente del Consiglio dei ministri e dell'Autorità delegata – la quale può, come attualmente accade con il sottosegretario Franco Gabrielli, ricevere dal Presidente la delega alla *cybersecurity* –, dei Ministri facenti parte del CISR, del direttore generale del DIS e dei direttori dell'AISE e dell'AISI, dei dipendenti del Sistema di informazione per la sicurezza (in casi eccezionali), ovvero, più in generale, può ascoltare «ogni altra persona non appartenente al Sistema di informazione per la sicurezza in grado di fornire elementi di informazione o di valutazione ritenuti utili ai fini dell'esercizio del controllo parlamentare» (art. 30, legge n. 124 del 2007)[22].

A tale attività di audizioni e indagini conoscitive – solitamente piuttosto densa, ma particolarmente in questo periodo di conflitto bellico in territorio ucraino e dei relativi (e frequenti) attacchi informatici – il COPASIR affianca la possibilità di trasmettere al Parlamento informative o

[22] Secondo A. PERRONE, *Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica*, cit., 25-26, ciò evidenzia «una maggiore e più incisiva relazione con l'Autorità politica ed i vertici delle Agenzie con i quali si è consolidato un canale di comunicazione istituzionale che ha comportato indubbi benefici: da un lato, il Parlamento, attraverso il Comitato, è venuto a conoscenza, se pur con modalità filtrate e tali da non compromettere esigenze di riservatezza, determinate scelte ed indirizzi di politica della sicurezza che lo stesso Governo ha interesse ad esternare nelle sue linee e motivazioni essenziali, anche allo scopo di rendere partecipi i gruppi di opposizione; dall'altro, lo stesso Comitato si fa interprete e garante di sollecitazioni e chiarimenti che i Gruppi politico- parlamentari – tramite i rispettivi componenti che siedono nell'organo bicamerale – intendono sottoporre all'attenzione dell'Autorità politica e dei Servizi».

relazioni urgenti[23], nonché la relazione annuale con cui riferisce dell'attività svolta, formulando altresì proposte o segnalazioni su questioni rientranti nella propria sfera di competenza (art. 35, legge n. 124 del 2007)[24].

A fronte di una tale attività di controllo e di indagine del COPASIR[25], nell'ambito della propria competenza di vigilare che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni (art. 30, comma 2, l. n. 124 del 2007), il Parlamento non si è dimostrato sempre (o almeno adeguatamente) attento alle suggestioni provenienti dal Comitato – mancando, ad esempio, di intervenire legislativamente sull'architettura istituzionale e sulla legge n. 124 del 2007, ovvero di un costante controllo parlamentare sul Governo e sulla *governance* della sicurezza nazionale attraverso gli appositi strumenti di controllo parlamentare[26] – a fronte, invece, di un'azione più efficace dell'esecutivo che ha adottato, a seguito della crisi ucraina, alcune disposizioni urgenti, convertite a dire il vero con modifiche dal Parlamento, su tutte quelle relative al caso degli antivirus russi in dotazione alle amministrazioni pubbliche italiane. Il riferimento è al d.l. 21 marzo 2022, n. 21 "Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina", convertito con modificazioni in legge 20 maggio 2022, n. 51, il cui Capo II reca "Cybersicurezza delle reti, dei sistemi informativi e dei servizi informatici e approvvigionamento di materie prime critiche". In particolare, l'art. 29 ("Rafforzamento della disciplina cyber") prevede che le pubbliche amministrazioni provvedano alla diversificazione dei servizi in uso – identificati da un'apposita circolare dell'Agenzia per la cybersicurezza nazionale nella sicurezza dei dispositivi (*endpoint security*), ivi compresi applicativi antivirus, *antimalware* ed «*endpoint detection and response*» (EDR), e nella protezione delle reti attraverso «*web application firewall*» – al fine di

[23] Tra le più significative dell'attuale legislatura v. "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica", doc. XXXIV, n. 1, 11 dicembre 2019.

[24] V. da ultimo "Relazione del Comitato parlamentare per la sicurezza della Repubblica sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022", doc. XXXIV, n. 8, 9 febbraio 2022.

[25] Secondo A. PERRONE, *Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica,* cit., spec. 5, la funzione di controllo è la «missione costitutiva» del COPASIR.

[26] *Ivi*, 27. Secondo l'A. «è indubbio che la finalità tradizionale del controllo parlamentare resti attuale, avendo quale destinatario naturale il potere esecutivo le cui determinazioni si riveleranno tanto più efficaci se sottoposte ad una costante attività di sorveglianza e di critica. D'altro canto, si assiste anche ad un orientamento, proveniente dall'ordinamento anglosassone, che tende a configurare il controllo parlamentare in una dimensione più ampia ed articolata di supervisione generalizzata (*oversight*) da parte del Parlamento e dei suoi organi che affianca agli strumenti classici del controllo – il potere d'inchiesta, le indagini conoscitive, le audizioni, le interrogazioni, le interpellanze, le mozioni – nuove facoltà che mirano ad esempio alla valutazione delle politiche pubbliche al fine di verificarne il grado di efficacia e di realizzazione sia degli obiettivi prefissati sia dei bisogni della collettività».

prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche che potrebbero derivare dal rischio che le aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Federazione Russa non siano in grado di fornire servizi e aggiornamenti ai propri prodotti poc'anzi individuati in conseguenza della crisi in Ucraina, nonché, più in generale, al fine di prevenire possibili pregiudizi per la sicurezza nazionale nello spazio cibernetico. In attuazione di tale disposizione è stata emanata dall'Agenzia per la cybersicurezza nazionale la circolare 21 aprile 2022, n. 4336, "Diversificazione di prodotti e servizi tecnologici di sicurezza informatica".

Tutto ciò in un ambito in cui il Parlamento dovrebbe essere costantemente partecipe con un'azione di più attenta vigilanza[27], nell'ottica di recupero in senso generale del controllo parlamentare anche di fronte ai nuovi fenomeni globali[28], proprio perché anche la cybersicurezza – la quale, come dimostrano le recenti vicende che vedono coinvolti il COPASIR e i Servizi di informazione per la sicurezza, ha sempre più di frequente ricadute anche sul contiguo settore dell'informazione, laddove il mezzo cibernetico è divenuto, in modo crescente, nell'ambito della cd. *information warfare*[29], uno strumento di manipolazione e diffusione mirata di false informazioni[30] – deve essere ricondotta all'interno del complessivo sforzo dell'ordinamento volto

[27] In questo senso si osservi quanto accaduto in Germania nel 2009; dapprima con l'introduzione dell'art. 45d della Legge fondamentale (*deutsches Grundgesetz*), attraverso la modifica costituzionale del 17 luglio 2009, è stato rafforzato il diritto del Parlamento alla propria prerogativa di controllo sul Governo nell'ambito dei servizi di informazione e sicurezza, non solo conferendo un rilievo costituzionale alla verifica parlamentare dell'attività dei servizi, anche a tutela dei diritti costituzionalmente garantiti ai cittadini, ma si è allo stesso tempo consolidato il diritto del Comitato di ricevere informazioni in tema di sicurezza nazionale da parte dello stesso Esecutivo. Inoltre, con la "Legge per l'ulteriore sviluppo del controllo parlamentare sui servizi di informazione e di sicurezza della Federazione" (*Gesetz zur Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes*) del 29 luglio 2009 è stato previsto un esplicito obbligo giuridico di collaborazione del Governo federale con il Comitato parlamentare, i cui poteri conoscitivi risultano considerevolmente ampliati, pur nel rispetto del principio di riservatezza delle informazioni governative ricevute. Sul punto cfr. CAMERA DEI DEPUTATI, *La disciplina dei servizi di informazione in Francia, Germania, Regno Unito e Spagna*, cit.

[28] Cfr. A. PERRONE, *Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica*, cit., spec. 27, e *ivi* i rimandi a E. GRIGLIO, *I poteri di controllo del Parlamento italiano alla prova del bicameralismo paritario*, in *Il Filangieri. Quaderno 2015-2016*, 2017, 199-238; G. FILIPPETTA, *Il controllo parlamentare e le trasformazioni della rappresentanza politica*, in *Osservatorio AIC*, 2/2014, 1-9; N. LUPO, *La funzione di controllo nell'ordinamento parlamentare italiano*, in *Amministrazione in cammino*, 4 marzo 2009.

[29] Cfr. U. GORI, L.S. GERMANI (a cura di), *Information warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, FrancoAngeli, 2011; F. RUGGE, *Mind hacking: la guerra informativa nell'era cyber*, in *Notizie di Politeia*, XXXIV, 132, 2018, 118-127.

[30] Si segnala a tal proposito che il COPASIR ha attivato una "Indagine conoscitiva sulle forme di disinformazione e di ingerenza straniere, anche con riferimento alle minacce ibride e di natura cibernetica", nell'ambito della quale sono stati finora auditi il Direttore del Servizio di polizia postale e delle comunicazioni Ivano Gabrielli (25 maggio 2022), il Capo della segreteria speciale e del servizio cifra del Gabinetto del Ministro Giovanni De Francisco (26 maggio 2022),

ad assicurare il rispetto delle regole democratiche fondamentali della democrazia rappresentativa e dello stato costituzionale[31].

il Sottosegretario alla Presidenza del Consiglio in materia di informazione e di editoria Rocco Giuseppe Moles (1 giugno 2022). Tale indagine conoscitiva fa seguito ad ulteriori audizioni già svolte dal Comitato su analoghi temi, in particolare del Ministro della difesa Lorenzo Guerini, coadiuvato dal Vice Capo di Gabinetto per la Politica militare Gianfranco Annunziata (2 marzo 2022), del Direttore generale dell'Agenzia per la cybersicurezza nazionale Roberto Baldoni (9 marzo 2022), del Presidente del Consiglio dei ministri Mario Draghi (5 aprile 2022), del Direttore dell'Agenzia informazioni per la sicurezza esterna (AISE) Giovanni Caravelli (3 maggio 2022), del Direttore dell'Agenzia informazioni e sicurezza interna (AISI) Mario Parente (11 maggio 2022), del Presidente dell'Autorità per le garanzie nelle comunicazioni (AGCOM) Giacomo Lasorella (18 maggio 2022), del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) Elisabetta Belloni (24 maggio 2022).

[31] G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, cit., spec. 76; v. inoltre sulla compatibilità tra tecnologia informatica e regole democratiche, tra gli altri S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 2004; G. DE MINICO, *Diritti Regole Internet*, in *Costituzionalismo.it*, 2/2011; A. SORO, *Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale*, Milano, Baldini - Castoldi, 2019.