

## Die parlamentarische Kontrolle digitaler Räume

### I. Einleitung

Der Begriff der Digitalisierung hat in den letzten Jahren einen beispiellosen Siegeszug gehalten. Dies betrifft zunächst wissenschaftliche und praktische Diskussionen zu den Fragen der zugrunde liegenden Technologien, hat sich inzwischen aber auf viele andere Felder erstreckt. Ausgehend von den technischen Innovationen haben sich neuartige, vor allem datenbasierte Geschäftsmodelle entwickelt, die sich durch eine erhebliche Volatilität auszeichnen und in den Wirtschaftswissenschaften intensiv erforscht werden.<sup>1</sup> Neben diesen beiden Hauptsträngen der technischen und ökonomischen Wissenschaften werden die Auswirkungen der Digitalisierung inzwischen aber auch in anderen Disziplinen untersucht. Dies betrifft beispielsweise Soziologie, Psychologie und Kulturwissenschaften,<sup>2</sup> aber auch die Rechtswissenschaften.<sup>3</sup>

---

<sup>1</sup> Zu den insbesondere datenbasierten Geschäftsmodellen und ihren Auswirkungen s. grundsätzlich Stengel/van Looy/Wallaschkowski (Hrsg.), *Digitalzeitalter – Digitalgesellschaft. Das Ende des Industriezeitalters und der Beginn einer neuen Epoche*, 2017; zur wirtschaftswissenschaftlichen Sicht näher *Berman, Strategy & Leadership* 40 (2012) 2, 16; *Weill/Woerner, MIT Sloan Management Review* 54 (2013) 3, 71; *Bharadwaj/El Sawy/Pavlou/Venkatraman, MIS Quarterly* 37 (2013) 2, 471; *Baden-Fuller/Haefliger, Long Range Planning* 46 (2013) 6, 419; *Fitzgerald/Kruschwitz/Bonnet/Welch, MIT Sloan Management Review* 55 (2014) 2, 1; *Lerch/Gotsch, Research-Technology Management* 58 (2015) 5, 45; s.a. unten II. 2.

<sup>2</sup> S. z.B. *Stalder, Kultur der Digitalität*, 2016; *Turkle, Leben im Netz. Identität in Zeiten des Internet*, 1999; *Allert/Asmussen/Richter* (Hrsg.), *Digitalität und Selbst. Interdisziplinäre Perspektiven auf Subjektivierungs- und Bildungsprozesse*, 2017; *Wallace, The Psychology of the Internet*, 2. Auflage 2016; *Katzer, Cyberpsychologie. Leben im Netz: Wie das Internet uns verändert*, 2016.

<sup>3</sup> Je nach Begriffsverständnis sind die zugrundeliegenden Rechtsfragen teils erheblich älter. In den letzten Jahren wird der Begriff der Digitalisierung für viele unterschiedliche Phänomene verwendet und dementsprechend auch mit sehr unterschiedlichen Rechtsfragen in Verbindung gebracht. S. nur aus jüngster Zeit als relativ beliebige Beispiel: Reform des BGB (*Wendehorst, NJW* 2016, 2609), Energiewende (*Lange/Möllnitz, EnWZ* 2016, 448), Arbeitsschutz (*Wiebauer, NZA* 2016, 1430), Verwaltungsmodernisierung (*Martini, DÖV* 2017, 443), Genossenschaften (*Peter/Jungmeister, ZfG* 2017, 133), Mitbestimmung (*Wisskirchen/Schiller/Schwinding, BB* 2017, 2105), Datenschutz (*Schmidt-fortzig, NdsVBl* 2018, 1), Arbeitskampf (*Giesen/Kersten, NZA* 2018, 1), kommunale Selbstverwaltung (*Götz, NdsVBl* 2018, 9), M&A-Transaktionen (*Grub/Krispenz, BB* 2018, 235) oder auch eine „Neuerfindung des Rechts“ (*Boehme-Neßler, NJW* 2017, 3031).

Nicht zuletzt hat das Schlagwort der Digitalisierung Einzug in politische Debatten gehalten<sup>4</sup> und bündelt hier viel Aktivität der Parlamente und Regierungen.<sup>5</sup> Letzteres wurde im Jahre 2017 besonders deutlich: Das Bundesministerium für Wirtschaft und Technologie benannte das von ihm organisierte jährliche Treffen einer Vielzahl von Entscheidungsträgern aus Wirtschaft und Politik rund um den IT-Standort Deutschland nach zehn Jahren von „IT-Gipfel“ in „Digital-Gipfel“ um.<sup>6</sup>

Trotz oder gerade wegen der umfassenden Diskussionen in Wissenschaft und Praxis weist der Terminus der Digitalisierung bislang festen Inhalt auf. Je nach Disziplin und Erkenntnisinteresse richtet er sich stärker auf die veränderten technischen Möglichkeiten und Rahmenbedingungen, die neuartigen individuellen Kommunikations- und Interaktionsmöglichkeiten, die Auswirkungen auf das Verhalten von Gruppen, Organisationen oder Netzwerken oder schließlich auf die sozialen Normen, die dieses Verhalten steuern. Deutlich ist aber jedenfalls, dass es um zentrale technische, ökonomische, politische und rechtliche Entwicklungen geht, die in absehbarer Zukunft alle gesellschaftlichen Bereiche betreffen und nur sehr wenige Individuen nicht betreffen werden.

Das Phänomen der Digitalisierung erfasst – wenig überraschend – auch das Verhältnis des Parlaments zur Exekutive. Wenn die Arbeit von Regierung und Verwaltung zunehmend in digitalen Räumen stattfindet, so ändert sich das Objekt parlamentarischer Kontrolle. Dies kann nicht ohne Auswirkungen auf die Akteure und die Modi bleiben, in denen sich diese Kontrolle vollzieht.

Im Weiteren wird deshalb zunächst die Frage aufgeworfen, wie sich derartige digitale Räume näher beschreiben lassen und unter welchen Gesichtspunkten sie sich von der bisherigen Tätigkeit der Exekutive unterscheiden (II.). Auf Basis dieser Annäherung lassen sich Charakteristika herausarbeiten, die zu allgemeinen Kontrolldefiziten führen, die bisher vor allem als Regulierungsprobleme diskutiert worden sind beziehungsweise an diese Probleme anschließen (III.). Für das engere Feld der parlamentarischen Kontrollierbarkeit digitaler Räume werden sodann drei paradigmatische Problemfelder identifiziert (IV.): Die Volatilität des Kontrollgegenstands, die Organisation der Kontrolle in allgemeinen und/oder spezifischen Bundestagsausschüssen sowie die Fragen der Kontrolle nachrichtendienstlicher Tätigkeit in digitalen Räumen. Im Ergebnis lassen sich erste Ansätze zu einer „digitalen parlamentarischen Kontrolle“ identifizieren (V.).

<sup>4</sup> Die Bundesregierung verfolgte in der letzten Legislaturperiode eine „Digitale Agenda 2014–2017“, s. den Legislaturbericht „Digitale Agenda“ 2014–2017, BT-Drucks. 18/12130.

<sup>5</sup> S. z. B. den Schlussbericht (BT-Drucks. 17/12550) sowie die Zwischenberichte (Übersicht ebd., 6) der Enquête-Kommission des Bundestags „Internet und digitale Gesellschaft“.

<sup>6</sup> S. <http://www.it-gipfel.de/>. Der Digital-Gipfel 2017 fand am 12. und 13.6.2017 in der Metropolregion Rhein-Neckar und hatte das Motto „vernetzt besser leben“.

## II. „Digitale Räume“ – eine Annäherung

Die parlamentarische Kontrolle der Exekutive muss sich – will sie effektiv sein – auf konkrete Akteure und konkrete Vorgänge beziehen.<sup>7</sup> Dem scheint die Metapher der digitalen Räume zunächst entgegenzustehen, weil beide Bestandteile diffus wirken und deshalb erläuterungsbedürftig sind. Gerade auf diesem Weg lassen sich jedoch die Herausforderungen für die parlamentarische Tätigkeit herausarbeiten.

### 1. Physische, körperlose und digitale Räume

Der Begriff des Raums bezeichnet in der klassischen Physik vor *Einstein* einen dreidimensionalen „Behälter“ für Materie und Felder, in dem sich bestimmte beobachtbare Vorgänge ereignen.<sup>8</sup> Dieses Verständnis ist relativ nahe an der Umgangssprache und im klassischen Sinne auch als Zuordnungsmechanismus für eine rechtliche Verantwortlichkeit geeignet: Das Eigentum kann eine Herrschaftsmacht über ein dreidimensional begrenztes Gebilde verleihen, die Existenz eines Staates die Staatsgewalt über ein dreidimensional begrenztes Staatsgebiet.

Der digitale Raum sperrt sich freilich gegen ein solches Denken in klassischen physikalischen Dimensionen. Vielmehr wird mit ihm häufig „das“ Internet bezeichnet,<sup>9</sup> freilich in einer spezifischen Weise, nämlich als „körperloser Sozialraum“.<sup>10</sup> Dieser ermöglicht seit einigen Jahren eine schon heute kaum noch zu überblickende und dennoch immer weiter zunehmende, in spezifischer Weise dis-

---

<sup>7</sup> Zur parlamentarischen Kontrolle der Regierung und Verwaltung s. grundsätzlich *Krebs*, Kontrolle in staatlichen Entscheidungsprozessen, 1984; *Steffani*, in: *Schneider/Zeh* (Hrsg.), *Parlamentsrecht und Parlamentspraxis in der Bundesrepublik Deutschland*, 1989, § 49; *Klein*, in: *Maunz-Dürig*, Art. 38 GG Rn. 51 ff.; *Schliesky*, in: *Morlok/Schliesky/Wiefelspütz* (Hrsg.), *Parlamentsrecht*, 2016, § 5 Rn. 66 ff., jeweils auch zu den Problemfeldern. Im Grundsatz dürfte die Rechenschaftspflicht der Exekutive gegenüber dem Parlament in allen westlichen Demokratien anerkannt sein. Die konkrete Ausgestaltung der Kontrolle, ihre Instrumente sowie insbesondere ihre Grenzen hängen aber stark von der spezifischen Verfassungsordnung ab. Dies gilt insbesondere für das Recht der Exekutive, in bestimmten, regelmäßig sicherheits- oder außenpolitisch sensiblen Bereichen nur lose durch die Legislative determiniert und von ihr kontrolliert zu werden. S. dazu für Deutschland den Beitrag von *Risse* in diesem Band.

<sup>8</sup> S. die Beschreibung als „container“ bei *Einstein*, Vorwort zu *Jammer*, *Das Problem des Raumes*, 1960, S. XIII ff.

<sup>9</sup> „Das“ Internet gibt es schon deshalb nicht, weil die weltweite und zunehmende Vernetzung technischer Geräte sich permanent wandelt, indem bestimmte Systeme ausgesondert und (sehr viel mehr) neue Systeme an das Netz angeschlossen werden. Systematisch wichtiger ist, dass das Internet aus einer Vielzahl unterschiedlicher Dienste besteht. Die bekanntesten sind die E-Mail und das World Wide Web (WWW), das umgangssprachlich häufig als „das Internet“ bezeichnet wird. S. zur Entwicklung *Hafner/Lyon*, *ARPA Kadabra oder Die Anfänge des Internet*, 3. Auflage 2008; lesenswerte Chronologie bei *Zakon*, *Hobbes' Internet Timeline*, <https://www.zakon.org/robert/internet/timeline/>.

<sup>10</sup> Mit dieser Bezeichnung schon *Roßnagel*, *ZRP* 1997, 26 (28).

tanzvermittelte Individual- und Massenkommunikation. Sie zeichnet sich dadurch aus, dass zum einen herkömmliche Kommunikationsformen substituiert werden, indem beispielsweise persönliche Nachrichten nicht mehr per Briefpost, sondern auf elektronischem Wege (per E-Mail, Instant-Messenger, Chat o.ä.) ausgetauscht werden. Zum anderen entstehen völlig neue Kommunikationsformen, die in Offline-Zusammenhängen nicht möglich wären. Das gilt seit einigen Jahren insbesondere für das sogenannte Web 2.0 (Social Media oder „Mitmach-Web“), das sich dadurch auszeichnet, dass die zuvor eher passiven Nutzerinnen und Nutzer nunmehr selbst in verschiedenen Mischformen als „Prosumer“ agieren.<sup>11</sup>

Es ist unmöglich anzugeben, welcher Anteil der gesamtgesellschaftlichen Kommunikation sich in digitalen Räumen abspielt. Sicher ist, dass dieser Anteil schon heute erheblich ist und bis auf weiteres immer weiter wachsen wird.<sup>12</sup> Dies betrifft sowohl rein privates und familiäres Handeln als auch praktisch jede Form von wirtschaftlichen Aktivitäten sowie den staatlichen Bereich, nämlich durch den Staat bereitgestellte Informationen, das Senden und Empfangen von Kommunikationsinhalten sowie – so die vielfache Hoffnung – in einer nicht allzu fernen Zukunft die durchgängige und medienbruchfreie Abwicklung von Transaktionen im Electronic Government.

Ein aktueller Trend der technischen Entwicklung verbindet diesen körperlosen Sozialraum mit physischen<sup>13</sup> Räumen. Nachdem Ideen eines Ubiquitous Computing<sup>14</sup> über lange Jahre mehr visionären Charakter hatten, drängt die Vernetzung physischer Objekte nunmehr mit Macht in die verschiedensten Lebensbereiche. Dies betrifft nicht nur „smarte“ Gegenstände wie Uhren, Vitalsensoren oder Fitnessarmbänder,<sup>15</sup> sondern zunehmend den Mobilitätsbereich (z.B. das vernetzte Automobil)<sup>16</sup> und insbesondere die Digitalisierung der produzierenden Industrie

<sup>11</sup> S. zu den Rechtsfragen z.B. die Beiträge in Hornung/Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media*, 2015.

<sup>12</sup> Dazu trägt insbesondere bei, dass digitale Räume heute ein wesentlicher Ort der Adoleszenz sind; s. dazu *Niemann/Schenk*, in: *Schenk/Niemann/Reinmann/Roßnagel*, *Digitale Privatsphäre*, 2012, S. 15 ff.; aus datenschutzrechtlicher Sicht *Roßnagel/Jandt*, ebd., S. 309 ff., 435 ff.

<sup>13</sup> Diese werden vielfach als „reale“ Räume bezeichnet. Soweit darin mitschwingt, die durch das Internet geschaffenen Räume seien nicht real, wäre dies ein jedenfalls in sozialer und kommunikativer Hinsicht fundamentales Missverständnis.

<sup>14</sup> S. aus technischer Sicht die Pionierarbeiten von *Weiser*, *Scientific American* 1991, H. 3, 66 ff.; s. ferner *Mattern* (Hrsg.), *Total vernetzt. Szenarien einer informatisierten Welt*, 2003; zu den rechtlichen Herausforderungen s. *Roßnagel*, *Datenschutz in einem informatisierten Alltag*, 2007; *Roßnagel/Geminn/Jandt/Richter*, *Datenschutzrecht 2016 – „Smart“ genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts*, 2016.

<sup>15</sup> S. *Hohmann*, *Datenschutz bei Wearable Computing. Eine juristische Analyse am Beispiel von Google Glass*, 2016; *Wilmer*, *K&R* 2016, 382; zum Einsatz am Arbeitsplatz *Weichert*, *NZA* 2017, 565; zu den Möglichkeiten einer Vernetzung mit dem Körper selbst s. *Hornung/Sixt*, *CR* 2015, 828.

<sup>16</sup> Zum vernetzten Automobil s. *Finken*, *Die Verwendung von Daten aus vernetzten Fahrzeugen*, 2017; ferner *Roßnagel*, *DuD* 2015, 353; *Lüdemann*, *ZD* 2015, 247; *Hornung*, *DuD* 2015, 359; zu den jüngsten Änderungen des StVG *Wagner/Goeble*, *ZD* 2017, 263; zu den Datennutzungsbefugnissen *Hornung/Goeble*, *CR* 2015, 265.

(Industrie 4.0).<sup>17</sup> Dieser Trend wird schon länger als Internet der Dinge bzw. Internet of Things (IoT) und in jüngerer Zeit vor allem als Einführung cyber-physischer Systeme (CPS) bezeichnet. Hier wird tatsächlich das digitalisiert, was bisher menschliche Räume ausmacht: Physische Objekte werden digital identifiziert, ihre Bewegungen mittels Lokalisierungstechnologien verfolgt und ihre Eigenschaften kontinuierlich mittels einer Vielzahl von Sensoren überwacht. Durch die Echtzeit-Speicherung und -Verarbeitung der dabei gewonnenen Daten erhalten sie digitale Repräsentanten, die in vernetzten Infrastrukturen analysiert, verwaltet und gesteuert werden können.

## 2. Das Phänomen der Digitalisierung

Als technisches Phänomen hat Digitalisierung zunächst keinen zwingenden Bezug zu Räumen gleich welcher Art (ob physisch, körperlos oder digital). Vielmehr lässt sich damit informationswissenschaftlich der Übergang von einer primär analogen zu einer digitalen Datenverarbeitung bezeichnen. Erst letztere erlaubt es, in großem Umfang Daten als Repräsentanten physischer Objekte oder kommunikativer Vorgänge zu erheben, zu speichern und weiterzuverarbeiten. Dies erfolgt in ebenfalls digitalen InformationsverarbeitungsKapazitäten.

Der Begriff der Digitalisierung lässt sich daneben aber auch eher transitional verstehen. Er beschreibt dann einen Umbruch, der allerdings nicht einmalig und eruptiv erfolgt, sondern permanente und grundlegende Veränderungen mit sich bringt („digitale Transformation“).<sup>18</sup> Dies betrifft maßgeblich neue, vor allem datenbasierte Geschäftsmodelle in der Wirtschaft, die häufig als Big Data oder Smart Data bezeichnet werden.<sup>19</sup> Die digitale Transformation bedingt daneben aber auch

---

<sup>17</sup> Zu den Rechtsfragen z.B. *Bräutigam/Klindt*, Digitalisierte Wirtschaft/Industrie 4.0, 2015; *Hornung/Hofmann*, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2015, S. 165 ff.; *dies.*, Industrie 4.0 und das Recht: Drei zentrale Herausforderungen, 2017; *Roßnagel/Jandt/Marschall*, in: Vogel-Heuser/Bauernhansl/ten Hompel (Hrsg.), Handbuch Industrie 4.0, 2017, S. 491 ff.

<sup>18</sup> Der Begriff der digitalen Transformation wird bislang vor allem in den Wirtschaftswissenschaften verwendet und bezeichnet dort die durch digitale Technologien und die darauf basierenden sozialen Verhaltensweisen bedingten Veränderungsprozesse in Unternehmen (v.a. Digitalisierung bestehender und Entstehung neuer Geschäftsmodelle), s. *Berman*, *Strategy & Leadership* 40 (2012) 2, 16; *Matt/Hess/Benlian*, *Business and Information Systems Engineering*, 57 (2015) 5, 339; paradigmatische Verwendungen z.B.: Proff/Fojcik (Hrsg.), *Mobilität und digitale Transformation. Technische und betriebswirtschaftliche Aspekte*, 2018; Schallmo et al. (Hrsg.), *Digitale Transformation von Geschäftsmodellen*, 2017; *Winkelhake*, *Die digitale Transformation der Automobilindustrie*, 2017; zur bisher noch heterogenen Begriffsbildung s. die Nachweise bei *Schallmo/Rusnjak*, in: Schallmo et al. (Hrsg.), *Digitale Transformation von Geschäftsmodellen*, 2017, S. 3 ff.; zum Zusammenhang mit sozialen Innovationen in Unternehmen *Zeuch*, in: Hildebrandt/Landhäußer (Hrsg.), *CSR und Digitalisierung*, 2017, S. 721 ff.; s.a. oben Fn. 1.

<sup>19</sup> S. zu den Rechtsfragen der datenbasierten Wirtschaft z.B. *Spindler*, DB 2018, 41; zu den Herausforderungen von Big Data *Fasel/Meier*, *Big Data: Grundlagen, Systeme und Nutzungspotenziale*, 2016; aus datenschutzrechtlicher Perspektive *Roßnagel*, ZD 2013, 562; *Weichert*, ZD 2013, 251; *Martini*, DVBl.

neue Regulierungs-, Regierungs- und Verwaltungsformen sowie schließlich neue Strukturen gesellschaftlicher Kommunikation insgesamt.

Je nachdem wie weit man den Begriff der Digitalisierung spannt, fällt ein zunehmender Teil der parlamentarischen Kontrolle in diesen Bereich – schlicht deshalb, weil das durch sie kontrollierte Handeln der Exekutive zunehmend in digitalen Räumen stattfindet. Nicht nur Regierung und Verwaltung, sondern auch die parlamentarische Arbeit sind deshalb Teil der digitalen Transformation.

### III. Kontrolldefizite digitaler Räume

Für Parlamente, ihre Untergliederungen und einzelne Abgeordnete bringt die digitale Transformation erhebliche Herausforderungen mit sich. Diese sind bisher vor allem als Probleme der Regulierung digitaler Räume diskutiert worden; insoweit stellen sich innerhalb der allgemeinen Diskussion um die Steuerbarkeit von Wirklichkeit durch Recht paradigmatische Fragen, weil digitale Räume sich aus den im Folgenden genannten Gründen (teilweise) mehr als andere Lebensbereiche gegen eine solche Steuerung widersetzen. Aus einer parlamentarischen Sichtweise zeigt sich im hier diskutierten Zusammenhang, dass viele dieser Besonderheiten nicht nur für die Steuerung, sondern auch für die Kontrolle der Regierungs- und Verwaltungstätigkeit in digitalen Räumen Bedeutung erlangen.

Hervorgerufen werden die Probleme maßgeblich durch technische und ökonomische Besonderheiten. Zu nennen sind zunächst die psychologischen und soziologischen Bedingungen distanzvermittelter Kommunikation. Wenn Menschen sich ganz offensichtlich unter den Bedingungen angenommener oder echter Anonymität im Internet anders verhalten als in der „offline-“ oder in der klassischen Medienkommunikation,<sup>20</sup> so spielt dies auch für das Handeln der Exekutive eine Rolle.

Überdies vollzieht sich ein zunehmender Teil der demokratischen Kommunikation und Willensbildung in den sogenannten Echokammern des Internets. In diesen sorgen technische Filtermechanismen gerade bei großen Kommunikationsplattformen wie Facebook dafür, dass zum einen zweifelhaft, aber effektiv inszenierte Informationen mit großer Reichweite ausgestattet werden, zum anderen Nutzer vor allem Informationen erhalten, die ihren eigenen Einstellungen und Vorlieben entsprechen. Dieses Phänomen der „Filter Bubble“ ist aus rechtswissen-

---

2014, 1481; *Hoffmann-Riem*, AöR 142 (2017), 1; *Hornung/Herfurth*, in: König/Schröder/Wiegand (Hrsg.), *Big Data – Chancen, Risiken, Entwicklungstendenzen*, 2018, S. 149; allgemeiner die Beiträge in *Hoffmann-Riem* (Hrsg.), *Big Data – Regulative Herausforderungen*, 2018.

<sup>20</sup> In der Psychologie spricht man von einem „Online Disinhibition Effect“, s. die Begriffsbildung bei *Suler*, *CyberPsychology & Behavior* 7 (2014), 321. Anonymität ist zwar nicht der einzige, aber ein wesentlicher Faktor, s. ebd. sowie *Lapidot-Lefler/Barak*, *Computers in Human Behavior* 28 (2012), 434; *Zimmerman/Ybarra*, *Psychology of Popular Media Culture*, 5 (2016), 181.

schaftlicher Sicht vor allem für soziale Netzwerke untersucht worden.<sup>21</sup> Inwieweit sich durch derartige technische Voreinstellungen tatsächlich individuelle Einstellungen oder soziale Handlungen wie Wahlentscheidungen beeinflussen lassen, ist weithin ungeklärt.<sup>22</sup> Eindeutig ist hingegen, dass sich durch diese technischen Instrumente die Formen politisch relevanter Kommunikation massiv verändern – mit Auswirkungen auch auf die Kontrolle der Exekutive. In Europa haben die genannten Veränderungen zwar bisher in aller Regel nur am Rande Regierung und Verwaltung erfasst. In anderen Ländern der Welt lässt sich jedoch beobachten, dass es zu erheblichen Rückkopplungseffekten kommt, wenn Staats- und Regierungschefs nur noch bestimmte Teile der Internetgemeinde als ihr Zielpublikum begreifen. So erweckt US-Präsident *Trump* regelmäßig den Eindruck, sich nicht etwa dem Kongress oder der Öffentlichkeit gegenüber verantwortlich zu fühlen, sondern mehr oder weniger ausschließlich seinen eigenen Twitter-Followern.<sup>23</sup> Dies birgt ein erhebliches Gefahrenpotenzial nicht nur für die als „fake news“ diffamierten klassischen Medien, sondern auch für die parlamentarische Kontrolle.

Weitere Herausforderungen ergeben sich durch technische Besonderheiten. Neben den Fragen der kurzen Innovationszyklen und der zunehmenden Intransparenz<sup>24</sup> betrifft dies das Grundcharakteristikum des Internets, nämlich die technische Vernetzung. Auch staatliche Akteure vernetzen sich, und dies birgt die Gefahr einer Verantwortungsdiffusion, die einer klaren Zuordnung exekutiver Bereiche und Ebenen zu bestimmten Rechenschaftspflichten entgegensteht. Ein instruktives Beispiel hierfür ist der auf der Basis von Art. 91c GG und dem IT-Staatsvertrag eingerichtete IT-Planungsrat.<sup>25</sup> Dieser ist grundsätzlich ein sinnvolles Instrument, um die aus der Perspektive der Bürgerinnen und Bürger und ihrer „Lebenslagen“<sup>26</sup> oftmals schwer verständlichen Zuständigkeiten und die fehlende Interoperabilität zwischen den einzelnen staatlichen Ebenen im föderalen Bundesstaat zu adressieren. Wenn es im IT-Planungsrat aber letztlich aufgrund der Mög-

---

<sup>21</sup> Grundlegend *Pariser*, *The Filter Bubble*, 2011; anschauliche Erläuterung am Beispiel von Suchmaschinen bei *Jürgens/Stark/Magin*, in: Stark/Dört/Aufenanger (Hrsg.), *Die Googleisierung der Informationssuche. Suchmaschinen zwischen Nutzung und Regulierung*, 2014, S. 98 ff.; umfassend zu den Rechtsfragen *Hartl*, *Suchmaschinen, Algorithmen und Meinungsmacht*, 2017.

<sup>22</sup> S. allerdings die Selbstdarstellung der Datenanalysefirma Cambridge Analytica, die angibt, neben der US-Präsidentenwahl auch Einfluss auf das britische Brexit-Referendum genommen zu haben, s. <https://www.heise.de/-3999001>. Inwieweit dies der Wahrheit entspricht, lässt sich kaum nachvollziehen.

<sup>23</sup> Dieses Publikum ist nicht nur ein sehr spezieller Ausschnitt aus der allgemeinen Öffentlichkeit, sondern überdies durch den Account-Inhaber beeinflussbar. Dieser kann zwar seine Follower regelmäßig nicht vollständig löschen, wohl aber die Kommunikation mit ihnen blockieren.

<sup>24</sup> S. zu diesen Punkten unten IV.1 und 3.

<sup>25</sup> S. aus rechtlicher Sicht *Siegel*, NVwZ 2009, 1128; *Schulz/Tallich*, NVwZ 2010, 1338; *Steinmetz*, NVwZ 2011, 467; die Entscheidungen des IT-Planungsrats, aber auch Projekte, Maßnahmen und Anwendungen sind unter <https://www.it-planungsrat.de/> abrufbar.

<sup>26</sup> Zu diesem Grundkonzept der Organisation des Electronic Government s. *Müller*, *Das Konzept von Lebenslagen bei der Erbringung öffentlicher Dienstleistungen – am Beispiel der Zielgruppe Senioren*, 2010; *Hunnius/Schuppan/Stockmeier*, VM 2016, 187; zur rechtlichen Einordnung *Eifert*, *Electronic Government. Das Recht der elektronischen Verwaltung*, 2006, S. 169 ff.

lichkeit von Mehrheitsentscheidungen nach Art. 91c Abs. 2 Satz 2 und 3 GG zu verbindlichen Regelungen für Länderverwaltungen kommt, die diese eigentlich nicht mittragen wollen,<sup>27</sup> so stellt sich die Frage, wer das staatliche Handeln in diesen Räumen kontrolliert, und mit welchen Instrumenten.

Auf Basis der technischen Vernetzung hat sich das Internet außerdem als ein inhärent internationales Phänomen entwickelt. Dieses Charakteristikum ist zwar nicht absolut. Vielmehr tendieren viele Staaten weltweit zu einer Art Re-Nationalisierung und versuchen, mittels nationaler Regelungen Einfluss auf kommunikative Inhalte oder sogar technische Infrastrukturen zu gewinnen. Allerdings erreichen die Regulierungsbemühungen regelmäßig nicht das Ausmaß der chinesischen Internetzensur,<sup>28</sup> sondern sehen wie beispielsweise das aktuelle deutsche Netzwerkdurchsetzungsgesetz „nur“ in spezifischen Fällen erweiterte Pflichten für Informationsintermediäre vor.<sup>29</sup> Derartige Versuche bleiben also Ausnahmen von der Regel der Internationalität. Diese ist hingegen für jede Form nationaler parlamentarischer Kontrolle ein Problem, weil weitreichende Entscheidungen zu den Strukturen des Internets nicht national getroffen werden (können) – und damit auch nicht national kontrollierbar sind.<sup>30</sup>

Hinzu kommt, dass im Internet Datenflüsse grundsätzlich nicht an nationalen Grenzen Halt machen. Dies betrifft sowohl personenbezogene Daten als auch Betriebs- und Geschäftsgeheimnisse sowie staatliche Informationen. Die grundsätzliche Möglichkeit grenzenloser Datenerhebungen und -übermittlungen durch den Staat ist eine erhebliche Herausforderung, weil Datenmacht im Internet nicht nur die Macht globaler Oligopole ist, sondern eben auch die Macht staatlicher Akteure, die grenzüberschreitend aufgebaut und ausgeübt, jedoch viel schwieriger kontrolliert werden kann.

Insgesamt zeigt sich, dass sowohl die Regulierung als auch die Kontrolle dieser Räume voraussetzungsvoll sind. In der Folge stellen sich neue Anforderungen an Abgeordnete, ihre Mitarbeiterinnen und Mitarbeiter sowie die Parlamentsverwaltungen. Hergebrachte Regulierungs- und Kontrollinstrumente müssen überdacht und angepasst sowie durch neue Instrumente ergänzt werden. Hinzu tritt die Notwendigkeit der Abstimmung und Vernetzung mit anderen Akteuren. Dies betrifft

<sup>27</sup> Dazu Siegel, NVwZ 2009, 1128 (1130); Steinmetz, NVwZ 2011, 467 (468 f.); Gröpl, in: Maunz/Dürrig, Art. 91c Rn. 17 ff.

<sup>28</sup> Dazu z. B. Denjyer, [https://www.washingtonpost.com/413afe78-fff3-11e5-8bb1-f124a43f84dc\\_story.html?utm\\_term=.8e82da7e097b](https://www.washingtonpost.com/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?utm_term=.8e82da7e097b).

<sup>29</sup> Netzwerkdurchsetzungsgesetz vom 1.9.2017 (BGBl. I 3352); zu den Rechtsfragen und zur Kritik s. z. B. Wimmers/Heymann, AfP 2017, 93; Spindler, ZUM 2017, 473; Nolte, ZUM 2017, 552; Guggenberger, NJW 2017, 2577; Müller-Franken, AfP 2018, 1; Peifer, AfP 2018, 14; positiver Eifert, NJW 2017, 1450; Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Policy Paper: Das Netzwerkdurchsetzungsgesetz, 2018.

<sup>30</sup> Die Regulierung des Internets spielt sich in einem komplexen Geflecht aus staatlichen und nicht-staatlichen Akteuren ab. Zu dieser Internet Governance s. Weber, in: Hoeren/Sieber/Holznapel (Hrsg.), Handbuch Multimedia-Recht, Teil 2; zum Beispiel des Governance-Modells der ICANN z. B. Dederer, AVR 47 (2009), 367; Grewlich, K&R 2006, 156; Voegeli-Wenzl, GRUR Int 2007, 807.

beispielsweise neue Formen regulierter Selbstregulierung (und -kontrolle) im Bereich der Internetwirtschaft, die Zusammenarbeit mit anderen nationalen Parlamenten, aber auch die Interaktion mit supra- und internationalen Organisationen.

#### IV. Die parlamentarische Kontrollierbarkeit digitaler Räume: drei Problemfelder

Für das engere Feld der parlamentarischen Kontrolle lassen sich auf dieser Basis drei exemplarische Problemfelder identifizieren.

##### 1. Die Volatilität des Kontrollgegenstands

Das wohl augenfälligste Charakteristikum digitaler Räume sind ihre kurzen Innovationszyklen. Dies gilt sowohl aus einer technischen als auch aus einer ökonomischen Perspektive. Technische Neuerungen können zwar in aufwendigen Prozessen proaktiv rechtskonform gestaltet werden,<sup>31</sup> in der Praxis folgt ihre Gestaltung aber häufig eher Paradigmen der Machbarkeit oder Nützlichkeit.<sup>32</sup> Gesetzgeberisches Handeln kommt dann vielfach zu spät und wirkt in dem Versuch der nachträglichen Einflussnahme auf technische Strukturentscheidungen hilflos. Die ökonomischen Veränderungen der Digitalisierung werden beispielsweise daran erkennbar, dass im Jahre 2006 nur ein einziges Unternehmen der sogenannten „New Economy“ unter den zehn wertvollsten Unternehmen der Welt war (Microsoft auf Platz vier), im Jahre 2017 jedoch bereits die ersten sieben Plätze von solchen Unternehmen eingenommen wurden.<sup>33</sup>

Die Volatilität der technisch-ökonomischen Entwicklung ist ein Problem jeder professionellen Befassung mit digitalen Räumen. Dies gilt auch für die effektive parlamentarische Kontrolle. Das Electronic Government mag nicht dieselbe Innovationsgeschwindigkeit haben wie der Electronic Commerce, aber die Geschwindigkeit ist immer noch beachtlich. Eine effektive Kontrolle muss sowohl ad hoc auf aktuelle Entwicklungen reagieren als auch bestimmte Routinen entwickeln.

---

<sup>31</sup> S. grundlegend *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung. Umriss einer Forschungsdisziplin, 1993; Beispiele aus Forschungsprojekten bei *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, 2011, S. 41 ff.

<sup>32</sup> Ausnahmen bestätigen die Regel: So führte beispielsweise das Unternehmen WhatsApp Inc. (seit 2014 Teil von Facebook Inc.) im Jahre 2016 eine Ende-zu-Ende Verschlüsselung ein. Diese mag keine vollständige Sicherheit bieten, ist aber mutmaßlich der Verschlüsselungsdienst, der weltweit mit Abstand die meisten Nutzer hat.

<sup>33</sup> S. <https://proagile.de/digitalisierung-daten-sind-das-neue-oe/> (am Maßstab der Marktkapitalisierung); diese Entwicklung ist zwar nicht für die parlamentarische Kontrolle der Exekutive, wohl aber für die Internetregulierung eines der größten Probleme. Die Marktmacht typischerweise US-amerikanischer Oligopole lässt nicht nur im Datenschutzrecht, sondern auch in anderen Gebieten wie dem Wettbewerbs- oder Steuerrecht hergebrachte Regulierungskonzepte erodieren.

Ein sich ständig veränderndes Kontrollobjekt sperrt sich jedoch zumindest tendenziell gegen feste Strukturen und Abläufe der Kontrolle.

Unter diesen Bedingungen darf jedenfalls die Medien- und Technikkompetenz der Kontrolleure nicht schwächer sein als die der Kontrollierten. Grundvoraussetzung der Kontrolle ist deshalb die individuelle Fortbildung der beteiligten Abgeordneten und ihrer Mitarbeiter. Hinzu muss eine entsprechende sachliche und personelle Ausstattung treten. In diesem Sinne ist der neue ständige Bevollmächtigte des Parlamentarischen Kontrollgremiums<sup>34</sup> nicht nur ein Instrument zu seiner Professionalisierung, sondern auch zur Verringerung des Informationsgefälles zwischen Exekutive und Legislative, das gerade durch die kurzen Innovationszyklen der Technik verursacht wird. Selbst wenn man mit derartigen Instrumenten und zusätzlichen Fortbildungen gegensteuert, könnte sich allerdings das Informationsgefälle als klassisches Problem der parlamentarischen Kontrolle in Zukunft im Bereich der digitalen Räume strukturell so vertiefen, dass die Kontrolle faktisch infrage gestellt wird.

Zu diesem allgemeinen Problem treten spezifische Gefahren der Volatilität. Wenn parlamentarische Regulierung und Kontrolle erst zeitlich versetzt stattfindet, so kann es sehr schwierig sein, bereits getroffene technisch-organisatorische Weichenstellungen wieder zu revidieren. Auch wenn der normative Anspruch des Rechts hier nicht vor dem finanziellen Aufwand kapituliert, erhöht dieser rein faktisch doch erheblich die Hürden für nachträgliche Änderungen.

Ohne eine entsprechende Technikkompetenz und ständige Beobachtung technischer Entwicklungen läuft die parlamentarische Kontrolle überdies Gefahr, die rechtliche Relevanz technischer Gestaltungsentscheidungen zu unterschätzen. So mag es beispielsweise aus der Perspektive der Verwaltung durchaus sinnvoll sein, die Administration der IT-Infrastruktur nicht nur der Landesverwaltung, sondern auch der Gerichte bei einer bestimmten Ministerialverwaltung oder sogar einem privaten Dienstleister zu zentralisieren.<sup>35</sup> Dass eine solche Administration die Unabhängigkeit der Justiz angreifen kann und welche Schlussfolgerungen daraus für die konkrete Gestaltung abzuleiten sind,<sup>36</sup> lässt sich nur analysieren, wenn man die Technik im Detail versteht.

---

<sup>34</sup> S. dazu *Huber*, ZRP 2016, 162 (166); *Brissa*, DÖV 2017, 765 (767 f.); *Bartodziej*, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Teil VII § 2 Rn. 93 ff. sowie den Beitrag von *Risse* in diesem Band.

<sup>35</sup> Im Beispiel des Landes Hessen (Fn. 36) war dies die Hessische Zentrale für Datenverarbeitung (HZD), ein dem Finanzministerium unterstehender Landesbetrieb. Das Justizministerium hatte die Verwaltung des EDV-Netzes der Hessischen Justiz der HZD überlassen.

<sup>36</sup> S. dazu DienstGH Frankfurt, Urteil v. 22.04.2010 – DGH 4/08: Der Anschluss von Richterarbeitsplätzen an ein zentrales EDV-Netz, das durch die Exekutive unter Fachaufsicht des Justizministers verwaltet wird, beeinträchtigt nur dann nicht die richterliche Unabhängigkeit, wenn die Behandlung von Dokumenten des richterlichen Entscheidungsprozesses zum Schutz vor einer Kenntnisnahme durch Dritte schriftlich geregelt und deren Einhaltung durch den Minister der Justiz im gleichberechtigten Zusammenwirken mit gewählten Vertretern der Richterschaft überprüft werden kann. Hinzu kommen weitere technische Vorgaben, s. dazu und zum Problem *Krüger/Möllers*, MMR 2016, 728. Die weiterge-

Ein strukturelles Problem könnte sich schließlich in Zukunft einstellen, wenn die Exekutive zunehmend technische Instrumente einsetzt, die in ihrer Funktionsweise schon für sie selbst nicht mehr wirklich transparent sind. Bisherige Systeme des predictive policing lassen sich zwar noch technisch analysieren und damit kontrollieren.<sup>37</sup> Künftig wird es in Zeiten von Big Data, selbstlernenden Systemen und künstlicher Intelligenz jedoch zunehmend Anwendungen geben, deren Verhalten selbst ihre Entwickler nicht mehr genau verstehen können. Jenseits von klassischen Problemen wie der Verwechslung von Korrelation und Kausalität stellen sich hier zentrale Fragen der Kontrollierbarkeit – nicht nur für Parlamente, sondern auch für Gerichte, die Öffentlichkeit und die Betroffenen. Der zur Lösung des Transparenzproblems vorgeschlagene Weg einer „Algorithmenkontrolle“<sup>38</sup> stößt jedenfalls dann an seine Grenzen, wenn auch eine Offenlegung des Quellcodes einer Software nicht mehr dazu führt, dass deren Verhalten rechtlichen Maßstäben unterworfen werden kann.<sup>39</sup>

## 2. Die Organisation der Kontrolle: spezifische Ausschüsse vs. Digitalisierung aller Politikfelder

Das Bundesverfassungsgericht betont schon lange, dass ein wesentlicher Teil der Informations-, Kontroll- und Untersuchungsaufgaben des Bundestages durch die Ausschüsse wahrgenommen wird, die auf diese Weise in die Repräsentation des Volkes durch das Parlament einbezogen sind.<sup>40</sup> Dies führt zu der Frage, wie die Ausschüsse mit Blick auf digitale Räume am effektivsten organisiert werden können.

Das Grundgesetz kennt keinen Pflichtausschuss für derartige Räume. Die Organisation obliegt also der Geschäftsordnungsautonomie des Bundestags.<sup>41</sup> Grundsätzlich bestehen hierfür zwei Optionen. In der traditionellen Form werden

---

hende Revision (BGH – Dienstgericht des Bundes, MMR 2012, 128) und die Verfassungsbeschwerde (BVerfG, NJW 2013, 2102) blieben erfolglos. Die genannten Vorgaben des DienstGH Frankfurt sind durch das Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten sowie zur Änderung von Rechtsvorschriften v. 16.12.2011 (GVBl. I 2011, 778) umgesetzt worden; s. a. Köbler, DRiZ 2012, 164.

<sup>37</sup> Zu den Rechtsfragen des predictive policing s. Rademacher, AÖR 142 (2017), 366; Singelstein, NSTz 2018, 1.

<sup>38</sup> Martini, DVBl 2014, 1481 (1488).

<sup>39</sup> Zu den Möglichkeiten des Einsatzes von Algorithmen zur Verhaltenssteuerung s. Just/Latzer, Media, Culture & Society 39 (2017), 238; aus rechtlicher Sicht Hoffmann-Riem, AÖR 142 (2017), 1.

<sup>40</sup> BVerfGE 44, 308 (317 f.); 80, 188 (221 f.); 84, 304 (323); 130, 318 (351); s. a. BVerfGE 112, 118 (133 ff.); zu den Bundestags-Ausschüssen s. näher Klein, in: Maunz-Dürig, Art. 40 GG Rn. 126 ff.; Zeh, in: Schneider/Zeh (Hrsg.), Parlamentsrecht und Parlamentspraxis in der Bundesrepublik Deutschland, 1989, § 39; zu den Aufgaben Winkelmann, in: Morlok/Schliesky/Wiefelspütz (Hrsg.), Parlamentsrecht, 2016, § 23 Rn. 20 ff.

<sup>41</sup> Pieroth, in: Jarass/Pieroth, Art. 40 GG Rn. 3; näher zum Geschäftsordnungsrecht Cancik, in: Morlok/Schliesky/Wiefelspütz (Hrsg.), Parlamentsrecht, 2016, § 9 Rn. 32 ff.

die Ausschüsse spiegelbildlich zur Regierungsorganisation gebildet.<sup>42</sup> Dies ist im Regelfall sowohl aus einer Kontroll-, als auch aus einer Kooperationsperspektive sinnvoll, weil es eine klare Zuordnung der Sachfragen und eine geordnete Kommunikation ermöglicht.

Die Alternative besteht in der ressortübergreifenden Organisation entlang bestimmter Sachprobleme. Diesen Weg hat der Bundestag in der 18. Legislaturperiode mit der Einsetzung des Ausschusses Digitale Agenda gewählt.<sup>43</sup> Eine solche Organisation ermöglicht die zentrale Behandlung einer Frage, die als besonders wichtig erkannt wird und/oder einen Querschnittscharakter hat. Sie führt jedoch zu einem erheblichen Abstimmungsbedarf mit den Ausschüssen, die den einzelnen für die Materie zuständigen Ministerien zugeordnet sind.

Ein ressortübergreifender Ausschuss kann entweder eine zentrale Zuständigkeit für seine Sachmaterie erhalten oder begleitend, also „mitberatend“ tätig sein. Welche Variante gewählt wird, muss sich aus den Funktionen der Ausschüsse ableiten. Diese bestehen insbesondere in der Arbeitsentlastung des Plenums, der Vorbereitung seiner Entscheidungen, der Möglichkeit der Spezialisierung einer Gruppe von Abgeordneten sowie der Betonung der Bedeutung einer bestimmten Sachmaterie gegenüber anderen Akteuren in Wirtschaft, Verwaltung und Öffentlichkeit. Die Spezialisierung trägt dabei auch zu einer effektiveren parlamentarischen Kontrolle der Exekutive bei, weil sie den Wissensvorsprung der typischerweise ebenfalls spezialisierten Akteure in Regierung und Verwaltung vermindert.

Die Digitalisierung dürfte „das“ Querschnittsthema der aktuellen gesellschaftlichen Entwicklung sein. Dies rechtfertigt jedenfalls im Ausgangspunkt einen eigenen Ausschuss des Parlaments. Gerade wegen des alles übergreifenden Querschnittscharakters ist es jedoch keine sinnvolle Option, die Kontrolle des gesamten exekutiven Handelns in digitalen Räumen nur einem einzigen Ausschuss zuzuweisen. Mit der fortschreitenden Entwicklung würde dies eine immer weiter wachsende Zuständigkeit für sehr heterogene Sachfragen begründen. Vielmehr muss die Kontrolle zumindest überwiegend bei den jeweiligen Fachausschüssen bleiben. Folglich sollten beispielsweise das polizeiliche Handeln im Internet im Innenausschuss, die elektronische Organisation auswärtiger Beziehungen im Auswärtigen Ausschuss und die Einführung und Fortentwicklung der Telematik-Infrastruktur im Gesundheitswesen im Ausschuss für Gesundheit behandelt und durch diese Ausschüsse kontrolliert werden. Schon diese Beispiele zeigen, dass eine zentrale

---

<sup>42</sup> S. Zeh, in: Schneider/Zeh (Hrsg.), *Parlamentsrecht und Parlamentspraxis in der Bundesrepublik Deutschland*, 1989, § 39 Rn. 9 f.; Dach, ebd., § 40 Rn. 1; zur historischen Entwicklung Winkelmann, in: Morlok/Schliesky/Wiefelspütz (Hrsg.), *Parlamentsrecht*, 2016, § 23 Rn. 15 ff.

<sup>43</sup> S. den Antrag zur Einsetzung, BT-Drucks. 18/482; für einen solchen ständigen Ausschuss hatte auch die Enquête-Kommission „Internet und digitale Gesellschaft“ plädiert, s. den Siebten Zwischenbericht „Demokratie und Staat“, BT-Drucks. 17/12290, S. 100. Vorläufer war der Unterausschuss „Neue Medien“ beim ständigen Ausschuss „Kultur und Medien“; s.a. die kritische kontinuierliche Berichterstattung unter <https://netzpolitik.org/tag/btada/>.

Zuständigkeit angesichts der Besonderheiten der einzelnen Themen eine völlige Überforderung eines einzigen Ausschusses wäre.

Dennoch kann ein zentraler Ausschuss sinnvolle Aufgaben übernehmen. Dies betrifft beispielsweise Rechtsfragen, die ebenfalls so querschnittsartig sind, dass eine Zuweisung zu nur einem Fachausschuss sie in einer bestimmten, nicht immer überzeugenden Weise verortet. Ein Beispiel ist die Querschnitts-Rechtsmaterie par excellence, nämlich das Datenschutzrecht. Die bisherige Zuordnung zum Bundesministerium des Innern und zum Innenausschuss ist historisch gewachsen, inhaltlich aber wenig überzeugend. Angesichts der Bezüge zu nahezu allen Bereichen von Verwaltung und Wirtschaft liegt eine Befassung durch einen übergreifenden Ausschuss wie den zur Digitalen Agenda vielmehr nahe.<sup>44</sup> Denkbar erscheint auch eine Zuordnung infrastruktureller Fragen, sofern man darunter mehr als das wichtige, aber eben doch relativ enge Problem des Breitbandausbaus versteht.

Sinnvoll ist daneben die Zuständigkeit für das Regierungshandeln, soweit dieses ebenfalls übergreifende Fragen thematisiert. Dass die Bundesregierung beispielsweise seit Herbst 2014 für ihre eigene „digitale Agenda“ in dem namensgleichen Ausschuss Bericht erstattete,<sup>45</sup> überzeugt. Nur in einem solchen Ausschuss können übergreifende Fragen thematisiert und die Gesamtstrategie bewertet werden. Der Ausschuss könnte auch der richtige Ort für eine entsprechende Mobilisierung der Öffentlichkeit für die Kontrolle der Exekutive sein. Das durch den Ausschuss Digitale Agenda eingerichtete Online-Tool für die Beteiligung<sup>46</sup> wurde zwar nur mäßig genutzt, ist aber jedenfalls ein Schritt in die richtige Richtung.

Für alle diese Fragen ist die Entscheidung zwischen primärer Zuständigkeit und Mitberatung wesentlich. Die Begleitung aller Probleme der Digitalisierung, die in Fachressorts auftreten, klingt nur auf den ersten Blick attraktiv. In der Praxis behindert sie nicht nur die Funktion der Arbeitsentlastung des Plenums, weil sich mehrere Ausschüsse mit bestimmten Fragen befassen. Auch aus der Perspektive der mitberatenden Abgeordneten eines solchen Spiegelausschusses waren die Erfahrungen offenbar eher frustrierend.<sup>47</sup> Zum einen besteht keine Entscheidungskompetenz, zum anderen ergibt sich eine natürliche Tendenz der Ministerien, sich mit relevanten Fragen direkt an „ihre“ Ausschüsse zu wenden. All dies spricht für eine deutliche Entflechtung. Diese sollte nach der Devise erfolgen, einem Ausschuss für digitale Räume weniger, dafür aber echte Zuständigkeiten zuzusprechen.<sup>48</sup>

---

<sup>44</sup> Will man diesen Weg nicht gehen, so hat eine Verortung im Bereich der Wirtschaft oder der Justiz eine mindestens ebenso große Berechtigung; angesichts der Grundrechtsrelevanz der Materie wäre letzteres am überzeugendsten.

<sup>45</sup> S. Unterrichtung durch die Bundesregierung: Legislaturbericht Digitale Agenda 2014 bis 2017, BT-Drucks. 18/12130.

<sup>46</sup> S. <https://www.bundestag.de/ada/beteiligung/forum.php>.

<sup>47</sup> S. z. B. Kaul, <http://www.taz.de/!5033662/>: „Der Ausschuss der Frustrierten“.

<sup>48</sup> Nicht vertieft werden kann hier, dass diese Überlegungen teilweise auch für die Regierungsorganisation gelten. Für bestimmte Aufgaben mag insoweit eine Zuständigkeit des Kanzleramts sinnvoll sein. Wenn aber am Ende Regierungshandeln mehr und mehr in digitalen Räumen stattfindet, stößt diese

### 3. Die Kontrolle der Kontrolle digitaler Räume: das Problem der Nachrichtendienste

Die Kontrolle der Nachrichtendienste ist der Kulminationspunkt für praktisch alle Probleme und Grenzen der parlamentarischen Kontrolle an sich. Die Grundfrage des „quis custodiet ipsos custodes?“<sup>49</sup> stellt sich in aktueller Form insbesondere, weil die Nachrichtendienste weltweit ihre Tätigkeit in digitalen Räumen massiv ausgeweitet haben.

Die dadurch verursachten Herausforderungen zeigen sich an drei Dimensionen. Erstens erleichtern digitale Räume die Informationssammlung auf Infrastrukturebene, also insbesondere an den großen Knotenpunkten und Leitungen des Internets. Das allgemeine Problem des Informationsvorsprungs der Exekutive wird durch diese Infrastrukturkomponente massiv verschärft. Zweitens erlauben digitale Räume in erheblichem Maße verdeckte Informationssammlungen und andere verdeckte Informationsoperationen. Das Netz ist zwar nicht völlig anonym, es erlaubt den Diensten aber vielfach, anonym zu handeln. Dies verstärkt die strukturelle Intransparenz und führt dazu, dass entscheidende Informationen über die nachrichtendienstliche Tätigkeit nur durch Whistleblower bekannt geworden sind.<sup>50</sup> So bedeutsam dieses Wissen ist, so wenig kann es eine effektive parlamentarische Kontrolle ersetzen. Dies gilt umso mehr, als die Informationspreisgabe durch Whistleblower in aller Regel nur punktuell stattfindet und deshalb schnell veraltet. Der Zeitraum, der seit den Veröffentlichungen von *Edward Snowden* im Sommer 2013 verstrichen ist, ist angesichts der technischen Entwicklung des Internets eine Ewigkeit – man muss mit anderen Worten davon ausgehen, dass die Öffentlichkeit so gut wie nichts darüber weiß, was genau die NSA derzeit im Internet tut.

Drittens zeigt sich am Beispiel der Nachrichtendienste paradigmatisch die Internationalität digitaler Räume. Dies führt zu mehreren Problemen. Nachrichtendienste sind nicht erst seit den Zeiten der Globalisierung auf den gegenseitigen Informationsaustausch mit „befreundeten“ Diensten angewiesen. Gerade wegen der Bedeutung fremder Informationen für die nachfolgende eigene Tätigkeit der Behörden ist es jedoch essenziell, dass der Informationsaustausch nicht gegen parla-

---

Bündelung an natürliche Grenzen. Dies spricht im Ergebnis gegen das von verschiedenen Seiten geforderte „Digital-Ministerium“ (s. z.B. <https://www.wiwo.de/13714138-2.html>; allgemeiner Enquete-Kommission „Internet und digitale Gesellschaft“, Siebter Zwischenbericht „Demokratie und Staat“, BT-Drucks. 17/12290, S. 100: die Bundesregierung solle „auch in ihrem Verantwortungsbereich eine entsprechende Spiegelung der Ausschussstruktur“ vornehmen, die eine „bessere Koordinierung im Bereich des Querschnittsthemas der Netzpolitik“ möglich mache).<sup>49</sup> *Juvenal*, *Satirae* VI, S. 347 f.

<sup>50</sup> Die Frage des Whistleblowings bei Nachrichtendiensten ist insbesondere seit den Enthüllungen *Edward Snowdens* vielfach diskutiert worden. Der Gesetzgeber hat 2016 mit dem neuen § 8 Abs. 1 Satz 4 PKGrG bestimmt, dass das Parlamentarische Kontrollgremium bei Eingaben von Angehörigen der Nachrichtendienste den Namen der mitteilenden Person nur bekanntgibt, soweit dies für eine Aufklärung des Sachverhalts erforderlich ist, s. *Gärditz*, DVBl 2017, 525 (533); zu den Grundproblemen z.B. *Deiseroth*, NG|FH 1/2/2014, 4; s.a. *Hornung*, in: *Morlok/Schliesky/Wiefelspütz* (Hrsg.), *Parlamentsrecht*, 2016, § 30 Rn. 27 ff.

mentarische Kontrolle immunisiert wird. Einfachgesetzlich ist dies vor allem ein Problem des Schutzes der internationalen Beziehungen als „zwingender Grund des Nachrichtenzugangs“ nach § 6 Abs. 2 PKGrG.<sup>51</sup>

Die weltweite Vernetzung erleichtert den deutschen Diensten überdies sowohl die Erhebung von Daten im Ausland, als auch von Daten mit Auslandsbezug in Deutschland (beispielsweise am DE-CIX, einem der weltweit größten Internetknoten, der in Frankfurt am Main betrieben wird) sowie mittels Satellitenkommunikation. Die Abgrenzung zwischen diesen Fallgruppen und die rechtliche Zulässigkeit der Datenerhebung werden in den letzten Jahren kontrovers diskutiert.<sup>52</sup> Das betrifft insbesondere die strikt abzulehnenden Versuche der Dienste, mittels einer Art „Weltraumtheorie“ für die Erfassung von Datenströmen aus Satellitenkommunikationsverbindungen während deren Übertragung zum Boden eine Bindung an die Grundrechte des Grundgesetzes zu verneinen.<sup>53</sup> Einfachgesetzlich ist die Zulässigkeit durch das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 erstmals geregelt worden.<sup>54</sup> Welche Herausforderungen diese Materie für die parlamentarische Kontrolle mit sich bringt, zeigt sich eindrücklich an den Arbeiten des NSA-Untersuchungsausschusses in der letzten Legislaturperiode.<sup>55</sup>

## V. Fazit: Elemente einer „digitalen“ parlamentarischen Kontrolle

Es ist deutlich geworden, dass die Entwicklung digitaler Räume eine erhebliche Herausforderung für die parlamentarische Kontrolle darstellt. Zugleich lassen sich aus den Charakteristika der Digitalisierung bestimmte Elemente einer „digitalen“ parlamentarischen Kontrolle ableiten.

Dies betrifft zunächst die Anforderung der Professionalisierung und Spezialisierung gerade mit Blick auf das Phänomen der Digitalisierung. Dies darf nicht auf einen einzigen Bundestagsausschuss und seine Mitglieder beschränkt bleiben, an

---

<sup>51</sup> S. grds. zu den damit zusammenhängenden Problemen *Warg*, NVwZ 2014, 1263; *Holzner*, DÖV 2016, 668; *Nees*, DÖV 2016, 674; *Huber*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 6 Rn. 6 ff.; *Nomos-BR/Hornung* PKGrG § 6 Rn. 2 ff.

<sup>52</sup> S. näher *Bäcker*, K&R 2014, 556; *Schantz*, NVwZ 2015, 873; *Gärditz*, Verw 2015, 463; *Papier*, DRiZ 2017, 18; *Karl/Soiné*, NJW 2017, 919.

<sup>53</sup> S. *Bäcker*, Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme v. 16.5.2014 zur Anhörung des NSA-Untersuchungsausschusses, SV-2/3 zu A-Drs. 54, S. 18 ff. m.w.N.; s.a. *Huber*, NJW 2013, 2572 (2575); *Papier*, DRiZ 2017, 18; grundsätzlicher *Durner*, in: Maunz-Dürig, Art. 10 GG Rn. 65 m.w.N.; a.A. z.B. *Proelss/Daum*, AöR 141 (2016), 373 (377 ff.).

<sup>54</sup> BGBl. I 2016, 3346; s. dazu *Gärditz*, DVBl 2017, 525; *Marxsen*, DÖV 2018, 218; kritisch *Huber*, ZRP 2016, 162.

<sup>55</sup> S. nur den Abschlussbericht, BT-Drucks. 18/12850, sowie zu den Rechtsfragen die Stellungnahmen der Gutachter *Papier*, *Hoffmann-Riem* und *Bäcker*, abrufbar unter <https://www.bundestag.de/ausschuesse/ausschuesse18/ua/1untersuchungsausschuss/-/280848>.

den die Kontrolle digitaler Räume dann eher pro forma delegiert würde. Vielmehr stellt die parlamentarische Kontrolle digitaler Räume neue Anforderungen an praktisch alle Politikbereiche.

Angeichts der strukturellen Intransparenz und des Informationsungleichgewichts in digitalen Räumen bedarf es überdies spezifischer Vorgaben für die Art, den Inhalt und den Zeitpunkt der Informationsflüsse von der Exekutive zur Legislative.<sup>56</sup> Derartige spezifiziertere Berichtspflichten gegenüber den Abgeordneten oder einem von ihnen bestellten Bevollmächtigten (wie im Beispiel der §§ 5a, 5b PKGrG) bedürfen überdies im Streitfall einer effektiven gerichtlichen Kontrolle.<sup>57</sup> Weitergehende Sanktionen für eine Verletzung von Informationspflichten wären wünschenswert; es ist aber bisher nicht erkennbar, welcher Art diese sein könnten.

Erst auf Basis der so gewonnenen Informationen lässt sich sinnvoll über neue Mechanismen der Kontrolle nachdenken. Hierfür bedarf es eines Baukastens, dessen konkreter Gebrauch sich im Einzelfall entscheidet. Im Bereich der internen Professionalisierung des Parlaments könnte dies eine entsprechende Stabsstelle der Parlamentsverwaltung umfassen. Daneben bietet sich ein umfassenderer Gebrauch des Instruments der Gesetzesfolgenabschätzung mit entsprechenden Berichtspflichten an.<sup>58</sup> Unverzichtbar ist die Zusammenarbeit zwischen Abgeordneten und Experten für die technischen, ökonomischen und rechtlichen Implikationen der Digitalisierung.<sup>59</sup> Als weiteres Instrument bietet sich die Nutzung internetgestützter Kommunikationsformen auch in der Ausschussarbeit an. Dies könnte für interessierte Bürgerinnen und Bürger die Möglichkeit eröffnen, über ein Online-Tool für öffentliche Ausschusssitzungen Fragen und Anregungen zu formulieren und zu erfahren, dass diese in der Sitzung auch tatsächlich behandelt werden. Die mit einer solchen Form der Öffentlichkeitsbeteiligung verbundenen quantitativen und mitunter auch qualitativen Probleme dürften beherrschbar sein<sup>60</sup> und jedenfalls

<sup>56</sup> Das BVerfG hat die verfassungsrechtlichen Vorgaben für diese Informationsflüsse in den letzten Jahren weiter präzisiert, s. v. a. BVerfGE 124, 161; 137, 185; 139, 194; BVerfG, NVwZ 2017, 1364.

<sup>57</sup> S. z. B. § 14 PKGrG (dazu *Hornung*, in: Morlok/Schliesky/Wiefelspütz (Hrsg.), Parlamentsrecht, 2016, § 30 Rn. 60 ff.). Dies betrifft wie in anderen Bereichen der parlamentarischen Kontrolle insbesondere das Problem der Minderheitenrechte.

<sup>58</sup> S. dazu *Sicko*, in: Dalibor et al. (Hrsg.), Risiko im Recht – Recht im Risiko. 50. Assistententagung Öffentliches Recht, 2011, S. 199; *Kahl*, in: Kluth/Krings (Hrsg.), Gesetzgebung, Rechtsetzung durch Parlamente und Verwaltungen sowie ihre gerichtliche Kontrolle, 2014, § 13; *Ziekow*, in: Montoro Chiner/Sommermann (Hrsg.), Gute Rechtsetzung – La Buena Legislaci, 2015, S. 31.

<sup>59</sup> Dementsprechend hat die Enquête-Kommission „Internet und digitale Gesellschaft“ eine „effiziente wissenschaftliche Begleitung der Arbeit des neu einzurichtenden Ausschusses“ vorgeschlagen, s. Siebter Zwischenbericht „Demokratie und Staat“, BT-Drucks. 17/12290, S. 100.

<sup>60</sup> Dies zeigt etwa das insoweit strukturell vergleichbare Instrument der E-Petition; dazu *Guckelberger*, DÖV 2008, 85; *Riehm/Böhle/Lindner*, Elektronische Petitionssysteme. Analysen zur Modernisierung des parlamentarischen Petitionswesens in Deutschland und Europa, 2013; *Hornung/Hühnlein/Sädler*, in: Lück-Schneider et al. (Hrsg.), Gemeinsam Electronic Government ziel(gruppen)gerecht gestalten und organisieren, 2014, S. 63 ff.; zu den Instrumenten s. *Kubicek*, in: Wirtz (Hrsg.): E-Government – Grundlagen, Instrumente, Strategien, 2010, S. 195; *Oertel/Kablich/Albrecht*, Online-Bürgerbeteiligung an der Parlamentsarbeit, 2018.

hinter den Vorteilen zurücktreten, die durch diese Rückkopplung an die Öffentlichkeit für die Legitimation der parlamentarischen Kontrolle und das Vertrauen in diese erzielt werden können.

Angesichts der weltweiten technischen Vernetzung digitaler Räume kann sich die Kontrolltätigkeit der Parlamente nicht mehr auf eine bestimmte staatliche Ebene oder einen Nationalstaat beschränken. Wenn sich Regierungs- und Verwaltungshandeln zunehmend in Netzwerken abspielt, so bedarf es auch einer netzwerkartigen Verflechtung der parlamentarischen Kontrolle. Erforderlich ist eine Internationalisierung, die auch eine Zusammenarbeit mit anderen Parlamenten umfassen muss.<sup>61</sup> Dies betrifft gerade den Bereich des internationalen Informationsaustausches zwischen Nachrichtendiensten, der nur auf der Basis einer Kooperation der Parlamente umfassend bewertet werden kann.

Besondere Herausforderungen, aber auch Chancen ergeben sich durch die Interaktion mit Pressevertretern und zivilgesellschaftlichen Akteuren. Informationen über interne Abläufe der Verwaltung werden nicht nur durch die Ausschussarbeit der Parlamente, sondern auch aufgrund presserechtlicher Auskunftsansprüche,<sup>62</sup> voraussetzungsloser Ansprüche auf Informationszugang<sup>63</sup> oder besonderer Transparenzpflichten der Verwaltung zur proaktiven Offenlegung<sup>64</sup> bekannt. Dies können sich auch die Parlamente zunutze machen. Die entsprechenden reaktiven und proaktiven Pflichten sollten dementsprechend nicht als Konkurrenz zu parlamentarischen Auskunftsansprüchen begriffen werden. Vielmehr erfüllen beide Bereiche komplementäre Funktionen und können sich gegenseitig stärken. Dies ist für die klassischen Auskunftsansprüche der Presse und ihre nachfolgende Informationsstätigkeit gegenüber der Öffentlichkeit seit langem anerkannt. Beide werden

---

<sup>61</sup> S. zu ersten Ansätzen in der Europäischen Union in diese Richtung *Eppler*, in: Eberbach-Born/Kropp/Stuchlik/Zeh (Hrsg.), *Parlamentarische Kontrolle und Europäische Union*, 2013, S. 317; *Konratb/Lieblich*, *ZöR* 2014, 315; zur spezifischen interparlamentarischen Zusammenarbeit nach Art. 12 lit. f EUV s. *Hölscheidt*, in: Grabitz/Hilf/Nettesheim EUV Art. 12 Rn. 80 ff.

<sup>62</sup> Diese ergeben sich aus den Presse- bzw. Mediengesetze der Länder. Im Bund besteht keine Regelung, weil der Bundesgesetzgeber sich die Ansicht des BVerwG (keine Länderkompetenz, s. BVerwGE 146, 56; 151, 348; s. z. B. *Huber*, *NVwZ* 2013, 1010; *Cornils*, *DÖV* 2013, 657; *Kloepfer*, *JZ* 2013, 892; zur weiteren Entwicklung *Cornils*, *AfP* 2016, 205; *Schnabel*, *NJW* 2016, 1692; s. a. *Raabe*, *Informations- und Auskunftsspflichten der öffentlichen Hand gegenüber der Presse*, 2010, S. 11 ff.) nicht zu eigen gemacht hat. Solange dies so ist, sind auf der Basis der Lösung des BVerwG mangels Ermächtigungsgrundlage zum Eingriff in die entsprechenden Grundrechte Auskünfte von Bundesbehörden verfassungswidrig, wenn sie personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse enthalten, s. *Hornung*, *AfP* 2017, 390 (393 f.).

<sup>63</sup> S. für den Bund § 1 Abs. 1 Satz 1 IFG. Mittlerweile haben 12 Bundesländer entsprechende Informationsfreiheitsgesetze verabschiedet. In Hessen befindet sich ein – sehr restriktiver – gesetzlicher Anspruch derzeit im parlamentarischen Verfahren, s. Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN vom 5.12.2017 für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit, LT-Drs. 19/5728.

<sup>64</sup> Vorreiter war hier das Hamburgische Transparenzgesetz; inzwischen gibt ein entsprechendes Landestransparenzgesetz in Rheinland-Pfalz; s. z. B. *Schnabel*, *NordÖR* 2012, 431; *Jauch*, *DVBl.* 2013, 16; *Stumpf*, *VerwArch* 2015, 499.

nicht als Konkurrenz, sondern als Ergänzung der parlamentarischen Kontrolle begriffen. Es gibt keinen Grund, dies für die neuen Pflichten nach den Informationsfreiheits- und Transparenzgesetzen anders zu bewerten.

In der Gesamtschau bleibt schließlich anzumerken, dass die Herausforderungen der parlamentarischen Kontrolle digitaler Räume zwar erheblich sind, aber immer noch hinter den Herausforderungen der Kontrolle (und Regulierung) anderer Bereiche wirtschaftlichen oder individuellen Handelns in diesen Räumen zurückbleiben. Immerhin verfügt die parlamentarische Kontrolle weiterhin über einen verhältnismäßig gut handhabbaren Kontrollgegenstand. Auch Nationalstaaten und ihre Verwaltungen vernetzen sich, und sie verfügen über erhebliche Einflussmöglichkeiten auf die Infrastruktur des Internets. Das ändert aber nichts daran, dass sie nach wie vor eine konkrete, kontrollierbare Organisationsstruktur aufweisen und es funktionierende Instrumente der justiziellen Kontrolle über sie gibt. Dies ist im Bereich der Kontrolle nichtstaatlichen Handelns im Internet weithin nicht der Fall, weil sich die zentralen Akteure nicht in Europa befinden und vielfach kein Konsens über rechtliche Maßstäbe für ihr Verhalten besteht. In diesem Sinne sollten die erläuterten Herausforderungen kein Anlass zur Resignation sein, sondern vielmehr zur Entwicklung effektiver und professioneller Instrumente für eine künftige digitale parlamentarische Kontrolle digitaler Räume.