GRUPPO di PISA
Dibattito aperto sul Diritto e la Giustizia Costituzionale

SECONDA EDIZIONE DEL SEMINARIO INTERNAZIONALE DI DIRITTO COMPARATO
«DIRITTO E NUOVE TECNOLOGIE TRA COMPARAZIONE E INTERDISCIPLINARITÀ»
- IN MEMORIA DEL PROF. PAOLO CARROZZA -

SICUREZZA CIBERNETICA E ORGANIZZAZIONE DEI POTERI: SPUNTI DI COMPARAZIONE

ALESSANDRO LAURO

1. *Introduzione: la sicurezza cibernetica come problema di diritto pubblico*

Il rapporto dell'associazione CLUSIT 2021 ha messo in luce che nel 2020, *annus horribilis* della pandemia, gli attacchi informatici nel mondo hanno subito un incremento del 12% rispetto all'anno precedente[1]. La guerra cibernetica è ormai una realtà che impone agli Stati di rafforzare i loro assetti interni legati alla difesa nel cyberspazio[2].

[1] CLUSIT, *Rapporto 2021 sulla sicurezza ICT in Italia*. Sul tema della cibersicurezza all'interno delle Pubbliche amministrazioni v. P.L. MONTESSORO, *Cybersecurity: conoscenza e consapevolezza come prerequisiti dell'amministrazione digitale*, in *Istituzioni del federalismo*, 3/2019, 783 ss.

[2] Estremamente significativo è l'*Executive Order on Improving the Nation's Cybersecurity*, adottato dal Presidente statunitense Biden il 12 maggio 2021. La sez. I dell'atto dà la misura dei contenuti: «*The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal*

Nel diritto internazionale solo alcuni strumenti di *soft-law* si occupano del tema (il più noto è il c.d. *Manuale di Tallin* elaborato dal Centro NATO per la Ciberdifesa[3]) e ciò non sorprende: esiste un'oggettiva difficoltà per lo *ius gentium* nell'applicare le categorie sue proprie ai nuovi fenomeni di belligeranza telematica: si pensi, fra tutti, al tema della riferibilità soggettiva di un atto ostile cibernetico ad uno Stato[4].

Peraltro, nella fluidità della rete senza confini fisici, sfuma la distinzione che intercorre, semplificando, fra attività di difesa – cioè di protezione armata dalle minacce esterne – e politiche di sicurezza – cioè di polizia interna ed esterna, volta a garantire l'incolumità di persone e beni[5]. Il che rende ancora più difficile comprendere sino a che punto potrebbe spingersi il diritto internazionale senza incespicare in ambiti domestici.

A partire dagli anni 10 del 2000 si sono moltiplicati gli atti statali volti a definire le politiche di sicurezza cibernetica: si è trattato, inizialmente, di atti programmatici, non tradotti in vere e proprie modifiche legislative, sviluppati soprattutto in ambito NATO[6].

È stato nel livello eurounitario che tale tendenza ha conosciuto un salto di qualità con il passaggio da strumenti di *soft law* a veri e propri atti legislativi che hanno disegnato la cornice fondamentale della disciplina degli Stati membri.

Il presente scritto propone di soffermarsi su alcuni aspetti di questo diritto di derivazione sovranazionale ed in particolare su come il suo recepimento nei vari Paesi offra un interessante spaccato relativo alla configurazione dei poteri pubblici in relazione ad una delle più pressanti sfide del tempo presente.

Ovviamente, non si intende (né si potrebbe) sminuire la pur centrale problematica di come debba essere conciliata l'attività di cibersicurezza con il rispetto e la garanzia dei diritti e delle libertà nell'era digitale, anche essa oggetto delle preoccupazioni del legislatore unionale[7].

Tuttavia, si ritiene che l'analisi del versante prospettato – anche perché forse meno frequentata nella riflessione dottrinale – possa offrire qualche spunto ulteriore alla

---

Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector».

[3] M.N. SCHMITT (a cura di), *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2016.

[4] In tema v. H. DINNIS, *Cyberwarfare and the laws of war*, New York, 2014.

[5] Sul punto v. più ampiamente G. DEVERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e dell'emergenza normalizzata,* in *Rivista AIC*, 4/2019, 67 ss. L'A. in particolare osserva che «[l'] endiadi sicurezza/difesa in termini militari tradizionali copre oggi una parte circoscritta del complesso ambito in cui gli interessi degli stati possono essere pregiudicati da aggressioni e ostilità di varia natura provenienti da interessi esterni. La conflittualità coinvolge l'informazione e l'attività diplomatica tradizionale, i rapporti economici, la competizione tecnologica – e in particolare i progressi dell'intelligenza artificiale e la gestione dei dati -l 'attività di *intelligence*» (68-69).

[6] Fra i vari documenti: nel Regno Unito *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digitalized World* (2011); negli Stati Uniti la *Strategy for Operating in Cyberspace* del *Department of Defense* (2011); in Canada la *Canada's Cyber Security Strategy* (2010).

[7] Si pensi al tema dei *data breaches* e alle procedure previste dal Regolamento 2016/679 (GDPR) per contenerne gli effetti pregiudizievoli sui privati (art. 33 GDPR). Sul tema v. L. SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), *Costituzioni e sicurezza*, Santarcangelo di Romagna, 2013, 425 ss.

riflessione costituzionalistica sul tema[8].

In particolare, dopo aver richiamato brevemente l'attuale disciplina europea, l'analisi si concentrerà su tre questioni nodali della sicurezza informatica: l'individuazione delle autorità nazionali competenti alla luce della normativa unionale; il rapporto di collaborazione fra pubblico e privato nelle politiche di *cybersecurity*; l'intarsio fra i nuovi assetti di poteri nella materia e i sistemi costituzionali esistenti.

È possibile già anticipare che in tutti e tre questi ambiti emergerà, in maniera ricorrente, la natura altamente deformalizzata delle modalità con cui si svolgono i rapporti istituzionali concernenti le politiche di sicurezza nel ciberspazio.

2. *Cenni all'evoluzione europea della disciplina*

L'attenzione europea al tema della sicurezza informatica si sviluppa sostanzialmente in due macrofasi.

Una prima, agli inizi degli anni 2000, consegue alla più estesa disciplina del mercato unico digitale[9]. In questa fase, con il regolamento CE n. 460/2004, viene istituita un'apposita Agenzia dedicata alla sicurezza delle reti[10].

Una seconda fase (attualmente in via di ulteriore sviluppo) segue invece la crisi economico-finanziaria del 2008-2010, e prende le mosse dalla Strategia europea elaborata dalla Commissione e presentata nel febbraio 2013. Tale atto richiede espressamente agli Stati membri di elaborare una propria strategia nazionale in accordo con le linee guida comuni.

Di lì a poco l'atto di indirizzo sarà seguito dal regolamento UE n. 526/2013 che, innovando il precedente regolamento, istituisce l'ENISA – l'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione – riplasmando la precedente Agenzia secondo più avvedute esigenze di coordinamento delle attività in materia di sicurezza informatica e con una maggiore consapevolezza circa la natura strategica di tale materia nello sviluppo economico.

Ma nei confronti degli Stati membri – e per l'ordinamento "multilivello" dell'Unione – il passaggio fondamentale avviene con la direttiva europea 2016/1148 (c.d. Direttiva "NIS", *Network and Information Security*), all'origine degli interventi normativi nazionali di cui ci si occuperà nel prosieguo, destinata a fissare un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.

---

[8] Sul tema della sicurezza nel diritto costituzionale v. G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012; T. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Bologna, 2010; A. TORRE, *Costituzioni e sicurezza*, cit.

[9] In questa fase vengono adottate, fra le altre, le direttive 2002/21/CE che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica e 2002/58/*CE* relativa al trattamento dei dati personali e alla tutela della vita privata. Nel giugno 2004 il Consiglio Europeo chiede peraltro la preparazione di una Strategia globale per le infrastrutture critiche, culminata nella direttiva 2008/114/CE (si veda il Considerando n. 1 della stessa).

[10] Adottata sul fondamento dell'art. 95 del trattato sulla Comunità europea (oggi art. 114 TFUE), sull'instaurazione e il funzionamento del mercato interno. Sull'evoluzione della disciplina europea cfr. C. CENCETTI, *Cybersecurity: Unione europea e Italia. Prospettive a confronto,* Roma, 2014, 21 ss.

Tale atto non è peraltro restato isolato, inserendosi in una più ampia cornice di misura dettate dal legislatore europeo per rafforzare la difesa di interessi, reti e beni strategici per gli Stati membri e per l'Unione nel suo complesso, concretizzatasi di recente con l'adozione del Regolamento 2019/881 sul potenziamento dell'ENISA e la creazione di un sistema di certificazione della cibersicurezza[11]. Tali indirizzi sono peraltro ancora in fase di evoluzione[12].

Accanto all'emanazione di questi atti, la stessa ENISA ha fornito un volume non indifferente di linee guida e raccolta di buone prassi in materia di sicurezza cibernetica.

Il risultato ultimo della legislazione unionale segue un andamento tipico – se è concesso dire – del diritto europeo[13]: attorno all'autorità europea (l'ENISA, in questo caso) si crea una rete di autorità nazionali[14] che debbono coordinarsi con questa e sono dotate di poteri di vigilanza, di sanzione e di natura talvolta mista, autorizzatoria e certificatoria. All'interno degli ordinamenti statali è possibile poi individuare delle autorità settoriali, cui è devoluta la competenza per i segmenti di attività economiche e sociali da loro presieduti. Accanto alla rete propriamente amministrativa, si costituisce anche una rete "tecnica" composta dai CSIRT nazionali (i Gruppi di intervento per la sicurezza informatica in caso di incidente)[15].

Insomma, se vista dall'alto, l'architettura della *governance* potrebbe far assomigliare il settore secur-cibernetico al dominio di una nuova generazione di autorità indipendenti.

Si tratta, però, di un'illusione prospettica o, quanto meno, di un fotogramma che non si presta a generalizzazioni, come dimostra la grande variabilità delle discipline nazionali di attuazione della direttiva NIS.

3. *La scelta delle autorità nazionali NIS: un panorama significativamente variegato tra tecnica, amministrazione e politica*

La natura tipicamente "trasversale" delle politiche di cibersicurezza e la loro conseguente difficile collocazione nel quadro ordinamentale emerge nitidamente allorché ci si focalizzi sulla natura delle autorità NIS individuate dai singoli Stati.

In effetti, possiamo verificare che l'attuazione è stata estremamente variegata, in ciò rilevandosi anche specifiche scelte di indirizzo politico-amministrativo interne agli Stati, riassumibili sostanzialmente in tre ipotesi.

---

[11] Tale regolamento sostituisce il citato regolamento UE n. 526/2013.

[12] Il 16 dicembre 2020 è stata infatti presentata una nuova proposta di direttiva detta NIS-2, volta ad ampliare i settori di intervento della precedente regolazione. Essa è stata contestualmente accompagnata da un nuovo documento programmatico europeo per la cibersicurezza intitolato "*La strategia dell'UE in materia di cibersicurezza per il decennio digitale"*.

[13] Si pensi alla rete delle Autorità per la concorrenza istituita con il regolamento n. 1/2003, nonché alle forme di "cooperazione e coerenza" previste per le Autorità di controllo in materia di dati personali dagli artt. 60 e ss. GDPR.

[14] L'art. 8 della Direttiva NIS prevede, da un lato, le autorità nazionali e, dall'altro, i "punti di contatto unici", vale a dire gli organismi di collegamento con l'Agenzia e gli altri Stati.

[15] Tali gruppi sono previsti dall'art. 9 della Direttiva NIS.

La prima è consistita nell'affidamento del ruolo ad Autorità amministrative indipendenti o, comunque, ad organismi tecnici di regolazione. Così, ad esempio, è successo in Lussemburgo, dove l'autorità per le telecomunicazioni è stata investita del ruolo, affiancata dalla sola autorità per i mercati finanziari per l'ambito di competenza[16]. Nel Regno Unito *ante Brexit* il ruolo di autorità nazionale era invece assegnato all'*Information Commissioner*[17]*,* alle cui cure già erano affidati i compiti discendenti dalla normativa europea sulla privacy.

La seconda opzione ha invece innestato poteri, doveri e competenze derivanti dalla direttiva NIS direttamente su apparati ministeriali o enti da questi dipendenti. Si tratta, in realtà, della scelta più frequente all'interno degli ordinamenti statali[18], sebbene poi l'identificazione del dicastero dipenda in buona parte dal numero di autorità settoriali individuate, ma – in fondo – anche dall'interpretazione che i legislatori nazionali danno alle politiche di cibersicurezza. Così facendo, in alcuni casi è l'aspetto infrastrutturale ad emergere (a Malta e in Irlanda il compito spetta al Ministero delle comunicazioni), in altri è il profilo prettamente legato alla sicurezza (in Germania è il Ministero degli Interni), in altri ancora è l'idea della lotta all'illegalità informatica (nei Paesi Bassi è il ministro della Giustizia).

Da ultimo, alcuni Paesi hanno scelto di conferire direttamente al capo del Governo o ad un'agenzia a questi sottoposta le funzioni di autorità nazionale NIS (così in Belgio[19], Francia[20], Portogallo[21], Austria[22]).

Questa diversità di trasposizione rivela la natura ibrida della cibersicurezza: si tratta di una questione tecnica da lasciare ad entità esperte? È una funzione amministrativa di polizia che i pubblici poteri devono esercitare a livello virtuale come nel mondo fisico? Oppure è una questione più densamente politica, che attiene alle strategie di fondo dell'azione statuale, ponendosi quindi al cuore stesso dell'indirizzo politico?

I contenuti della direttiva NIS – a ben vedere – trattano tutti e tre gli aspetti,

---

[16] Secondo la *loi du 29 mai 2019,* Le autorità competenti sono la *Commission de surveillance du secteur financier* e l'*Institut luxembourgeois de régulation,* ciascuno per il proprio settore di regolazione (i mercati finanziari e le telecomunicazioni).

[17] Cfr. *The Network and Information Systems Regulations 2018*, sez. 3.

[18] Questi alcuni dei Paesi che hanno individuato l'autorità nazionale NIS in un ministero o in un apparato alle dirette dipendenze di questo: Germania (Ministero dell'Interno); Spagna (Ministero dell'Interno, Ministero dell'Economia e Ministero della difesa); Paesi Bassi (Ministero della Giustizia); Malta (Ministero delle comunicazioni); Irlanda (Ministero per la comunicazione, l'azione climatica e l'ambiente).

[19] La *loi du 7 avril 2019* ha rinviato ad un *arrêté royal* l'individuazione dell'autorità nazionale. Tale atto (adottato il 18 luglio 2019) ha conferito il ruolo al *Centre pour la Cybersécurité Belgique*, che è posto alle dirette dipendenze del Primo Ministro (*arrêté royal* del 10 ottobre 2014).

[20] In questo caso il tema della cibersicurezza è stato integrato direttamente nel *Code de la défense* dalla *loi* n. 2015-917 (*loi actualisant la programmation militaire 2015-2019*)*,* che ha inserito l'articolo L. 1332-6-1, il quale attribuisce al Primo Ministro il potere di fissare le regole necessarie alla protezione dei sistemi informatici di interesse pubblico. L'autorità nazionale è rappresentata dall'*Agence Nationale de la sécurité des systèmes d'information,* che dipende dal Servizio generale della difesa e della sicurezza nazionale del Primo Ministro.

[21] Si tratta del *Centro Nacional de Cibersegurança* che, ai sensi dell'art. 7 della *lei* 46/2018, opera nell'ambito del *Gabinete Nacional de Segurança*, a sua volta sotto la direzione del Primo Ministro.

[22] I compiti del *Bundeskanzler* sono evidenziati dalla *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen* (§4). Egli è assistito dal *Büro für Strategische Netz- und Informationssystemsicherheit*.

mettendo l'accento tanto sul versante tecnico (più precisamente individuato nella rete europea e nei punti di contatto: art. 9), quanto sul versante amministrativo (con i poteri riconosciuti alle autorità nazionali: art. 8) ed anche – seppure in maniera meno incisiva – sul lato politico, domandando l'adozione di specifiche strategie nazionali (art. 7).

Tuttavia, è chiaro che l'afflusso di nuovi, significativi poteri di derivazione europea, che attingono interessi fondamentali dello Stato (la sicurezza e la difesa), non potesse lasciare indifferenti le strutture di governo[23], né si sarebbe potuta realizzare silenziosamente la fuoriuscita di queste facoltà dall'orbita di una loro titolarità politica. Sicché non sorprende che, da un lato, il ricorso alle autorità indipendenti sia stato in definitiva ridotto e, dall'altro, i vertici del potere esecutivo siano stati direttamente coinvolti nella definizione delle architetture nazionali di cibersicurezza, soprattutto ove già detenessero competenze in materia di sicurezza e servizi segreti. A questo proposito (e vi si ritornerà anche *infra*, par. 6.3) è particolarmente significativo l'esempio dell'Italia.

4. *Segue: l'altalenante legislazione italiana nella materia*

La recezione da parte dell'ordinamento italiano delle novità maturate a livello europeo merita una menzione a parte, se non altro per l'andamento altalenante che l'ha caratterizzata.

In effetti, la prima fonte di attuazione (o, meglio, di anticipazione) degli orientamenti europei è stata la legge 7 agosto 2012 n. 133 che, intervenendo sulla legge 3 agosto 2007 n. 124 sulla sicurezza della Repubblica, ha posto il Presidente del Consiglio al vertice delle politiche nazionali di protezione cibernetica e sicurezza informatica[24]. In questo modo il tema della cibersicurezza veniva concretamente introiettato nella dinamica della forma di governo nel nostro Paese. A seguito della novella, e sul fondamento della nuove norme introdotte, il Presidente del Consiglio dettava una strategia nazionale sul modello di quanto da lì a poco avrebbe fatto formalmente anche l'Unione Europea[25].

La direttiva NIS, invece, trova applicazione in Italia con il d.lgs. 18 maggio 2018 n. 65, adottato – si noti – dal Governo Gentiloni, dimissionario a seguito delle elezioni del marzo 2018 (dunque limitato, nella sua attività, agli affari correnti): non a caso vi è stata una ricezione minimale della normativa, poi integrata nel 2019. In particolare, il decreto legislativo, pur riconoscendo al Presidente del Consiglio il potere di adozione

---

[23] Cfr. A. COLELLA, *Analisi comparata delle architetture decisionali in materia di sicurezza cibernetica dei paesi dell'area euro-occidentale*, in A. TORRE, *Costituzioni e sicurezza*, cit., 439 ss.

[24] L'art. 1, comma 3 bis, come aggiunto nel 2012 recita: «Il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali». Sull'impianto generale della legge n. 124/2007 v. il commento di T. GIUPPONI, *Servizi di informazione e segreto di Stato nella legge n. 124/2004*, in AA.VV., *Studi in onore di Luigi Arcidiacono*, IV, Torino, 2010, 1677 ss.

[25] DPCM 24 gennaio 2013: "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale"

della strategia nazionale (art. 6), delegava a vari Ministeri la competenza settoriale in materia cibernetica (art. 7). Tale scelta di *governance* è stata in parte – e a dire il vero surrettiziamente – rivista con il successivo d.l. 21 settembre 2019 n. 105, che ha attribuito al Presidente del Consiglio in Italia importanti poteri (sia normativi[26], che preventivi[27], ma anche sanzionatori[28]) al fine di garantire un livello elevato di sicurezza delle reti in conformità con la direttiva NIS. In particolare il decreto da ultimo citato ha creato il "perimetro di sicurezza nazionale cibernetica", affidando al capo del Governo la vigilanza degli operatori pubblici e privati ivi inclusi e fornendogli vari poteri di difesa in caso di crisi cibernetica[29].

Nel 2021, il Governo Draghi ha adottato un nuovo decreto-legge (14 giugno 2021 n. 82) con cui – oltre a riaffermare l'architettura nazionale di sicurezza cibernetica con al vertice il Presidente del Consiglio – viene creata l'Agenzia Nazionale per la cibersicurezza nazionale (sotto l'egida del capo del Governo), a cui si affidano le funzioni di Autorità nazionale ai fini della direttiva NIS, superando l'assetto stabilito nel 2018 e riportando coerenza fra i vari interventi succedutisi.

5. *Consulenza e collaborazione nella definizione dell'indirizzo politico: alleanze strategiche fra pubblico e privato*

Il secondo punto di analisi si focalizza invece sulla collaborazione fra pubblico e privato nell'ambito delle politiche di *cybersecurity*[30].

Conviene qui partire da una premessa: secondo il costituzionalismo europeo[31], nel mondo fisico la difesa e la sicurezza sono funzioni che appartengono tipicamente allo Stato (due delle c.d. *fonctions régaliennes*), come attributi della sua sovranità e dell'esercizio del suo potere sui consociati[32]. Sul versante interno, la sicurezza è dunque

---

[26] L'art. 1, comma 2, del decreto-legge prevede l'adozione di vari DPCM con il compito di definire un ampio spettro di nozioni, quali i soggetti da includere nel perimetro, i rischi, gli obblighi tecnici di prevenzione, le procedure di notificazione ecc. Il Consiglio di Stato, nel suo parere n. 983/2020 del 26 maggio 2020 ha affermato che a detti DPCM debba «senz'altro riconoscersi natura regolamentare».

[27] Art.1, comma 6, lett. c).

[28] Art. 1, comma 12. Sono irrogabili sanzioni anche a carico di enti pubblici. Secondo il *Dossier dell'11 novembre 2019* predisposto dai Servizi Studi di Camera e Senato per l'esame del decreto (p. 28-29), si tratta del secondo caso in cui la legislazione prevede poteri amministrativi di carattere sanzionatorio in capo alla Presidenza del Consiglio (l'altro caso è previsto dall'art. 3-bis della legge 6 marzo 2001 n. 64 in capo all'Ufficio centrale per il Servizio Civile costituito presso la Presidenza).

[29] L'art. 5 prevede in particolare un potere di "spegnimento", con cui si ordina la disattivazione di prodotti, apparati o snodi infrastrutturali inseriti nel perimetro ed esposti a fragilità in caso di grave rischio nazionale: una sorta di virtuale "ponte levatoio" che si richiude per proteggere la rete nel suo complesso.

[30] Sul tema della compartecipazione dei privati alla definizione delle politiche pubbliche v. S. CASSESE, *La partecipazione dei privati alle decisioni pubbliche. Saggio di diritto comparato*, in *Rivista trimestrale di diritto pubblico*, 1/2007, 13 ss.

[31] Come è noto, la prospettiva è diversa negli Stati Uniti, dove il Secondo Emendamento stabilisce il diritto all'autodifesa tramite il possesso di armi, anche se pure sul punto si sono registrate oscillazioni dottrinali: cfr. D.B. KATES JR., *The Second Amendment and the Ideology of Self-Protection,* in *Constitutional Commentary*, 9/1992, 87 ss.

[32] Cfr. la nota teoria di M. WEBER, *Wirtschaft und Gesellschaft*, Tubinga, 1922 sul monopolio della coercizione fisica in capo allo Stato, così come l'enunciazione da parte di G. JELLINEK, *Allgemeine*

appannaggio dell'autorità pubblica[33] e solo in specifici casi e a particolari condizioni essa può essere parzialmente "privatizzata"[34].

Nel ciberspazio non è così, per ragioni ampiamente note, a partire dal fatto che la rete internet è nata come infrastruttura privata, fino alla constatazione contemporanea della "confusione dei poteri" che si realizza nel mondo virtuale, dominato da *puissances privées* e non da istituzioni pubbliche[35].

Non è dunque un caso che, sin dai primi documenti programmatici nella materia, il riferimento alla collaborazione fra autorità e privati nella realizzazione delle politiche di sicurezza informatica sia sempre stato presente[36] e tale necessità venga ribadita e promossa negli atti europei successivi[37]. Peraltro, il Libro verde sul partenariato pubblico-privato del 2004 arriva proprio negli anni in cui si redigevano i primi atti europei in materia di cibersicurezza.

Ed in effetti il prototipo di ibridazione fra attività d'impresa privata e interessi pubblici nella materia è rappresentato dal caso americano di In-Q-Tel, società privata che opera nel settore della difesa cibernetica ed ha come unico cliente e partner commerciale il Governo degli Stati Uniti[38].

La collaborazione pubblico-privata nel campo cibernetico assume varie forme e l'ENISA cura appositi atti di *soft-law* che codificano le "buone prassi", al fine di meglio direzionare gli sforzi congiunti[39].

Alcune esperienze meritano particolare attenzione, anche perché si assiste non ad una semplice cooperazione – in particolare finanziaria, sul modello della *joint venture* – al fine di sviluppare nuove tecnologie (il che rappresenta la forma più classica di

---

Staatslehre, Berlino, 1900 dello Stato Si veda per l'Italia, da ultimo, la sent. n. 236/2020 sulla competenza regionale a disciplinare "controlli di vicinato". Peraltro, in sede di promulgazione di una modifica al codice penale concernente la legittima difesa (legge 26 aprile 2019 n. 36), il Presidente Mattarella scrisse una lettera ai Presidenti delle Camere e del Consiglio sottolineando «la primaria ed esclusiva responsabilità dello Stato nella tutela della incolumità e della sicurezza dei cittadini, esercitata e assicurata attraverso l'azione generosa ed efficace delle Forze di Polizia» come "corporazione" dotata di un potere di dominazione originario.

[33] Si veda per l'Italia, da ultimo, la sent. n. 236/2020 sulla competenza regionale a disciplinare "controlli di vicinato". Peraltro, in sede di promulgazione di una modifica al codice penale concernente la legittima difesa (legge 26 aprile 2019 n. 36), il Presidente Mattarella scrisse una lettera ai Presidenti delle Camere e del Consiglio sottolineando «la primaria ed esclusiva responsabilità dello Stato nella tutela della incolumità e della sicurezza dei cittadini, esercitata e assicurata attraverso l'azione generosa ed efficace delle Forze di Polizia».

[34] Si pensi al regime delle autorizzazioni di polizia in materia di armi previsto dagli artt. 40 e ss. del TULPS.

[35] Sui poteri privati nella rete v. da ultimo M. BETZU, *Libertà di espressione e poteri privati nel cyberspazio*, in *Diritto costituzionale*, 1/2020, 117 ss.

[36] Cfr. i *Considerando* n. 11 e 22 del Regolamento CE n. 460/2004.

[37] V. COMMISSIONE EUROPEA, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro,* Bruxelles, 2013, 5; nonché il *Considerando* n. 35 della Direttiva NIS e il suo art. 7, comma 1, lett. c), il quale impone espressamente agli Stati di prevedere nelle Strategie nazionali misure di collaborazione fra settore pubblico e privato.

[38] In-Q-Tel è una *company* formalmente autonoma e indipendente, ma finanziata dalla CIA per sviluppare e finanziare tecnologie informatiche al di fuori del perimetro propriamente istituzionale. Cfr. J.T. REINERT, *In-Q-Tel: The Central Intelligence Agency as Venture Capitalist*, in *Northwestern Journal of International Law & Business*, 2013, 678 ss.

[39] Cfr. ENISA, *Good Practice Guide on Cooperatve Models for Effective Public Private Partnershipss,* 2011.

intervento collaborativo del pubblico), ma ad esperimenti di alta consulenza e di concertazione nell'elaborazione dell'indirizzo governativo.

A tal proposito, viene in rilievo il caso della Germania, dove è stato istituito un *National Cybersicherheitsrat*che vede la partecipazione, oltre che di vari Ministri e di rappresentanti dei *Länder*[40], di rappresentanti delle imprese tedesche. Si tratta di un organo da carattere semi-informale – la sua istituzione è infatti prevista esclusivamente dalla strategia nazionale per la cibersicurezza del 2011[41], dunque da un atto di *soft law* – con compiti di analisi, pianificazione ed indirizzo nella materia[42]. Si tratta indubbiamente di un esperimento notevole, poiché l'organo di governo si apre al raccordo con soggetti privati del mercato, confermando così la constatazione iniziale: la sicurezza delle reti non è né una questione meramente statale, né una questione privata, ma una sfida per un intero "sistema Paese"[43]. Peraltro, è da segnalare l'esistenza di un altro organismo che coopera a stretto contatto con il Consiglio di cibersicurezza: l'*UP Kritis*, che rappresenta un partenariato pubblico-privato per la difesa delle infrastrutture critiche[44].

Anche in Francia si è realizzato un tentativo di raccordo fra il pubblico e privato nella materia: si tratta del *Groupement d'Intérêt Public Action contre la Cybermalveillance,* entità di diritto pubblico[45] che raccoglie rappresentanti delle amministrazioni ed esponenti della società civile sia a fini di analisi e di elaborazione di proposte normative, sia per progettazione e finanziamento di attività miste nel campo della difesa cibernetica. Il gruppo, nato con la Strategia nazionale del 2015, raccoglie oggi circa 50 aderenti fra Agenzie governative e entità private di varia natura (associazioni di consumatori, sindacati, imprese)[46].

In Italia per il momento la collaborazione con i privati si concretizza nella possibilità di creare *joint venture,* ipotesi inizialmente prevista dal disegno di legge di bilancio per il 2021 con la costituzione, sotto forma di fondazione, di un Istituto italiano

---

[40] Nel 2009 in Germania si è infatti introdotto l'art. 91 c nella *Grundgesetz*, relativo ai sistemi di informazione e alla cooperazione fra Federazione e *Länder* in materia di tecnologie della comunicazione e loro standard di sicurezza.

[41] Cfr. BUNDESMINISTERIUM DES INNERN, *Cyber-Sicherheitsstrategie für Deutschland*, Berlino, 2011, 9.

[42] *Ivi*, 10: «*Der Nationale Cyber-Sicherheitsrat soll die präventiven Instrumente und die zwischen Staat und Wirtschaft übergreifenden Politikansätze für Cyber-Sicherheit koordinieren. Die Arbeit des Nationalen Cyber-Sicherheitsrates ergänzt und verzahnt die Aufgaben mit der IT-Steuerung Bund und dem IT-Planungs-rat im Bereich der Cyber-Sicherheit auf einer politisch-strategischen Ebene*».

[43] Si riprende qui un termine che designa una delle Direzioni generali del Ministero degli Affari esteri italiano e che rappresenta l'esigenza di promuovere "tutte le componenti [del Paese]" (art. 5, comma 5, lett. A del D.P.R. 19 maggio 2010 n. 95 sulla riorganizzazione del Ministero).

[44] L'iniziativa – che veda una stretta collaborazione fra Governo ed imprese operatrici nei settori delle infrastrutture critiche – ha preso le mosse dall' *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen,* approvato nel 2007. Nel 2013 il piano è stato aggiornato con la creazione della cooperazione permanente, recepita nel documento *Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen-Grundlagen und Ziele*, disponibile all'indirizzo https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Fortschreibungsdokument.html;jsessionid=6736030FF6DEAD9F1DB8A707C7EB9FA6.1_cid355?nn=1902622 .

[45] Il *groupement d'intérêt public* è una "persona morale di diritto pubblico", creata per convenzione fra più soggetti pubblici o fra un soggetto pubblico e soggetti privati: v. l'art. 98 della legge n. 2011-525 del 17 maggio 2011.

[46] Si v. il sito https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/membres.

per la cibersicurezza, ma poi eliminata nel corso della lettura parlamentare[47]. Con il d.l. n. 82/2021, è alla nuova Agenzia per la cibersicurezza nazionale che viene devoluto il compito di interfacciarsi fattivamente anche con operatori privati[48], mentre al Comitato interministeriale pure previsto dalla nuova normativa – di cui si parlerà nel paragrafo seguente – spetta l'adozione di iniziative necessarie per favorire la collaborazione con il settore privato (art. 4, comma 2, lett. c).

Se questi esempi dimostrano come sfumi, nell'universo digitale, la garanzia della sicurezza che nel mondo fisico gli ordinamenti europei riconoscono indiscutibilmente allo Stato, non si può di certo affermare che vi sia una ritrazione dei pubblici poteri. Anzi, i singoli Paesi hanno dovuto farsi carico delle novità tecniche e giuridiche, organizzando così nuovi apparati in seno agli assetti di governo.

6. *Politiche di* cybersecurity *e rapporti fra organi costituzionali*

Come già accennato, il tema della sicurezza cibernetica ha imposto un ripensamento nella distribuzione di poteri e competenze fra vari plessi delle Amministrazioni statali. È interessante quindi osservare come questa nuova sfida ordinamentale si sia tradotta nel livello supremo dei poteri statali, cioè come essa abbia avuto impatto sull'assetto degli organi costituzionali. Ciò si rivela ancor più interessante ove si consideri la sovrapposizione e l'interazione fra gli assetti dei poteri di guerra e difesa e i nuovi poli decisionali consacrati alla vigilanza del ciberspazio.

A questo scopo, allora, sono tre i punti di osservazione che si propongono: a) la creazione di organi infragovernativi consacrati alle politiche di cibersicurezza; b) la questione del controllo parlamentare; c) una riflessione più specifica sulla scelta che potremmo definire "primo-ministeriale" attuata, in particolare, in Italia e in Francia.

6.1. *Organi infragovernativi*

Una tendenza che si registra in vari ordinamenti europei è la creazione di organi interni al Governo, precipuamente dedicati al tema della sicurezza cibernetica.

L'idea che comitati ristretti rispetto all'organo governativo collegiale si dedichino espressamente ai temi della cibersicurezza sembra sottintendere, in particolare, che l'attività governativa non si esplicherà tanto attraverso atti generali d'indirizzo o proposte legislative specifiche, quanto piuttosto attraverso direttive e indirizzi connotati – oltre che da un comprensibile grado di riservatezza – da un significativo tasso di informalità o, forse sarebbe meglio dire, di "informità"[49].

---

[47] Cfr. A. DI CORINTO, *Scontro nella maggioranza blocca l'Istituto italiano di cybersicurezza: tutti i retroscena*, in *Agendadigitale.eu*, 18 novembre 2020.

[48] Cfr. art. 7, comma 1, lett. s) e t).

[49] Con ciò intendendo l'assenza di atti vincolanti e la fuoriuscita degli indirizzi governativi nella materia dalle forme tipiche assunte dagli atti dell'Esecutivo.

Ad esempio, in Spagna, con la Strategia nazionale del 2013, è stato creato il *Comité especializado de Ciberseguridad* (divenuto poi *Consejo Nacional de Ciberseguridad*) presieduto dal Segretario di Stato con delega alla sicurezza informatica. Si tratta di un organo di supporto al *Consejo Nacional de Seguridad*, a sua volta "commissione delegata del Governo"[50] incaricata di assistere il Presidente del Governo nella politica di sicurezza[51]. Tale comitato, nato per via informale, ha trovato un'identificazione legislativa indiretta con l'atto di attuazione della direttiva NIS, il Real Decreto-Ley 12/2018[52].

In Italia il modello della "comitologia" interministeriale[53] ha riscontrato un buon successo anche nell'ambito del ciberspazio: prima, con la legge n. 133/2012 e in seguito con il c.d. "decreto-legge perimetro", il Comitato interministeriale per la sicurezza della Repubblica – inserito nell'ordinamento dei servizi segreti – si è visto ampliare le sue competenze per abbracciare le sfide cibernetiche. Nel 2021, il decreto-legge n. 82 ha creato un nuovo Comitato interministeriale *ad hoc* (CIC: Comitato interministeriale per la cibersicurezza), cui sono state attribuite tutte le competenze in materia appartenenti al CISR – con una sola eccezione[54] – insieme alla definizione di un ruolo strategico di indirizzo.

Un ulteriore esempio è rappresentato dal *Conselho Superior de Segurança do Ciberespaço,* stabilito in Portogallo dall'art. 5 della legge n. 46/2018 attuativa della direttiva NIS. Si tratta di un organo a composizione esclusivamente pubblicistica, in cui oltre a Ministri ed esponenti delle Amministrazioni statali interessate, vengono coinvolti alti dirigenti di imprese pubbliche, rappresentanti dei Governi delle regioni autonome delle Azzorre e di Madeira e – è interessante sottolinearlo – da due deputati designati dall'Assemblea parlamentare. Anche in questo caso tale consiglio assiste il Primo Ministro cui sono demandati i compiti in materia di cibersicurezza e la legge indica le varie competenze dell'organo, chiamato in particolare a verificare l'attuazione della strategia nazionale, ma anche a proporre "decisione di carattere programmatico relative alla definizione ed esecuzione della Strategia Nazionale"[55]. Il Consiglio deve inoltre approvare, con cadenza annuale, una relazione sull'effettiva attuazione della Strategia Nazionale, documento che deve poi essere inviato al Parlamento lusitano entro il 31 marzo di ciascun anno[56].

---

[50] Ai sensi dell'art. 6 della legge 50/1997 sul Governo.

[51] Cfr. l'art. 17 della legge 36/2015 del 28 settembre.

[52] In particolare, l'art. 9, comma 2, recita: «*El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes*».

[53] In tema v. D. CODUTI, *I Comitati interministeriali tra affermazione e crisi del "governo maggioritario"*, Napoli, 2012.

[54] Il d.l. 82/2021 esclude infatti la competenza prevista dall'art. 5 de d.l. n. 105/2019 (il c.d. potere di spegnimento), che rimane appannaggio del Comitato interministeriale per la sicurezza della Repubblica.

[55] Art. 6, comma 1, lett. e) della legge n. 46/2018.

[56] Art. 6, comma 2 della legge n. 46/2018.

6.2. *Il controllo parlamentare*

L'esempio portoghese da ultimo citato si rivela interessante nella misura in cui mette in evidenza un ulteriore profilo legato all'organizzazione dei poteri cibersecuritari: il rapporto fra l'Esecutivo (cui questi poteri appartengono) e gli organi parlamentari.

Si tratta di un tema le cui precedenti declinazioni (ad esempio sui poteri di guerra, sul controllo dei servizi segreti e sulla tutela degli interessi fondamentali dello Stato) hanno rappresentato uno snodo classico della riflessione costituzionalistica[57]; oggi, però, la questione collocata nel ciberspazio richiede una certa "attualizzazione" dovuta almeno a due fattori. Da un lato, la velocità e la pervasività degli attacchi cibernetici (dall'interno o dall'esterno) richiede una prontezza che mal si attaglia alle procedure classiche di coinvolgimento delle assemblee parlamentari[58]. Dall'altro lato, per garantire la sicurezza delle reti informatiche – il che, oggi, significa assicurare il buon andamento dell'economia e del mercato, l'erogazione dei servizi pubblici, lo svolgimento ordinato di vari momenti della vita sociale – è necessaria un'estesa attività di polizia, preventiva e continuativa, per la quale è impensabile un controllo puntuale da parte dei Parlamenti. Ecco che però si crea un circolo (se non "vizioso") altamente problematico: se sono necessari poteri sempre più ampi a favore degli Esecutivi per confrontarsi con le sfide del presente, occorre che questi poteri trovino dei contraltari e dei controlli nello stesso circuito democratico-rappresentativo[59].

L'interrogativo di come garantire un maggior coinvolgimento dei consessi parlamentari nella definizione delle politiche "*cyber*" si è posto, tant'è che l'Unione Inter-Parlamentare ha adottato il 1 aprile 2015 ad Hanoi, nel corso della sua 132ema Assemblea, una risoluzione intitolata "*CYBER WARFARE: A SERIOUS THREAT TO PEACE AND GLOBAL SECURITY*"[60]. Fra le varie raccomandazioni dirette ai Parlamenti, si evidenziano in particolare i richiami ai poteri di controllo e di informazione delle Assemblee, per meglio comprendere il fenomeno e monitorare l'attuazione e l'avanzamento delle legislazioni nazionali. Un invito a parte è formulato nel senso di

---

[57] Cfr. G. DE VERGOTTINI, *Guerra e Costituzione: nuovi conflitti e sfide alla democrazia*, Bologna, 2004; A. VEDASCHI, À la guerre comme à la guerre? *La disciplina della guerra nel diritto costituzionale comparato,* Torino, 2007. Sul tema della sicurezza nazionale riconnessa in particolare ai segreti di Stato v. in prospettiva comparata D. COLE, F. FABBRINI, A. VEDASCHI (a cura di), *Secrecy, National Security and the Vindication of Constitutional Law*, Londra, 2013. Per l'Italia v. E. RINALDI, Arcana imperii. *Il segreto di Stato nella forma di governo italiana*, Napoli, 2016.

[58] In un inchiesta parlamentare della Commissione Difesa del *Bundestag* emerge netta la considerazione che "nel ciberspazio si confondo i confini fra attacco e difesa": cfr. *Protokoll der Öffentliche Anhörung Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlaments-vorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internatio-naler Normen,* 15 marzo 2021.

[59] Cfr. le limpide considerazioni di E. RINALDI, Arcana imperii, cit., 156: «Quando le condizioni di esistenza dello Stato-comunità sono minacciate si impone, del resto, una concentrazione in capo al Presidente-Ministro della (responsabilità relativa alla) direzione unitaria della vita politica dello Stato e della gestione operativa; a tale concentrazione di potere dovrebbe tuttavia essere speculare un controllo penetrante del Parlamento, ché la possibilità di demandare interamente alla responsabilità politica governativa il compito di riequilibrare il potere esercitato dovrebbe essere correlata alla possibilità che si svolga un dibattito parlamentare».

[60] Disponibile all'indirizzo http://archive.ipu.org/conf-e/132/Res-1.htm.

sovrintendere all'allocazione delle risorse destinate alle attività di cibersicurezza. Tuttavia, il punto che rimane parzialmente in ombra è come collocare i Parlamenti non tanto all'interno della regolazione del fenomeno (leggi nazionali o ratifiche di trattati internazionali passeranno comunque dalle Assemblee), quanto nella sorveglianza sull'attività dei pubblici poteri (riconducibili all'Esecutivo) nel ciberspazio, permettendone una almeno parziale conoscibilità al pubblico e garantendo così l'inveramento del principio di responsabilità politica nella sua forma più essenziale, cioè come *accountability*.

La risposta italiana a tale necessità è stata individuata nel Comitato parlamentare per la sicurezza della Repubblica (Copasir), creato nel 2007 dalla legge n. 124, in sostituzione del preesistente Comitato parlamentare di controllo sui servizi segreti (Copaco) voluto dalla legge n. 801/1977. Va peraltro sottolineato che il "modello Copasir" ha avuto anche un discreto successo a livello comparato: in Francia nel 2007 è stata creata una *Délegation parlamentaire au renseignement* composta da membri dell'Assemblea Nazionale e del Senato[61], così come in Spagna la *ley de Seguridad Nacional* del 2015 ha introdotto la *Comision Mixta Congreso-Senado de Seguridad Nacional*[62].

Le varie normative italiane che hanno investito il tema della sicurezza non hanno mai tralasciato di citare (e dunque ampliare) le competenze del comitato bicamerale[63]. In particolare, il decreto-legge sul perimetro di sicurezza nazionale cibernetica ha previsto il coinvolgimento preventivo del Copasir nell'adozione degli atti del Presidente del Consiglio nella materia[64]. Lo stesso Comitato deve essere obbligatoriamente informato delle determinazioni del Presidente del Consiglio in caso di crisi cibernetica (art. 5, comma 1-bis).

Ancora, il decreto-legge n. 82 ha ulteriormente specificato i rapporti fra Presidente del Consiglio e Copasir, prevedendo l'informazione preventiva dell'organo per le nomine dei vertici dell'Agenzia nazionale per la cibersicurezza, di competenza del capo del Governo (art. 1, comma 3). Ancora, il Copasir può chiedere l'audizione del direttore dell'Agenzia (art. 5, comma 6) ed esprime un parere preventivo sui regolamenti che disciplinano il funzionamento dell'organismo (art. 6, comma 3), anche in materia contabile (art. 11, comma 3), di contrattualistica pubblica (art. 11, comma 4) e di personale (art. 12, comma 8). Peraltro, i fabbisogni di bilancio a favore dell'Agenzia devono anch'essi essere previamente comunicati al Comitato (art. 11, comma 1), cui perverranno in seguito il bilancio consuntivo e la relazione della Corte dei Conti (art. 11, comma 4). Infine, il Presidente del Consiglio è tenuto ad inviare una relazione annuale all'organo parlamentare sulle attività svolte dell'Agenzia (art. 14, comma 2).

---

[61] Art. 6 nonies de l'*Ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assembléesparlementaires,* introdotto dalla legge n. 2007-1443 del 9 ottobre 2007.

[62] Art. 13, comma 2 della *ley de Seguridad Nacional*.

[63] Così in generale ha fatto la legge n. 133/2012, rinforzando i poteri di controllo dell'organo sull'attività del Presidente del Consiglio.

[64] Si tratta sia di atti a carattere regolamentare (DPCM previsti all'art. 1, commi 2 e 3 del decreto), sia dell'atto amministrativo generale coperto dal segreto sull'individuazione dei soggetti da inserire nel perimetro di sicurezza nazionale (comma 2-bis).

Ora, alla luce di questa trama normativa è difficile affermare che il Copasir non abbia un ruolo assolutamente rilevante nell'assetto istituzionale italiano (lo confermano peraltro alcuni fatti di cronaca recenti[65]). Un dubbio però sorge: il ruolo del Copasir, pur fondamentale, non è forse troppo *limitante* rispetto alla vastità di ambiti cui ormai presiede e *limitato* tanto nella composizione che nelle forme di pubblicità assai affievolita per contribuire ad un più vasto e cosciente dibattito pubblico[66]? Non v'è dubbio che il Comitato lavori a stretto contatto con i vertici del Governo; tuttavia, ricreare una "bolla" di potere separata dagli altri organi (in particolare dalle Camere) non contribuisce all'esercizio di un controllo democratico effettivo[67].

D'altra parte, nel momento in cui ricadono nell'ampio raggio della sicurezza *cyber* attività e fenomeni che nel mondo fisico sarebbero stati riconducibili alle attività di difesa – e, in ultimissima istanza, all'art. 78 Cost. – occorrerebbe forse riflettere sulla necessità che vengano affinati strumenti di controllo parlamentare ulteriori[68], pur nel delicato bilanciamento con le peculiari esigenze sottese alla difesa nazionale che giustificano una maggiore opacità rispetto agli atti del potere[69].

Certo è che se si osserva lo scivolamento dalle sedi principali e tipiche dei poteri interessati (gli organi collegiali come il Consiglio dei Ministri per il Governo o le assemblee nel caso del Parlamento) alle sedi distaccate e ristrette degli stessi (i Comitati interministeriali o le Commissioni parlamentari apposite), non si può che constatare una sorta di "diluizione" della responsabilità politica nella materia, che fugge dai suoi poli naturali per annidarsi in snodi apparentemente minori e conseguentemente meno esposti all'attenzione dell'opinione pubblica. E si badi: tale sottolineatura non deriva da un malsano desiderio di trasparenza a tutti costi – di *voyeurismo*, avrebbe detto Guy Carcassonne[70] - ma dalla constatazione che nella rete passano oramai tutti i principali interessi, pubblici e privati, di una comunità. Dunque, senza allarmismi ed evocazioni di scenari distopici, pare comunque opportuno evidenziare che i controllori pubblici del

---

[65] O. CARAMASCHI, *La sicurezza della Repubblica alla prova delle regole legislative e della prassi parlamentare: il caso del COPASIR*, in *Consulta Online*, 2/2021, 431 ss.

[66] *Mutatis mutandis*, cfr. M. GUILLAUME, *Parlement et secret(s)*, in *Pouvoirs*, 97, 2001, 67: «Agora du débat public, le Parlement est le lieu d'échange démocratique. Il se veut aujourd'hui encore davantage, dans une société d'information et d'immédiateté, un lieu d'ouverture et non de confidentialité. Ces exi-gences sont contradictoires avec les impératifs qui guident le secret».

[67] Ciò sembra perpetuare la *ratio* "consociativistica" alla base della creazione del Copaco nel 1977, durante il periodo del compromesso storico in cui vennero create, come è noto, varie commissioni parlamentari volte a controllare l'attività governativa in vari ambiti, di modo che il principale partito di opposizione (il Partito comunista italiano, come è noto) potesse essere associato all'azione di governo guidata dalla Democrazia cristiana senza essere formalmente coinvolto nel ministero. Il che, si badi, non è affatto detto che sia un male (data anche la sensibilità degli interessi in gioco), ma non è scontato sia sufficiente ai fini indicati.

[68] Ad esempio, delle sedute specifiche annuali di controllo e dibattito sui temi della difesa e della sicurezza cibernetica, che vadano oltre la mera presa d'atto delle Relazioni trasmesse dalle istanze competenti (come la relazione annuale del Copasir prevista dall'art 35 della legge n. 124/2007).

[69] Si ricorderà la tranciante frase della Corte costituzionale italiana nella celebre sentenza n. 1 del 2013 sull'attività riservata del Capo dello Stato: «va ricordato come il Capo dello Stato presieda il Consiglio supremo di difesa ed abbia il comando delle Forze armate, e come sia chiamato ad intrattenere, anche nelle vesti indicate, rapporti e comunicazioni del cui carattere riservato non occorre dare particolare dimostrazione» (punto 9 del *Considerato in diritto*).

[70] G. CARCASSONNE, *Le trouble de la transparence*, in *Pouvoirs*, 97, 2001, 17 ss.

ciberspazio sono, loro, meno controllati di quanto non avverrebbe (o non avveniva) nella dimensione non virtuale.

6.3. *Segue: ritorno sulla scelta primo-ministeriale, con particolare riferimento ai casi italiano e francese*

Alla luce delle riflessioni precedenti, conviene ritornare sulla scelta compiuta da alcuni ordinamenti, in particolare dall'Italia e dalla Francia, di affidare la competenza in materia di sicurezza cibernetica al Primo Ministro o ad agenzie a lui riferibili, scelta che definiamo appunto "primo-ministeriale".

All'apparenza, potrebbe sembrare un'opzione particolarmente favorevole ad un più stretto controllo politico del tema: allocare tale funzione al vertice dell'Esecutivo parrebbe sottintenderne non solo la fondamentale valenza di indirizzo, ma anche l'assunzione massima di responsabilità per le politiche concretamente perseguite.

In realtà, verrebbe da dire che il grande rafforzamento sul piano giuridico del capo del Governo non si accompagna ad un bilanciamento in termini di controllo.

Per l'Italia, già si è sottolineato che il rapporto privilegiato fra Presidente del Consiglio e Copasir, nell'esercizio delle competenze "securitarie" del primo, circoscrive in realtà il controllo ad una dialettica di cui si conosce poco o nulla all'esterno.

Non dissimile è in realtà il caso francese: se il codice della difesa – novellato a varie riprese a partire dal 2013 – riconosce all'autorità del Primo ministro le competenze in materia di sicurezza cibernetica (concretizzando così l'art. 21 della *Constitution* che lo vede come "*responsable de la défense nationale*"), non bisogna dimenticare che nell'ordinamento francese gli obblighi informativi dell'Esecutivo nei confronti del Parlamento sono piuttosto blandi per costante giurisprudenza del *Conseil constitutionnel* (ed anzi, solo nel 2020 è stata affermata in termini generali l'esistenza di un potere parlamentare di richiedere informazioni al Governo[71]).

Peraltro, la scelta primo-ministeriale comporta un ulteriore profilo, ovvero il rapporto con il Capo dello Stato. Ciò si pone in particolare per quei Paesi – come Francia e Italia, appunto – che, se pur a livelli diversi, riconoscono ai Presidenti della Repubblica un ambito non indifferente di intervento nelle materie della politica estera e della difesa[72]. Dunque, l'integrazione dei poteri legati alla difesa cibernetica avrebbe dovuto

[71] Cfr. la decisione n. 2020-800 DC dell'11 maggio 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions,* cons. n. 82.

[72] Dal punto di vista squisitamente formale, le costituzioni francese ed italiana non differiscono significativamente, riconoscendo l'una (art. 15) che il Presidente è capo dell'esercito e presiede i Consigli e comitati superiori della difesa nazionale, l'altra (art. 87) che il Presidente ha il comando delle forze armate e presiede il Consiglio supremo di difesa. In Francia si parla del c.d. *domaine réservé* del Capo dello Stato, di gaulliana memoria. V. sul tema J. GUISNEL, *Un domaine absolument « réservé »: la politique étrangère et la défense,* in R. FALIGOT, J. GUISNEL (a cura di), *Histoire secrète de la Vè République*, Parigi, 2007, 297 ss. V. altresì G. CARCASSONNE, *Le Premier ministre et le domaine dit réservé*, in *Pouvoirs*, 83, 1997, 65 ss. Per l'Italia cfr. S. GALEOTTI, *Brevi note in tema di "potere estero" e divisione del potere nella costituzione italiana*, in ID., *Il Presidente della Repubblica garante della Costituzione*, Milano, 1992, 271 ss.

teoricamente prendere in considerazione tale circostanza, ma così non è stato in nessuno dei due ordinamenti considerati.

In Francia si è giustamente osservato che la problematica della *cyberdéfense* è lo "specchio della complessità del potere esecutivo"[73] e costituisce una "giustificazione supplementare per una chiarificazione istituzionale"[74], poiché senza nulla dire del Capo dello Stato, apparentemente gli interventi normativi più recenti hanno considerevolmente dilatato i poteri del Primo ministro[75]. Che ciò non crei sostanzialmente problemi di tenuta pratica è garantito dalla consonanza politica fra le "due teste" dell'Esecutivo e dalla subordinazione politica del Primo ministro che, nel regime della "captazione presidenziale" del parlamentarismo francese[76], deve la sua nomina ad un grazioso atto del Presidente.

In Italia la questione è (di norma[77]) più complessa poiché la legittimazione del Presidente del Consiglio, proveniente dalla maggioranza parlamentare, non garantisce che vi sia sintonia politico-istituzionale fra Palazzo Chigi ed il Quirinale e dunque potrebbero più facilmente insorgere delle frizioni fra i due organi, anche alla luce di norme non particolarmente specifiche.

L'allocazione delle competenze in materia di sicurezza in capo al Presidente del Consiglio discende dall'interpretazione dell'art. 95 Cost. che la Corte costituzionale diede nella sent. n. 86 del 1977 in tema di segreto di Stato, conseguentemente allargata all'ambito dei servizi segreti con la legge n. 801/1977, riformata poi nel 2007. Le norme in materia di sicurezza cibernetica si sono inserite in questo filone interpretativo e così, insieme a varie altre discipline in materia di governo dell'innovazione[78], hanno costituito

---

[73] X. LATOUR, *La souverineté numerique et la cyberdéfense en France*, in P. TURK, C. VALLAR (a cura di), *La souveraineté numérique. Le concept, les enjeux*, Parigi, 2017, 142 ss.

[74] *Ibidem*, 145.

[75] V. gli artt. L1332-6-1 e ss., introdotti a partire dalla legge 2013-1168 (*relative à la programmation militaire pour les années 2014 à 2019*). Anche il *code de la sécurité intérieure,* modificato dalla legge n. 2018-607 diprogrammazione militare 2019-2025*,* prevede importanti poteri in capo al Primo Ministro, soprattutto in relazione all'accesso a dati di connessione per prevenire minacce agli interessi nazionali (artt. L. 854-2 e ss.).

[76] V. per tutti A. LE DIVELLEC, *Parlementarisme négatif et captation présidentielle. La démocratie française dans la «cage d'acier» du présidentialisme*, in D. CHAGNOLLAUD, B. MONTAY (a cura di), *Les 60 ans de la Constitution 1958-2018*, Parigi, 2018, 91 ss.

[77] Ci si permette di introdurre questo inciso perché in più di un'occasione recente si è assistito a nomine del Presidente del Consiglio dettate dal Capo dello Stato, sia nel caso di governi c.d. "tecnici" (pensiamo da ultimi ai Governi Monti e Draghi), sia nel caso di Esecutivi più dichiaratamente "partitici" (come nel caso del Governo Letta). In questi casi le distanze fra i due versanti delle Alpi appaiono ancora più ridotte. Sulle ultimissime vicende del 2021 sia consentito rinviare ad A. LAURO, *Note critiche sulla crisi del Governo Conte II e la formazione del Governo Draghi*, in *Consulta Online*, 2/2021, 379 ss.

[78] Così, ad esempio, il decreto-legge 22 giugno 2012 n. 83, creando l'Agenzia per l'Italia digitale, ne ha affidato la vigilanza al Presidente del Consiglio (artt. 19 e ss.); la legge 11 gennaio 2018 n. 7 ha attribuito al Presidente del Consiglio l'alta direzione in materia di politica spaziale ed aerospaziale (art. 1); il decreto-legge 14 dicembre 2018 n. 135 (art. 8) ha attribuito alla Presidenza del Consiglio i compiti spettanti all'Agenzia in materia di Agenda Digitale italiana (superando così il d.lgs. 26 agosto 2016 n. 179). Questi vari compiti sono poi stati affidati al Dipartimento per la trasformazione digitale (DPCM 19 giugno 2019). Si tratta di una parabola che non può essere qui approfondita ulteriormente, ma che rimanda ad una "tecnificazione" della stessa Presidenza del Consiglio secondo un paradigma diffuso nell'amministrazione italiana (cfr. S. CIVITARESE MATTEUCCI, L. TORCHIA, *La tecnificazione dell'amministrazione*, in ID. (a cura), *A 150 anni dall'unificazione amministrativa italiana. Vol. IV La tecnificazione*, Firenze, 2016, 7 ss.), secondo un percorso tutt'altro che lineare (come dimostrato dal fallimento dell'Autorità per l'informatica

una sorta di attuazione spuria e composita dell'art. 95, primo comma, trasformando la Presidenza del Consiglio in un "super-ministero" delle nuove tecnologie e riconoscendo alla responsabilità generale del Presidente del Consiglio, predicata dalla medesima norma, una valenza di "surrogato" per altre forme di compartecipazione parlamentare a decisioni salienti nell'ordinamento costituzionale[79].

Tuttavia, le attribuzioni del Consiglio Supremo di difesa (previste dalla legge 28 luglio 1950, n. 624, poi confluita nel Codice dell'ordinamento militare) sono sufficientemente late[80] per includere – ragionevolmente – le questioni legate al ciberspazio. Col che viene dunque a crearsi una stratificazione di centri decisionali (il Consiglio supremo, il Comitato interministeriale, il Presidente del Consiglio) il cui buon funzionamento complessivo deriva sostanzialmente dalla capacità pratica di raccordo che si sviluppa fra le amministrazioni e dai rapporti (istituzionali, ma non solo) fra i due Presidenti. Dunque, è ancora nel segno dell'informalità e della riservatezza che la separazione dei poteri deve operare nel campo del ciberspazio.

7. *Conclusioni*

Anche il punto da ultimo esaminato conferma l'impressione che emerge dai vari aspetti analizzati nel corso del lavoro: l'ordinamento della sicurezza cibernetica presenta una natura sfuggente e sfumata che lo rende difficilmente *saisissable* in tutte le sue sfaccettature. Da un lato, esso impone di collocarsi al crocevia fra diverse discipline (questioni prettamente costituzionali incontrano tematiche amministrativistiche, senza poter prescindere dal diritto europeo e, talvolta, dal diritto internazionale, senza considerare le conoscenze tecniche extra-giuridiche). Dall'altro lato, la natura cangiante del fenomeno che deve regolare ne impedisce una costrizione in schemi normativi chiari e costanti.

Tutto questo, però, giustifica a maggior ragione l'attenzione che si è voluta dare al tema, riconoscendo che – per forza di cose – nel prossimo futuro esso assumerà sempre maggiore centralità ed imporrà ancora riflessioni circa la distribuzione e l'esercizio dei poteri connessi a questa nuova dimensione "metafisica". Tuttavia, la difficoltà delle nuove sfide non potrà far perdere di vista le preoccupazioni classiche che derivano dal costituzionalismo moderno: in particolare, la legittimazione democratica del potere ed i contro-limiti al suo utilizzo continueranno a richiedere un'attenta verifica degli equilibri giuridici ed istituzionali, pur in una dimensione dinamica come quella "*cyber*".

---

nella pubblica amministrazione- AIPA, sulla cui stessa natura non vi era chiarezza: cfr. F. ANGELINI, *L'Autorità per l'Informatica nella Pubblica Amministrazione: natura giuridica*, in *Informatica e diritto*, 1/1996, 133 ss.).

[79] Come sarebbe nel caso dell'art. 78 Cost.

[80] «Il Consiglio supremo di difesa, nel presente titolo denominato Consiglio, esamina i problemi generali politici e tecnici attinenti alla difesa nazionale e determina i criteri e fissa le direttive per l'organizzazione e il coordinamento delle attività che comunque la riguardano» (art. 2 del Codice).