Martin Schallbruch

Schwacher Staat im Netz

Wie die Digitalisierung den Staat in Frage stellt

Springer

Schwacher Staat im Netz

Martin Schallbruch

Schwacher Staat im Netz

Wie die Digitalisierung den Staat in Frage stellt

Springer

Martin Schallbruch
Digital Society Institute
ESMT Berlin
Berlin, Deutschland

ISBN 978-3-658-19946-3 ISBN 978-3-658-19947-0 (eBook)
https://doi.org/10.1007/978-3-658-19947-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Verantwortlich im Verlag: Jan Treibel

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

INHALT

1 EINLEITUNG

Im Lokschuppen des Deutschen Technikmuseums in Berlin hatten wir das Rednerpult mit dem Bundesadler aufgebaut, direkt vor einer alten roten Lokomotive der Deutschen Reichsbahn. Hinter dem Pult stand Bundesinnenminister Thomas de Maizière und hielt eine Rede: »Perspektiven deutscher Netzpolitik« war sein Thema[1]. Gemeinsam mit dem Minister und meinen Mitarbeitern hatte ich wochenlang an der Rede gearbeitet. Damals, im Juni 2010, markierte die Rede eine Art Schlusspunkt der ersten Phase deutscher Internetpolitik. Die ersten Debatten um Internetsperren, Urheberrecht und Bundestrojaner lagen hinter uns. Die neu gegründete Piratenpartei hatte das Thema besetzt und begann ihre kurze Erfolgsperiode. Mit der Rede an diesem symbolträchtigen Ort wollte der Innenminister dem Thema eine Struktur geben, Grundsätze entwickeln, Linien aufzeigen, die helfen sollten, Netzpolitik konsistent zu gestalten.

Acht Jahre später ist aus Netzpolitik die Digitalpolitik geworden. Sie ist kaum weniger unübersichtlich als damals. Noch immer tut sich Politik schwer, mit digitalen Technologien und Geschäftsmodellen, neuen Lebensformen im Netz oder auch Kriminalitätsphänomenen im Cyberspace angemessen umzu-

M. Schallbruch, *Schwacher Staat im Netz*,
https://doi.org/10.1007/978-3-658-19947-0_1

gehen. Politische Diskussionen über Künstliche Intelligenz oder selbstfahrende Autos, über Cyberkriege oder den bevorstehenden Untergang des Datenschutzes werden von Teilen der politisch interessierten Öffentlichkeit als Schicksalsfragen geführt, von anderen geflissentlich ignoriert. Bei jedem netzpolitischen Problem wird das Verhältnis von Staat und digitaler Welt aufs Neue diskutiert: Big Data im Gesundheitswesen, Verbot von Verschlüsselung, Bekämpfung von Hate-Speech bei Facebook, autonom fahrende Autos. Die von de Maizière angestoßene Debatte hat es nicht vermocht, die Orientierungslinien und Leitplanken für eine demokratische Digitalpolitik zu entwickeln, die wir uns im Jahr 2010 erhofft hatten.

Über zehn Jahre deutscher Netzpolitik haben zu Tage treten lassen, dass es einen zentralen Grund für die Schwierigkeiten der Politik mit dem Netz gibt. Die Digitalisierung fordert den Staat nicht einfach nur heraus. Sie überfordert ihn. Sie stellt in Frage, wie wir 70 Jahre lang unser Gemeinwesen gesteuert, organisiert und verteidigt haben. Unser demokratischer Staat mit seinen klassischen Institutionen und Verfahren tut sich schwer, seine bisherige Rolle auch im digitalen Raum zu spielen. Die Wirksamkeit von Gesetzen steht im Internet in Frage, Cyberangriffe können alles und jeden treffen, globale Plattformen sind nur mühsam zu bändigen, digitale Verwaltung kommt seit Jahren kaum voran.

Mit diesem Buch spitze ich meine Erfahrungen aus mehr als zehn Jahren deutscher Netzpolitik zu – auf die Erörterung einer zentralen Frage: Warum ist der Staat schwach geworden im Netz? Und was können wir tun, um unsere demokratisch gewählten Institutionen in die Lage zu versetzen, auch morgen noch Demokratie und Freiheit zu verteidigen – auch im digitalen Raum?

Um die Schwäche des Staates zu verstehen und die Gründe zu erkennen, müssen wir uns auf eine Reise zu den verschiedenen Orten der digitalen Welt begeben und auf die neuen Machtkonstellationen schauen: Wer trägt die Verantwortung für das, was im Digitalen geschieht? Wer setzt die Regeln? Wer schützt uns? Welche Rolle spielt der Staat? Und welche sollte er spielen?

In diesem Buch fasse ich meine persönliche Sicht auf diese Fragen zusammen. Sie ist geprägt von der Ausbildung und der Berufstätigkeit an der Schnittstelle von Informatik und Recht – und von einer langjährigen Arbeit im Bundesinnenministerium. Dort war ich verantwortlich für Informationstechnik, Digitalisierung und Cybersicherheit, für Gesetze und IT-Projekte, war tagtäglich konfrontiert mit den Fragestellungen dieses Buches. Die Herausforderungen an den Staat durch die Digitalisierung und seine Antworten habe ich selbst erlebt und selbst mitgestaltet, bisweilen zu zaghaft, bisweilen zu forsch. Heute blicke ich von außen auf die staatlichen Institutionen und ihre Mühe mit der Digitalisierung. Doch auch heute, als Wissenschaftler an der führenden Business School der deutschen Wirtschaft, ist mir eines mehr als klar: ein schwächelnder Staat in der Digitalisierung ist ein Risiko für uns alle. Wirtschaft und Gesellschaft brauchen leistungsfähige und verlässliche Institutionen, die uns den Raum zur persönlichen und wirtschaftlichen Entfaltung garantieren – auch im Digitalen.

2 ANNÄHERUNGEN AN NETZPOLITIK

Kampf um das Urheberrecht ◆ Netzsperren und Zensursula ◆ Bundestrojaner und Stasi 2.0 ◆ Beulen, Blessuren und Lernkurven

2.1 KAMPF UM DAS URHEBERRECHT

Mit finanzieller Unterstützung seines Onkels gründete der 19-jährige Musikstudent Shawn Fanning im Mai 1999 ein eigenes Unternehmen. Napster Inc. mit Sitz in Boston bot eine Software an, die das Tauschen von Musik im Internet revolutionierte. Wer die Software installierte, gab die Musikstücke auf der eigenen Festplatte frei für einen Tausch und konnte im Gegenzug auf die Musikstücke aller Napster-Nutzer zugreifen. In kürzester Zeit war über Napster nahezu alle beliebte Musik verfügbar. Megabyte um Megabyte an Musik wurden in kürzester Zeit kostenfrei kopiert. In wenigen Monaten erreichte Napster über 20 Millionen aktive Nutzer und wurde zum bis dato am schnellsten wachsenden Angebot im Internet.

Sehr zum Ärger der Musikindustrie, die gerichtlich gegen die Tauschbörse vorging. Eine erste einstweilige Anordnung gegen Napster wurde Mitte 2000 von einem Berufungsgericht wieder aufgehoben. Die Zahl der Nutzer wuchs weiter auf 37 Millionen. Der damalige Bertelsmann-Chef Thomas Middelhof ließ sich von dem Tauschbörsen-Boom anstecken und vereinbarte im Spätherbst 2000 eine Kooperation von

M. Schallbruch, *Schwacher Staat im Netz*,
https://doi.org/10.1007/978-3-658-19947-0_2

Bertelsmann mit Napster[1]. Viel Geld floss aus Gütersloh an Shawn Fanning und sein Team. Doch das Ende kam schnell: Im März 2001 wurde Napster gerichtlich gezwungen, alle urheberrechtlich geschützten Stücke zu filtern. Das war das Ende der Tauschbörse. Im Mai 2002 meldete sie Konkurs an.

Der Napster-Fall war die erste große Schlacht um das Urheberrecht in der digitalen Welt. Schon die Möglichkeit zum digitalen Kopieren von CDs hatte die Musikindustrie als Bedrohung ihres Geschäftsmodells angesehen, erst Recht aber die Verbreitung über das Internet. Mit der immer größeren Bandbreite im Netz konnten immer mehr Daten in kurzer Zeit digital verbreitet werden – auch Musik, Filme und Bücher. Der Download eines MP3-Musikstücks dauerte mit einem analogen Modem noch bis zu 30 Minuten, mit ISDN dann nur noch etwa 7 Minuten. Mit heutigen DSL-Geschwindigkeiten sind es nur noch Sekunden. Ganze Alben können schnell geladen und weitergegeben werden.

Anfang der 2000er rüstete sich die Musikindustrie zur großen Schlacht gegen den Musikvertrieb über das Internet. Die Branche war höchst alarmiert von den Jahr für Jahr sinkenden CD-Verkäufen. Zur Verteidigung des Geschäfts wurden gleich mehrere Fronten aufgemacht: CDs wurden mit Kopierschutz versehen, um eine Digitalisierung zu verhindern. Diese Verfahren codieren die Musik so, dass der CD-Player sie auslesen kann, nicht aber eine Software auf dem Computer. Tauschbörsen-Betreiber und -Nutzer wurden massiv rechtlich verfolgt, die Gesetzgeber gedrängt, gegen Tauschbörsen vorzugehen. Der europäische Gesetzgeber und auch die deutsche Politik beugten sich dem Druck. Schon im September 2003 trat der sogenannte »erste Korb« der Novellierung des Urheberrechtes in Kraft. Das sogenannte Recht auf Privatkopie wurde eingeschränkt, die Nutzung von Tauschbörsen im Internet

de facto verboten. Privatkopien waren zuvor erlaubt gewesen, also die selbst gebrannte CD zur Nutzung im Autoradio oder zur Weitergabe an Freunde. Dazu zählte auch die Digitalisierung einer CD, um sie zum Beispiel auf dem MP3-Player hören zu können. Mit dem Gesetz wurden Privatkopien für solche Fälle verboten, in denen der Hersteller seine CD mit einem Kopierschutz versehen hatte. Die meisten Kopierschutzverfahren werden nach einiger Zeit von Hackern »geknackt« und können dann mit entsprechender Spezialsoftware umgangen werden. Ihre Benutzung wurde verboten, ebenso die Herstellung oder Verbreitung solcher Umgehungsprogramme. Neben der Privatkopie ging es auch den Tauschbörsen an den Kragen: Mit einem gesetzlichen Verbot, Kopien von »offensichtlich rechtwidrigen Vorlagen« anzufertigen, wurden die Nutzer von Tauschbörsen adressiert. Wer Musikstücke aus einer Tauschbörse herunterlädt, kann von der Musikindustrie vor den Kadi gezerrt werden.

Der erste Korb des Urheberrechts war noch weitgehend ohne große öffentliche Debatten durch den Bundestag gegangen. Das änderte sich, als die damalige Justizministerin Brigitte Zypries im September 2004 den »zweiten Korb« vorlegte. Zwar fielen die weiteren Verschärfungen zu Gunsten der Musikindustrie vergleichsweise harmlos aus und Ministerin Zypries hatte sogar eine Bagatellklausel für Tauschbörsennutzer und für Privatkopien im Freundeskreis vorgesehen. Doch etwas hatte sich verändert: das digitale Leben war im Alltag vieler Menschen angekommen. Eingriffe des Staates in die eigene digitale Welt wurden mit größerer Vehemenz diskutiert als zuvor: Warum darf ich mit den Daten auf meiner Festplatte nicht machen, was ich will? Warum mischt sich der Staat ein? Das sind meine Dateien, meine digitalen Güter, meine Privatsache!

Der Streit um den zweiten Korb entzündete sich an den so-

genannten Urheberrechtsabgaben: Hersteller von Computern und Druckern, CD- und DVD-Brennern und einigen weiteren Geräten sollten eine Abgabe zahlen, um den Urhebern aus diesen Mitteln eine Entschädigung für Kopien zukommen zu lassen. Gegen die Urheberrechtspauschale liefen nicht nur Verbraucherschützer Sturm, auch die IT-Industrie stieg in die Lobbyschlacht um das Urheberrecht ein. Auf der Gegenseite standen die Verlage, Musikverlage, Filmverleiher und andere sogenannte »Rechteinhaber«[2]. Am Ende dauerte es über drei Jahre, bis der zweite Korb Gesetz werden konnte – mit Urheberrechtspauschalen, aber ohne Bagatellgrenzen für Tauschbörsennutzer und Privatkopierer. Die Musikindustrie hatte sich – weiter fallende CD-Umsätze vor Augen – noch einmal durchgesetzt.

Der Streit um das Urheberrecht hatte eine Nebenwirkung: eine wachsende Zahl von Menschen in Deutschland begann, die staatliche Einflussnahme auf das Internet skeptisch und kritisch zu sehen. Die selbst gekaufte CD konnte man nicht mehr auf den MP3-Player kopieren. Der Staat schickte sich an, dieses Verhalten der Unternehmen durch Gesetze zu schützen. Für viele Menschen war dies ein Beleg dafür, dass die Politik ihre Wünsche und Bedürfnisse in der aufziehenden digitalen Welt nicht verstand. Politik und Verwaltung wurde die Kompetenz abgesprochen, mit IT und Internet angemessen umzugehen. Die Sicht der anderen Seite war nicht weniger fundamental: Wie sollen wir mit dem Verkauf von Musik zukünftig noch Geld verdienen, wenn jeder alle Musik kostenfrei über das Internet kopieren kann? »Das Internet darf kein rechtsfreier Raum sein!« oder »Was offline verboten ist, muss auch online verboten sein« waren die zugehörigen Slogans.

Der Streit um das Urheberrecht war ein erstes plastisches

Beispiel für die Schwierigkeiten des Staates im Umgang mit dem Netz: Die Digitalisierung aller Lebensbereiche, zum Beispiel des Kaufens und Hörens von Musik, ist mehr als ein Einsatz von Technik. Jeder einzelne Lebensbereich wird durch die Digitalisierung neu gestaltet – durch Anbieter und Kunden, durch Weiterentwicklung von Bedürfnissen und Weiterentwicklung von Märkten. Der Versuch, mit Hilfe staatlicher Gesetze althergebrachte Geschäftsmodelle auch im digitalen Raum zu bewahren, geht meistens schief.

Die Musikindustrie kann mittlerweile wieder einigermaßen ruhig schlafen, weil ihr Geschäft den Schritt in das Internet geschafft hat: 2003, inmitten der deutschen Schlacht um das Urheberrecht, eröffnete Steve Jobs seinen iTunes-Store. In den ersten zehn Jahren seines Bestehens verkaufte diese Plattform 35 Milliarden Songs. Doch auch dieses Angebot ist wohl ein Übergangsmodell: mit dem Erfolg von Streamingdiensten wie Spotify, Deezer, Amazon Music und Apple Music bewegt sich der Musikmarkt auf ein ganz anderes Geschäftsmodell zu. Die gelingende digitale Transformation des Marktes zeigt sich auch bei den Umsätzen: Der Umsatzrückgang der Musikindustrie wurde 2013 gestoppt, seitdem steigen die Umsätze wieder deutlich an – vor allem über das Internet[3].

2.2 NETZSPERREN UND ZENSURSULA

Ende 2008 erreichte mich eine Bitte meines Ministers, auf die ich zunächst skeptisch reagierte, weil sie ein Novum darstellte: einen aktiven staatlichen Eingriff in das Internet. Die Bitte war, dass ich mit meiner technischen Expertise die damalige Familienministerin Ursula von der Leyen in ihrem Kampf ge-

gen die Verbreitung von Kinderpornografie im Internet unterstützen sollte. Ihr Ziel war es, die Internet-Provider dazu zu bringen, die Verbindung zu Servern im Netz zu kappen, über die Fotos von missbrauchten Kindern verbreitet wurden. Die Debatte um solche Netzsperren hatte der damalige BKA-Präsident Jörg Ziercke im Sommer 2008 angestoßen. Jahrzehntelang war die Verbreitung von Kinderpornografie verborgen auf dem Postweg erfolgt. Nun hatte sie den Weg in das Internet gefunden. Auf Servern im Ausland, vor allem in den USA, lagerten viele tausend Bilder und konnten von überall in der Welt erworben werden. Das Abschalten der Server durch Zusammenarbeit mit ausländischen Polizeien hatte sich als zu langwierig erwiesen: wenn der Server endlich vom Netz genommen war, hatten die Täter die Dateien auf einem anderen Server bereitgestellt.

Meine Skepsis gegen Netzsperren wurde geringer, als das BKA einige Beispiele für das vorführte, um die es ging. Ich war nicht der einzige: Wer einmal gesehen hat, wie Bilder des Missbrauchs kleiner Kinder im Internet angeboten werden, ist fest entschlossen, alles zu tun, was möglich ist, um diesen Markt auszutrocknen und den Missbrauch zu stoppen. Viele Fragen aber blieben: Wie sorgt man dafür, dass nur Kinderpornografie ausgesperrt wird und nicht andere Angebote im Internet? Werden die Kinderpornografie-Anbieter permanent den Server wechseln, sich vielleicht auch auf seriösen Online-Plattformen verbergen? Wer entscheidet über die zu sperrenden Server? Ist eine Sperre überhaupt ausreichend wirksam oder kann sie jeder halbwegs versierte Internet-Nutzer umgehen? Rechtfertigt das Blockieren des vergleichsweise kleinen Marktes für Kinderpornografie, dass alle Internetanbieter alle Internetverbindungen aller Kunden filtern?

In den Gesprächen der Regierung mit den Internet-Pro-

vidern ging es vor allem um die technische Wirksamkeit, die Kosten des Einbaus solcher Sperren und die Frage, wer für fehlerhafte Sperrungen haftet. In der öffentlichen Debatte stand etwas Anderes im Mittelpunkt: Zensur! Der Staat baut mit den Netzsperren gegen Kinderpornografie eine universelle Zensur-Infrastruktur auf, die nach Gusto jederzeit auch für das Sperren anderer Internetinhalte genutzt werden kann. Blitzschnell erhielt Ursula von der Leyen von Gegnern der Netzsperren den Spitznamen »Zensursula«. 140 Organisationen und Verbände schlossen sich zu einem Bündnis gegen Netzsperren zusammen. Eine Online-Petition erreichte innerhalb von Wochen 130 000 Unterschriften. Die damalige Große Koalition im Bund ließ sich von den Protesten nicht beeindrucken. Im ersten Schritt wurde im Frühjahr 2009 mit den fünf größten Providern ein Vertrag geschlossen, solche Sperrungen in Zusammenarbeit mit dem BKA vorzunehmen. Die Provider drängten jedoch darauf, dass eine Sperrung eine gesetzliche Grundlage bräuchte. Der Vertrag wurde daher nur bis Ende 2010 befristet.

Im Juni 2009 verabschiedete der Deutsche Bundestag mit den Stimmen von CDU/CSU und SPD das sogenannte »Zugangserschwerungsgesetz«. Darin wurden die Provider verpflichtet, alle Internet-Adressen und Websites, die in einer vom BKA übermittelten Sperrliste enthalten sind, binnen sechs Stunden zu sperren. Beim Versuch des Zugriffs zu einer solchen Seite im Internet sollte statt des kinderpornografischen Inhalts ein Stopp-Schild angezeigt werden. Das Zugangserschwerungsgesetz ging in die Geschichte ein. Denn es wurde de facto niemals angewendet. Mit der Bundestagswahl im Herbst 2009 bildete sich eine schwarz-gelbe Koalition. Die FDP als entschiedene Gegnerin von Netzsperren forderte eine Aufhebung des Gesetzes.

So erreichte mich ein Jahr nach der ersten Bitte in Sachen Netzsperren nun erneut eine Bitte meines Ministers: wie könne man den politischen Willen der neuen Koalition umsetzen und erreichen, dass das beschlossene Gesetz nicht angewandt werde? Und so warf ich einen anderen Blick auf das gleiche Gesetz, das die Regierung gerade noch gegen erhebliche politische Widerstände durchgesetzt hatte: wo war die Lücke, die man nutzen konnte, es nicht anzuwenden? Sie war schnell gefunden. Denn auf die Sperrlisten sollte das BKA nur die Angebote nehmen, bei denen eine Löschung nicht möglich war. Wie lange man sich erfolglos um die Löschung bemüht haben musste, sagte das Gesetz nicht. So trat das Gesetz zwar im Frühjahr 2010 formal noch in Kraft. Das BKA erstellte auf Weisung des Innenministeriums jedoch keine Sperrlisten. Mit breiter Mehrheit hob der Deutsche Bundestag das Gesetz im Mai 2011 wieder auf. Zensursula war gescheitert.[4]

Bei dem gescheiterten Versuch der Einführung von Netzsperren hat die Politik viel Lehrgeld bezahlt. Das Internet hat Strukturprinzipien, die es fast unmöglich machen, einzelne Inhalte zu sperren. Riesige Datenbestände können in Sekundenschnelle auf neue Server übertragen werden. Zugriffe auf Server können auf Umwegen geführt werden, um den Weg zu verschleiern. Illegale Angebote können sich inmitten legaler Angebote verstecken. Zudem stellen viele Anbieter im Internet, kommerziell oder ehrenamtlich, Hilfsmittel bereit, um Sperren zu umgehen. Das hilft Demokratiebewegungen in Diktaturen, sich zu organisieren. Das hilft ebenso Kriminellen, ihre Identität zu verschleiern.

Eine Art »deutsche Sicht« auf das globale Netz zu produzieren, indem mit Hilfe staatlicher Sperrlisten Teile des Internet für deutsche Nutzer unsichtbar gemacht werden, hat sich als technisch schwer umsetzbar und politisch unklug heraus-

gestellt. Einige Länder wie Norwegen und Schweden setzen solche Netzsperren zwar bis heute ein – jedoch mit mäßigem Erfolg. Das Angebot an Kinderpornografie geht dadurch nicht zurück. Gleichzeitig entstehen neue Risiken. Mehrfach sind die von den dortigen Polizeien erstellten Sperrlisten schon im Internet aufgetaucht und helfen den Konsumenten von Kinderpornografie beim Auffinden von Angeboten.

Trotzdem sind Netzsperren auch heute wieder Teil des deutschen Rechts. Im Sommer 2017 hat der Deutsche Bundestag gleich zwei »Netzsperren-light« verabschiedet: Mit der endlich erfolgten Abschaffung der Haftung für Betreiber offener WLANs ist verbunden, dass WLAN-Betreiber unter Umständen eine Sperre einrichten müssen. Wird aus einem WLAN auf urheberrechtlich geschütztes Material zugegriffen und gelingt es dem Urheber nicht, die Inhalte aus dem Netz zu entfernen, dann kann er unter Umständen den WLAN-Betreiber zur Einrichtung einer Sperre zwingen[5]. Die andere Sperrmöglichkeit betrifft die Verhinderung von Cyberangriffen. Im Telekommunikationsrecht wurde im Juni 2017 verankert, dass Internet-Provider die Kommunikation mit bestimmten Servern sperren, von denen eine Gefahr ausgeht. Das können Server sein, die Cyberangriffe steuern, z. B. ein sogenanntes Botnetz anleiten. Das können auch Server sein, bei denen gestohlene Daten deponiert werden[6].

Bei beiden Sperrmöglichkeiten im Internet hält sich der Staat aber zurück und lässt andere die Sperrentscheidung treffen. Zensursula und ihre Mitstreiter hatten sich die Finger verbrannt.

2.3 BUNDESTROJANER UND STASI 2.0

Am 9. Oktober 2011 erschien eine ungewöhnliche Ausgabe der Frankfurter Allgemeinen Sonntagszeitung (FAS). Programmcode und hexadezimale Zahlen dominierten die Titelseite des Blattes. Unter der Überschrift *Der Staatstrojaner wurde geknackt* berichtete die Zeitung über einen Coup des Chaos Computer Club (CCC). Den Hackern war es gelungen, den Programmcode einer Software zu bekommen, die von Bayerischen Sicherheitsbehörden eingesetzt wurde, um heimlich die Festplatten Verdächtiger zu durchsuchen. Die Veröffentlichung der FAS und die Analyse der Software durch den CCC war Futter für diejenigen, die eine heimliche Durchsuchung von Festplatten durch den Staat mit Vehemenz ablehnten.

Der Streit hatte fünf Jahre zuvor begonnen. Im Juli 2006 legte der damalige FDP-Innenminister von Nordrhein-Westfalen, Ingo Wolf, einen Gesetzentwurf vor, der die Rechte des Verfassungsschutzes zur Terrorismusbekämpfung betraf. Die seit 9/11 geltenden Sonderrechte sollten verlängert werden. Gleichzeitig war eine Modernisierung der Befugnisse geplant. Die Verfassungsschützer hatten erkannt, dass viele Zielpersonen des Nachrichtendienstes ihre Aktivitäten vor allem elektronisch abwickelten. Daher strebte der Verfassungsschutz an, im Rahmen der heimlichen Beobachtung potentieller Verfassungsfeinde auch ihre elektronische Welt anzuzapfen. Der Gesetzentwurf enthielt erstmals in Deutschland eine ganz neue Befugnis für einen Nachrichtendienst: der »heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel«, später bekannt geworden als »Online-Durchsuchung«.

In Nordrhein-Westfalen wurde diese Vorschrift Ende 2006 Gesetz, sogleich aber vor Gericht angefochten: Der frühere Bundesinnenminister Gerhard Baum (FDP) verklagte seinen nordrhein-westfälischen Parteifreund Wolf vor dem Bundesverfassungsgericht. Baum hielt das Gesetz für verfassungswidrig. Nur auf Verdacht könne die gesamte private Lebenswelt, Korrespondenz, Fotos, aufgerufene Websites und vieles mehr ausgelesen werden. Dies sei nicht mehr verhältnismäßig. Was bei Verabschiedung des nordrhein-westfälischen Gesetzes öffentlich nicht bekannt war: schon seit 2005 hatte das Bundeskriminalamt vom damaligen Innenminister Otto Schily die Erlaubnis zur Durchführung von Online-Durchsuchungen der Festplatten Verdächtiger erhalten. Anfang 2007, zeitgleich mit den Verfassungsbeschwerden von Baum und anderen, stoppte der Bundesgerichtshof diese Praxis: die geltenden Gesetze des Bundes ließen eine solche Online-Durchsuchung nicht zu. Wenn der Bund Online-Durchsuchungen machen wolle, dann müsse dafür ein neues Gesetz her[7].

Das war der Auftakt für eine leidenschaftliche bundespolitische Debatte um die Online-Durchsuchung. Von ihren Gegnern wurde die Maßnahme »Bundestrojaner« genannt, in Anlehnung an das Trojanische Pferd, das Holzpferd, mit dem es Soldaten in der griechischen Mythologie gelungen war, heimlich nach Troja einzudringen. Computerprogramme, die heimlich auf einem Computer ausgeführt werden, verhalten sich ähnlich. Die Benutzerinnen und Benutzer des Computers merken nicht, dass ein solcher Computertrojaner heimlich die Daten von der Festplatte ausliest.

Auf der Seite der Befürworter diese Maßnahme stand der damalige Bundesinnenminister Schäuble, Gegner kamen aus den Parteien der Grünen, Linken und FDP – und der gerade gegründeten Piratenpartei. Auch der Chaos Computer Club und

viele Informatiker lehnten die Online-Durchsuchung vehement ab, vor allem auch unter Verweis auf das technische Risiko und die Bedrohung für die Sicherheit der IT, die mit einem staatlichen Trojaner verbunden sind.

Will der Staat die Festplatte eines Verdächtigen durchsuchen, dann muss unbemerkt eine Software, der Trojaner, auf der Festplatte installiert werden. Diese Software muss die Festplatte durchsuchen, die ausgespähten Daten auslesen und an den staatlichen Auftraggeber senden. Allein der technische Ablauf wirft eine Fülle von Fragen auf. Die Installation der Software aus der Ferne ist nur möglich, wenn eine Schwachstelle in dem Betriebssystem und/oder der Sicherheitssoftware des Computers ausgenutzt wird. Eine Schwachstelle ist ein Programmierfehler, der es erlaubt, heimliche Operationen auszuführen. Solche Schwachstellen sollten eigentlich unverzüglich geschlossen werden. Kriminelle könnten sie ausnutzen. Wenn der Staat eine Schwachstelle kennt, müsste er dann nicht eher den Hersteller der Software warnen, um Millionen von Kunden zu schützen, statt die Schwachstelle selbst auszunutzen? Diese Frage wird uns noch beschäftigen.

Gelingt das Platzieren des Trojaners auf dem Computer des Verdächtigen, stellt sich die nächste Frage: wird die Software dort nur das anrichten, was sie (im Auftrag des Staates) tun soll, nämlich die Festplatte nach terroristischen Anschlagsplänen oder anderem durchsuchen? Jeder Computer ist ein bisschen anders. Aus der Ferne kann der Schöpfer des Trojaners nicht genau erkennen, in welche Umgebung er sein Programm platziert. Vielleicht sind auf dem Computer Dateibereiche, die anderen Personen gehören, gegen die sich die Maßnahme nicht richtet? Vielleicht hat der Computer eine wichtige Funktion zur Steuerung von Geräten, die durch den

Trojaner vielleicht gestört werden? Kann der Computer vielleicht ausfallen? Was ist, wenn er dringend benötigt wird, vielleicht auch für lebenswichtige Zwecke? All das ist aus der Ferne nur schwer abzuschätzen.

Schließlich stellt sich noch ein drittes technisches Problem: wie werden die Daten ausgeleitet? Wie könnte eine Kommunikation an Firewalls vorbei organisiert werden, um die bei der Durchsuchung aufgefundenen Informationen an Polizei oder Verfassungsschutz zu schicken? Wie verhindert man das Mitlesen durch Dritte? Wie verhindert man, dass kriminelle Hacker die von der Polizei geschaffene Hintertür ihrerseits nutzen, um Daten auszuschleusen?

Mit dem Bundesamt für Sicherheit in der Informationstechnik auf der einen und den Verantwortlichen für das BKA auf der anderen Seite habe ich diese Fragen damals intensiv diskutiert. Wir alle hatten eine Vorstellung davon, was passieren soll und passieren kann, wenn der Staat üblicherweise mit polizeilichen Mitteln im Einsatz ist, auf Streife, bei der Wohnungsdurchsuchung oder einer Festnahme. Aber was sind die Umstände, was sind die Risiken, wo sind die Grenzen, wenn die Polizei heimlich auf der Festplatte aktiv ist? Das ist eine technische und eine rechtliche Herausforderung. Und das ist bis heute eine politische Herausforderung. Die heimliche Aktivität des Staates in unserer immer komplexeren digitalen Welt, in den Computern und Smartphones, Tablets und Haushaltsgeräten, wirft sofort die Assoziation von Orwells »1984« auf. Wie kann die Überwachung gesteuert, beherrscht und eingegrenzt werden? Wo führt das hin? Ist der Staat mit Staatstrojanern demnächst auch im digitalen Heizungsventil oder im Fitnessarmband oder im Herzschrittmacher eines Verdächtigen?

Auch rückblickend ist es nicht erstaunlich, dass die Debatte große Wellen geschlagen hat. An vielen Laternenpfählen in Deutschland hingen Aufkleber mit dem Konterfei von Bundesinnenminister Schäuble und der Unterschrift »STASI 2.0«. 2007 kam das iPhone auf den Markt. Viele »Early Adopter«, der Technik besonders aufgeschlossene Menschen, verlagerten mehr und mehr ihrer Alltagsgeschäfte in die digitale Welt. Das Unbehagen über die heimlichen Aktivitäten des Staates reichte schnell weit in das bürgerliche Lager hinein. Die Zustimmung in der Bevölkerung für die Online-Durchsuchung sank: waren 2007 noch 65 % für die Online-Durchsuchung[8], sprachen sich vier Jahre später 52 % der Bürger dagegen aus[9]. Das Unbehagen erreichte schließlich auch das Bundesverfassungsgericht. Der Berichterstatter für die Klage gegen das nordrhein-westfälische Verfassungsschutzgesetz war Wolfgang Hofmann-Riem. Der Fall ließ ihn nicht schlafen. Er arbeitete sich tief in die Materie ein.

Im Februar 2008 erging das auf seiner Arbeit beruhende Urteil des Bundesverfassungsgerichts. Die Befugnis zur Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz wurde für verfassungswidrig erklärt und aufgehoben. Zwar sei eine Online-Durchsuchung nicht völlig unmöglich, sie müsse wegen ihres sehr einschneidenden Charakters aber an viel strengere Voraussetzungen geknüpft und mit stärkeren Auflagen verbunden werden. Das Gericht nutzte den Fall, sich sehr intensiv mit der Frage staatlichen digitalen Handelns zu beschäftigen. In den Mittelpunkt der Überlegungen stellte das Gericht – erstmals – die Frage, welche Bedeutung digitale Systeme heutzutage für die Bürgerinnen und Bürger haben und die Wahrnehmung ihrer Grundrechte. Die Achtung der Menschenwürde und der Schutz des Persönlichkeitsrechts müssten, so das Gericht, im Zeitalter der Digitali-

sierung auch das menschliche Handeln mithilfe von IT-Systemen umfassen. Aus diesem Gedanken heraus entwickelte das Bundesverfassungsgericht ein neues Grundrecht, das *Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.* Der Titel ist leider ein bisschen sperrig geraten, aber der Inhalt hat es in sich: Aus Art. 1 und Art. 2 des Grundgesetzes entwickelte das Gericht ein Grundrecht, das den einzelnen davor schützt, dass seine IT-Systeme ausgespäht und manipuliert werden. Die Literatur hat das Grundrecht später »IT-Sicherheitsgrundrecht« genannt, ich selbst würde es eher »Digitale Handlungsfreiheit« nennen. Im Kern geht es darum, dass viele unserer Handlungen mittlerweile nicht direkt und unmittelbar erfolgen, sondern durch digitale Systeme vermittelt werden. Indem der Staat auf diese Systeme heimlich zugreift, sie gegebenenfalls manipuliert, kann er mein ganzes Leben beeinträchtigen, meinen Alltag stören, mein Bild bei anderen verfälschen, möglicherweise sogar körperliche Schäden anrichten. Denken Sie nur an selbstfahrende Autos. Das ist weit mehr als der heimliche Zugriff auf Daten (der bereits durch das 1983 erfundene Recht auf informationelle Selbstbestimmung geschützt war).

Hoffmann-Riems neues Grundrecht ist weise und zukunftsweisend. Leider ist es der Politik bislang nicht gelungen, daraus eine umfassende rechtliche Regelung zum Schutz der persönlichen IT-Systeme zu entwickeln. Doch das Grundrecht hat ausgestrahlt in viele Gesetzesvorhaben und dafür gesorgt, dass Fragen der IT-Sicherheit größere Bedeutung bekommen haben, vom intelligenten Stromzähler bis zum Gesundheitswesen.

Einen Stopp der Online-Durchsuchung bewirkte die Entscheidung allerdings nicht. In Nordrhein-Westfalen, anderen Bundesländern und dem Bund wurden Gesetze erlassen, die

Online-Durchsuchungen erlauben, allerdings unter höheren Voraussetzungen als bisher. Zudem sind die Anforderungen an die Durchführung, die Risikoabschätzung, die Dokumentation und die Sorgfalt aller Beteiligten deutlich höher. Seit 2009 hat das BKA die Befugnis zur Online-Durchsuchung, allerdings nur im Zusammenhang mit dem internationalen Terrorismus. Das entsprechende Gesetz wurde 2016 vom Bundesverfassungsgericht mit kleineren Korrekturen akzeptiert. Die technischen Schwierigkeiten der Durchführung solcher heimlichen Operationen auf der Festplatte von Verdächtigen aber bleiben. Die hohen Anforderungen des Gerichts machen die Software noch aufwändiger. Trotz erheblicher personeller Aufstockung kann das BKA die Software nicht vollständig selbst entwickeln. Externe Firmen und deren Spionagesoftware werden eingebunden. Das wirft neue Fragen auf: wer kann die korrekte Funktionsweise überprüfen? Die Analyse des bayerischen Staatstrojaners durch den Chaos Computer Club ergab technische Funktionen der am Markt eingekauften Spionagesoftware, die nicht mit den Vorgaben des Verfassungsgerichts vereinbar sind. Wer kann zukünftig garantieren, dass das nicht der Fall ist? Wer erkennt, ob ein externer Auftragnehmer Hintertüren in das Programm eingebaut hat? Hacker, die Schwachstellen auffinden und Software entwickeln, mit der man heimlich in IT-Systeme eindringen kann, gehören zu den bestbezahlten Fachleuten der Welt. Der Staat kann ihre Gehälter kaum bezahlen.

All diese Fragen sind bis heute ungeklärt. Gleichzeitig hat der Bundestag die Befugnis zur Online-Durchsuchung im Sommer 2017 deutlich erweitert, nicht zuletzt wegen der weiteren Digitalisierung der Kriminalität. Heimliche Zugriffe auf die Festplatte sind nun bei einer ganzen Reihe weiterer schwerer Straftaten erlaubt. Tatsächlich aber hat das BKA bislang nur

eine Handvoll Online-Durchsuchungen durchgeführt. Genaue Zahlen werden nicht bekanntgegeben. Derweil entwickelt sich die digitale Welt ständig weiter. Heute einsatzfähige »Staatstrojaner« sind morgen nicht mehr tauglich. Heute überwindbare Schutzmaßnahmen der Kriminellen werden morgen aufgerüstet sein. Es bleibt ein dauerhaftes Problem, ob, wie und in welchem Umfang der Staat heimlich in der digitalen Welt seiner Bürger agiert – rechtsstaatlich korrekt und ohne Kollateralschäden. Die Diskussion um »Stasi 2.0« kann jederzeit wiederaufleben.

2.4 BEULEN, BLESSUREN UND LERNKURVEN

Klarmachen zum ändern – mit diesem Motto trat die im September 2006 gegründete Piratenpartei an, den Etablierten das Internet beizubringen. Die Debatte um das Urheberrecht war der Auslöser für das Entstehen der Partei. Die anderen netzpolitischen Themen beförderten ihr Wachstum auf über 34 000 Mitglieder. 2011 und 2012 konnte sie mit Ergebnissen um die 8 % in die Landesparlamente von Berlin, Saarland, Schleswig-Holstein und Nordrhein-Westfalen sowie in viele Kommunalparlamente einziehen. Damit war der Zenit allerdings schon erreicht: Bei der Bundestagswahl 2013 kamen die Piraten nur noch auf 2,2 % und verabschiedeten sich seitdem wieder aus allen Landtagen.[10]

Die kurze Erfolgsgeschichte der Piratenpartei war ein netzpolitischer Weckruf für die anderen Parteien. Denn der schnelle Erfolg der Ein-Themen-Partei hing stark damit zusammen, dass die Menschen den etablierten Parteien nicht zutrauten, die mit dem Internet zusammenhängenden Fragen zu verste-

hen. Zu sehr hatte sich die Politik in den Debatten um Urheberrecht, Netzsperren und Online-Durchsuchung als unsensibel und über weite Strecken auch ungeschickt präsentiert. In einer repräsentativen Umfrage von FORSA für BITKOM gaben 2010 immerhin 17 % der Befragten an, keine der etablierten Parteien verstünde etwas vom Internet.[11] Aufgerüttelt durch die Piratenpartei reagierte die Politik – wenn auch vorsichtig: Nach der Bundestagswahl 2013 wurden zunächst einmal ein Ausschuss für Digitale Agenda gegründet. Die Digitalpolitik erhielt damit einen festen Ort im Parlament.

Die Vertrauenskrise in die netzpolitische Kompetenz ist die eine Lehre, die man aus den drei Beispielen ziehen kann. Doch es gibt viel weitergehende Problemlagen, die in Netzsperren, Urheberrecht und Staatstrojaner aufscheinen: Der Staat bewegt sich mit seinen Gesetzen und Behörden in einem neuen Raum, in dem andere Gesetzmäßigkeiten gelten. Mal zu drastisch wie bei den Netzsperren, mal zu ungeschickt wie bei der Online-Durchsuchung, mal zu früh wie beim Urheberrecht, mal auch zu spät wie mit Sicherheit beim Datenschutz, zu dem wir später noch kommen.

Die erste Annäherung der Politik an eine Gestaltung des Internets war eher holzschnittartig. Das kann man gut an dem vielzitierten Begriff des »rechtsfreien Raums« festmachen. Das Internet sei kein rechtsfreier Raum, hieß es. Es dürfe kein rechtsfreier Raum werden. Was in der analogen Welt gelte, das müsse auch im Netz durchgesetzt werden. Diese Aussagen lassen sich fast immer in der politischen Begründung früher staatlicher Interventionen im Netz finden. Mit dem Ziel einer möglichst 1:1-Übertragung wurden Analogien entwickelt und entsprechende gesetzliche Maßnahmen entworfen und beschlossen: Wohnungen darf ich durchsuchen, also auch Festplatten. Einem Spediteur kann ich die Nicht-Beför-

derung bestimmter Güter vorschreiben, also auch einem Internet-Unternehmen. Eine CD nachzupressen ist illegal, also muss es auch die digitale Kopie sein.

Fast immer scheitern diese einfachen Analogien an der Andersartigkeit des digitalen Lebens. Die Digitalisierung kennt keine 1:1-Entsprechungen. Unser »analoges« Leben (was immer das sein soll) wird nicht durch »digitales« Leben ersetzt, sondern durch Digitalisierung zu etwas Neuem gemacht. Und dieses Neue folgt eigenen Regeln. Ein Staat, der das neue Leben mitgestalten (und regeln) will, muss die neuen Wirkungszusammenhänge zunächst einmal verstehen. Einige dieser Spielregeln haben wir schon kennengelernt: Was irgendwo im Netz ist, bekommt man selten entfernt oder gesperrt. Wenn der Staat im digitalen Raum handelt, dann produziert er ganz neuartige Gefahren. Wer herkömmliche Geschäftsmodelle schützen will, wird das auf globalen digitalen Märkten nicht schaffen. Alles ganz schön schwer zu schlucken für Politik und Beamte, die es gewohnt waren, umsetzen zu können, was man durchsetzen will.

Aus den ersten Gehversuchen in der Netzpolitik haben Politik und Verwaltung gelernt. Auch ich persönlich habe bei den drei Beispielen viele Lernerfahrungen gemacht. Das war auch nötig, denn was als nächstes kommt, ist viel wichtiger: Alles wird digitalisiert, es brennt an allen Ecken – und der Staat muss seine Rolle im digitalen Raum umfassend – neu – bestimmen.