SWP-Aktuell
NR. 62 OKTOBER 2021

Indien als ambivalenter Partner in der Digitalpolitik

Potential und Grenzen der Kooperation bei Digitalwirtschaft und Internet-Governance

Daniel Voelsen/Christian Wagner

Die Zusammenarbeit in der Digitalpolitik gilt als eines der aussichtsreichsten Felder der strategischen Partnerschaft zwischen Indien und der Europäischen Union (EU). In der Umsetzung zeigen sich jedoch tiefgreifende Differenzen, etwa im Hinblick auf Datenschutz, Kompetenzen der Sicherheitsbehörden und die künftige globale digitale Ordnung. Ähnliche Probleme werden in den Verhandlungen der EU mit den USA zu Fragen des digitalen Handels bearbeitet. Mögliche Kompromisse dort könnten auch Bestandteile einer Verständigung mit Indien bilden.

Das Bemühen um eine verstärkte Zusammenarbeit Europas mit Indien wird immer wieder mit dem Verweis auf gemeinsame demokratische Werte begründet. In ihrer Roadmap 2025 bekräftigen Indien und die EU ihr Interesse, einen »offenen, freien, stabilen und sicheren Cyberraum« zu fördern und die Cyberkriminalität zu bekämpfen. Doch der Weg dahin erweist sich als steinig, denn bei der Umsetzung tun sich in einigen Bereichen fundamentale Differenzen auf. Strittig zum Beispiel sind die Handhabung des Datenschutzes und die Gestalt der künftigen digitalen Ordnung.

Datenschutz, wirtschaftliche Zusammenarbeit, Strafverfolgung

Kommen sich Europa und Indien bei Fragen der digitalen Wirtschaft entgegen, birgt dies erhebliches Potential für beide. Zwar hatten 2018 in Indien nur 20 Prozent der Bevölkerung Zugang zum Internet, in der EU dagegen 82 Prozent. Bei diesen 20 Prozent handelte es sich aber um gut 270 Millionen Menschen. Außerdem ist damit zu rechnen, dass Indiens Digitalisierung in den nächsten Jahren weiter voranschreitet.

Für Europa ist es attraktiv, auf diesen Zukunftsmarkt zu gelangen. Der europäische Markt bietet wiederum indischen Unternehmen große Chancen. Für beide Seiten geht es darum, eigene Dienstleistungen und Produkte anbieten zu können sowie neue Möglichkeiten für Investitionen zu schaffen.

Fragen des Datenschutzes sind dabei essentiell, denn Kundendaten zu verarbeiten bildet die Basis für die meisten digitalen Produkte und Dienstleistungen. Diese können überhaupt nur gehandelt werden,

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

wenn geklärt ist, dass die dafür notwendigen grenzüberschreitenden Datentransfers datenschutzrechtlich zulässig sind.

Das gilt besonders auch für Anwendungen im Bereich Künstlicher Intelligenz (KI). Zum Teil kann es sich hierbei um Unternehmensdaten handeln, etwa um Daten aus Produktionsabläufen und Lieferketten. Oft aber kommen personenbezogene Daten hinzu, die in den Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) fallen. Sie sieht unter anderem vor, dass Betroffene eigens und ausdrücklich zustimmen müssen, wenn aus der EU heraus ihre Daten an Entitäten übermittelt werden, die nicht an europäisches Recht gebunden sind. Das kann abschreckend auf Kunden wirken und bedeutet in jedem Fall einen nicht geringen zusätzlichen Aufwand für alle Beteiligten. Um diese Komplikationen zu vermeiden, gibt es einen politischen Mechanismus, welcher es der EU-Kommission ermöglicht, die Angemessenheit (adequacy) der Datenschutzvorgaben anderer Staaten anzuerkennen. Ist dies geschehen, werden Datentransfers in diese Länder rechtlich so behandelt wie jene innerhalb der EU. Damit ist eine gesonderte Zustimmung der Betroffenen zum Datentransfer über die Grenzen der EU hinaus nicht mehr notwendig. Für einige Staaten wurde diese juristische Kompatibilität bereits festgestellt, unter anderem für die Schweiz, Japan und jüngst das Vereinigte Königreich.

Noch offen hingegen ist, ob und wie es gelingt, hier eine Einigung mit den USA zu erlangen. In der Vergangenheit wurden Datentransfers zwischen der EU und den USA nicht über eine Angemessenheitsfeststellung seitens der Kommission geregelt. Stattdessen gab es spezifische vertragliche Normenkollisionsregime, nämlich das Safe-Harbor-Abkommen aus dem Jahr 2000 und den darauf aufbauenden Privacy Shield von 2016.

Wie schon das Vorgängerabkommen wurde der Privacy Shield 2020 vom Europäischen Gerichtshof (EuGH) für unzulässig erklärt. Angesichts der Befugnisse und öffentlich bekannt gewordenen Praktiken der US-Nachrichtendienste, so der EuGH, sei für Bürgerinnen und Bürger der EU in den USA nicht gewährleistet, dass ihre Daten in einer Weise geschützt seien, die in etwa dem Niveau innerhalb der EU entspreche. Seither und verstärkt seit der Präsidentenwahl in den USA 2020 bemühen sich die beiden Seiten um eine neue rechtliche Grundlage für den transatlantischen Datentransfer, doch bisher ohne Ergebnis.

Datenschutz in Indien

Auch im Verhältnis der EU zu Indien stellt sich die Frage, ob das indische Datenschutzrecht hinreichend kompatibel mit den Anforderungen der DSGVO ist. In Indien haben die Expansion des Onlinehandels und die Einführung elektronischer Verwaltungsverfahren wie der Aadhaar-Karte eine Diskussion über den Datenschutz entfacht.

Die Aadhaar-Karte enthält eine zwölfstellige persönliche Identifikationsnummer, die vor allem den ärmeren Bevölkerungsgruppen besseren und einfacheren Zugang zu staatlichen Transferleistungen verschaffen soll. Durch diese direkte Kommunikation soll zugleich die grassierende Korruption bekämpft werden. Mit der Einführung entbrannte eine politische und rechtliche Auseinandersetzung darüber, für welche Zwecke die Karte genutzt werden muss. Auch gibt es Berichte über gefälschte Karten und Identitätsdiebstahl. Bei einem Test gelang es Indiens oberstem Telekom-Regulierer, die Aadhaar-Karte zu fälschen.

In einer Entscheidung über die Nutzung der Aadhaar-Karte stellte das indische Verfassungsgericht 2017 fest, die Verfassung gestehe allen Bürgerinnen und Bürgern ein Recht auf Privatsphäre zu. 2019 legte die Regierung einen Entwurf für ein Datenschutzgesetz (Personal Data Protection Bill) vor, das allerdings bis heute nicht verabschiedet wurde. Damit fehlt eine wesentliche Grundlage für intensivere Kooperation zwischen der EU und Indien in Fragen der Digitalwirtschaft. Ein weiteres, eng hiermit verbundenes Hindernis bilden die unterschiedlichen Befugnisse und Kontrollmechanismen der Sicherheitsbehörden.

Die jüngsten Enthüllungen über die Pegasus-Spionagesoftware haben auch in Indien erneut Forderungen laut werden lassen, die Geheimdienste stärker zu kontrollieren. Nicht nur bei regierungskritischen Journalisten, sondern auch bei Beamten und Militärs war die Software installiert. Im Zuge der Enthüllungen wurde ein weiteres Mal deutlich, dass die Geheimdienste des Landes teils ohne ausreichende gesetzliche Grundlage operieren und keiner parlamentarischen Kontrolle unterliegen. Angesichts der ohnehin zunehmenden autoritären Tendenzen in der indischen Demokratie nährt dieser Skandal die Sorge vor einer ausufernden Überwachung der Bevölkerung mit Hilfe digitaler Technologien. Manche staatlichen Einrichtungen setzen zudem bereits Software zur Gesichtserkennung ein, ohne dass es hierfür eine rechtliche Basis gibt.

Aufgrund der beschriebenen Defizite dürften die Kommission oder der EuGH kaum zu der Einschätzung kommen, dass europäischen Bürgerinnen und Bürgern in Indien ein vergleichbares Datenschutzniveau gewährleistet wird wie in der EU. Ähnlich gelagerte Probleme hat die EU mit den USA. Will sie ihren eigenen Rechtsrahmen ernst nehmen, kann sie keine Rechtsordnung in diesem Punkt als weitgehend gleichwertig anerkennen, in der das europäische Datenschutzniveau stark unterschritten wird. Jenseits der rechtlichen Details ist eine politische Lösung deshalb so schwierig, weil der Stein des Anstoßes die Befugnisse der Nachrichtendienste sind — und die Debatte sich damit unmittelbar um Fragen der nationalen Sicherheit dreht.

Indiens unklare Position in der globalen Internet-Governance

Wesentliche Entscheidungen über die Zukunft der Digitalisierung werden auf globaler Ebene getroffen. In den Strukturen der Vereinten Nationen, aber auch in einigen Multistakeholder-Formaten wird darüber verhandelt, nach welchen Normen die globale digitale Ordnung geregelt werden soll.

Dabei steht einiges auf dem Spiel. Die Strukturen des Internets und viele der bis heute wichtigsten Dienstleistungen wurden in den USA entwickelt. Daher ist die globale digitale Ordnung hauptsächlich von liberalen Prinzipien US-amerikanischer Provenienz geprägt. Hierzu zählen die Verankerung eines weit gefassten Verständnisses von Meinungsfreiheit in den Strukturen des Internets und die starke Rolle privater Akteure in Entwicklung und Betrieb digitaler Infrastrukturen. Ausdruck hiervon ist die klare Präferenz vieler westlicher Staaten (auch Deutschlands) für Multistakeholder-Ansätze in der globalen Internet-Governance.

Das liberale Modell der globalen digitalen Ordnung gerät nun aber zunehmend unter Druck. Zum einen zeigen sich Risse in dem Modell selbst. Technisch etwa ist die globale Internet-Infrastruktur in Teilen veraltet, mit Folgen für die Sicherheit wie auch die Privatsphäre der Nutzer. Zum anderen bemühen sich immer mehr Staaten darum, die Kontrolle über »ihren« Teil des Internets auszubauen. Die prominentesten Beispiele hierfür sind China und Russland, doch folgt mittlerweile eine Reihe von Staaten diesem Ansatz einer autoritären Digitalisierung. Während die meisten dieser Staaten dabei zunächst nach innen blicken, verbindet China damit auch den Anspruch auf Umgestaltung der globalen digitalen Ordnung.

Aus Sicht Deutschlands und Europas wäre es attraktiv, Indien als Demokratie auf der Seite der Verfechter einer liberalen globalen Ordnung zu wissen. Allerdings tritt Indien außenpolitisch seit jeher für nationale Souveränität und Nichteinmischung in innere Angelegenheiten ein. Zudem betonen indische Regierungen ihre außenpolitische Unabhängigkeit und Eigenständigkeit und lehnen es ab, sich politischen Lagern zuzuordnen.

In Indien haben autoritäre Tendenzen seit 2014 zugenommen. Das zeigt sich unter anderem in der Herabstufung des Landes im Freedom House Index 2021. Überdies belegt Indien seit Jahren nur hintere Plätze im Index zur Pressefreiheit und ist zugleich das Land mit den meisten und auch den läng-

sten von der Regierung veranlassten Internet-Shutdowns.

Indiens Haltung zu Fragen der digitalen Ordnung liegt damit meist näher an den Vorstellungen autoritärer Regime, wie auch die Auseinandersetzungen in den Foren der globalen Internet-Governance zeigen. Im Rahmen der Vereinten Nationen wird seit vielen Jahren über Normen für Rechte und Pflichten der Staaten im digitalen Raum diskutiert, am intensivsten in der dazu eingerichteten Group of Governmental Experts (GGE). Als bedenkliches Signal hat dabei zu gelten, dass Indien 2018 erklärte, sich in Fragen der Cybersicherheit und gerade mit Blick auf den GGE-Prozess eng mit Russland abstimmen zu wollen.

Als weiterer Indikator kann das Abstimmungsverhalten in der Generalversammlung der Vereinten Nationen dienen. Auch hier ist das Ergebnis ernüchternd: Bei zwei Resolutionen zum Thema Cybercrime, die 2018 (A/RES/73/187) und 2019 (A/RES/74/247) eingebracht wurden, stimmte Indien mit Russland und damit gegen die von Deutschland und den anderen Mitgliedstaaten der EU vertretene Position. Überraschend ist das aber nicht, folgt indische Außenpolitik doch auch in anderen Fragen vorwiegend den Prinzipien nationale Souveränität und Nichteinmischung in innere Angelegenheiten.

Dies erklärt auch die Zurückhaltung oder bestenfalls Ambivalenz der indischen Regierung gegenüber Multistakeholder-Formaten der globalen Internet-Governance. Zwar engagiert sich Indien in einigen dieser Formate, etwa bei der Internet Corporation for Assigned Names and Numbers (ICANN) oder im Internet Governance Forum (IGF). An anderer Stelle wirbt das Land indes für die Aufwertung der International Telecommunication Union (ITU) als klassisch multilateraler, zwischenstaatlicher Gegenpol zur Multistakeholder-Governance.

Schwierige Kompromisse

Eine digitalpolitische Zusammenarbeit mit Indien würde Europa große Chancen eröffnen: Wirtschaftlich sind Erleichterungen beim Zugang zum indischen Markt attraktiv; politisch wäre es ein großer Fortschritt, Indien als Partner in den Debatten über die Zukunft der globalen Internet-Governance zu gewinnen.

In beiderlei Hinsicht jedoch zeigt sich die damit verknüpfte Ambivalenz: Einerseits gibt es gemeinsame Interessen und Wertvorstellungen sowie den erklärten Wunsch nach verstärkter Zusammenarbeit. Andererseits existieren erhebliche Differenzen. Die noch fehlenden gesetzlichen Grundlagen zum Datenschutz sowie die weitreichenden und dabei ungeklärten Befugnisse der indischen Nachrichtendienste sind mit den europäischen Prinzipien des Datenschutzes kaum vereinbar. Auch hat Indien sich in den Disputen über globale Internet-Governance wiederholt gegen die Bemühungen Europas und seiner Verbündeten um eine liberale Ordnung des Digitalen gestellt.

Eine einfache Lösung ist nicht in Sicht. Notwendig wären tragfähige Kompromisse. Eine Chance dafür läge im noch ausstehenden indischen Datenschutzgesetz. Denkbar wäre beispielsweise, in diesem Gesetz oder damit verbundenen Gesetzesvorhaben die Befugnisse der Nachrichtendienste beim Zugriff auf personenbezogene digitale Daten neu zu regeln. Vor allem wäre zu erwägen, die Möglichkeiten gerichtlicher Prüfung nachrichtendienstlicher Aktivitäten in diesem Bereich zu stärken. Rechtlich wie politisch könnte dies die Grundlage für weitere Gespräche auf dem Weg zu einer datenschutzrechtlichen Angemessenheitsfeststellung der EU-Kommission bilden.

Dieses Thema ist für Indien jedoch mit Fragen nationaler Sicherheit verknüpft. Daher dürften Differenzen fortbestehen. Ähnlich verhält es sich bei der Internet-Governance. Dort ist eine punktuell verstärkte Kooperation vorstellbar, doch wird Indien seine grundsätzliche außenpolitische Orientierung kaum ändern.

Die EU muss also für sich klären, auf welche Kompromisse sie sich einlassen würde und welche Form diese annehmen könnten. Was datenschutzrechtliche Fragen betrifft, könnten dabei die zurzeit intensiv geführten Verhandlungen der EU mit den

USA zu ähnlichen Themen hilfreiche Anregungen bieten. Eine Einigung wird der EU auch hier Zugeständnisse abverlangen. Sie ist nach der Entscheidung des EuGH letztlich aber nur möglich, wenn die USA zu einem gewissen Entgegenkommen bei der Kontrolle über ihre Nachrichtendienste bereit sind.

Sowohl Brüssel als auch Washington haben die Brisanz dieser Fragen erkannt und stehen unter dem Druck von Wirtschaft und Zivilgesellschaft, rasch eine Lösung zu finden. Entsprechend umfangreich sind die Bemühungen der beiden Seiten. Ein erstes Resultat ist die Einrichtung des EU-US Trade and Technology Council (TTC). Ob und wann sich USA und EU in der Sache einigen werden, ist noch nicht abzusehen. In jedem Fall aber scheint es vielversprechend, die dort angestellten Überlegungen und vorgebrachten Lösungsansätze daraufhin zu prüfen, ob sie in angepasster Form auch für die Gespräche mit der indischen Regierung genutzt werden können.

Dr. Daniel Voelsen ist Leiter der Forschungsgruppe Globale Fragen.
Dr. habil. Christian Wagner ist Senior Fellow in der Forschungsgruppe Asien.

© Stiftung Wissenschaft und Politik, 2021
Alle Rechte vorbehalten

Das Aktuell gibt die Auffassung der Autoren wieder.

In der Online-Version dieser Publikation sind Verweise auf SWP-Schriften und wichtige Quellen anklickbar.

SWP-Aktuells werden intern einem Begutachtungsverfahren, einem Faktencheck und einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
doi: 10.18449/2021A62