Die digitale Selbstbehauptung der EU

Bendiek, Annegret; Berlich, Christoph; Metzger, Tobias

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Die digitale Selbstbehauptung der EU

Annegret Bendiek / Christoph Berlich / Tobias Metzger

Institutionen und Mitgliedstaaten der EU treiben derzeit mit Hochdruck die digitale Integration voran. In Anbetracht der vielfältigen Herausforderungen – vom Schutz kritischer Infrastrukturen über die Wahrung persönlicher Freiheitsrechte bis zur Schaffung grenzübergreifender Märkte – ist die »positive Integration«, also regulative Vorgaben durch die EU, der richtige Weg, um gegen Marktversagen im Binnenmarkt und darüber hinaus anzugehen. Auf EU-Ebene sollen Regulierungen geschaffen werden, die inner- und außereuropäische Wirkung entfalten. Vehikel dazu sind die Strategie für einen digitalen Binnenmarkt (DSM), die Datenschutzgrundverordnung (DSGVO) und die Richtlinie zur Gewährleistung einer gemeinsamen Netzwerk- und Informationssicherheit (NIS). Die digitale Integration ist Voraussetzung dafür, europäische Standards und Normen auch in der internationalen Politik effektiver durchzusetzen.

Im grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehr spielen digitale Informationssysteme, allen voran das Internet, eine wesentliche Rolle. Deren rechtliche Regelung auf allen Ebenen der Politik kann jedoch mit der rasanten technischen Entwicklung kaum mithalten. Viele Bereiche gelten als nicht hinreichend reguliert. Dauerhaftes Vertrauen der Bevölkerung in die Zuverlässigkeit der Technologie und Rechtssicherheit im Umgang mit ihr sind aber für die wirtschaftliche Entwicklung unabdingbar. So schätzt die Europäische Kommission für ihre laufende Amtszeit, dass die Schaffung eines vernetzten digitalen Binnenmarktes ein zusätzliches Wachstum von bis zu 250 Mrd. Euro bringen könnte.

Legt man das Konzept der negativen und positiven Integration (Fritz W. Scharpf) zugrunde, so gibt es zwei Handlungsoptionen staatlicher (De-)Regulierung als Antwort auf die Erweiterung des Wirtschaftsraums über nationalstaatliche Grenzen hinaus. Bei der negativen Integration werden Beschränkungen des freien Handels (etwa Zölle) und des Wettbewerbs beseitigt. Dies wirkt marktschaffend. Maßnahmen positiver Integration sollen Marktergebnisse korrigieren und Marktversagen überwinden. Hierfür sind wirtschaftspolitische Koordinierung sowie regulatorische Kompetenzen auf EU-Ebene erforderlich. Analog zur wirtschaftlichen ist daher die digitale Integration als Ausbau einheitlicher gesellschaftlicher Handlungsräume zu verstehen, die gemeinsamen Regeln unterliegen und durch die

Dr. Annegret Bendiek ist Senior Associate, Christoph Berlich und Tobias Metzger sind Projektmitarbeiter in der SWP-Forschungsgruppe EU / Europa

Aufhebung institutioneller Grenzen zwischen den EU-Mitgliedstaaten gekennzeichnet sind. Die Regulierung des Marktes findet grundsätzlich auf verschiedenen Ebenen statt. Globale Standards sollten in internationalen Foren gesetzt werden, der Datenschutz sollte einheitlich auf der EU-Ebene geregelt sein und die Verfolgung digitaler Straftaten gehört auch auf die nationale Ebene (und sollte, wenn nötig, EU-weit koordiniert werden). Die digitale Regulierung ist daher als Mehrebenenstruktur zu verstehen. Die EU ist aufgrund der Existenz des Binnenmarktes nicht nur ein wichtiger Ort der Regulierung, sondern gleichzeitig ein starker wirtschaftlicher Akteur mit globalem Anspruch digitaler Selbstbehauptung. Standards wie MP3, SMS oder Compact Disk, die sich in Europa durchsetzen konnten, haben Anpassungsdruck auf nichteuropäische Marktteilnehmer erzeugt. Wie das Beispiel Airbus gezeigt hat und das Satellitennavigationssystem Galileo eventuell ab 2018 zeigen wird, kann der Gemeinschaftsrahmen es staatlichen und nichtstaatlichen Akteuren ermöglichen, globale Standardsetzung in einem Ausmaß zu beeinflussen, das einzelstaatlichem und privatem Handeln verwehrt bleibt.

Herausforderungen des digitalen Binnenmarktes

Die Herausforderungen bei der Schaffung eines digitalen Binnenmarktes lassen sich anhand des Datenweges einer E-Mail illustrieren. Mit welcher 1) Hard- bzw. Software wird eine E-Mail geschrieben, über welche 2) Routinginfrastrukturen via Internet übertragen, auf welchen 3) Datenservern und bei welchen Cloud-Anbietern gespeichert, dabei mit welchen 4) Techniken verschlüsselt und durch welche 5) datenschutz- und wettbewerbsrechtlichen Vorgaben geschützt? Am Beispiel digitaler Wegmarken lässt sich nicht nur zeigen, dass es Regulierungsbedarf gibt, sondern auch, dass die EU der angemessene Ort für die Regulierung ist:

Erstens ist Europa in der Soft- und Hardware-Branche heute mit wenigen Ausnahmen, wie SAP oder Alcatel-Lucent, kaum noch ein relevanter Akteur. Die europäische Industrie ist derart von US-amerikanischen und chinesischen Komponenten abhängig, dass ein völlig eigenständiger europäischer Markt nicht denkbar ist. Viele Branchen, etwa die der Suchmaschinen, werden derzeit von Quasi-Monopolen beherrscht, sei es von Microsoft, Google, Cisco oder Huawei. Zu den führenden PC-Herstellern zählen Apple, Dell, HP (alle USA), MSI, ASUS, Acer (alle Taiwan), Samsung (Südkorea), Lenovo (China) und Toshiba (Japan). Einige von ihnen sind auch beim Verkauf von Smartphones in der Weltspitze vertreten, flankiert von Huawei (China) und LG (Südkorea). Hardwarekomponenten für Heimnetzwerke stammen hauptsächlich von Cisco (USA) oder Huawei (China). Bei der Server-Hardware für Rechenzentren wiederum liegt HP vor Dell und IBM. Weil der Marktanteil europäischer Anbieter (Siemens, Nokia) geschrumpft ist, besteht de facto ein Duopol aus US-amerikanischen und asiatischen Anbietern (Huawei, ZTE).

Zweitens sollte ein verlässliches europäisches Kommunikationsnetz im öffentlichen Interesse betrieben und verwaltet werden. Einzelinteressen sollten nur dort ihren Platz finden, wo sie dem allgemeinen Interesse nicht zuwiderlaufen. Genau das Gegenteil ist heute in Europa der Fall. Das Netz besteht aus nationalen Teilnetzen mit Kontrolleuren, die jeweils partikulare Interessen verfolgen. In der Theorie setzt sich das Internet aus den Netzen verschiedener Internetdienstanbieter (ISPs) zusammen, welche an neutralen Stellen (sogenannten Internetknotenpunkten) zum Gesamtnetz, dem Netz der Netze, zusammengeschlossen sind. In der Praxis kann von Neutralität keine Rede sein. DE-CIX ist der größte der weltweit 321 Internetknotenpunkte und gehört eco, dem Verband der deutschen Internetwirtschaft. DE-CIX wird in einer Weise betrieben, die dem BND Zugriffsmöglichkeiten erlaubt, wobei vor allem Daten nichtdeutscher Akteure betroffen sind. Ob hier das europäische Interesse gewahrt bleibt, kann bezweifelt werden.

Drittens stellen sich im Hinblick auf Cloud Computing sowie verteilte Bearbeitung und Speicherung von Daten vielfältige neue Anforderungen. Für die positive Regulierung des europäischen Konsumenten- und Datenschutzes entsteht hier das Problem, dass rechtliche und ökonomische Räume nicht identisch sind. Wo Daten und Zugriffe darauf an Orten jenseits der Reichweite europäischen Rechts liegen, greifen europäische Gesetze ins Leere. Daten, die auf Cloud-Plattformen abgelegt werden, können gestohlen werden. Die Gefahr eines solchen Diebstahls im großen Stil lauert vor allem bei außereuropäischen Servern. Geschäftsbedingungen, die dritten Akteuren Zugriffsrechte einräumen, können ebenfalls unabsehbare Folgen haben. Demnach müssen nicht nur amerikanische Anbieter auf Anfrage Kundendaten herausgeben, die auf europäischen Servern gespeichert sind (siehe den Streitfall irische Microsoft-Tochtergesellschaft versus US-Regierung). Auch europäische Firmen, die in den USA tätig sind, unterliegen dieser Verpflichtung.

Viertens hat die Digitalisierung der Kommunikation das Recht auf Privatheit ausgehöhlt. Die Snowden-Veröffentlichungen haben gezeigt, dass staatliche Sicherheitsbehörden jederzeit in der Lage sind, unverschlüsselte Mails auszuwerten. Die Güter Privatheit und Freiheit sind Grundvoraussetzungen für den Markt selbst. Deshalb liegt es in seinem Interesse, sie zu schützen. Für liberale Gesellschaften ist das Recht auf Privatheit zudem konstitutiv, denn ohne Privatheit kann es auch keine Freiheit geben. Es bedarf einer europäischen Antwort auf die Gefährdung privater Daten und damit der gesellschaftlichen Freiheit. Da sich die Telekommunikationsinfrastruktur in privatwirtschaftlichem Besitz befindet und Netze Ländergrenzen überschreiten, liegt derzeit der Schwerpunkt auf besseren Verschlüsselungsverfahren. Doch die Verschlüsselungstechnologie darf keine versteckten Zugriffsmöglichkeiten bereithalten, die zuletzt nicht nur von der chinesischen, sondern auch von der US-amerikanischen und der britischen Regierung für Ermittlungszwecke gefordert wurden. Und auch aus verschlüsselten E-Mails lassen sich viele Informationen gewinnen. Die Metadaten, quasi der Briefumschlag einer E-Mail, verraten, wer mit wem wann und wie häufig in Kontakt steht, ja sogar den Betreff der Nachricht.

Fünftens sind Quasi-Monopolstellungen großer Unternehmen grundsätzlich problematisch. Kartellbildungen oder andere Formen der Marktbeherrschung führen zu höheren Preisen, schlechteren Produkten und anderen gravierenden Abweichungen vom Ideal des freien Marktes. Es gibt zwar Fusionskontrollen, doch das europäische Wettbewerbsrecht reagiert erst dann mit Sanktionen, wenn Marktbeherrschung auch tatsächlich Missbrauch nach sich zieht. Trotzdem wird die Frage einer marktbeherrschenden Stellung des US-Unternehmens Google im Binnenmarkt ausgiebig diskutiert. Der damalige Wettbewerbskommissar Joaquín Almunia hatte schon im November 2010 ein Verfahren gegen Google eingeleitet. Seine Nachfolgerin Margrethe Vestager hat es nun wiederbelebt, weil vieles darauf hinweise, dass Google in seinen Suchergebnissen systematisch eigene Dienste gegenüber denen der Konkurrenz bevorzugt. Zudem geht die Wettbewerbskommissarin gegen mehrere Staaten vor, weil diese möglicherweise Konzernen wie Amazon oder Apple Vorteile durch Steuervorentscheide (tax rulings) verschaffen. Diese sind zumindest dann wettbewerbswidrig, wenn einzelne Unternehmen auf Kosten ihrer Konkurrenten begünstigt werden.

Die Vertiefung der digitalen Integration

Regulatorische Herausforderungen wie jene, die anhand digitaler Wegmarken veranschaulicht wurden, haben in der europäischen Geschichte oft zu anspruchsvollen Integrationssprüngen beigetragen. Schlagendes Beispiel dafür ist die Schaffung des Binnenmarktes durch die Einheitliche Euro-

päische Akte im Jahr 1987. Um die digitale Integration zu vertiefen, treiben daher Andrus Ansip, seit Amtsantritt der neuen Europäischen Kommission im November 2014 deren zuständiger Vizepräsident, und Günther Oettinger, Kommissar für Digitale Wirtschaft und Gesellschaft, den Aufbau des digitalen Binnenmarktes voran. Ziel ist es, die Vorzüge des europäischen Binnenmarktes auf den digitalen Raum auszuweiten. Von den technischen Neuerungen rund um Big Data, Cloud Computing und Internet der Dinge könne man nur dann profitieren, wenn Ideen digitaler Souveränität zugunsten einer europäischen Harmonisierung nationaler Märkte überwunden würden. Als Impulsgeber für die Schaffung des digitalen Binnenmarktes kann das Grundsatzurteil des Europäischen Gerichtshofs (EuGH) vom April 2014 zur Vorratsdatenspeicherung gelten, verlangt es doch ein Mehr an Datenschutz und -sicherheit auf Grundlage europäischen Rechts. Aus der Jurisdiktion ergeben sich rechtliche Grenzen für die Speicherung von Daten der Unionsbürger in Drittstatten und wirtschaftliche Anreize für den Aufbau einer europäischen Netzinfrastruktur.

Die Strategie für einen digitalen Binnenmarkt

Die Anfang Juni 2015 von der Europäischen Kommission vorgestellte Strategie für einen digitalen Binnenmarkt umfasst 16 Maßnahmen, die bis Ende 2016 umgesetzt werden sollen. Sie beruht auf drei Säulen: 1) besserer Zugang für Verbraucher und Unternehmen zu digitalen Waren und Dienstleistungen in ganz Europa, 2) Schaffung von Infrastrukturen für digitale Netze und Dienste und 3) Ausschöpfung von Wachstumspotentiale, die in der digitalen Wirtschaft liegen.

Mit Hilfe marktschaffender Maßnahmen, die in der ersten Säule festgelegt wurden, sollen Unternehmen gegenüber dem nationalen Handel im digitalen Binnenmarkt künftig keinen oder nur kleinstmöglichen Hemmnissen unterliegen (negative Integration). Hierzu sollen das Vertragsrecht und die Mehrwertsteuer-Regelungen harmonisiert und grenzübergreifende Lieferdienste für Datenpakete verbessert werden. Auch hat die Strategie zum Ziel, Zugriffseinschränkungen (Geo-Blocking) zu entfernen, etwa indem das Urheberrecht vereinheitlicht wird. Die Kommission will Schranken beim E-Commerce abbauen, Steuerregeln harmonisieren und die Marktmacht von Online-Plattformen wie Suchmaschinen oder sozialen Netzwerken sowie den Rechtsrahmen für audiovisuelle Medien überprüfen.

Im Kontext der zweiten Säule setzt die Kommission auf neue Regelungen (positive Integration). Mit der geplanten NIS-Richtlinie sollen Betreiber kritischer Infrastrukturen in die Haftung genommen werden. Neben besserer IT-Sicherheit ist vorgesehen, dass Anbieter von Diensten wie Handelsplattformen, Zahlungssystemen, sozialen Netzwerken, Suchmaschinen und Daten-Clouds schwerwiegende Cyberangriffe künftig melden müssen. Fortan müssten sie angemessene Schutzmaßnahmen gemäß den geplanten EU-Vorgaben ergreifen. Auch die Endanwender als schwächstes Glied in der Kette sollen in die Lage versetzt werden, Störungen zu erkennen und zu beseitigen. Zu diesem Zweck sollen Provider einer Meldepflicht für den Fall von Sicherheitsverletzungen und Integritätsverlust (Informationsverfälschung) unterworfen werden. Technische Normen sollen harmonisiert, vertrauenswürdige Cloud-Anbieter zertifiziert werden. Des Weiteren will die Kommission Haftungsfreistellungen für von der E-Commerce-Richtlinie betroffene Provider prüfen und Verfahren vereinheitlichen, mit denen rechtswidrige Inhalte, etwa terroristische Propaganda, Kinderpornographie oder Urheberrechtsverstöße, im Netz gelöscht werden. Daneben wird derzeit im Europäischen Parlament (EP) eine umfassende Urheberrechtsreform diskutiert.

In der dritten Säule geht es sowohl um den Ausbau der europäischen digitalen Wirtschaft als auch die Nutzung von Digitaltechnik in der herkömmlichen Industrie. Mittelständische Unternehmen und Start-ups sollen gefördert werden,

indem sie vereinfachten Zugang zu Investitionskapital erhalten. Ferner sollen rechtliche Vorgaben für Portabilität, Interoperabilität und Standardisierung beim Cloud Computing und bei Big Data umgesetzt werden. Das Hauptaugenmerk der EU-Regulierung gilt dem Schutz vertraulicher Daten, die aufgrund mangelnder Sicherheitsvorkehrungen oder nachteiliger rechtlicher Rahmenbedingungen in die Hände Dritter gelangen können. Restriktive Gesetze zum Datenstandort oder zu Verschlüsselungsverfahren sollen hierzu vereinheitlicht werden, damit alle europäischen Marktteilnehmer in jeder Hinsicht gleich behandelt werden. Denn die Verteilung von Datenpaketen (Routing), zum Beispiel die Kommunikation zwischen Estland und Italien, kann durchaus über US-Server erfolgen.

Die mutmaßlichen Folgen einer solchen Datenverbindung für den Datenschutz rufen daher immer mehr Verfechter eines auf den Schengen-Raum begrenzten Routings auf den Plan. Dieses ist allerdings aus Gründen der Ausfallsicherheit und Ökonomie problematisch. Die US-Handelsbehörde USTR sieht darin eine Verletzung internationaler Handelsvereinbarungen, obwohl es ähnliche Regelungen auch in den USA gibt.

Überzeugender ist ein Vorschlag der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Er enthält Möglichkeiten der Ende-zu-Ende-Verschlüsselung für verschiedene Anwendungen, also dafür, dass Daten beim Abschicken und Empfangen gesichert werden und nicht nur beim Transfer. Methoden zur Verschleierung von Metadaten werden ebenfalls erwogen, etwa mit Hilfe virtueller privater Netzwerke oder Onion-Routing: Dabei kann eine E-Mail mehrfach verschlüsselt werden. Die Verschlüsselungsschichten legen sich dann wie Briefumschläge um die eigentliche Nachricht und jede beteiligte Stelle kann nur auf diejenigen Informationen zugreifen, die sie unbedingt benötigt, um die Nachricht weiterzuleiten.

Datenschutz als Standortvorteil

Um der rechtswidrigen Ausbeutung geschützter Daten und Inhalte im Internet entgegenzuwirken, sollen auch Urheber-, Daten- und Verbraucherrechte auf nationaler wie europäischer Ebene weiterentwickelt werden. Die Durchsetzung des Datenschutzes mit Hilfe der geplanten europäischen Datenschutzgrundverordnung (DSGVO) soll mehr Rechts- und Planungssicherheit für die Wirtschaft im Binnenmarkt schaffen. Nach über drei Jahren Verhandlungen haben sich die Innen- und Justizminister der EU im Juni 2015 auf eine gemeinsame Position zur Datenschutzreform verständigt. Der Reformvorschlag wird nun im Trilog zwischen Rat, Kommission und EP diskutiert. Die neue Grundverordnung soll die derzeit gültige Datenschutzrichtlinie aus dem Jahr 1995 ablösen und ab 2018 geltendes Recht werden. Demnach sollen Unternehmen in der Technik, die sie verwenden, datenschutzfreundliche Voreinstellungen einführen; außerdem sollen Verbandsklagen gegen Datenschutzverstöße ermöglicht, die Zusammenarbeit nationaler Aufsichtsbehörden verbessert und ein einheitliches Aufsichtsinstrumentarium geschaffen werden. Nicht zuletzt ist eine Sanktionierung von Datenschutzverstößen vorgesehen. Gemäß dem ursprünglichen Entwurf der Europäischen Kommission soll diese bei 2% des weltweiten Jahresumsatzes des Unternehmens liegen. Das Europäische Parlament hingegen fordert, die Strafe auf 5% des Jahresumsatzes und mindestens 100 Mio. Euro zu erhöhen.

Ein zentraler Punkt der Verordnung ist das sogenannte »Recht auf Vergessen«, das der Spanier Mario Costeja González im Urteil des EuGH vom 13. Mai 2014 gegen Google erstritten und das die digitale Wirtschaft Europas verändert hat. Im Urteil heißt es, dass Suchmaschinen sich an gültige Datenschutzrichtlinien halten müssen und auch dann nicht auf amerikanisches Recht berufen können, wenn der Mutterkonzern seinen Sitz in den USA hat und die Daten aus dem dortigen Netz verarbeitet werden. Jeder EU-Bürger habe das Recht,

Suchmaschinen zur Löschung personenbezogener Daten aufzufordern. Allein bei Google sind bis zum 6. August 2015 nach eigenen Angaben 293 004 Löschersuchen eingegangen. 41,3 Prozent dieser Wünsche wurden erfüllt.

Laut Artikel 23 (1) der DSGVO muss Datenschutz künftig direkt in Prozesse, Systeme und Produkte eingebaut werden. Sensible Daten von EU-Bürgern dürfen ausländischen Sicherheitsbehörden nur dann übermittelt werden, wenn dies durch ein Rechtshilfeabkommen gedeckt wird. Nach derzeitiger Rechtslage ist es verboten, personenbezogene Daten aus Mitgliedstaaten in Länder zu übertragen, die nicht über einen mit dem EG-Recht vergleichbaren Datenschutz verfügen. Dies ist ein wichtiges Thema, da das europäische Verfassungsverständnis deutlich von dem der USA abweicht. Dort liegt der Schwerpunkt nicht auf dem Schutz der Menschenwürde, sondern auf Freiheit im Sinne von *liberty* als Bürgerrecht des Individuums, das »frei sein will von gesetzlicher Regulierung«. Mit der neuen DSGVO und der vorgesehenen Richtlinie für Strafverfolgungsbehörden sollten aber Garantierechte für EU-Bürger bei der Rechtsbeihilfe durchgesetzt werden. Daher wird die Verordnung Auswirkungen auf alle derzeit zu verhandelnden bilateralen Abkommen mit den USA zum Datentransfer in den Bereichen Sicherheit und Wirtschaft haben. Dies betrifft unter anderem den Austausch personenbezogener Daten, das Rahmenabkommen zum Datenschutz, das bilaterale Rechtshilfeabkommen sowie den Austausch von Fluggastdaten.

Europa in der digitalen Welt

Die europäische Regelsetzung beschränkt sich nicht auf den EU-Binnenmarkt, sondern hat eine globale Dimension. Die europäische Informations- und Kommunikationswirtschaft ist hochgradig mit anderen Märkten verflochten. Um diesen wechselseitigen Abhängigkeiten der europäischen und globalen Standard- und Regelsetzung Rechnung zu tragen, sind die Europäische Kommission und einzelne Mitgliedstaaten in internationalen Gremien zu den zentralen Themen Internet Governance und Cybersicherheit aktiv. Aus diesem Grund umfasst die digitale Integration auch außenpolitische Dimensionen staatlicher Politik, die nicht nur die Erweiterung des digitalen Binnenmarktes über nationale Grenzen hinaus betreffen, sondern auch die Cyberaußen- und Cybersicherheitspolitiken der Mitgliedstaaten. In diesem Sinne sprechen sich die EU-Mitgliedstaaten in ihren Ratsschlussfolgerungen zur Internet Governance vom November 2014 sowie zur Cyberdiplomatie vom Februar 2015 für den »Multistakeholder-Ansatz« aus. Danach sollen Regierungen sowie Vertreter von Wirtschaft, technischer Community, Wissenschaft und Zivilgesellschaft gleichermaßen Berücksichtigung finden. Außerdem soll eine enge Cyberdiplomatie mit den USA stattfinden, etwa in der Group of Governmental Experts (GGE) auf VN-Ebene.

In einschlägigen Dokumenten von Februar 2013 und Februar 2014 vertritt die EU die Auffassung, dass Freiheit, Sicherheit und Stabilität im Cyberraum und für die Internet Governance unerlässlich sind. Unter Internet Governance wird die Entwicklung und Anwendung gemeinsamer Prinzipien, Normen und Vorgehensweisen bei der globalen Kommunikation verstanden. Seit Juni 2011 verfolgt die Europäische Kommission das Ziel der Schaffung eines »einzigen, offenen, freien und unfragmentierten Netzwerkes von Netzwerken, welches denselben Gesetzen und Normen unterliegt, die offline gelten« (in EU-Terminologie COMPACT genannt). Um staatliche Einflussnahme zu Lasten des Multistakeholder-Ansatzes zu verhindern, will die EU die Rolle des Internet Governance Forum (IGF) stärken, dem Multistakeholder-Forum auf globaler Ebene mit 3700 Mitgliedern aus 144 Ländern (2014). Über die Fortsetzung des Formats wird die VN-Generalversammlung Ende 2015 entscheiden. Gleichzeitig fordert die EU wichtige Organisationen auf, sich zu »internationalisieren«. Das richtet sich vorrangig an die ICANN (Internet Cor-

poration for Assigned Names and Numbers), welche für stabiles Funktionieren des Internet zuständig ist, und ihre Abteilung IANA (Internet Assigned Numbers Authority), die Nummern und Namen im Internet zuordnet, vor allem IP-Adressen. Die EU will verhindern, dass einzelne Staaten oder Privatinteressen die Verwaltung von Internetressourcen dominieren. Hier liegt sie (zumindest offiziell) über Kreuz mit den USA, die eine federführende Rolle in der ICANN spielen. Die Ausarbeitung von Verfahren verbesserter Rechenschaftslegung, etwa zur Anfechtung von Entscheidungen des ICANN-Direktoriums, dauert an. ICANN-Chef Fadi Chehadé erklärte, die Abgabe der Aufsicht über Kernfunktionen der Internetverwaltung könne nicht wie geplant im September 2015 abgeschlossen werden. Daher werde ICANN seine Verträge mit dem US-Handelsministerium verlängern.

Ein anderer Schauplatz der Multistakeholder-Diskussion war die NETmundial-Konferenz im Jahr 2014. Dort wurde der Schwerpunkt auf Menschenrechte und das Recht auf Privatheit im Internet gesetzt. Als Ergebnis wurde im Juli 2015 ein Europäer VN-Sonderberichterstatter zum »Recht auf Privatheit« im VN-Menschenrechtsrat, der Malteser Joseph Cannataci.

Auf Anstoß des Weltwirtschaftsforums (WEF), des brasilianischen Internet-Lenkungsausschusses CGI und der ICANN wurde darüber hinaus im Januar 2015 die sogenannte NETmundial-Initiative (NMI) gestartet. Europäische Teilnehmer üben jedoch Kritik an ihrer Zusammensetzung und mangelnder Abgrenzung zum IGF. Unter anderem deshalb hat sie sich bisher nicht im Internet-Governance-System etablieren können.

Die EU tritt auf VN-Ebene nicht als einheitlicher Block auf. In einem offenen Schreiben vom April 2015 formulieren Federica Mogherini, Hohe Vertreterin der EU für Außen- und Sicherheitspolitik, und der niederländische Außenminister Bert Koenders den kleinsten gemeinsamen Nenner der EU. Sie weisen auf die Notwendigkeit hin, Staaten für Angriffe aus ihrem nationalen Cyberraum verantwortlich zu machen. Zudem betonen sie, dass unzureichender Schutz zentraler Infrastrukturelemente nicht nur eine Bedrohung für die nationale, sondern auch für die internationale Sicherheit darstelle.

Dieser kleinste gemeinsame Nenner wurde in der vierten Runde der Regierungsexperten zur Cybersicherheit (GGE) von fünf EU-Staaten vertreten. Insgesamt verhandeln dort 20 Staaten (Antigua und Barbuda, Weißrussland, Brasilien [Vorsitz], China, Kolumbien, Ägypten, Estland, Frankreich, Deutschland, Ghana, Israel, Japan, Kenia, Malaysia, Mexiko, Pakistan, Russland, Spanien, Vereinigtes Königreich, USA). Die Regierungsvertreter in der GGE analysieren Sicherheitsrisiken des Cyberraums und entwickeln Ansatzpunkte für Kooperation. Die letzte Sitzung der vierten Runde fand Ende Juni 2015 in New York statt; die Verabschiedung des Abschlussberichts durch die Generalversammlung steht noch aus. Konfliktpunkt bleibt die konkrete Anwendung des Völkerrechts auf den Cyberraum. Unvereinbare Auffassungen zur Informationssicherheit machen eine substantielle und inhaltliche Auseinandersetzung auf VN-Ebene nahezu unmöglich. Strittige Punkte sind etwa der Umfang des Themenfeldes, die Bedrohungswahrnehmung oder die Rolle der VN und der Regierungen gegenüber privatwirtschaftlichen und zivilgesellschaftlichen Akteuren. Zwar herrscht weitgehend Einigkeit darüber, dass Staaten für ihr Verhalten im Cyberraum verantwortlich gemacht werden müssen. Doch während Deutschland und die USA geltendes Völkerrecht als rechtliche Ausgangslage für den Cyberraum betrachten, wollen Russland, China und andere Staaten ein eigenes Cybervölkerrecht definieren. Daneben sind vor allem die G77-Staaten daran interessiert, das Thema Cybersicherheit in eine offene Arbeitsgruppe oder auch in die Genfer Abrüstungskonferenz zu tragen. Bei all diesen Fragen gibt es eine europäische Absprache zwischen Deutschland, Frankreich und Großbritannien sowie mit der

Gruppe westlicher Gleichgesinnter unter den Regierungsexperten. Da Russland sich schon jetzt für weitere GGE-Beratungen in einer fünften Runde einsetzt, spricht vieles dafür, dass die dort künftig vertretenen EU-Staaten stärker denn je das europäische Interesse im Auge behalten müssen.

Anforderungen an die deutsche Politik

Die digitale Gesamtstrategie der EU gilt vielen als zu wenig ehrgeizig, um die digitale Selbstbehauptung Europas gegenüber den USA und China vorantreiben zu können. Selbst ein großer Mitgliedstaat wie Deutschland kann nur in Zusammenarbeit mit EU-Institutionen und anderen Mitgliedstaaten global gestalten. Die Regierungsexpertengruppe »Friends of Presidency on Cyber Issues (FoP Cyber)« leistet zur Unterstützung der jeweiligen EU-Ratspräsidentschaft innereuropäische Koordinierungsdienste und sollte ihre Wirkung auch in internationalen Organisationen entfalten. Die digitale Selbstbehauptung der EU bedarf auch internationaler Flankierung, um die Werte Freiheit und Demokratie in Europa zu stabilisieren und ihnen global mehr Geltung zu verschaffen. Die Bundesregierung hat als Ziel formuliert, »Maßnahmen zur Rückgewinnung der technologischen Souveränität« zu ergreifen und »einen europäischen Vertrauensraum« zu schaffen. In der Logik negativer und positiver Integration (Scharpf) wäre technologische Souveränität im Binnenmarkt aber nur dort legitim, wo sie wesentliche Errungenschaften von sozialer Marktwirtschaft und Demokratie nicht torpediert. Der Binnenmarkt basiert auf grundsätzlichem Vertrauen in die freien Marktkräfte und auf den Prinzipien Offenheit und Nichtdiskriminierung. Dem Aufbau national oder europäisch subventionierter Unternehmen gilt es daher mit Skepsis zu begegnen. Staatliche Interventionen in den Markt sind nur dann angezeigt, wenn dieser bei der Bereitstellung wichtiger Güter wie Datensicherheit und Gewährleistung von Privatheit versagt. Wechselseitige globale Abhängigkeiten sind nicht per se problematisch, werden aber dann inakzeptabel, wenn sie die informationelle Steuerungs- und Selbstbestimmungsfähigkeit der Europäer gegenüber illiberalen Regierungen untergraben. Staaten, die Werte wie freie Marktwirtschaft, Demokratie und Freiheit ablehnen, sollten auch nur beschränkt als legitime Herkunftsorte strategisch wichtiger Ressourcen für die europäische Kommunikationsinfrastruktur gelten. Zum Beispiel sind Seltene Erden aus Australien zwar teurer, doch durch den Kauf dort wird eine Politik doppelter Standards vermieden.

Estland ist ein Beispiel für eine qualifizierte Digitalisierungsstrategie. Das nur 1,3 Mio. Einwohner zählende Land ist Vorreiter der Digitalisierung in Europa. Die nationale e-ID-Infrastruktur wird von mehr als 90 Prozent aller Bürger genutzt. Die ID-Karte, eine Art digitaler Personalausweis mit einer Vielzahl von Funktionen, kann im Netz überall dort eingesetzt werden, wo die Identitätsüberprüfung unerlässlich ist, etwa bei Banktransaktionen oder Wahlen. Estland operiert dabei weitestgehend ohne Rückgriff auf russische Technologie und hat ein starkes Sicherheitsnetz mit weltweit acht Duplikaten in befreundeten Staaten wie Großbritannien, Deutschland, USA, Kanada, Südafrika und Japan aufgebaut. Was die elektronische Administration betrifft, sind kleine Länder wie Estland deutlich weiter entwickelt als die großen EU-Staaten.

Je mehr die EU ihre digitale Integration in Form des Europarechts vorantreibt, desto mehr wird ihre digitale Selbstbehauptung erstarken, sowohl innereuropäisch als auch international. Das Marktortprinzip, ein wesentliches Instrument des Binnenmarktes, gewährleistet die Gleichbehandlung in- und ausländischer Unternehmen. Digitale Selbstbehauptung steht und fällt mit der Bereitschaft der Mitgliedstaaten, Quantität und Qualität des Europarechts auszubauen. Nur die EU hat das Potential, einen dritten Weg jenseits der technologischen Dominanz der USA und Chinas zu weisen, nicht einzelne Mitgliedstaaten.

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 1611-6364