# Russlands "Souveränes Internet": Digitale Abschottung nach außen und verstärkte Kontrolle im Inneren

Burkhardt, Fabian

Erstveröffentlichung / Primary Publication
Arbeitspapier / working paper

Unveröffentlichtes Manuskript

# Russlands „Souveränes Internet“
# Digitale Abschottung nach außen und verstärkte Kontrolle im Inneren

Fabian Burkhardt

| | |
|---|---|
| Anmerkung | Das Manuskript wurde während der Tätigkeit an der Stiftung Wissenschaft und Politik in Berlin verfasst und im August 2019 abgeschlossen und seither nicht mehr aktualisiert. |
| Empfohlene Zitierung | Burkhardt, Fabian. „Russlands ‚Souveränes Internet‘. Digitale Abschottung nach außen und verstärkte Kontrolle im Inneren.“ Unveröffentlichtes Manuskript, Berlin, August 2019. |

Russlands „Souveränes Internet“

Digitale Abschottung nach außen und verstärkte Kontrolle im Inneren

*Fabian Burkhardt*

Am 01. Mai unterzeichnete Präsident Wladimir Putin ein wegweisendes Gesetz, das auf die Autarkie russischer Internetinfrastruktur im Gefahrenfall abzielt. Das sogenannte Gesetz über das „Souveräne Internet“ markiert einen bisherigen Höhepunkt in der Digitalpolitik des Kremls, mit dem das Internet von einem ehemals vernachlässigten Politikbereich zu einem strategischen Sektor avanciert. Der Entwurf wurde als direkte Reaktion auf die neue US-amerikanische Cybersicherheitsstrategie vom September 2018 am 14. Dezember 2018 in die Duma eingebracht, sein Ursprung lässt sich allerdings bis zum Anfang der Ukraine-Krise 2014 zurückführen. Das Gesetz wurde von Hardlinern forciert, die auf weitere Isolation Russlands vom Westen, stärkere Kontrolle im Innern und Importsubstitutionen durch staatliche und staatsnahe Unternehmen setzen. Das Gesetz tritt stufenweise ab November 2019 und Januar 2021 in Kraft. Russland wird es in absehbarer Zeit nicht gelingen, einen Firewall nach chinesischen Vorbild zu errichten. Dennoch wird das Gesetz mittelfristig bedeutende innen- und außenpolitische Wirkung entfalten.

Das am 14. 12. 2018 von drei Parlamentariern initiierte Gesetz zielt laut Urheber darauf ab, die Infrastruktur des russischen Segments des Internets (Runet) derart umzurüsten, dass dieses uneingeschränkt autark funktionieren kann, falls die USA „den Schalter“ (kill switch) umlegen würden, um Russland vom globalen Domain Name System (DNS) abzuschneiden. In einer möglichen Eskalationsspirale könnten die USA etwa ihre Sanktionen auf die nach kalifornischem Recht registrierte *Internet Corporation for Assigned Names and Numbers* (ICANN) ausweiten, so dass der Zugang zur russischen Domäne .ru von Russland nicht mehr möglich wäre. Der Leiter der Internetaufsichtsbehörde Roskomnadsor Aleksandr Scharow betonte, dass es sich bei dem Gesetz lediglich um eine Abschreckungsmaßnahme handle, eine Art „Atomwaffe im Standby-Modus“. Sie soll signalisieren, dass Eingriffe in das Runet von außen fruchtlos sind und dass ausländische Unternehmen erfolgreich gesperrt werden können, wenn diese sich nicht an russische Gesetze halten.

## Die Neuerungen im Detail: Zentralisierte Kontrolle über Infrastruktur

Um das „stabile, sichere und integre Funktionieren“ des Internets auf dem russischen Staatsgebiet sicherzustellen, sollen folgende Neuerungen umgesetzt werden:
Internetanbieter (ISP), Eigentümer von Internetknoten (IXP) und grenzüberschreitenden Netzwerken, Betreiber von technologischen Netzen und Inhaber von Autonomen Systemnummern sind an das Gesetz gebunden. ISP müssen in ihrem Netz technische Geräte anbringen, die im Gefahrenfall eine zentrale Steuerung des Runets und im Normalbetrieb das Blockieren von gesetzlich verbotenen Diensten und Inhalten (mit *deep packet inspection,* DPI) erlauben. Die Kosten für die Bereitstellung der Geräte werden aus dem Staatshaushalt getragen, allerdings sind weitere Ausgaben für Wartung und Erneuerung nicht geregelt. Internetanbieter werden explizit von der Haftung für mögliche Schäden ausgenommen, die im Zuge der Gefahrenabwehr für private Nutzer, Unternehmen und Staat durch Internetausfälle entstehen können. Die 2008 gegründete und formal dem Telekommunikationsministerium unterstehende Behörde Roskomnadsor hat die Koordinations- und Überwachungsfunktion inne und führt ein Register, in dem sich Eigentümer von grenzüberschreitenden Netzwerken und Internetknoten eintragen lassen und Informationen über Eigentumswechsel und Verbindungen mit anderen, insbesondere im Ausland registrierten, Inhabern von Autonomen Systemnummern, sowie Routing-Informationen übermitteln müssen. Internetanbieter und Infrastruktureigentümer werden verpflichtet, an Übungen zur Gefahrenabwehr teilzunehmen. Vorgeschrieben wird ebenso, dass Maßnahmen von Fahndungs- und Sicherheitsbehörden in ihren Netzen technisch zu gewährleisten sind, gleichzeitig wird ihnen darüber eine Schweigepflicht auferlegt. Außerdem soll Roskomnadsor ein Internetmonitoring- und Steuerungszentrum sowie eine entsprechendes Informationssystem schaffen. Im Normalbetrieb wird von diesem Zentrum lediglich die Infrastruktur und der Datenverkehr registriert und beobachtet, im Gefahrenfall soll jedoch das Runet und dessen Routing zentral gesteuert werden, entweder über die installierten technischen Geräte, oder über direkte Anweisungen des Zentrums an die Anbieter. Weitere Bestimmungen zielen auf die Verwendung von russischer Soft- und Hardware durch staatliche und im Staatsbeschaffungswesen beteiligten Organisationen ab, die sukzessive ausländische ersetzen müssen. Datenbanken, die diese Organisationen nutzen, dürfen sich nicht auf ausländischem Staatsgebiet befinden. Die Kommunikation zwischen diesen Organisationen muss den nationalen

Verschlüsselungsstandards entsprechen. Bis Januar 2021 muss ein nationales Domain Name Systems (DNS) geschaffen werden, dessen Koordination von einer nichtkommerziellen Organisation übernommen wird, zu deren Gründern der russische Staat gehören und die eingetragene Eigentümerin dieser Domänen bei den für Domänennamen verantwortlichen internationalen Organisationen (sprich: ICANN) sein muss. Derzeit ist dies das Koordinationszentrum für die Top-Level-Domains .ru/.рф.

## Die Vorgeschichte: Spätfolgen der Krim-Annexion

Das Begleitschreiben des Gesetzes nennt als konkreten Anlass die im September 2018 veröffentlichte US-Cyberstrategie, in der Russland, Iran und Nordkorea „rücksichtsloser Cyberattacken" beschuldigt werden. Die Genese lässt sich allerdings bis auf den Beginn der Ukraine-Krise im Jahr 2014 zurückführen. In russischen und internationalen Medien wurde oft Regimestabilität als Hauptmotiv für das Gesetz genannt: Putin wolle die Internetkontrolle verschärfen und bei innenpolitischen Krisen wie Massenprotesten das Internet abschalten können. Eine tiefergehende Analyse der Vorgeschichte sowie der Befürworter und Gegner zeigt, dass vor allem die Verwundbarkeit durch Eingriffe von außen sowie die Abhängigkeit von grenzüberschreitender Internetinfrastruktur und transnationalem Informationsfluss , die die staatliche Souveränität Russlands einschränken, als maßgebliche Triebkraft des Gesetzes dienten. Gleichzeitig ermöglichen die vorgesehenen technischen Maßnahmen aber auch eine stärkere Kontrolle des Runets in innenpolitischen Fragen und können dazu beitragen, Meinungsfreiheit weiter einzuschränken und Massenmobilisierung gegen das Regime zu verhindern. Dreh- und Angelpunkt des Gesetzes ist ein weit gefasstes Verständnis der Gefahren, die zu zentraler Steuerung führen können. Zu den Gefahren gehören etwa Umweltkatastrophen und technische Ausfälle, nicht erlaubtes Eindringen in russische Soft- und Hardware, destabilisierende Informationseinwirkung aus dem Aus- und Inland oder der Zugang zu Informationen und Ressourcen, die in Russland gesetzlich verboten sind. Durch eine breite Auslegung der Gefahren hat Roskomnadsor einen sehr großen Spielraum, einen „digitalen Notstand" auszurufen.

## Fünf Jahre bis zum Ziel: Hardliner und deren Kritiker

Der lange, fünfjährige Weg von der Agendasetzung im Jahr 2014 bis zur Unterzeichnung des Gesetzes 2019 ist durchaus typisch für den russischen Politikprozess. Präsident Putin lanciert eine strategische Vision, zieht sich dann aber weitestgehend aus dem Tagesgeschäft zurück und überlässt die konkrete Ausgestaltung Vertrauten, die jedoch häufig auf Widerstand von bürokratischen und unternehmerischen Interessensgruppen stoßen. Als Ideengeber des „souveränen Internets" gilt eine Allianz von Hardlinern um den Sekretär des russischen Sicherheitsrats Nikolaj Patruschew und einer eigens dafür eingerichteten Arbeitsgruppe in der Präsidialverwaltung.

Die größten Hindernisse wurden ausgeräumt, bevor das Gesetz überhaupt ins Parlament eingebracht wurde, die Öffentlichkeit spielte keine wesentliche Rolle. In der Duma gab es lediglich eine öffentliche Anhörung am 17.01.2019 in einer Sitzung des Ausschusses für Informationspolitik, auf der eine Aussprache der wichtigsten Stakeholder stattfand, ohne dass diese jedoch wesentlichen Einfluss auf den Gesetzgebungsprozess gehabt hätte. Auch die Proteste von etwa 15 000 Menschen am 10. März 2019 gegen Internetkontrolle waren zwar verhältnismäßig zahlreich, konnten aber am Ergebnis nichts mehr ändern.

Dies sollte nicht darüber hinwegtäuschen, dass es sowohl aus dem Regierungslager als auch der Wirtschaft massive Kritik an dem Gesetzesentwurf gab. Dieser wurde mit unterschiedlicher Intensität in Gutachten der Regierung selbst, der Arbeitsgruppe „Telekommunikation & IT" des Expertenrats der Regierung, der staatlich kontrollierten Trägerorganisation des Nationalprojektes „Digitale Wirtschaft", des vom Präsidenten eingesetzten Internetbeauftragten Dmitrij Marinitschew, des Rechnungshofes, des wichtigsten Branchenverbandes, der Russländischen Assoziation für Elektronische Kommunikation (RAEK), und am allerdeutlichsten vom größten Arbeitgeberverband, der Russländischen Verbands der Industriellen und Unternehmer (RSPP), zum Ausdruck gebracht. Auch die vier Mobilfunkanbieter zeigten sich vor allem wegen zusätzlicher Kosten und Netzwerkqualität besorgt. Ganz im Gegensatz dazu sprachen sich die beiden Internetgiganten Yandex und Mail.ru in der Hoffnung auf größere Marktanteile insgesamt für das Gesetz aus, obwohl Yandex im März 2019 bei einem der Tests für die Geräte, die nach dem Inkrafttreten des Gesetztes zum Einsatz kommen sollen, massive technische Ausfälle erlitten hatte. Nach der zweiten Lesung im April wurde der Gesetzesentwurf aufgrund dieser Einsprüche in einigen Punkten abgeschwächt: Die

Kompetenzen von Roskomnadsor wurden reduziert, und das ab 2021 einzuführende nationale Domain Name System soll in bestehende internationale Strukturen integriert und kompatibel werden und ist somit als Duplizierung, nicht aber als Ersatz mit einem eigenen Rootserver konzipiert.

## Die Ukraine-Krise als Katalysator

In der Risikokalkulation des russischen Sicherheitsrates bestand nach den ersten, am 06. März 2014 verabschiedeten, US-Sanktionen die Möglichkeit, dass auch das russische Internet mit Strafmaßnahmen belegt werden könnte. In Folge einer Sicherheitsratssitzung wurde am 26. Juli 2014 eine Übung unter Leitung des damaligen Telekommunikationsministers Nikolaj Nikiforow abgehalten, bei der Vertreter von Verteidigungsministerium, Inlandsgeheimdienst FSB, Innenministerium, das staatlich kontrollierte Telekommunikationsunternehmen Rostelecom und die zentrale Domänen-Registrierungsstelle „Technisches Zentrum Internet“ (TZI) anwesend waren. Eine zentrale Rolle kam dem größten russischen und weltweit fünftgrößten, von Rostelecom kontrollierten Internetknotenpunkt MSK-IX zu, durch den derzeit etwa 60% des russischen Datenverkehrs fließen. Obwohl wenig Details über die Übung bekannt wurden, lässt sich das Bedrohungsszenario rekonstruieren: Ziel war es die Funktionsfähigkeit des Runets in einem hypothetischen Fall zu testen, in dem ICANN die Information über die russische Domäne .ru/.рф von ihren Root-Servern löscht oder den Zugang verwehrt. Die Auflösung der Runet-Domänenamen sollte über einen von MSK-IX betriebenen Server erfolgen, auf dem die bei ICANN hinterlegten Datenbanken in Kopie gespeichert sind. Ausgegangen wurde dabei explizit nicht von einer dauerhaften Isolation Russlands, sondern von einer kurzzeitigen Störung, während derer die wichtigsten Funktionalitäten des Runets aufrechterhalten sollten.

## Schleichende Verstaatlichung

De facto ist die Koordination und Registrierung der russischen Domäne .ru schon seit vier Jahren in staatlicher Hand. Im Jahr 2015 wurden zwei für die russische Domäne zentrale Organisationen unter staatliche Kontrolle gebracht: Das Telekommunikationsministerium erwirkte eine Satzungsänderung des Koordinationszentrums der Nationalen Domäne und fungierte von nun an mit dem staatlich kontrollierten Institut für die Entwicklung des Internets (IRI) als weiteres Gründungsmitglied. Als Einflussverlust der Internetbranche muss auch der

Wechsel an der Spitze des Koordinationszentrums gewertet werden, da der im Sommer 2015 ernannte Direktor Andrej Worobjow zuvor Mitarbeiter von IRI war und deswegen als Vertreter staatlicher Interessen gilt. 2018 schließlich übernahm Rostelecom die Funktionen des Technischen Zentrums Internet (TZI).

## Importsubstitutionen mit mäßigem Erfolg

Seit dem Jahr 2015 unternimmt die Regierung Anstrengungen, Russlands Abhängigkeit von ausländischer Software zu verringern. Diese Importsubstitutionen gehen bisher nur schleppend voran. Die große Abhängigkeit von amerikanischen Produkten im russischen Staatssektor wird in den kommenden Jahren weiterbestehen.

Durch ein am 29. Juni 2015 in Kraft getretenes Gesetz sollen föderale, regionale und kommunale Verwaltungen nur noch Software für Computer und Datenbanken erwerben können, die in einem ab Anfang 2016 geführten Verzeichnis für heimische Produkte eingetragen sind. Als Begründung werden nicht nur Verfassungsschutz, Sicherheit und Landesverteidigung angeführt, sondern auch die Unterstützung von russischen Herstellern durch protektionistische Maßnahmen. Während im Gesetz die Rahmenbedingungen abgesteckt werden, welche Produkte als „russisch“ gelten, wurde dessen Umsetzung in einem Regierungserlass vom 16.11.2015 im Detail geregelt. Ein Expertenrat entscheidet über die Aufnahme von Produkten in das Verzeichnis und stimmt über Ausnahmen ab, wenn russische Erzeugnisse nicht den Anforderungen von staatlichen Anwendern entsprechen. Im Dezember 2017 wurde zudem der Import von Software aus Mitgliedsländern der Eurasischen Wirtschaftsunion gestattet. Bis Ende 2020 soll gewährleistet sein, dass in Behörden, staatlichen Unternehmen und solchen mit staatlichem Anteil vorwiegend Software russischer Hersteller zum Einsatz kommt. Nach Einschätzung des Ministers Nikiforow belief sich der Anteil russischer Hersteller im Staatssektor, deren Weltmarktanteil mit 2% gering ist, im Jahr 2014 auf zwischen 3 und 25% je nach Produkt, bis 2025 sollte dieser auf deutlich über 50% gesteigert werden. In der Staatsbeschaffung konnte laut offiziellen Angabe 2019 der Anteil russischer Software von 20% im Jahr 2015 auf 65% gesteigert werden, 2024 soll sich dieser Anteil in Behörden auf 90% und in staatlichen Unternehmen auf 70% belaufen.

## Langsame Umsetzung von Datensouveränität und Erfassung kritischer Infrastruktur

In der ersten Hälfte des Jahres 2016 kursierte im Umkreis des Telekommunikationsministeriums erstmals ein Referentenentwurf eines Gesetzespakets, der auf die Autonomisierung des russischen Segments des Internets abzielte. Der Entwurf enthielt die meisten Kernelemente des späteren Gesetzes, dennoch bestanden viele Ungereimtheiten. So sieht etwa das Staatsprogramm „Informationsgesellschaft" nicht nur vor, dass bis 2020 99% des russischen Datenverkehrs innerhalb der Staatsgrenzen verlaufen sollen (2014: 70%), sondern dass bis dahin auch 99% der kritischen Internetinfrastruktur gedoppelt werden soll, um bei Ausfällen Ausweichmöglichkeiten zu haben (2014: 0%, Mitte 2016: 40%). Zu diesem Zeitpunkt bestand allerdings noch keine Einigkeit, was konkret als kritische Infrastruktur zu verstehen wäre, die dann unter staatliche Aufsicht gebracht werden sollte. Ein Definitionsversuch wurde in einem vom Inlandsgeheimdienst FSB vorangetriebenen und am 01. Januar 2018 in Kraft getretenen Gesetz unternommen, welches erstmalig den Begriff „bedeutsames Objekt kritischer Informationsinfrastruktur" einführte. Das entsprechende Verzeichnis registrierter Objekte dient als Grundlage für das FSB-Cyberbedrohungssystem GosSOPKA. Allerdings erwies sich die Erfassung als problematisch und verzögert somit die Umsetzung: Viele kritische Infrastrukturobjekte, allen voran Banken und Mobilfunkanbieter, verweigerten sich dieser Inventarisierung, zögerten diese hinaus oder gaben eine möglichst niedrige Bedrohungsstufe an, um zusätzlicher Regulierung und möglichen Eingriffen durch Sicherheitsorganen zu entgehen, bis Anfang 2019 ließen sich etwa lediglich 15% der geschätzten 180 000 Objekte in das Verzeichnis eintragen. Zwar listete die Ende 2016 veröffentlichte Neufassung der seit 2000 nicht mehr aktualisierten Informationssicherheitsdoktrin eine Reihe von Gefahren auf, die von „grenzübergreifendem Informationsfluss" ausgehen. Diese Bedrohungen sind allerdings allgemein formuliert, und die vom Sicherheitsrat ausgearbeiteten konkreteren Ausformulierungen nur für bestimmte staatliche Behörden zugänglich, was eine Risikoabwägung – etwa im Falle einer zentralen Steuerung des Runets - für Inhaber kritischer Informationsinfrastruktur schwierig bis unmöglich macht.

## Lokale Vorratsdatenspeicherung erzeugt Konflikte mit globalen Unternehmen

Roskomnadsor trieb das Gesetz über das „Souveräne Internet“ auch voran, um gegenüber ausländischen Unternehmen eine rechtlich wie auch technisch mächtigeres Instrumentarium in die Hand zu bekommen, um diese besser drosseln und blockieren zu können. Bisher sind die politischen Risiken für Roskomnadsor selbst hoch, da etwa Google, Facebook und Instagram viele Nutzer haben und keine Sicherheit besteht, dass die Großkonzerne auch wirklich zuverlässig blockiert werden könnten.

Seit September 2015 sind Telekommunikationsunternehmen gesetzlich verpflichtet, personenbezogene Daten auf Servern zu speichern, die sich auf dem Staatsgebiet der Russischen Föderation befinden. Erwartungsgemäß stellte sich dies für ausländische Unternehmen aus Datenschutzgründen als problematisch dar: Das in Russland populäre Berufsnetzwerk LinkedIn etwa weigerte sich, die Daten seiner russischen Nutzerinnen und Nutzer lokal zu speichern. Prompt wurde der Service im November 2016 in Russland gesperrt. Während Apple zumindest formal den Forderungen nachkam, dauert das Ringen der Aufsichtsbehörde Roskomnadsor mit den amerikanischen Großkonzernen Twitter und Facebook noch an. Im Frühjahr 2019 wurden die sozialen Netzwerke mit einer geringen Ordnungsstrafe von 3000 Rubel (etwa 40€) belangt. Roskomnadsor konnte sich bisher noch nicht zu einer Blockade entschließen, dennoch wurde eine endgültige Entscheidung darüber schon für Anfang 2020 angekündigt, zwischenzeitlich waren Strafen in einer Höhe bis zu einem Prozent des russischen Jahreserlöses der Unternehmen im Gespräch.

Im Rahmen einer Mitte 2016 verabschiedeten Anti-Terrorgesetzgebung, die nach der Initiatorin den Namen „Jarowaja-Paket“ erhielt, wurde das Strafrecht verschärft und Telekommunikationsunternehmen und sogenannten „Organisatoren von Informationsverbreitung“ (ORI) zusätzliche Anforderungen auferlegt. Als ORI werden nicht nur klassische Messengerdienste wie Whatsapp, Telegram oder WeChat klassifiziert, sondern jede Webseite, die es Usern ermöglicht, Nachrichten auszutauschen, also etwa auch Blogs und Foren mit Kommentarfunktionen. Laut des am 01. Juli 2018 in Kraft getretenen Jarowaja-Pakets sind Telekommunikationsunternehmen und ORI verpflichtet Daten und Metadaten, zu denen auch Text, Audio- und Videoinhalte gehören, bis zu sechs Monate zu speichern, um diese auf Anfrage an Sicherheitsbehörden weiterzugeben. Diese Daten müssen nicht nur auf russischen Staatsgebiet gespeichert sein, sondern sich ebenfalls durch die russischen Sicherheitsbehörden

entschlüsseln lassen. Die bei LKW-Fahrern beliebte und bei Protesten gegen die LKW-Maut genutzte Walkie-Talkie App Zello ist seit Mitte 2017 relativ zuverlässig blockiert und im Google-Appstore nicht mehr verfügbar. Ein Fiasko erlitt Roskomnadsor mit dem von dem Exilrussen Pawel Durow gegründeten Messenger Telegram: Durow hatte sich Mitte 2018 geweigert, den Sicherheitsbehörden die Entschlüsselung der Nachrichten zu ermöglichen, der Blockadeversuch scheiterte kläglich, obwohl zwischenzeitlich bis zu 18 Millionen IP-Adressen gesperrt gewesen waren und die Kollateralschäden für russische Unternehmen enorm waren. Die praktische Umsetzung des Jarowaja-Pakets erweist sich sogar bei grundsätzlich kooperativen Unternehmen als schwierig: selbst wenn diese die entsprechenden Gerätschaften (im Rahmen von SORM, Russlands System der Telekommunikationsüberwachung) anschafften zog sich die Lizenzierung beim Inlandsgeheimdienst FSB auf bis zu sechs Monate hin. Für Provider bedeutet dies, dass sie eigentlich schon ein Gesetz erfüllen müssen, was wohl erst frühestens ein Jahr nach in Kraft treten Ende 2019 technisch möglich sein wird. Ähnliche Verzögerungen sind auch für das „Souveräne Internet"-Gesetz zu erwarten.

### Haushaltsplanung vor Einbringung des Gesetzes

Letzter Meilenstein auf dem Weg zur Einbringung des Gesetzesentwurfs über das „Souveräne Internet" ist das Staatsprogramm „Digitale Wirtschaft", welches im Verlauf des Jahres 2017 Gestalt annahm. Im Unterbereich „Informationssicherheit" wurde im Januar 2018 eine umfangreiche Road Map verabschiedet. Der Maßnahmenkatalog sah auch die Einbringung des Gesetzes über das „Souveräne Internet" vor. Im Herbst 2017 wurde der Entwurf auf dem Portal für Gesetzesfolgenabschätzung publiziert, um frühzeitig Beschwerden in Bezug auf Kosten für Stakeholder abzufangen. In der Tat wurde nach Widerspruch der großen vier Mobilfunkanbieter sowie des Wirtschafts-, Finanz- und Justizministeriums und des FSB eine zentrale Passagen abgeändert: Internetknoten wurden restriktiver definiert, und das Verbot von einem Anteil über 20% von ausländischen Aktionären aufgehoben, mit Ausnahme des strategisch wichtigsten Knotenpunkts MSK-IX. In der früheren Version wären die „Großen Vier", die einen großen Anteil an Auslandseigentümern ausweisen, zu Gunsten des staatlichen Telekommunikationsriesen Rostelecom benachteiligt worden. Die Einbindung des „Souveränen Internets" in das nach den Präsidentschaftswahlen 2018 in ein Nationalprojekt umgewandelte Staatsprogramm „Digitale Wirtschaft" erklärt auch, warum im russischen Haushalt für die drei

Jahre bis 2021 schon 30 Mrd. Rubel (etwa 400 Mio. €) veranschlagt waren, bevor das Gesetz überhaupt erst in die Staatsduma eingebracht worden war.

## Auswirkungen des Gesetzes

Das Gesetz enthält viele allgemein gehaltene Formulierungen und muss deswegen in knapp 40 Regierungs- und Ministerialerlassen ausgestaltet werden. Dennoch lässt die windungsreiche Genese eine Bewertung der möglichen Auswirkungen zu.

**Erstens** ist das Bedrohungsszenario, das dem Gesetz zu Grunde liegt zwar möglich, aber äußerst unwahrscheinlich. So weist etwa der *Chief Technology Officer* von ICANN David Conrad darauf hin, dass die USA theoretisch ICANN dazu zwingen könnten, die russische Topleveldomain .ru vom Rootserver zu entfernen. Dies würde aber zu einem dramatischen Vertrauensverlust in die USA führen, der die Vorteile eines solchen Schrittes weitaus überwiegen würde. Zudem ist keinesfalls gegeben, dass sich die für den eurasischen Raum zuständige *Regional Internet Registry* RIPE NCC mit Sitz in Amsterdam im Konfliktfall an Vorgaben von ICANN halten würde. So weigerte sich RIPE NCC, der Forderung der Ukraine nachzukommen, keine IP-Adressen und Autonome Systemnummern an die von Russland kontrollierte Donezker Volksrepublik zu vergeben, und damit den Internetzugang zu verweigern, obgleich die holländische NGO an EU-Sanktionen gebunden ist. Zudem verfügt Russland schon über eine eigene DNS-Rootserverstruktur in allen Föderalbezirken, so dass selbst im Extremfall das Runet zumindest für eine gewisse Zeit funktionsfähig bleiben würde. Deswegen befürchten Gegner des Gesetzes in Regierung und Wirtschaft, dass im Fall einer Zentralisierung des Routings das Runet anfälliger für Ausfälle oder gar Angriffe werden könnte.

**Zweitens** ist eine weitere Zielsetzung des Gesetzes, den Datenverkehr im Runet innerhalb des russischen Staatsgebietes zu halten. In ihrem Länderbericht aus dem Jahr 2019 kommt RIPE NCC zu dem Schluss, dass Russland über eine robuste und stabile Internetinfrastruktur verfügt, die resistent gegenüber Ausfällen ist, was wiederum durch die hohe Konnektivität gewährleistet wird. Dabei verbleibt die überwiegende Mehrheit des Datenverkehrs innerhalb von Russland. In einer von der russischen Regierung in Auftrag gegebenen Studie aus dem Jahr 2017 kommt die „Assoziation für Dokumentation im Telekommunikationswesen“ zu dem Ergebnis, dass sich in Russland eines der autonomsten und in sich geschlossenen Internetökosysteme herausgebildet hat, da weniger als 3% des Routings über das Ausland

verläuft. Kritiker befürchten, dass eine Verringerung der Konnektivität trotz belegter, schon bestehender Autonomie die Funktionsfähigkeit des Runet negativ beeinflussen könnte, etwa durch die Reduzierung der bisher 913 Unternehmen mit Lizenz für grenzüberschreitenden Internetverkehr.

**Drittens** besteht in der Internetbranche Einigkeit, dass die bisher im Staatshaushalt veranschlagten Gelder nicht für die Kosten ausreichen werden, die die Internetanbieter zu tragen haben und somit letztendlich auch auf den Endverbraucher umgelegt werden. Unabhängige Beobachter vermuten aufgrund von zusätzlicher Regulierung, Vergabe von Staatsaufträgen und Lizenzverfahren erhebliche Korruptionsrisiken, die die Kosten weiter in die Höhe treiben und gleichzeitig die Netzqualität negativ beeinträchtigen werden. Allerdings versprechen sich einige Internetanbieter paradoxerweise auch Verdienstmöglichkeiten, die erhöhte Ausgaben durch die im Jarowaja-Paket erforderliche lokale Vorratsdatenspeicherung teilweise kompensieren können: die *deep packet inspection*-Technologie der zu installierenden Geräte soll durch tiefere Analyse der Datenpakete eine gezielte Drosselung von Traffic erlauben. Kommerziell könnte dies genutzt werden, um Gebühren von besonders datenintensiven Streamingdiensten oder sozialen Netzwerken zu kassieren. De facto würde das aber auch bedeuten, dass die bisher in einem Schreiben der Antimonopolbehörde (FAS) aus dem Jahr 2016 festgehaltene Netzneutralität aufgehoben wird. Politische Risiken bestehen durch DPI in zweifacher Hinsicht: Zum einen könnten in Zukunft politisch unliebsame Dienste und Webseiten deutlich wirksamer gedrosselt werden, als dies bisher mit Telegram gelungen war. Denkbar wäre dieser Einsatz etwa bei innenpolitischen Krisen wie Massenprotesten. Zudem könnte DPI gegen ausländische Großkonzerne wie Facebook und Twitter eingesetzt werden, die sich weigern der russischen Datenlokalisierungsgesetzgebung nachzukommen. Im Gegensatz zu Blockaden von IP-Adressen, die über die Verbotsliste von Roskomnadsor öffentlich nachvollziehbar sind, funktioniert die DPI-Technik intransparenter und macht deswegen eine öffentliche Kontrolle deutlich schwieriger.

## Ausblick

Die Verschlechterung der amerikanisch-russischen Beziehungen nach der Wahl von Donald Trump wirkte sich auch auf die Digitalpolitik aus und gab Hardlinern gute Argumente, um den Gesetzesentwurf in die Duma einzubringen. Obwohl das Bedrohungsszenario (die Isolierung

Russland vom globalen Internet durch die USA) als sehr unwahrscheinlich gilt, avanciert das Gesetz zu einer tragenden Säule der Netzpolitik des Kremls. Russland wird es dennoch kurz- und mittelfristig nicht gelingen, einen Firewall nach chinesischen Vorbild zu errichten. Der große Widerstand gegen das Gesetz innerhalb der Regierung und der Wirtschaft wird die Umsetzung in die Länge ziehen. Gleichzeitig fehlt es derzeit an nötigen Ressourcen, Produktions- und Humankapital und technischem Knowhow, um zentralisiertes Routing und Blockieren zuverlässig zu gewährleisten sowie Geräte mit den benötigten DPI-Kapazitäten zu produzieren, zu lizensieren und einzusetzen. Abzuwarten bleibt, inwieweit Russland bereit ist, sich in Abhängigkeit von chinesischen Anbietern zu begeben. Allerdings zeigt die Genese des Gesetzes, dass eine anfänglich vage strategische Vision nach Jahren in die Tat umgesetzt wird und längerfristig Pfadabhängigkeiten schafft. Mittelfristig ist zu erwarten, dass das Gesetz vor allem innenpolitische Wirkung entfalten wird, etwa durch die Einschränkung von Meinungsfreiheit im Internet, durch Internet-Shutdowns als Reaktion auf Massenproteste oder durch die Verlangsamung von technischem Fortschritt bei der Nutzung von 5G-Technologien. Blockadeversuche von internationalen, in Russland agierenden Unternehmen, könnten zu außenpolitisch Verwerfungen führen. Insgesamt gilt, dass eine robustere und autonome russische Internetinfrastruktur dazu führen wird, dass russische Cyberangriffe auf Gegner risikoärmer werden, da sich Russland vor Eingriffen von außen besser gewappnet glaubt.