BYE BYE GLOBALES INTERNET?

Internet Governance zwischen nationalen Interessen und geteilter Verantwortung

„One World. One Net. One Vision." Unter diesem Titel tagte das Internet Governance Forum (IGF) der Vereinten Nationen (UN) vom 25. bis 29. November 2019 in Berlin. Das IGF wurde 2005 für den Austausch über die politischen Aspekte des Internets eingerichtet und bietet unter anderem Diskussionsforen zu Cyber-Sicherheit, Daten und neuen technologischen Entwicklungen. Nebenbei erlaubt es eine moderne Perspektive auf Möglichkeiten, Notwendigkeiten und Grenzen internationaler Kooperation im 21. Jahrhundert.

Der multistakeholder-Ansatz ist in die DNA des IGF eingeschrieben. Staaten, Wirtschaft, Wissenschaft und Zivilgesellschaft sind gleichberechtigte Teilnehmer dieses UN-Forums. Da laut Mandat keine konkreten politischen Entscheidungen vorgesehen sind, steht vor allem der Austausch zwischen ExpertInnen aus dem digital-technischen Bereich im Vordergrund.

Jenseits dieser hochspeziellen aber nicht minder interessanten Fachdebatten,[1] erfüllt das IGF eine interessante Funktion. Es fungiert beispielhaft als Bühne für die Diskussion zweier zentraler Fragen: Inwiefern ist internationale Zusammenarbeit derzeit überhaupt möglich? Und wer trägt die Verantwortung für sozioökonomische und technologische Entwicklungen?

Zerstückelung des Internets?

Gleich zu Beginn des IGF ging Bundeskanzlerin Angela Merkel überraschend klar auf eine Entwicklung ein, bei der jenseits des ursprünglich mehr oder weniger global zugänglichen Netzes nationale Internets entstehen. Sie erklärte, „dass manchem auf der Welt ein Internet der Freiheit und der Offenheit sowie die vielen dezentralen Strukturen des Internets ein Dorn im Auge sind" und dass „nichtdemokratische Staaten und ihre Staatsführungen" in die Freiheiten eingriffen, die das Internet schaffe. „Sie versuchen eigene oder nationale Interessen durchzusetzen und hierfür ihre Netze vom globalen Internet abzuschotten." Diese Aussagen haben besondere Relevanz, wenn man sich vergegenwärtig, wen es implizit adressiert: China.

China ist Vorreiter im nationalen Internetausbau

China ist das Land, in dem der Ausbau eines nationalen Internets am weitesten fortgeschritten ist. Nicht nur hat die chinesische Regierung in den letzten 15 Jahren massiv in den Ausbau der „Great Firewall" investiert, sowohl technisch durch Zensursoftware wie auch mit extrem restriktiver Gesetzgebung. Die einstige Nutzung des Internets als Werkzeug der Bevölkerung zur Kritik am Staat oder an Behörden und zum Austausch über Missstände ist faktisch zum Erliegen gekommen. Chinas Regierung und Wirtschaft haben hierfür perfekte Bedingungen geschaffen. Der Großteil der im Land verkauften Hard- und Software stammt mittlerweile aus chinesischer Produktion oder wird speziell für den chinesischen Markt produziert. Die großen, globalen Internetplattformen wie Google, Twitter und Facebook sind innerhalb Chinas nicht zugänglich. Die Nutzung von VPNs, die den Ort des Einloggens verschleiern und Zugang zu nicht-chinesischen Seiten ermöglichten, ist eingeschränkt und teilweise verboten.

Begründet werden diese Maßnahmen, die Menschenrechte in China massiv einschränken, mit dem Schutz der Bevölkerung vor Bedrohungen und dem Recht des Staates auf Nichteinmischung in innere Angelegenheiten. Auch Russland versucht sich an Internetzensur bspw. durch das „Internetsouveränitätsgesetz". Offiziell soll es Russlands Internet im Falle einer Trennung vom globalen Internet oder vor Cyber-Attacken schützen. Faktisch wird so aber jeglicher Internetverkehr in und aus Russland durch eine staatlich kontrollierte Netzinfrastruktur laufen, die unter anderem Massenüberwachung ermöglicht.

Datenlokalisierung versus freier Datenfluss

Ein Werkzeug staatlicher Kontrolle nationaler Netze ist die lokale Speicherung von Daten. Viele netzpoli-

© UN Photo/Tobias Hofsaess

UN-Generalsekretär Antonio Guterres eröffnete im November 2019 das Internet Governance Forum in Berlin.

tische AktivistInnen lehnen Datenlokalisierung innerhalb nationaler Grenzen ab, mit dem Verweis auf potentiellen staatlichen Missbrauch. Das ist häufig richtig und wichtig, zeigt sich doch weltweit eine deutliche Zunahme von Datenlokalisierungsgesetzgebungen in den letzten 30 Jahren.

Ganz unkritisch ist ein freier, unbeschränkter Datenfluss allerdings auch nicht. Er hat insbesondere in der kommerziellen Nutzung auch zum Verlust der Kontrolle über die Daten durch die Datenbereitstellenden (wir) geführt. Zudem sind Daten derzeit vor allem auf Servern in den USA und Europa (und China) gespeichert, aber kaum im Globalen Süden. Das ist insbesondere hinsichtlich Datenschutzregulierungen und steuerlicher Abgaben digitaler Konzerne relevant.

Auch die EU ist nicht frei von in diesem Fall regionaler Bestrebungen im digitalen Raum. Die Datenschutzgrundverordnung hat sicherlich Fortschritte hin zu mehr Verbraucherschutz in der EU gebracht. Langfristig geht es der EU aber um ein Bestehen im internationalen Wettbewerb. Sie strebt an, einen Daten-Binnenmarkt zu schaffen mit freiem Verkehr nichtpersonenbezogener Daten. VerbraucherschützerInnen sollten genau hinschauen, inwiefern Menschenrechte berücksichtigt werden und welchen weiteren Entwicklungen Vorschub geleistet wird. Denn Datenlokalisierung ist bspw. ein kritisches Thema in EU-Handelsabkommen. Es steht zu befürchten, dass durch ein Verbot von Datenlokalisierung und die Vereinbarung eines freien Datenflusses zwischen den Vertragsparteien europäische Datenschutzstandards unterminiert werden könnten. Zivilgesellschaftliche Organisationen weltweit fordern unter anderem deswegen, dass Datenströme und Datenlokalisierung nicht in EU-Handelsabkommen geregelt werden dürfen.

Internationaler Beschluss zum Zugang zum globalen Internet nötig

Zurück zum IGF. Dass die chinesische Regierung beim IGF prominente Rederollen hat und neuste Zensurgesetze vorstellen kann, ist ernüchternd und zeigt die Schwäche internationaler (UN-)Diskurse, Autokratien angemessen zu konfrontieren. Vor allem dann, wenn es wirtschaftliche Interessen und Wettbewerbsängste gibt.

Umso interessanter die Rede von Angela Merkel – umso interessanter der Slogan des IGF „One World. One Net. One Vision.". Für Milliarden Menschen gibt es dieses eine Internet nicht mehr. Was es bräuchte, wäre gerade hinsichtlich der gravierenden Einschränkung von Menschenrechten eine internationale Ächtung der Bildung dieser nationalen Internets und Unterstützung für freien Internetzugang für alle Menschen. Das ist eine Aufgabe für die Staatengemeinschaft, genauso wie der mächtigen, global agierenden IT-Unternehmen und Plattformen.

Geteilte Verantwortung von wem?

Womit wir bei der zweiten Frage wären, wer eigentlich die Verantwortung trägt für Entwicklungen im digitalen Raum? Ist es der Staat, den es betrifft? Die internationale Staatengemeinschaft? Der Hersteller oder die Plattform? Die NutzerInnen? Oder die Technik selber?

Die Notwendigkeit, hierüber international zu sprechen, zeigt sich besonders drastisch in der Frage der IT-Sicherheit. Mit zunehmender Ausweitung des Internets auf unserer Lebens- und Arbeitsbereiche sowie der Verbreitung billiger Technologien auf globalen Märkten wachsen die globalen Sicherheitsrisiken. Massive Hackerangriffe sind bereits aufgetreten, wie der Hackerangriff auf die Internetinfrastruktur im Osten der USA, der im Oktober 2016 mehrere Stunden lang den Internetzugang fast der gesamten Ostküste lahmlegte.

Es ist zu erwarten, dass diese Art von Cyber-Angriffen zunehmen werden, mit dem Einzug von immer mehr digitalen Technologien in unseren Alltag. Bereits jetzt gibt es weltweit schätzungsweise über sieben Milliarden mit dem Internet verbundene Geräte, bis 2025 werden es wohl mindestens 21 Milliarden sein. Darunter fallen im Internet der Dinge Smartphones, digitale Haushaltsgeräte, Geräte in Fabriken und öffentlicher Infrastruktur. Wir leben in eng vernetzten, digitalen Welten, die von lauter Laien genutzt werden. Viele der Geräte weisen Sicherheitslücken auf, auch weil es bisher keine entsprechenden verbindlichen Standards gibt. Schnell und billig zu produzieren ist weltweites Geschäftsmodell. Darin ist kein Platz für Sicherheitschecks. Regulierer alleine sind hier häufig überfordert, schon im Verständnis dessen, was eigentlich zu regeln wäre.

Ohne dem IGF und seinem durchaus kontrovers diskutierten Multistakeholder-Ansatz zu viel Bedeutung geben zu wollen, kann es wie ein durch die Lupe betrachtetes Experiment für modernen Multilateralismus gesehen werden. Dass internationale Kooperation bei Internetbelangen notwendig ist, liegt in der Natur der Sache. Bestrebungen, das durch nationale Ansätze aufzukündigen, werden kritisiert. Grundsätzlich scheint Konsens darüber zu bestehen, dass HerstellerInnen, RegulierernInnen und Zivilgesellschaft gemeinsame Strategien bspw. hinsichtlich der Sicherheit von Technik erarbeiten müssen. Gesetzliche Regelungen werden schon aus rein marktwirtschaftlichen Überlegungen (wer versichert z. B. ein unsicheres Gerät) auch von HerstellerInnenseite nicht grundsätzlich abgelehnt. Die Schwäche des IGF ist seine Unverbindlichkeit. Vielleicht ist aber ein offener, internationaler Austausch alles, was wir uns derzeit überhaupt erhoffen können.

Marie-Luise Abshagen

Die Autorin ist Referentin für nachhaltige Entwicklung beim Forum Umwelt & Entwicklung.

1 Ein Blick in die umfassenden Video-Aufzeichnungen des IGFs lohnt sich: https://www.youtube.com/user/igf/playlists.

4/2019

RUNDBRIEF

Forum Umwelt & Entwicklung

Die Geister, die wir riefen

Chemikalien belasten zunehmend Mensch und Umwelt – Zeit zu handeln!

ISSN 1864-0982