Mauro Santaniello

Monocratic cybersecurity

MONOCRATIC CYBERSECURITY

Cybersecurity has arisen as a compelling public policy issue at all government levels. Political studies on this topic, although growing in number and variety, have still fallen short of providing a theoretical framework to connect cybersecurity policies to political transformations occurring in contemporary democratic regimes. This paper deploys Musella's theory of monocratization in order to analyze the cybersecurity policy field in the Usa between 2009 and 2021, corresponding to the last three concluded presidential terms. The analysis seems to support the thesis of a monocratization of the cybersecurity policy-making, consisting of normative and communicative leadership of the presidency on the matter, privatization and personalization of the exercise of public powers, and fragmentation of the governance space. More in detail, findings show that the structure of the cybersecurity policy field in the Usa can be described as a «distributed monocracy», where «personal public-private partnerships» get institutionalized and state action becomes a function of decisions taken by a galaxy of micro-monocrats on the basis of individual interests. Finally, the paper discusses the political outcomes of the process of monocratization of cybersecurity policies, particularly what is defined as «personalized mass surveillance», in which surveillance targets are selected and magnified against a background of massive and generalized control.

KEYWORDS *Cybersecurity, Monocratic Government, Digital Policy, Political Regimes, Internet Governance.*

1. Introduzione

Negli ultimi anni il tema della *cybersecurity* ha rapidamente scalato l'agenda politica di organizzazioni intergovernative, governi nazionali e autorità locali, posizionandosi stabilmente tra le priorità delle istituzioni di governo (Karpiuk e Kostrubiec 2022; Dunn Cavelty e Egloff 2019; Harknett e Stever 2011). La lista delle organizzazioni intergovernative che hanno istituito agenzie, gruppi di lavoro e task force per fronteggiare le minacce internazionali alla sicurezza cibernetica si allunga di anno in anno, e comprende tanto organizzazioni operanti su scala globale – come l'Onu, l'Oecd, il Wto, il Wco, il G8, il G24, la Nato, l'Interpol, ecc. – quanto organizzazioni regionali come l'Unione

Mauro Santaniello, Dipartimento di Studi Politici e Sociali/DISPS – Università degli Studi di Salerno – Via Giovanni Paolo II, 132 - 84084 Fisciano, Salerno, email: msantaniello@unisa.it, orcid: 0000-0001-5582-622X.

ISSN 2785-0072

europea, l'Unione africana, la Cooperazione economica Asia-Pacifico (Apec), l'Associazione delle nazioni del sud-est asiatico (Asean), l'Organizzazione degli stati americani (Oas), ecc.[1] Queste organizzazioni, e gli Stati nazionali che ne sono membri, nel tentativo di mitigare e gestire i rischi derivanti da una crescente «cyber-insicurezza» globale, stanno producendo una galassia di processi negoziali, accordi, procedure, arene di *policy-making* e strumenti di politica estera che configurano nuovi modelli e nuove prassi della diplomazia contemporanea (Schemeil 2022; Fracchiolla 2022; Kello 2013; Chhabra 2020). Sul piano nazionale, ben centoquindici paesi si sono dotati di una strategia di cyber-sicurezza nazionale, e molti di essi aggiornano i propri piani in materia con cadenza compresa tra i due e i cinque anni (Itu 2023)[2]. Tali strategie hanno prodotto ovunque una riarticolazione dei poteri statuali e una ridefinizione delle modalità di esercizio dell'autorità pubblica (Follis e Fish 2020), con l'istituzione di agenzie nazionali *ad hoc* deputate al coordinamento delle iniziative di difesa cibernetica, con l'insediamento di comandi *cyber* ai più alti livelli delle gerarchie militari, e con unità di contrasto al cyber-crimine formate presso tutti i corpi di polizia, sia con funzioni investigative che di repressione. A livello locale, seppur con variazioni significative soprattutto in termini di implementazione ed efficacia, le politiche di sicurezza cibernetica sono diventate parte integrante dei piani di digitalizzazione dei servizi pubblici erogati da enti territoriali, in particolar modo a seguito della pandemia di Covid-19 e del conflitto russo-ucraino, che hanno causato un incremento della frequenza e della tipologia di attacchi informatici contro reti e sistemi delle pubbliche amministrazioni (Norris *et al.* 2022).

Quella che fino a pochi anni fa era una questione ancillare rispetto ai temi chiave dell'economia digitale (accesso, alfabetizzazione digitale, liberalizzazione e apertura dei mercati, protezione della proprietà intellettuale, armonizzazione dei framework regolativi, ecc.), è diventata oggi il principale problema di rilevanza pubblica nell'ambito delle politiche digitali. Un problema collettivo che, in quanto tale, ha prodotto una serie di risposte pubbliche, cui corrisponde un crescente interesse conoscitivo nel campo delle scienze politiche. Diversi studi, partendo da una prospettiva costruttivista, hanno evidenziato un processo di securitizzazione del cyber-spazio che procede per il tramite di elementi discorsivi quali narrazioni, frame e metafore relativi alla *cybersecurity* (Zeffiro *et al.* 2022; Lawson e Middleton 2019; Miao *et al.* 2019; Dunn Cavelty 2013, 2009; Lawson 2012; Hensen e Nissenbaum 2009), mostrando

[1] Sulle origini di questo processo di veda Portnoy e Goodman (2009).

[2] L'elenco delle strategie nazionali di *cybersecurity* è tenuto dall'International telecommunications union delle Nazioni unite, online: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

come il discorso pubblico sulla sicurezza cibernetica influenzi la produzione di specifici strumenti di *policy* e design istituzionali (Stevens 2018; Lawson 2013; Nissenbaum 2005; Birnhack e Elkin-Koren 2003). Altri studi si sono concentrati sulle condizioni che, in determinati contesti nazionali, favoriscono o inibiscono i cambiamenti nelle politiche di *cybersecurity*, identificando come variabili chiave il consolidamento delle procedure burocratiche, la determinazione dei leader politici a riformulare le politiche precedenti, e i cambiamenti sistemici relativi tanto allo sviluppo tecnologico quanto alle relazioni internazionali (Shively 2021). Un corpo più consistente di analisi è stato prodotto da una prospettiva comparata, con l'obiettivo di identificare i fattori economici, culturali, legali e politico-istituzionali che determinano i differenti approcci nazionali alle politiche di *cybersecurity* (Creese *et al.* 2021; Huang *et al.* 2021; Karatas 2020; Stitilis *et al.* 2017; Min *et al.* 2015; Karabacak *et al.* 2014). Altri filoni di ricerca, infine, hanno preso in esame i processi di cooperazione internazionale attivati negli ultimi anni nel settore, sia in termini di *capacity building* e *policy transfer* (Blumfelde 2022; Homburger 2019), sia come strumento di partnership intergovernativa (Christou e Lee 2021). Nonostante un incremento sensibile di analisi, report di ricerca e articoli scientifici sulle politiche di sicurezza informatica, il contributo delle scienze politiche alla comprensione dei problemi di *cybersecurity* e delle relative risposte istituzionali è ancora limitato (Loiseau *et al.* 2020). Una volta riconosciuto il carattere costituente delle politiche di sicurezza digitale, restano, tra l'altro, ancora da esplorare le modalità con cui le caratteristiche precipue di tale ambito di *policy* interagiscono con i principali processi di trasformazione in atto nei regimi politici contemporanei. In altri termini, va ancora ricercato, nel campo della sicurezza digitale, un nesso – storico e funzionale – tra *policy* e *politics*. L'obiettivo di questo saggio è avviare una riflessione su questo rapporto, e produrre, attraverso l'analisi del caso statunitense, una migliore comprensione delle questioni politiche connesse all'espansione del campo della *cybersecurity*. Nel prossimo paragrafo viene brevemente richiamato il quadro teorico che si utilizza per l'identificazione dei principali vettori di trasformazione dei regimi democratici, e viene presentato l'impianto metodologico della ricerca. Nel paragrafo successivo, vengono presentati e discussi i dati prodotti dall'analisi, che forniscono una rappresentazione delle forme assunte da tali processi trasformativi entro i confini specifici delle politiche di *cybersecurity*. Nel paragrafo conclusivo vengono avanzate alcune considerazioni di carattere generale sul rapporto tra regimi democratici e politiche di sicurezza digitale, vengono identificati alcuni limiti della presente ricerca, e si delinea una possibile agenda di ricerca per il loro superamento.

2. Regimi politici e politiche monocratiche

Quadro teorico

Una delle trasformazioni più ampie e significative dei regimi politici contemporanei è quella che Musella (2018, 103) definisce «l'ascesa del governo monocratico». Con questa espressione l'autore fa riferimento a un processo di centralizzazione del potere politico presso le leadership di partito e di governo, a discapito degli organi collegiali di decision-making, come assemblee e parlamenti. Tale processo non riguarda soltanto i regimi autocratici o in transizione, ma caratterizza anche l'evoluzione dei regimi democratici più maturi, fino a configurare una nuova forma di governo, o quanto meno una nuova variante delle democrazie contemporanee. Muovendo dagli studi sulla presidenzializzazione della politica (Poguntke e Webb 2005) e sulla personalizzazione del potere esecutivo (Lowi 1985) e dei partiti politici (Calise 2000), Musella (2018, 2022) definisce il governo monocratico come la risultante di diversi processi trasformativi tra loro interrelati. Il primo consiste in un assorbimento delle funzioni legislative da parte degli organi esecutivi, che si manifesta con un incremento della produzione normativa dei governi nazionali e dei capi di governo a detrimento della normazione di origine parlamentare. Musella (2022, 8; 2018, 13) descrive questo processo come «l'affermazione di un principio monocratico di azione politica», che diventa particolarmente significativa in casi di crisi ed emergenze nazionali, e che si sostanzia nella produzione di decreti e ordini presidenziali che mettono sotto tensione il principio della separazione dei poteri (cfr. anche Criscitiello 2020). Il secondo processo costitutivo della tendenza alla monocratizzazione è rappresentato dallo sviluppo di una comunicazione diretta ed emotiva tra capi di governo e cittadini, che si avvale dei social network per aggirare i circuiti della comunicazione politica tradizionale e i suoi intermediari: organi di partito, uffici stampa e testate giornalistiche. Da questo punto di vista, l'autore evidenzia una prassi ormai consolidata nei paesi democratici, ossia l'anticipazione a mezzo social dei provvedimenti governativi, che consente ai capi degli esecutivi nazionali di fornire una risposta immediata – puramente comunicativa – a problemi collettivi e situazioni di emergenza (Musella 2020). Una terza dimensione del processo di monocratizzazione riguarda la sistematica alterazione del rapporto pubblico-privato nell'esercizio del potere politico. Tale trasformazione comporta, da un alto, l'invasione degli interessi privati nella sfera politica, e, dall'altro, l'utilizzo a fini personali delle risorse relazionali e reputazionali accumulate durante un mandato pubblico. Musella rileva questa tendenza osservando i percorsi di carriera dei capi di governo, evidenziando che, se il movimento dal business alla

politica è ancora un fenomeno decisamente limitato, il movimento opposto, ossia dal ruolo di presidente o premier a quello di businessman, rappresenta sempre più la norma. La quarta dimensione della monocratizzazione, infine, fa riferimento a un processo di «crescente frammentazione degli attori collettivi tradizionalmente deputati al controllo e al controbilanciamento del potere dei leader politici, come parlamenti e partiti politici» (Musella 2022, 8). Questo processo, che a volte assume i tratti di una vera e propria disintegrazione, si verifica tanto a livello elettorale – con elevati livelli di mobilità delle preferenze e un aumento significativo della polarizzazione dell'arena politica – quanto a livello istituzionale, dove da un lato aumenta il numero dei partiti e dall'altro sono sempre più frequenti cambi di casacca da parte dei parlamentari. La frammentazione, sostiene Musella, conduce a un indebolimento di partiti e parlamenti, e a una legittimazione dell'intervento governativo nell'arena legislativa, visto come risolutivo di situazioni di stallo e ingovernabilità.

Metodo e dati

In sintesi, dunque, la monocratizzazione dei regimi politici è un processo complesso che consta di differenti, seppur interrelate, traiettorie evolutive: lo slittamento delle funzioni legislative verso gli organi esecutivi, la comunicazione diretta leader-cittadini, il deterioramento della distinzione tra funzioni pubbliche e interessi privati, e la frammentazione dei corpi collettivi. L'ipotesi da cui muove questo articolo è che queste quattro traiettorie producano effetti significativi anche nell'ambito dei processi di *policy-making* relativi alla sicurezza digitale. Per verificare l'ipotesi di una monocratizzazione delle politiche di *cybersecurity*, si analizzerà il campo di *policy* della *cybersecurity* così come si è strutturato negli Stati Uniti d'America dal 2009 agli inizi del 2021, ossia in corrispondenza degli ultimi tre mandati presidenziali conclusi: Obama I (20 gennaio 2009 - 20 gennaio 2013), Obama II (20 gennaio 2013 - 20 gennaio 2017), e Trump (20 gennaio 2017 - 20 gennaio 2021). La scelta del caso statunitense discende dalla considerazione che tanto la personalizzazione della politica quanto l'istituzionalizzazione della *cybersecurity* come ambito di *public policy* sono processi che originano negli Usa e che, pertanto, in quel paese hanno raggiunto il livello più avanzato di maturità. Inoltre, la democrazia statunitense rappresenta un modello di riferimento per tutti i sistemi politici democratici, e le trasformazioni politico-istituzionali che avvengono a Washington hanno effetti importanti su tutti i regimi democratici contemporanei. La scelta della *cybersecurity* come ambito di *policy* in cui verificare la presenza di processi di monocratizzazione, invece, è giustificata dal carattere emergenziale delle politiche di sicurezza cibernetica (Fouad 2022), che le rende particolarmente pre-

disposte a istituzionalizzare nuove procedure per la gestione di situazioni di crisi e casi di urgenza.

Sulla base del modello teorico esposto in questo paragrafo, nella prossima sezione del saggio verrà presentata un'analisi delle politiche statunitensi di *cybersecurity* orientata a identificare e discutere le dimensioni costitutive del processo di monocratizzazione.

Il rapporto tra produzione normativa di origine parlamentare (*public law*) e atti normativi di origine governativa (piani e strategie) o presidenziale (direttive e ordini esecutivi) viene utilizzato per comprendere in che misura le politiche statunitensi di *cybersecurity* siano oggetto di interventi diretti da parte dell'esecutivo, e in particolare del presidente. A tal fine, si analizzano tutti i provvedimenti normativi prodotti sul tema nel periodo di riferimento, raccolti attraverso una ricerca per parole chiave sul portale del Congresso (https://www.congress.gov). L'insieme delle parole chiave utilizzate in questa ricerca è stato composto a partire da una sistematica revisione della letteratura sulla *cybersecurity* che ha consentito di identificare le principali issues di *cybersecurity policy*. La lista delle parole chiave è stata altresì integrata in modo induttivo man mano che si procedeva con l'analisi dei documenti di *policy*. I documenti di *policy* così raccolti sono 66.

Per rilevare le modalità di comunicazione dei temi relativi alla sicurezza digitale da parte del presidente sono stati raccolti circa 35.000 tweet pubblicati dagli account personali dei presidenti nel corso dei rispettivi mandati. La scelta di Twitter come fonte di dati deriva dal carattere intrinsecamente personale della comunicazione che tale piattaforma abilita, enfatizzato dalla struttura di relazioni basata su un rapporto tra un leader e i suoi follower. La scelta di analizzare i contenuti pubblicati dagli account personali dei presidenti anziché quelli istituzionali deriva dal fatto che i processi comunicativi della monocratizzazione si attivano tipicamente tra la persona del presidente e i suoi follower. Inoltre, come ha notato Mickoleit (2014, 2) sui social media i capi di Stato e di governo sono in generale molto più popolari delle istituzioni che rappresentano. I tweet rilevanti sono stati selezionati sulla base di una ricerca per parole chiave con le stesse modalità già descritte per l'individuazione degli atti normativi, e sono stati classificati in base alla specifica issue di *cybersecurity* oggetto del messaggio, al loro carattere emotivo, informativo o professionale, e ai rapporti interistituzionali cui essi rimandano. Il carattere emotivo/informativo/professionale dei messaggi è stato analizzato sulla base dell'indice di personalizzazione istituzionale elaborato da Amoretti, Fittipaldi e Santaniello (2021) a partire dai lavori di Van Santen e Van Zoonen (2010) e di Metz *et al.* (2020). Per quanto riguarda la visione dei rapporti interistituzionali sottesa ai messaggi presidenziali, sono stati rilevati quei tweet che annunciavano provvedimenti

diretti del presidente, o che sollecitavano il supporto popolare per sostenere o contrastare un'iniziativa legislativa del Congresso. Per quanto riguarda l'analisi del ruolo dei privati nella definizione e implementazione delle politiche pubbliche di *cybersecurity*, si fa riferimento, da un lato, alle interviste realizzate nell'ambito di due distinte ricerche sui rapporti pubblico-privato nel campo della *cybersecurity* Usa, e dall'altro, ai dati sul mercato del lavoro della *cybersecurity* e sui percorsi di carriera del personale impegnato in attività di *cybersecurity* nelle forze di polizia, nell'intelligence e nelle forze armate. Infine, la frammentazione dei corpi collettivi viene ri-concettualizzata come frammentazione del campo di *policy* della *cybersecurity*, che sortisce, come verrà argomentato, gli stessi effetti di rafforzamento della leadership di governo descritti da Musella.

3. Monocratic cybersecurity

La legislazione Usa sulla cybersecurity

Durante il primo mandato del presidente Obama nessuna legge relativa alla *cybersecurity* è stata approvata dal Congresso. La gestione del problema di *policy* è stata assunta completamente dall'organo esecutivo e, in particolare, dal presidente. Delle dodici iniziative di *cybersecurity policy* di quel periodo, sette sono a firma del presidente (quattro ordini esecutivi e tre direttive presidenziali), e cinque sono documenti strategici prodotti dai Dipartimenti (Dipartimento di Stato, Dipartimento della difesa, e Dipartimento della sicurezza interna). Nel corso del secondo mandato di Obama, il Congresso riesce ad approvare cinque leggi relative a questioni di *cybersecurity*. Il presidente firma otto *Executive order* (Eo) e quattro *Presidential policy directives* (Ppd), mentre i dipartimenti elaborano cinque documenti strategici. Il rapporto tra atti governativi e iniziative parlamentari è di tre a uno. Con la presidenza Trump si ha un'impennata del numero di Eo, che arrivano a rappresentare il 75% circa dell'intera produzione normativa sulla *cybersecurity*.

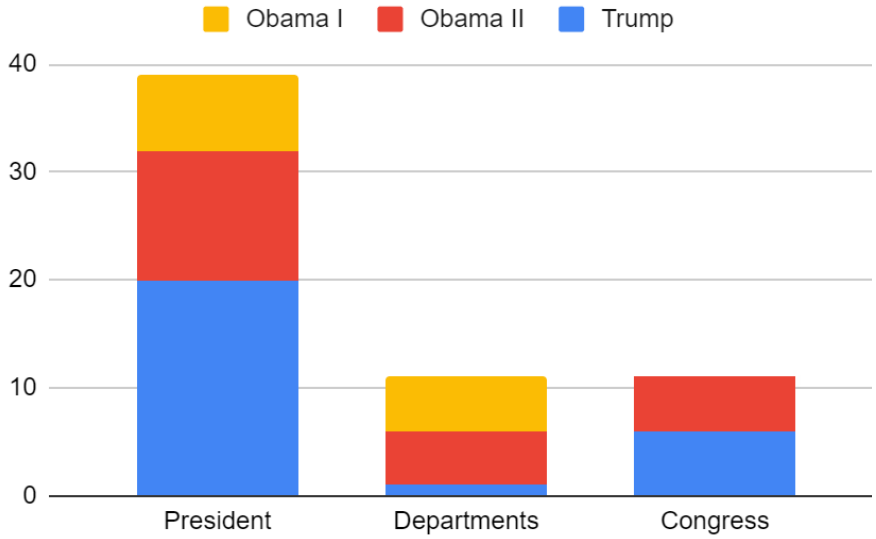

Fig. 1. Fonti della produzione normativa statunitense sulla *cybersecurity* (2009-2022).
Fonte: Elaborazione dell'autore su dati del Congresso.

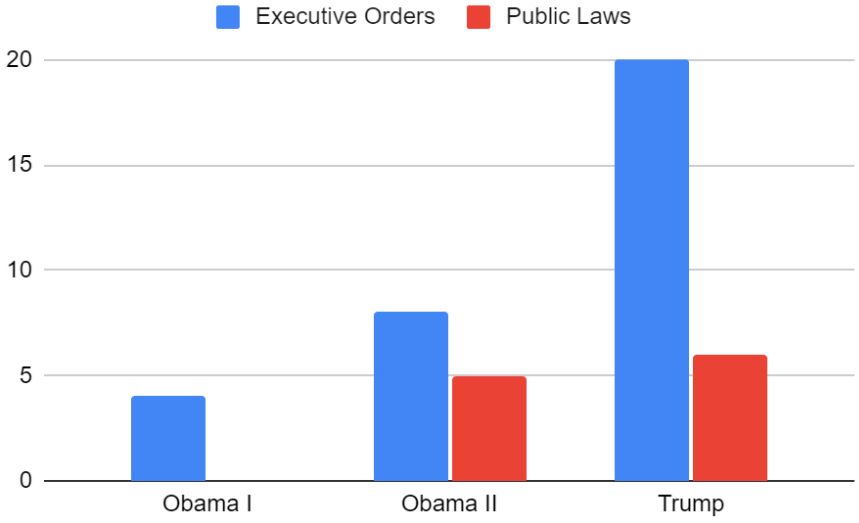

Fig. 2. *Cybersecurity Executive order*s e *public law*s (2009-2022).
Fonte: Elaborazione dell'autore su dati del Congresso.

Se si osserva, inoltre, il contenuto di Eo e Ppd, si nota che, sin dal primo mandato di Obama, questi atti normativi presidenziali non si sono limitati a disciplinare il funzionamento dell'esecutivo e delle sue diramazioni funzionali e territoriali, ma, in linea con la teoria della monocratizzazione, definivano

politiche, stabilivano strutture, codificavano procedure, normavano comportamenti. La direttiva di Obama del febbraio 2009, «Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure», ad esempio, avocava la leadership delle politiche di *cybersecurity* alla Casa Bianca, e assegnava al governo federale la responsabilità della sicurezza cibernetica nazionale. La direttiva «U.S. Cyber operations policy», inizialmente adottata come memorandum top secret nell'ottobre del 2012, introduceva nuove pratiche e nuovi principi nella conduzione delle operazioni di *cybersecurity*, con importanti conseguenze sia in termini di tutela dei diritti individuali dei cittadini, statunitensi e stranieri, sia in termini di politica estera. In particolare, essa sanciva l'adozione di forme di collaborazione volontaria tra governo e industria privata del settore It per la conduzione di operazioni *cyber* al di fuori del territorio e dei network statunitensi, e saldava in un'unica *policy* la *cybersecurity* e la cyber-intelligence:

> Gli Stati Uniti hanno un persistente interesse a sviluppare e mantenere l'uso del cyberspazio come parte integrante delle proprie capacità nazionali di raccogliere informazioni, e identificare, reprimere o sconfiggere qualsiasi avversario che cerchi di danneggiare gli interessi nazionali statunitensi in tempi di pace, crisi o guerra (Obama 2021).

Stoddart (2013), inoltre, nota come questa direttiva, insieme all'*Executive order* «Improving critical infrastructure cybersecurity» adottato da Obama all'inizio del secondo mandato, non siano altro che i passaggi con cui il presidente democratico aggirava il fallito tentativo di introdurre una nuova legge sulla *cybersecurity* in un Congresso controllato dai Repubblicani. Nel corso del secondo mandato di Obama, l'Eo del febbraio 2015 «Promoting private sector cybersecurity information sharing», strutturava e normava le relazioni tra gli apparati statali dediti alla *cybersecurity* nazionale e il settore privato, istituendo le organizzazioni miste pubblico-privato «di condivisione e analisi delle informazioni», e avviava un processo di standardizzazione di tali organizzazioni e delle loro procedure operative. Nell'aprile dello stesso anno l'Eo «Blocking the property of certain persons engaging in significant malicious cyber-enabled activities» introduceva per la prima volta il concetto di *cyber sanctions*, e con esso la possibilità di sanzionare soggetti stranieri per il loro comportamento ostile nel cyber-spazio[3]. Tra gli ordini esecutivi di Trump più emblematici del processo di allargamento delle funzioni legislative del presidente, rientrano l'Eo del 9 febbraio 2017 «Enforcing federal law with respect to transnational criminal organizations and preventing international

[3] In questo caso la lista delle entità sanzionate comprendeva compagnie di telecomunicazioni e dirigenti dei servizi di intelligence siriani e iraniani.

trafficking», che ampliava i poteri delle agenzie di law enforcement e i margini di collaborazione tra agenti federali e agenzie straniere, e avviava una revisione della legislazione federale relativa al crimine transnazionale; l'Eo dell'11 maggio 2017 «Strengthening the cybersecurity of federal networks and critical infrastructure», in cui si stabiliva che «la politica degli Stati Uniti per la gestione del rischio di sicurezza informatica è un'attività del ramo esecutivo»; e l'Eo del 28 maggio 2020 «Preventing online censorship», che avviava la programmazione di iniziative per fronteggiare il potere di piattaforme digitali come Twitter, Facebook, Instagram, e YouTube «di censurare, cancellare o occultare informazioni e di controllare ciò che le persone vedono e non vedono». A questi ordini esecutivi si aggiungono quelli diramati dal presidente per contrastare l'ascesa di aziende tecnologiche cinesi come Huawei (di fatto bandita con l'Eo del 15 maggio 2019 «Securing the information and communications technology and services supply chain») WeChat e TikTok (messe al bando dal presidente con due distinti Eo del 6 agosto 2020, entrambi bloccati subito dopo da una corte californiana).

I dati sopra esposti indicano una chiara leadership della Casa Bianca nella normazione della *cybersecurity* statunitense nel corso del periodo di riferimento. Il contributo del Congresso, sebbene sia cresciuto negli anni, non sta al passo con le iniziative governative, soprattutto quelle presidenziali. In linea con la teoria della monocratizzazione, l'iniziativa normativa in tema di *cybersecurity* è saldamente nella mani del presidente, che ne personalizza contenuti e forme. Per quanto riguarda i primi, su una tendenza di fondo verso il consolidamento della leadership presidenziale, il populismo trumpiano si distingue per l'alto numero di provvedimenti ad personam, mentre per ciò che concerne le forme, prolifera quella dell'*Executive order*, che è sempre più lo strumento primario dell'azione statale nel campo della *cybersecurity* Usa.

La comunicazione presidenziale della cybersecurity

Tra i circa 37.000 tweet[4] pubblicati dagli account personali dei presidenti nel periodo di riferimento, il tema della *cybersecurity* è poco frequente. Le questioni di *policy* relative alla sicurezza digitale sono state oggetto di soli tre messaggi di Obama nel primo mandato, di diciotto tweet nel suo secondo mandato, e di 55 tweet di Trump. Due dei tre tweet del primo Obama riguardavano la network neutrality, una questione di *policy* che solo tangenzialmente tocca il campo della *cybersecurity* (Wu 2003) e che in quegli anni è stata fortemente politicizzata negli Usa (Faris *et al.* 2015). Nel mezzo di uno scontro

[4] Il dataset di tweet utilizzati comprende 4.514 tweet di Obama nel corso del primo mandato, 6.409 nel secondo mandato, e 26.239 tweet di Trump, per un totale di 37.162.

con il Senato che si avviava a legiferare nel senso di una riduzione del principio della neutralità dell'infrastruttura di rete, Obama twittava: «President Obama pledges to veto the anti-*net neutrality* legislation pending in the Senate». L'altro tweet riguardava invece il lancio di un'iniziativa legislativa per la tutela della privacy online: «Read up on President Obama's plan to protect consumers on the Internet-the Consumer Privacy Bill of Rights». Nessuno dei tre tweet aveva carattere emotivo, nemmeno il primo che preannunciava l'opposizione del veto alla legislazione anti-*net neutrality*, e che con l'utilizzo della terza persona assumeva carattere informativo. Nel corso del secondo mandato, il presidente Obama cambiava registro, introducendo elementi emotivi nel suo repertorio retorico e personalizzando la comunicazione con l'utilizzo della prima persona. Per esempio, il 12 gennaio 2015, rilanciando il discorso sulla sicurezza cibernetica tenuto quel giorno presso la *Federal trade commission* (Ftc), l'account personale di Obama twittava sia messaggi di carattere informativo sia contenuti emotivi. I primi orientati ad anticipare le nuove iniziative legislative in materia e a mettere sotto pressione il Congresso, come «I'm announcing new steps to protect the identities and privacy of the American people» e «I hope Congress joins us in this national movement to protect the privacy of our children». I secondi per enfatizzare la leadership statunitense nello sviluppo delle reti digitali con toni patriottici, come «When we Americans put our minds together and our shoulder to the wheel there's nothing we can't do. #Cybersecurity». Oltre alla privacy, temi oggetto dei tweet presidenziali nel corso del secondo mandato di Obama sono la disinformazione e il furto d'identità online. Molto più articolato l'insieme delle issue affrontate dal presidente Trump con i suoi 55 tweet relativi alla *cybersecurity*, gran parte dei quali di carattere emotivo: il potere delle big tech, la protezione delle infrastrutture critiche, la *cyber war*, il 5G, la competizione tecnologica con la Cina, la sorveglianza elettronica, la disinformazione. In quanto ai contenuti, i tweet di Trump contengono tutto il repertorio della comunicazione monocratica: dalle anticipazioni normative alle promesse di veto, dalle pressioni sul congresso e sui partiti, in primis il suo, ai licenziamenti di personale governativo in diretta social e agli attacchi diretti contro i nemici politici, siano essi oppositori, alleati o soggetti economici come le grandi corporation del digitale. In particolare contro queste ultime Trump ingaggiava una serrata battaglia di tweet che mostra nelle sue estreme forme la comunicazione di tipo monocratico. All'apice di una lunga controversia contro le piattaforme digitali che, a detta del presidente, avrebbero operato pratiche censorie contro Trump e il partito repubblicano, la Casa Bianca aveva chiesto di introdurre nell'atto annuale di autorizzazione alla spesa militare una revisione della Sezione 230 del *Communications decency act*, che solleva gli intermediari online da ogni responsabilità relativa ai conte-

nuti pubblicati dagli utenti sulle piattaforme. La pertinenza di una simile disposizione rispetto a un atto di bilancio era stata argomentata da Trump sulla base di una presunta minaccia alla sicurezza nazionale posta dalle piattaforme digitali, e annunciata su Twitter in questa forma:

> Section 230, which is a liability shielding gift from the U.S. to "Big Tech" (the only companies in America that have it - corporate welfare!), is a serious threat to our National Security and Election Integrity. Our Country can never be safe and secure if we allow it to stand. ... Therefore, if the very dangerous and unfair Section 230 is not completely terminated as part of the *National Defense Authorization Act* (Ndaa), I will be forced to unequivocally VETO the Bill when sent to the very beautiful Resolute desk. Take back America NOW. Thank you!

Il 3 dicembre, il Congresso, dopo un lavoro bipartisan, presentava ufficialmente l'*Annual national defense authorization act*, detto anche *Defense bill*, che però non conteneva i riferimenti alla Sezione 230 voluti da Trump. Preannunciando il suo veto via Twitter il presidente scriveva: «But doesn't get rid of Big Tech's windfall, Section 230, a grave threat to National Security. I will VETO!». Pochi giorni dopo, in vista del voto alla Camera per il superamento del veto presidenziale, Trump tornava su Twitter per fare pressioni sul suo partito:

> I hope House Republicans will vote against the very weak National Defense Authorization Act (Ndaa), which I will VETO. Must include a termination of Section 230 (for National Security purposes), preserve our National Monuments, and allow for 5G and troop reductions in foreign lands!

Alla fine del mese di dicembre, quando era ormai diventato chiaro che la Camera si accingeva a votare a favore del superamento del veto, Trump pubblicava un nuovo doppio tweet per attaccare il suo partito:

> Weak and tired Republican "leadership" will allow the bad Defense Bill to pass. Say goodbye to VITAL Section 230 termination, your National Monuments, Forts (names!) and Treasures (inserted by Elizabeth "Pocahontas" Warren), 5G, and our great soldiers....
>
> ...being removed and brought home from foreign lands who do NOTHING for us. A disgraceful act of cowardice and total submission by weak people to Big Tech. Negotiate a better Bill, or get better leaders, NOW! Senate should not approve NDAA until fixed!!!

Al di là di questa controversia, numerosi sono i tweet di Trump che forniscono testimonianza di una comunicazione monocratica in tema di *cybersecurity*. Il 16 luglio del 2019, ad esempio, il presidente aveva preso di mira Google, considerato alla stregua di un nemico politico:

> Billionaire Tech Investor Peter Thiel believes Google should be investigated for treason. He accuses Google of working with the Chinese Government. @ foxandfriends A great and brilliant guy who knows this subject better than anyone! The Trump Administration will take a look!

Il 18 novembre 2020, nel pieno delle polemiche sui presunti brogli elettorali, Trump licenziava il capo della *cybersecurity* statunitense in diretta Twitter: «...votes from Trump to Biden, late voting, and many more. Therefore, effective immediately, Chris Krebs has been terminated as Director of the *Cybersecurity* and Infrastructure Security Agency». Infine, quando nel dicembre del 2020 veniva scoperto il cosiddetto *Cyber hack*, ossia la più grande operazione di cyber spionaggio di cui siano state vittime il governo e l'industria statunitense (Santaniello 2021), Trump rifiutava l'attribuzione di responsabilità a un gruppo di hacker russi, puntava il dito sui cinesi, e il 19 dicembre attaccava la stampa nazionale:

> The Cyber Hack is far greater in the Fake News Media than in actuality. I have been fully briefed and everything is well under control. Russia, Russia, Russia is the priority chant when anything happens because Lamestream is, for mostly financial reasons, petrified of.

Questi dati suggeriscono che la comunicazione monocratica abbia almeno tre funzioni. La prima è quella di comunicare la normazione, rappresentare l'atto potestativo a prescindere dalla sua concreta portata, fornire una narrazione dell'esercizio del potere presidenziale. La seconda funzione è quella di esercitare pressione politica su partiti e assemblee, che si esortano, si anticipano, si minacciano, in una partita a scacchi in cui è sempre il presidente a compiere la prima mossa. Infine, nel caso di leadership populiste, la funzione della comunicazione monocratica è quella di individuazione – nel senso letterale del termine – di un nemico del popolo, e di costruzione di un processo pubblico contro di esso. Nei suoi tweet Trump giudica, attribuisce colpe e sancisce condanne, in un assalto finale alla tripartizione dei poteri dello stato. È in questo senso che il presidente, senza alcuna variazione formale di regime, si fa uno e trino nella sua narrazione social, assumendo su di sé i poteri esecutivo, legislativo e giudiziario.

(Personal) public-private partnership

Garantire la sicurezza è da sempre funzione fondamentale degli Stati nazionali, a prescindere dalla loro forma di governo. Laddove, come tipicamente è avvenuto nelle democrazie liberali, gli elementi costitutivi del ciberspazio (infrastrutture, codici, elaboratori, piattaforme) sono stati privatizzati o svi-

luppati direttamente da organizzazioni commerciali in un regime di mercato transnazionale, lo stato si ritrova nella paradossale situazione di essere chiamato a proteggere la sicurezza di cittadini e imprese in uno spazio controllato da soggetti privati, spesso stranieri (Dunn Cavelty e Brunner 2007). Questo paradosso spiega perché le strategie di cybersicurezza dei paesi occidentali, sin dalla loro prima occorrenza con il *National plan for information systems protection* siglato da Bill Clinton nel 2000, si affidino alla *public-private partnership* (Ppp) come principale strumento di *policy* (Carr 2016). Nelle Ppp il settore pubblico collabora con due tipi di digital corporation. Il primo tipo include le società che possiedono o gestiscono le risorse critiche della Rete: compagnie di telecomunicazione, *server farm*, piattaforme, software house, e organizzazioni ibride come l'*Internet* corporation for assigned names and numbers (Icann) che gestisce i nomi di dominio, gli indirizzi Ip, e i protocolli di base di *Internet*. Il secondo tipo di digital corporation coinvolto nelle Ppp per la *cybersecurity* è rappresentato dai fornitori privati di sicurezza, una galassia di imprese che forniscono, allo stato e alle aziende, servizi di protezione cibernetica. D'altra parte, nella sua analisi delle politiche di *cybersecurity* relative alla protezione delle infrastrutture critiche negli Usa e nel Regno unito, Madeline Carr dimostra che, nonostante le Ppp siano spesso menzionate come «meccanismo chiave attraverso cui mitigare la minaccia» (Carr 2016, 43), «cosa esattamente comporti la partnership pubblico-privato è sempre stato poco chiaro» (Carr 2016, 61)[5]. In particolare, la ricerca di Carr mostra come il settore pubblico e quello privato, sul tema, abbiano visioni, interessi e aspettative differenti rispetto alla natura e al concreto svolgimento della collaborazione, al punto che le Ppp vengono definite «partnership disfunzionali» (*ibidem*) «caratterizzate non da responsabilità condivise, ma da responsabilità contese» (Carr 2016, 58). In tali partnership, ed è questo il punto che qui più rileva, forti rapporti personali e/o professionali tra il personale del settore pubblico e quello delle aziende private coinvolte nelle partnership risultano determinanti per l'efficacia delle attività di collaborazione. In altri termini potremmo dire che, per funzionare, le Ppp devono assumere la forma incidentale di «personal public-private partnership». Anche il lavoro di Christensen e Petersen (2017), pur contestando la visione pessimistica di Carr sull'efficacia delle Ppp nella *cybersecurity*, enfatizza l'importanza di variabili personali per il successo delle Ppp, come i sentimenti di solidarietà, patriottismo e lealtà del personale coinvolto nei partenariati, le loro relazioni interpersonali, l'impegno verso la propria azienda e la propria professione, la condivisione dei percorsi di carriera tra gli addetti del settore

[5] Sui limiti delle Ppp nel campo della sicurezza delle infrastrutture critiche si veda anche Dunn Cavelty e Suter (2009).

pubblico e del settore privato. Un «collante sociale che tiene assieme le partnership e crea uno spazio per la leadership e l'orientamento» (Christensen e Petersen 2017, 1437). Questa personalizzazione della funzione pubblica, che si pone in evidente contrasto con il principio weberiano dell'impersonalità della burocrazia e che è tratto distintivo della monocratizzazione, è rilevabile anche nei percorsi di carriera dei cosiddetti «cyberwarriors». Se è vero che in generale la corporate security è un settore in cui, soprattutto negli Usa, il passaggio da agenzie di law enforcement al business privato è molto frequente (Petersen 2014), nel campo della *cybersecurity* questa tendenza assume contorni particolarmente impattanti sulla produzione di politiche pubbliche e sulla capacità del settore pubblico di dotarsi di una forza lavoro idonea a fronteggiare i rischi connessi alla *cybersecurity*. Diversi studi condotti sul mercato del lavoro della *cybersecurity* nel Nord America mostrano come il tasso di abbandono del personale sia più alto in questo settore che in generale nel comparto It, e che le organizzazioni operanti in questo mercato competano tra loro mediante un'aggressiva politica di reclutamento (Vogel 2016), la cui conseguenza principale è che il 21% degli addetti ha cambiato posto di lavoro negli ultimi 12 mesi (Isc2 2022). La gran parte di questi trasferimenti di personale riguarda dipendenti di agenzie pubbliche che lasciano il proprio lavoro per un contratto con aziende private. In un articolo dal titolo eloquente, «The big quit: Why *cybersecurity* pros are leaving government», Holly Rosenkrantz (2021) nota come nel settore pubblico statunitense manchino più di 36.000 addetti alla *cybersecurity*, di cui 1.700 nel solo Dipartimento della sicurezza interna, e, riprendendo le parole di Ari Schwartz, ex direttore della *cybersecurity* dell'amministrazione Obama, parla esplicitamente di un punto di crisi.

L'alto tasso di turnover nel settore della *cybersecurity* è determinato da un notevole *skills gap*: attualmente, a fronte di 1.108.725 persone impiegate negli Usa, restano ancora da coprire 769.736 posizioni (CyberSeek 2022). Se poi si considera che nel settore privato della *cybersecurity* il personale gode di remunerazioni medie più alte del 14% rispetto al settore pubblico (Rosenberg 2022), diventano evidenti le ragioni del fatto che sia soprattutto la pubblica amministrazione a soffrire gli effetti di un vero e proprio *brain drain*. Su questo fenomeno ha di recente indagato la cronista del New Yorker Nicole Perlroth, che, in un corposo volume sulla corsa agli armamenti cibernetici, mostra come «alcuni dei migliori hacker della Nsa [*National security agency*] si stavano trasferendo oltreoceano, molti nel Golfo [persico]» (Perlroth 2021, 182). L'inchiesta di Perlroth testimonia come il personale di alto livello delle agenzie nazionali di sicurezza cibernetica, incentivato da stipendi raddoppiati e a volte persino quadruplicati, nonché dalla promessa di aiutare gli alleati degli Stati uniti a difendersi dai cyber attacchi, sia finito per utilizzare gli strumenti e le

metodologie sviluppati dalle agenzie pubbliche per sottoporre a sorveglianza elettronica i nemici dei monarchi mediorientali: leader di paesi ostili, oppositori politici, giornalisti e attivisti per i diritti umani. Si dispiegano, in questo caso, gli effetti più perversi della personalizzazione della burocrazia pubblica nella *cybersecurity*. Da un lato, infatti, le dinamiche del mercato del lavoro appena illustrate sottraggono allo Stato risorse umane, intese non soltanto in termini di personale dipendente ma anche come patrimonio di saperi, conoscenze, abilità e strumenti che quel personale ha sviluppato o appreso nel corso della sua funzione pubblica. Dall'altro lato, questa privatizzazione del personale mette sotto pressione la tutela delle libertà civili e politiche scolladola dalle garanzie degli stati costituzionali e, in ultima analisi, inficia la stessa sicurezza nazionale attraverso la produzione e l'esportazione incontrollata di tecniche di cyberinsecurity.

Il riferimento alla Nsa è utile anche per illustrare un altro aspetto dei rapporti pubblico-privato nel campo della *cybersecurity*. Come ha dimostrato Snowden, a partire dagli attentati del 2001, negli Usa fu istituzionalizzata un'efficace Ppp tra le agenzie governative di sicurezza elettronica e le digital corporation proprietarie degli elementi fondamentali della rete, in particolare piattaforme e operatori delle telecomunicazioni. Obiettivo della partnership era quello di operare, dentro e fuori i confini nazionali, un sistema di sorveglianza elettronica di massa. Esula dalle finalità di questo contributo una discussione, pur interessante, degli effetti di tali *policy* secretate sui regimi politici democratici. Ciò che è qui rilevante è che, come argomentato più ampiamente altrove (Santaniello 2021), gli strumenti sviluppati per la sorveglianza di massa dalle agenzie governative finiscano spesso per fungere da strumenti di sorveglianza personalizzata, un tipo di sorveglianza, cioè, che seleziona il suo target da uno sfondo di individui costantemente monitorati.

Quelle che qui abbiamo definito «personal public-private partnership», assieme alle dinamiche del mercato del lavoro della *cybersecurity* e del mercato transnazionale della sorveglianza personalizzata di massa, fanno luce su un processo di personalizzazione delle funzioni pubbliche di *cybersecurity* che va oltre la delega, l'esternalizzazione e la privatizzazione delle funzioni statali. Tale processo, infatti, mostra che il principio di azione monocratica non riguardi soltanto l'azione politica, ma anche la produzione e l'implementazione di politiche pubbliche, configurando un quadro, apparentemente paradossale, di monocratizzazione diffusa, in cui l'azione statale diventa funzione delle decisioni assunte da una galassia di micro-monocrati sulla base di interessi individuali.

Frammenti di cybersecurity

Myriam Dunn Cavelty e Andreas Wenger (2022, 4) sostengono che «uno dei tratti costitutivi della politica della cybersecurity» sia la «frammentazione del potere politico». Tale frammentazione, secondo gli autori, sarebbe l'esito sia dei rapporti tra autorità governativa e soggetti esterni, sia di processi interni all'amministrazione. Per quanto riguarda i primi, la frammentazione dipenderebbe da una decentralizzazione di autorità e compiti, che vengono «delegati verso il basso (localizzazione), verso l'alto (sopranazionalizzazione), o di lato (privatizzazione)» (*ibidem*). All'interno delle organizzazioni pubbliche, invece, la frammentazione si alimenterebbe di quei processi di «crescente differenziazione funzionale dell'amministrazione» che comportano la necessità di «conoscenza esperta altamente specifica» che «appanna i confini tra settore pubblico e settore privato» (*ibidem*) con modalità di cui abbiamo già discusso poc'anzi. Altrove, gli autori fanno riferimento a un processo di «frammentazione dell'autorità e della responsabilità» come sfida chiave della governance della *cybersecurity* (Dunn Cavelty e Wenger 2020, 16). Un processo che deriva dalla natura «multistakeholder» delle arene politiche della governance delle reti, che «crea problemi di cooperazione e coordinamento orizzontali e verticali nel governo e all'intersezione tra stato, economia e società» (Dunn Cavelty e Wenger 2020, 20). Sembrerebbe dunque che, mentre la leadership della presidenza nella definizione delle politiche di *cybersecurity* evidenzia un processo di centralizzazione del potere politico, sul piano implementativo ed esecutivo, la caratteristica principale dell'esercizio del potere politico nell'ambito della *cybersecurity* sia la sua frammentazione in una moltitudine di spazi di governance. Questi due processi, centralizzazione e frammentazione, non sono nei fatti contraddittori. Innanzitutto perché è su questo puzzle di frammenti che attori individuali inseriti in molteplici reti di governance esercitano forme di micropotere. Alcuni di questi individui, come abbiamo visto in precedenza, sono esperti tecnici arruolati nelle istituzioni della sicurezza nazionale. Altri sono invece individui attivi nelle numerose arene decisionali multistakeholder che sono emerse a partire dai primi anni del 2000 a livello globale. Sebbene il modello multistakeholder sia spesso associato a una pluralizzazione delle arene di *policy*, nei fatti, ciascuno stakeholder è monocrate, o delegato di un'autorità monocratica. Come dimostrato in una precedente ricerca sui meccanismi dell'*Internet* governance multistakeholder (Palladino e Santaniello 2021), in questo tipo di arene operano quattro categorie di attori individuali: tecnici, attivisti, delegati di governi e delegati di aziende. I tecnici, che si riconoscono nella cosiddetta «technical community», e gli attivisti, che si concepiscono come rappresentanti della «global civil society», sono a tutti gli effetti *policy*

entrepreneurs che agiscono sulla base dei propri interessi e delle proprie reti di relazioni professionali e personali dentro un'eterogenea comunità epistemica transnazionale. Non sorprende dunque che tra queste prime due categorie di stakeholder e le altre due – personale di aziende e funzionari di governo – siano molto frequenti dinamiche di cooptazione, con casi numerosi di *revolving doors* (cioè di personale che nel corso della propria carriera passa dalle organizzazioni tecniche o della società civile a organizzazioni pubbliche o commerciali) e di *multi-hat* (ossia di soggetti che allo stesso tempo ricoprono posizioni sia nelle organizzazioni tecniche o nelle Ong, sia nelle industrie It o in organismi governativi). Ancora una volta, è il carattere personale dell'esercizio del potere l'aspetto dirimente per la comprensione della governance della *cybersecurity*, che si presenta come una *networked governance* i cui nodi sono rappresentati da singoli monocrati o da delegati di poteri monocratici. In secondo luogo, in queste arene frammentate, il settore pubblico è tipicamente rappresentato da delegati governativi, mentre la partecipazione di rappresentanti di corpi collettivi come partiti, parlamenti e sindacati è quantitativamente scarsa e politicamente irrilevante. Se la frammentazione, dunque, introduce maggiore pluralismo nell'arena politica della *cybersecurity* affiancando all'azione statale quella di attori privati, all'interno degli stessi stati essa ha un effetto centralizzante, che tende a conferire più potere agli esecutivi e ai loro leader, e a complicare enormemente le funzioni normative degli organismi collegiali.

Nella stessa direzione muove il processo di «tecnificazione» delle questioni pubbliche di *cybersecurity*. La tecnificazione, spiegano Hansen e Nissenbaum (2009), è un dispositivo discorsivo che «costruisce una questione di *policy* come dipendente da una conoscenza tecnica esperta [...] che presuppone un'agenda politicamente e normativamente neutrale [...] che favorisce una particolare costituzione di autorità epistemica e legittimità politica» (Hansen e Nissenbaum 2009, 1167). In questo scenario, la depoliticizzazione della *cybersecurity* riduce lo spazio di manovra degli organi politici collegiali, incapaci di elaborare risposte normative di carattere generale alle sfide della *cybersecurity*, e rinsalda le posizioni degli individui che, in virtù delle loro conoscenze tecniche, vengono legittimati nel ruolo di sovrani, più o meno assoluti, dello spazio di *policy*. Uno spazio che diventa opaco, costituito da luoghi decisionali e linguaggi inaccessibili al pubblico, con dinamiche simili a quelle descritte dalla letteratura sui triangoli di ferro. Inoltre, come rilevato da diversi studiosi di *cybersecurity*, la frammentazione, intesa come presenza di un numero eccessivo di stakeholder, crea fenomeni significativi di ingovernabilità e incertezza (Lupovici 2022; Eriksson e Giacomello 2022; Jusufi 2022), rispetto ai quali il potere esecutivo si può porre come forza risolutiva e fattore di stabilizzazione. Di conseguenza, così come la frammentazione dei corpi collettivi di Musella

rafforza la leadership di governo, che si legittima come strumento, ad un tempo, di governabilità e *responsiveness*, la frammentazione dell'autorità pubblica di cui parlano Dunn Cavelty e Wenger e la tecnificazione cui fanno riferimento Hansen and Nissenbaum sfociano in una personalizzazione del (micro)potere politico che si dispiega senza forme collettive di controbilanciamento e senza i limiti imposti dal controllo pubblico. È dunque dentro questo contesto di sovranità in frammenti e di iper-professionalizzazione che, secondo la teoria della securitizzazione della Scuola di Copenaghen, un discorso securitario diventa dominante e orienta le scelte di *policy*. Ed è su questo sfondo politico-istituzionale che la leadership presidenziale si legittima e si esercita priva di sostanziali *check and balances*. Essa assume carattere episodico, procedendo per singole controversie, mentre una legislazione di carattere generale ha più difficoltà ad emergere.

4. Conclusioni

La teoria della monocratizzazione postula un progressivo scivolamento dei regimi democratici contemporanei verso forme di governo più simili alle autocrazie. In questo saggio abbiamo argomentato come questo processo di trasformazione sia riscontrabile anche nella produzione di politiche pubbliche relative ai problemi di *cybersecurity*. L'analisi del caso statunitense nel periodo compreso tra il 2009 e il 2021 ha mostrato che i vettori della monocratizzazione abbiano effetti significativi nell'articolazione dei poteri statuali e nella definizione dell'azione istituzionale nel campo della sicurezza cibernetica. In particolare, abbiamo osservato che, sia con Obama che con Trump, la *cybersecurity* Usa viene intesa come compito della presidenza. Lo stile presidenziale, di conseguenza, influisce molto sulle modalità e sui contenuti del *policy-making* relativo ai problemi di sicurezza digitale, ma una tendenza strutturale alla monocratizzazione del campo di *policy* sembra evidente. Tale tendenza si manifesta, sul piano normativo, con l'alto numero di provvedimenti ad personam, inaugurati dalle disposizioni di Obama note come *cyber sanctions*, e con un utilizzo crescente dello strumento dell'*Executive order*. Sul piano comunicativo, invece, sebbene il tema della *cybersecurity* sia affrontato dai presidenti in modo sporadico, sui social media si dispiega secondo i canoni della comunicazione monocratica, ossia una comunicazione emotiva diretta tra presidente e cittadini, che, come argomentato, ha tre funzioni principali: – la rappresentazione dell'esercizio del potere presidenziale; – l'esercizio di pressione politica sugli organismi collegiali dell'arena legislativa, come i parlamenti e i partiti; – l'individuazione dei nemici del popolo e la loro sottoposizione a un processo

mediatico. Se a livello normativo e comunicativo la monocratizzazione delle politiche pubbliche di *cybersecurity* si traduce in una leadership della presidenza nel definire priorità e obiettivi di *policy*, e, in ultima analisi, in una centralizzazione del potere politico, a livello implementativo essa assume le forme di un potere personalizzato e frammentato. L'efficacia del principale strumento di *policy* adottato dai piani di *cybersecurity*, le *public-private partnership*, come abbiamo visto, dipende in larga misura da variabili di tipo individuale, e in particolare dalle relazioni personali pregresse tra gli addetti dei settori pubblico e privato. Abbiamo inoltre osservato che la struttura del mercato del lavoro della *cybersecurity* produce un processo di privatizzazione continua delle risorse umane delle organizzazioni pubbliche. Tale processo conduce a quella che abbiamo definito «monocratizzazione diffusa», in cui l'azione statale diventa funzione delle decisioni assunte da una galassia di micro-monocrati sulla base di interessi individuali, e a fenomeni di sorveglianza personalizzata di massa, in cui gli obiettivi della sorveglianza vengono selezionati e ingranditi su uno sfondo di controllo massivo e generalizzato. La personalizzazione dell'esercizio del potere pubblico e la diffusione del principio di azione politica monocratica a livello micro si alimentano, inoltre, di un processo di frammentazione degli spazi di *policy* della *cybersecurity*, in cui le finzioni della rappresentanza multistakeholder e le opacizzazioni prodotte dalla tecnificazione delle questioni di *policy* concorrono a depoliticizzare le decisioni politiche, sottraendole, ad un tempo, all'autorità degli organi politici collegiali e allo scrutinio del pubblico. In questo scenario, la monocratizzazione della *cybersecurity* sottopone a inedite tensioni alcuni principi fondamentali delle democrazie contemporanee: la tripartizione del potere, l'impersonalità delle funzioni pubbliche, l'astrattezza e la generalità della norma, la tutela dei diritti costituzionali, la pubblicità dei processi decisionali. La personalizzazione del potere, sia a livello macro che micro, modella confini e processi del *policy-making* relativo alla *cybersecurity*, e allo stesso tempo riconfigura l'architettura democratica progettando nuove forme, nuovi pesi e nuove misure.

In conclusione, la teoria della monocratizzazione sembra fornire coordinate concettuali utili nel catturare ed elaborare i processi costitutivi delle politiche di *cybersecurity*, e nell'inquadrare le interazioni sistemiche esistenti tra l'espansione della *cybersecurity* come campo di *policy* e le trasformazioni politiche dei regimi democratici contemporanei. L'analisi presentata in questo lavoro risente delle specificità del caso statunitense e del limite temporale dello studio, e non può supportare generalizzazioni rivolte a definire i rapporti tra democrazia e *cybersecurity*, o tra monocratizzazione e politiche pubbliche. D'altra parte, essa può avviare una riflessione e una linea di ricerca che si occupi di indagare e valutare i processi di monocratizzazione delle politiche digitali,

a partire da quelle relative alla sicurezza. Da questa prospettiva, è possibile fissare almeno tre obiettivi di una simile agenda di ricerca. Il primo, è quello di elaborare e affinare una metodologia quali-quantitativa per il rilevamento delle traiettorie della monocratizzazione in differenti ambiti di *policy*. Il secondo obiettivo è incrementare il numero di casi di studio per analizzare il rapporto tra monocratizzazione e *cybersecurity*, e di procedere ad analisi comparative tra diversi regimi democratici e tra regimi democratici e non democratici. Il terzo obiettivo è comparare diverse politiche digitali, per meglio comprendere i processi di monocratizzazione in contesti in cui le dinamiche della securitizzazione siano meno determinanti rispetto a quanto avviene nel campo della *cybersecurity*. Si tratta, con tutta evidenza, di un'agenda ambiziosa e per sua natura multidisciplinare, che appare pur tuttavia necessaria per governare la cyber-insicurezza e la cyber-paura globale (Stocchetti 2022), ed evitare che alla cosiddetta rivoluzione digitale segua un regime del (cyber)terrore.

Riferimenti bibliografici

Amoretti, F., Fittipaldi, R. e Santaniello, M. (2021), *Poteri monocratici e comunicazione politica ai tempi della pandemia. Dal governo Conte II al governo Draghi*, in «Comunicazione politica», 3, pp. 333-356.

Birnhack, M. D. e Elkin-Koren, N. (2003), *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, in «SSRN Electronic Journal», doi:10.2139/ssrn.381020.

Blumfelde, S. (2022), *The role of international organizations in global cybersecurity governance*, in «Rivista di Digital Politics», 2(3), pp. 331-350.

Calise, M. (2010), *Il partito personale: I due corpi del leader*, Roma-Bari, Laterza.

Carr, M. (2016), *Public-private Partnerships in National Cyber-security Strategies*, in «International Affairs», 92(1), pp. 43-62.

Chhabra, R. (2020), *Twitter Diplomacy: A Brief Analysis*, Observer Research Foundation (ORF). https://www.orfonline.org/wp-content/uploads/2020/01/ORF_IssueBrief_335_TwitterDiplomacy.pdf.

Christensen, K. K. e Petersen, K. L. (2017), *Public-private Partnerships on Cyber Security: A Practice of Loyalty*, in «International Affairs», 93(6), pp. 1435-1452.

Creese, S., Dutton, W. H. e Esteve-González, P. (2021), *The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions*, in «Personal and Ubiquitous Computing», 25(5), pp. 941-955.

Criscitiello, A. (2020), *Il potere normativo del Presidente del Consiglio in Italia*, in F. Musella (a cura di) *L'emergenza democratica. Presidenti, decreti, crisi pandemica*, Napoli, Editoriale Scientifica, pp. 47-87.

CyberSeek (2022), *Cybersecurity Supply/Demand Heat Map*. https://www.cyberseek.org/heatmap.html.

Dunn Cavelty, M. (2009), *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*, London, Routledge.

Dunn Cavelty, M. (2013), *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse*, in «International Studies Review», 15(1), pp. 105-122.

Dunn Cavelty, M. e Brunner, E. M. (2007), *Introduction: Information, Power, and Security – An Outline of Debates and Implications*, in M. Dunn e S. F. Krishna-Hensel (a cura di), *The Resurgence of the State: Trends and Processes in Cyberspace Governance*, London, Routledge, pp. 1-17.

Dunn Cavelty, M. e Egloff, F. J. (2019), *The Politics of Cybersecurity: Balancing Different Roles of the State*, in «St Antony's International Review», 15, pp. 37-57.

Dunn Cavelty, M. e Wenger, A. (2020), *Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science*, in «Contemporary Security Policy», 41(1), pp. 5-32.

Dunn Cavelty, M. e Wenger, A. (2022), *Cyber Security between Socio-technological Uncertainty and Political Fragmentation*, in M. Dunn Cavelty e A.Wenger (a cura di), *Cyber Security Politics: Socio-technological Transformations and Political Fragmentation*, London, Routledge, pp. 1-13.

Eriksson, J. e Giacomello, G. (2022), *Cyberspace in Space*, in M. Dunn Cavelty e A. Wenger (a cura di), *Cyber Security Politics*, London, Routledge, pp. 95-108.

Faris, R., Roberts, H., Etling, B., Othman, D. e Benkler, Y. (2015), *Score Another One for the Internet? The Role of the Networked Public Sphere in the U.S. Net Neutrality Policy Debate*, in «SSRN Electronic Journal», doi:10.2139/ssrn.2563761.

Follis, L. e Fish, A. (2020), *Hacker States*, Cambridge MA, MIT Press.

Fouad, N. S. (2022), *The non-Anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity*, in «Review of International Studies», 48(4), pp. 766-785.

Fracchiolla, D. (2022), *La cyber-diplomacy, la nuova frontiera delle relazioni internazionali*, in «Rivista di Digital Politics», 2(3), pp. 463-484.

Hansen, L. e Nissenbaum, H. (2009), *Digital Disaster, Cyber Security, and the Copenhagen School*, in «International Studies Quarterly», 53(4), pp. 1155-1175.

Harknett, R. J. e Stever, J. A. (2011), *The New Policy World of Cybersecurity*, in «Public Administration Review», 71(3), pp. 455-460.

Homburger, Z. (2019), *The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace*, in «Global Society», 33(2), pp. 224-242.

Huang, K., Madnick, S., Zhang, F. e Siegel, M. (2022), *Varieties of Public-private co-governance on Cybersecurity within the Digital Trade: Implications from Huawei's 5G*, in «Journal of Chinese Governance», 7(1), pp. 81-110.

Itu (2023), *National Cybersecurity Strategies Repository*, International Telecommunications Union, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

Isc2 (2022), *Cybersecurity Workforce Study*, pp. 1-86, https://www.isc2.org/Research/Workforce-Study.

Jusufi, I. (2022), *Uncertainty, Fragmentation, and International Obligations as Shaping Influences*, in M. Dunn Cavelty e A. Wenger (a cura di), *Cyber Security Politics*, London, Routledge, pp. 172-185.

Karabacak, B., Tatar, U., Karabacak, O. e Celik, M. (2014), *A Comparative Analysis of the National Cyber Security Strategies of Leading Nations*, International Conference on Cyber Warfare and Security. https://fuse.franklin.edu/facstaff-pub/38.

Karataş, A. (2020), *The Comparative Analysis of National Cyber Security Policies: United States*, United Kingdom and Turkey Examples, in «Journal Of Academic Social Resources», 5(19), pp. 737-751.

Karpiuk, M. e Kostrubiec, J. (2022) (a cura di), *The Public Dimension of Cybersecurity*. Institute for Local Self-Government, http://www.lex-localis.press/index.php/LexLocalisPress/catalog/book/ThePublicDimensionofCybersecurity.

Kello, L. (2013), *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, in «International Security», 38(2), pp. 7-40.

Lawson, S. (2012), *Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States*, in «First Monday». doi:10.5210/fm.v17i7.3848.

Lawson, S. (2013), *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats*, in «Journal of Information Technology and Politics», 10(1), pp. 86-103.

Lawson, S. e Middleton, M. K. (2019), *Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016*, in «First Monday», doi:10.5210/fm.v24i3.9623.

Loiseau, H., Ventre, D. e Aden, H. (2020) (a cura di), *Cybersecurity in Humanities and Social Sciences: A Research Methods Approach*, Hoboken, Wiley.

Lowi, T. J. (1988), *The Personal President: Power Invested, Promise Unfulfilled*, Ithaca, Cornell University Press.

Lupovici, A. (2022), *Uncertainty and the Study of Cyber Deterrence*, in M. Dunn Cavelty e A. Wenger (a cura di), *Cyber Security Politics*, London, Routledge, pp. 128-137.

Metz, M., Kruikemeier, S. e Lecheler, S. (2020), *Personalization of Politics on Facebook: Examining the Content and Effects of Professional, Emotional and Private Self-personalization*, in «Information, Communication and Society», 23(10), pp. 1481-1498.

Miao, W., Xu, J. e Zhu, H. (2019), *From Technological Issue to Military-Diplomatic Affairs: Analysis of China's Official Cybersecurity Discourse* (1994-2016), in J. Hunsinger, M. M. Allen e L. Klastrup (a cura di), *Second International Handbook of Internet Research*, Heidelberg, Springer Netherlands, pp. 1-13.

Mickoleit, A. (2014), *Social Media Use by Governments: A Policy Primer to Discuss Trends*, Identify Policy Opportunities and Guide Decision Makers, OECD Working Papers on Public Governance, 26, doi:10.1787/5jxrcmghmk0s-en.

Min, K.-S., Chai, S.-W. e Han, M. (2015), *An International Comparative Study on Cyber Security Strategy*, in «International Journal of Security and Its Applications», 9(2), pp. 13-20.

Musella, F. (2018), *Political Leaders beyond Party Politics*, London, Palgrave Macmillan.

Musella, F. (2020), *Capi di Governo. Dalla primazia all'emergenza*, in F. Musella (a cura di), *L'emergenza democratica. Presidenti, decreti, crisi pandemica*, Napoli, Editoriale Scientifica, pp. 9-45.

Musella, F. (2022), *Monocratic Government: The Impact of Personalisation on Democratic Regimes*, Berlino, De Gruyter.

Nissenbaum, H. (2005), *Where Computer Security Meets National Security*, in «Ethics and Information Technology», 7(2), pp. 61-73.

Norris, D. F., Mateczun, L. e Forno, R. (2022), *Cybersecurity and Local Government*, Hoboken, Wiley.

Palladino, N. e Santaniello, M. (2021), *Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance Analyzing IANA Transition*, London, Palgrave Macmillan.

Perlroth, N. (2021), *This is How they Tell me the World Ends: The Cyberweapons Arms Race*, London, Bloomsbury Publishing.

Petersen, K. L. (2014), *The Politics of Corporate Security and the Translation of National Security*, in K. Walby e R. K. Lippert (a cura di), *Corporate Security in the 21st Century*, London, Palgrave Macmillan, pp. 78-94.

Poguntke, T. e Webb, P. (a cura di) (2005), *The Presidentialization of Politics: A Comparative Study of Modern Democracies*, Oxford, Oxford University Press.

Rosenberg, S. (2022), *Cybersecurity's Public-private Salary Gap*, in «Axios», https://www.axios.com/2022/08/30/cybersecurity-public-private-salary-gap.

Rosenkrantz, H. (2021), *The Big Quit: Why Cybersecurity Pros Are Leaving Government*, in «Tanium», https://www.tanium.com/blog/the-big-quit-why-cybersecurity-pros-are-leaving-government/.

Santaniello, M. (2021), *Sunburst. La grande eclissi della cybersecurity Usa*, in «Rivista di Digital Politics», 1(1), pp. 179-194.

Schemeil, Y. (2022), *Undiplomatic Ties: When Internet Blocks Intermediation*, in M. Marzouki e A. Calderaro (a cura di), *Internet Diplomacy: Shaping the Global Politics of Cyberspace*, Lanham, Rowman and Littlefield, pp. 21-44.

Shively, J. (2021), *Cybersecurity Policy and the Trump Administration*, in «Policy Studies», 42(5-6), pp. 738-754.

Stevens, T. (2018), *Global Cybersecurity: New Directions in Theory and Methods*, in «Politics and Governance», 6(2), pp. 1-4.

Štitilis, D., Pakutinskas, P. e Malinauskaitė, I. (2017), *EU and NATO Cybersecurity Strategies and National Cyber Security Strategies: A Comparative Analysis*, in «Security Journal», 30(4), pp. 1151-1168.

Stocchetti, M. (2022), *Knowledge, democracy and the politics of (cyber)fear*, in «Rivista di Digital Politics», 2(3), pp. 351-368.

Stoddart, K. (2016), *Live Free or Die Hard: U.S.-UK Cybersecurity Policies*, in «Political Science Quarterly», 131(4), pp. 803-842.

Van Santen, R. e Van Zoonen, L. (2010), *The Personal in Political Television Biographies*, in «Biography», 33(1), pp. 46-67.

Vogel, R. (2016), *Closing the Cybersecurity Skills Gap*, in «Salus journal», 4(2), pp. 32-46.

Wu, T. (2003), *Network Neutrality, Broadband Discrimination*, in «SSRN Electronic Journal», doi:10.2139/ssrn.388863.

Zeffiro, A., Niessen, G., Oberst, C., McEwan, S., Cochrane, A. e Durand, J. (2022), *Discourses on Cybersecurity. The Politics of the Data Breach as a Security Crisis*, in «Rivista di Digital Politics», 2(3), pp. 369-398.