Schleichende Nationalisierung Der Kreml hat die gesetzlichen Grundlagen für ein rein russisches Internet geschaffen. Es geht darum, die Kontrolle zu erlangen.

Von Philipp Dietrich und Alena Epifanova

Russland hat mit einem Gesetz über das sogenannte „souveräne Internet“ weltweit für Schlagzeilen gesorgt. Die im November 2019 abgesegneten neuen Regulierungen dürften weitreichende Folgen für das russische, aber auch das globale Internet haben. Ziel der russischen Regierung ist es, das bislang noch weitgehend freie Internet unter staatliche Kontrolle zu bringen. Russland zeichnet damit quasi seine Staatsgrenze in die digitale Sphäre ein und schafft einen eigenen Rechtsraum für das nationale Segment im Cyberspace. Das Land entkoppelt sich vom global vernetzten Internet.

Die aufgeregten Reaktionen aus dem Ausland auf die Gesetzesänderung sind nicht verwunderlich, denn bislang gibt es keinen Präzedenzfall, bei dem ein vollständig ins Internet integrierter Staat ein nationales Parallelsystem aufbaut, das völlig unabhängig vom internationalen Netz operieren können soll. In einem solchen „souveränen Internet“ wäre der Staat die zentrale Instanz, die die vollständige Kontrolle über den Informationsfluss ausübt. Anders als China, wo die staatliche Kontrolle seit den ersten Tagen des Internets errichtet wurde, ist der russische Staat aktuell zu dieser Herkulesaufgabe nicht imstande. Eine russische „Great Firewall“, die das russische Netz vom globalen Internet abschirmt, ist noch außer Reichweite. Allerdings versucht die Regierung, „digitale Souveränität“ auf drei Ebenen gleichzeitig zu erreichen: Kontrolle der Infrastruktur, zentralisierte Verwaltung sowie Priorisierung inländischer Software und Internetdienste.

Entkopplung wird nicht einfach

Der Blick zurück zeigt, dass das russische Internet seit Beginn der 1990er Jahre Stück für Stück in das globale Internet eingebunden wurde. Über die Jahre hat sich so ein komplexes Gewebe an Netzinfrastruktur über das gesamte Land gelegt, mit unzähligen Knotenpunkten und Verbindungen zum Ausland. Russland ist ein fester Bestandteil des globalen Internets geworden. Und auch im Land ist das Internet angekommen: Schätzungen gehen davon aus, dass bereits fast 80 Prozent der Bevölkerung Zugang zum Netz

Philipp Dietrich studiert Politikwissenschaften, Geschichte, Wirtschaft, Recht und Soziologie am Sciences Po Paris und an der Higher School of Economics in Moskau (HSE).

haben. Die infrastrukturelle Verflechtung Russlands mit dem globalen Internet erschwert dabei eine zentralisierte Kontrolle und macht eine vollständige Abschaltung – wie beispielsweise im Iran – nahezu unmöglich.

Iran ist nur über wenige Knotenpunkte ans Ausland angebunden. Falls auch nur eine dieser Verbindungsstellen ausfällt oder gekappt wird, droht die gesamte Internetverbindung des Landes zusammenzubrechen. Daher nennt man diese Knotenpunkte auch „choke points" („Engpässe").

Das Internet in Russland ist auch stark von internationalen Internetunternehmen und ihren Diensten abhängig – zum Beispiel von sozialen Netzwerken, Suchmaschinen, Finanzdienstleistungen und Software as a Service (SaaS). Die US-Unternehmen Google und Facebook gehören auch in Russland zu den meistgenutzten Internetdiensten. Da ihre Nutzerdaten aber nicht in Russland gespeichert werden, hatte der KGB-Nachfolger FSB auf die Daten bis zur jüngsten Gesetzesänderung nur sehr begrenzten Zugriff.

Überwachung des Datenverkehrs

Dies soll sich nun grundlegend ändern: Die Gesetzesänderungen, die im November 2019 in Kraft getreten sind, sollen den russischen Behörden zentralisierte Befugnisse über das Internet geben. Roskomnadsor, der föderale Dienst für die Aufsicht im Bereich der Kommunikation, Informationstechnologie und Massenkommunikation, soll den Datenverkehr auf der Infrastrukturebene überwachen, steuern und gegebenenfalls abschalten. Die einzige Möglichkeit jedoch, staatliche Kontrolle tatsächlich durchzusetzen, besteht darin, die Abhängigkeit von ausländischen Servern und Diensten nach und nach abzubauen – und ein technisch souveränes nationales Internet aufzubauen.

Dies wird mit den drei Kernmaßnahmen der Gesetzesänderung verfolgt:

1. Internetanbieter werden verpflichtet, staatlich vorgegebene Geräte „zur Gefahrenabwehr" in ihren zentralen Knotenpunkten zu installieren. Es steht zu befürchten, dass mit diesen obligatorischen Bauteilen Deep Packet Inspection (DPI) gemeint ist, eine Technologie, die massenhaft Nutzerdaten auslesen, bestimmte Nutzeranfragen verlangsamen oder gar blockieren kann.
2. Eine Zentralverwaltung aller Telekommunikationsnetze wird eingerichtet, die im „Gefahrenfall" die komplette Kontrolle über den russischen Internetverkehr übernehmen kann.
3. Ein nationales russisches Domain-Namen-System (DNS) soll ab 2021 eingeführt werden, das vollständig auf einer eigenen Infrastruktur basiert, d.h. aus eigenen Root-Servern und Domainnamen. Die Agentur Roskomnadsor wird die Regeln für die Nutzung des nationalen DNS festlegen.

Die Gesetzesänderungen sind vage formuliert und müssten durch weitere Regierungsverordnungen ausgeführt werden, um tatsächlich angewendet werden zu können. Im Ergebnis könnte dies zu starker staatlicher Überwachung und Zensur in Russland führen. Der Austausch von regierungskritischen Informationen innerhalb der Zivilgesellschaft könnte viel leichter eingedämmt werden. Aus Sicht der russischen Regierung leuchtet dies ein,

Massenproteste sollen sich bei den Parlaments- und Präsidentschaftswahlen 2021 und 2024 nicht wiederholen

Alena Epifanova ist Programmmitarbeiterin im Robert Bosch-Zentrum für Mittel- und Osteuropa, Russland und Zentralasien bei der DGAP.

denn gesellschaftlicher Druck baut sich vor allem im Internet auf: Regierungskritische Aktivisten und Videoblogger wie Alexei Nawalny oder Juri Dud erreichen mit ihren Videos und Social-Media-Posts ein Millionenpublikum, berichten über Korruption, Vetternwirtschaft und Machtmissbrauch und untergraben laufend die Legitimität des Regimes.

Spätestens im Zuge der Massendemonstrationen nach den Wahlfälschungen 2011 wurde dieses Mobilisierungspotenzial deutlich. Damals rief die Opposition über das Internet zu Demonstrationen auf, denen sich Tausende Menschen anschlossen. Solche Proteste sollten sich aus Kreml-Sicht nach den kommenden Parlaments- und Präsidentschaftswahlen 2021 beziehungsweise 2024 nicht wiederholen. Die geplante Zentralisierung des Internets soll für solche Fälle die Möglichkeit schaffen, das Internet schnell und effektiv einzuschränken oder abzuschalten.

Zudem ermöglichen die DPI-Systeme die Priorisierung des „traffic", das heißt die Bevorzugung oder Behinderung bestimmter Datenströme. So könnte der Abruf mancher Webseiten so verlangsamt werden, dass Nutzer zu anderen Angeboten wechseln – beispielsweise nicht länger Facebook verwenden, sondern die russische Plattform Vkontakte (VK).

So werden potenziell auch Unternehmen benachteiligt – und könnten dadurch unter staatlichen Druck und indirekte Kontrolle kommen. Regierungsnahe Unternehmen würden wiederum von der Priorisierung profitieren, weil ihre Daten schneller übermittelt werden. Da die technischen Eigenschaften der Geräte zur „Gefahrenabwehr", die installiert werden müssen, nicht definiert werden, und die Installation und Anwendung völlig intransparent sind, dürften auch hier die Gefahren des staatlichen Machtmissbrauchs und der Überwachung sehr groß sein. Somit macht sich Russland zu einem unberechenbaren Partner für ausländische Unternehmen, die im Land geschäftlich aktiv sind oder dort investiert haben.

Bild nur in Printausgabe verfügbar

Big Brother is watching you: Die geschlossene Infrastruktur eines eigenständigen Datennetzes, perfekt kontrollierbar, ist der Traum vieler Autokraten.

Mit den Kontrollmechanismen an der Grenze und der Einführung eines DNS versucht die Regierung, das Internet in Russland immer weiter zu isolieren. Sobald alle Schaltstellen der Internetinfrastruktur

zwischen Russland und dem Ausland unter Kontrolle der Behörden sind, können leicht „choke points“ kreiert und Russland perspektivisch komplett vom globalen Internet abgekoppelt werden.

Der Aufbau einer eigenen russischen DNS und die Trennung russischer Webseiten vom internationalen DNS würden wahrscheinlich dazu führen, dass sie im Rest der Welt nicht mehr verfügbar wären und russische Nutzer nicht mehr Zugriff auf nichtrussische Webseiten hätten. Das Internet würde zum „Splinternet“ zersplittern, und nicht nur der technische Zusammenhalt zwischen Russland und dem Rest der Welt stünde auf dem Spiel.

„Made in Russia“ wird bevorzugt

Doch unter dem souveränen Internet versteht der russische Staat nicht nur die Kontrolle der Internetinfrastruktur und die zentrale Verwaltung des Internets. Langfristig sollen ausländische Dienste durch russische Programme ersetzt werden. Gemäß einer Regierungsrichtlinie soll bis 2021 der Anteil der inländischen Software in Behörden und Kommunalverwaltungen sowie in staatlichen Unternehmen mehr als 50 Prozent betragen. Derzeit verwenden Staatsunternehmen gerade einmal zu 10 Prozent Software aus Russland.

Im Dezember 2019 wurde ein weiteres Gesetz verabschiedet, das die obligatorische Vorinstallation von inländischer Software auf Smartphones, Tablets, Computer und Smart TVs aller Gerätehersteller vorschreibt. Bei der Auswahl der Software ist für den Gerätehersteller entscheidend, dass sie einen russischen Rechteinhaber hat und in Russland vertrieben wird. Welche Softwaretypen laut Gesetz bereits ab dem 1. Juli 2020 vorinstalliert werden müssen, ist noch offen. Höchstwahrscheinlich geht es dabei um Internet-Suchmaschinen, Antivirus-Programme, Kartenprogramme und Messenger-Dienste, soziale Netzwerke und Zahlungssysteme. Dadurch könnten vielfältige Nutzerdaten leichter überwacht werden. Und es dürfte dazu führen, dass die Qualität der russischen Software abfällt, da sie nicht mehr im Wettbewerb mit internationalen Anbietern steht.

In seiner Rede zur Lage der Nation im Januar 2020 forderte Präsident Wladimir Putin, dass bei allen „sozial relevanten inländischen Internetdiensten“ für die Nutzer kein Datenverbrauch mehr berechnet werden sollte. Eine Liste solcher Dienste und das Verfahren soll die Regierung zusammen mit der Präsidialadministration bestimmen.

Auch wenn wiederum völlig offen ist, um welche Dienste es konkret geht, ist die Strategie dahinter eindeutig: Russische Nutzer sollen vor allem russische, besser überwachbare Internetdienste nutzen. Da internationale Unternehmen wie Google, Facebook und Co. nicht verboten werden können, würden sie schlicht so erheblich benachteiligt, dass Nutzer sie verlassen und sich stattdessen – scheinbar freiwillig – in ein Netz begeben, in dem der Staat größtmögliche soziale Kontrolle ausüben kann.

Auf allen Ebenen ist damit eine schleichende Nationalisierung des Internets in Richtung eines vollkommen souveränen russischen Netzes zu beobachten. Ob Russland dieses ambitionierte Ziel erreicht, bleibt noch offen, da die technische Umsetzung äußerst schwierig ist. Die Entwicklung kann jedoch einen Präzedenzfall für andere nichtdemokratische Länder schaffen, die mehr Kontrolle über die Informationen ihrer Gesellschaften anstreben – und letztlich über die Gesellschaften selbst.

Wie schon in China weitet sich also der „digitale Autoritarismus“ in Russland aus – mit Folgen, die den Europäern nicht gleichgültig sein können. IP