DIGITALE WELT UND REALE WELT – KEINE GEGENSÄTZE MEHR

DANIEL LAMBACH

PD Dr. Daniel Lambach ist Heisenberg-Fellow an der Goethe-Universität Frankfurt und Senior Associate Fellow am Institut für Entwicklung und Frieden der Universität Duisburg-Essen. In seiner Forschung beschäftigt er sich mit Konstruktionen von Territorium in unregulierten Räumen. 2019 ist sein Artikel "The Territorialization of Cyberspace" in der International Studies Review erschienen.

Über das Internet wird seit jeher gesprochen, als wäre es ein ferner Ort. 2013 bezeichnete es Bundeskanzlerin Angela Merkel als zu erforschendes „Neuland". Rechts- und Innenpolitiker warnen gerne vor Wildwestzuständen in diesem angeblich so „rechtsfreien Raum". 1996 erklärte John Perry Barlow, libertärer Internetvisionär, sogar die Unabhängigkeit des Cyberspace. Diese Äußerungen beruhen auf einem Verständnis des Netzes als eines eigenen, mit der „Offlinewelt" nur lose verbundenen Raums. Eine derartige Vorstellung geht aber immer mehr an der Wirklichkeit vorbei, wenn sie überhaupt jemals korrekt war. Stattdessen beobachten wir eine wechselseitige Durchdringung und Vermischung der „digitalen" und der „realen" Welt.

Diese Vermischung geschieht in beide Richtungen. Das Digitale kommt in die physische Welt durch Smartphones, optische Displays, das Internet der Dinge und viele andere, immer kleinere und immer alltäglichere Geräte. Die physische Welt kommt in den digitalen Raum durch Techniken der Geolokation, die den Charakter des Netzes zunehmend verändern. Geolokation ist ein Mittel, den geographischen Standort eines Nutzers zu ermitteln und digital zu verarbeiten. Über IP-Adressen, GPS-Daten, Funkmastverbindungen, WLAN-Zugänge oder Bluetooth-Verbindungen lassen sich extrem präzise Standortinformationen generieren, selbst innerhalb von Gebäuden. Wer beim Besuch eines Geschäfts schon einmal von Google Maps aufgefordert worden ist, eine Bewertung für das Geschäft abzugeben, ist Ziel solcher Techniken geworden. Neben solchen ortsbezogenen Angeboten wird Geolokation auch für das so genannte Geoblocking verwendet, bei dem Zugang zu Daten und Inhalten anhand des Standorts geregelt wird. Auf diese Weise ist Geolokation ein wichtiges Hilfsmittel geworden, um geistiges Eigentum nach Ländern differenziert zu vermarkten oder zur Umsetzung nationaler Gesetze

(z.B. zu Meinungsäußerung) im Netz.

Auf diese Weise erodieren die Grenzen zwischen digitaler und physischer Welt – mit ambivalenten Folgen. Zum einen kann dies zu einer effektiveren Umsetzung von Gesetzen genutzt werden, indem z.B. für deutsche Nutzerinnen und Nutzer eine an deutsches Recht angepasste Version einer Webseite bereitgestellt wird. Auch in wirtschaftlicher und sozialer Hinsicht ergibt dies Vorteile, indem der Zugang zu Kommunikations- und Informationsmöglichkeiten immer leichter wird. Zum anderen bestehen darin aber auch Gefahren. Beispielsweise kann eine Hybridisierung von Online- und Offlinewelten das grenzüberschreitende Potenzial des Netzes bedrohen, wenn man ihm dabei die territoriale Logik der Offlinewelt überstülpt. Außerdem generieren Geolokationstechniken unglaublich große, personenbezogene Datenmengen, deren Schutz bislang nicht ausreichend gewährleistet wird. Kurz gesagt: Wir sollten uns von dem Denkmodell verabschieden, wonach der digitale Raum getrennt von der „realen Welt“ existiert. Onlineaktivitäten und Datenzugang werden ein immer alltäglicherer Teil des sozialen Lebens werden.

Dies wird weitreichende Folgen für Gesellschaft und Politik haben, von denen sich viele schon heute abzeichnen. Dazu gehören die Entgrenzung sozialer Sphären wie öffentlich/privat oder Beruf/Freizeit, aber auch die Vereinigung von Online- und Offline-Identitäten. Der alte Spruch „On the internet nobody knows you’re a dog“ trifft dann nicht mehr zu. Der Staat muss seine klassischen, territorial gebundenen Steuerungsapparate um neue, deterritorialisierte Instrumente erweitern. In den letzten Jahrzehnten betraf dies beispielsweise, wie Mehrwertsteuern auf Onlinehandel erhoben, wie verbotene Meinungsäußerungen (z.B. Holocaust-Leugnung) sanktioniert oder wie Datenschutz im Netz gewährleistet werden kann und all dies ohne die Dynamik und das Potenzial des Internets durch einen allumfassenden Kontroll- und Spähapparat abzuwürgen. Der deutsche Staat hat dazu schon einiges unternommen, z.B. die Schaffung einschlägiger Gesetze, von Schwerpunktstaatsanwaltschaften für Internetkriminalität, von polizeilichen Ermittlungskapazitäten im Internet und zuletzt des Kommandos Cyber- und Informationsraum der Bundeswehr. Dass bei deren Gründung oft noch das Internet als eigener Raum gedacht wird, steht einer vernetzten Handlungsweise nicht im Wege. Internetkriminalität geschieht oft in Verbindung mit Straftaten im physischen Raum, und auch die Verteidigung gegen Cyberangriffe kann nicht losgelöst von anderen Formen der Landesverteidigung gedacht werden.

Während die Schaffung dieser Kapazitäten ein unerlässlicher Schritt war,

besteht ein noch nicht zufriedenstellend gelöstes Problem in der Durchsetzung von Gesetzen und Gerichtsurteilen, z.B. wenn ein Gerichtsurteil gegen Nutzerinnen und Nutzer großer Internetplattformen wie Facebook oder gar die Unternehmen selbst durchgesetzt werden soll. Zwar unterliegen diese Plattformen nationalen Gesetzen, aber deren Anwendung wird durch die Vielzahl der beteiligten bzw. betroffenen Staaten erschwert, zumal es oft Unterschiede in der politischen und rechtlichen Bewertung von Straftaten gibt. In solchen Umständen entsteht schnell der Eindruck, der Staat sei handlungsunfähig angesichts der neuen, entgrenzten Realitäten der digital-realen Welt.

Dies ist jedoch irreführend. Politik ist weiterhin gestaltungsfähig, selbst wenn traditionelle Herangehensweisen versagen. Tatsächlich verfügen Staaten über eine Vielzahl von Kontroll- und Einflussmöglichkeiten, denn sie haben Zugriff auf alle Komponenten, die die Digitalisierung ausmachen. Sie können die technische Infrastruktur von Kabeln, Servern und Funkmasten regulieren, z.B. durch rechtliche Standards oder Zugriff zu Überwachungszwecken. Auch die Regelung von Codes und Algorithmen ist eine Möglichkeit, die derzeit verstärkt mit Bezug auf Künstliche Intelligenz, „smart cities“ oder autonomes Fahren diskutiert wird. Staaten versuchen auch zunehmend Kontrolle über Daten zu gewinnen, indem sie Datenlokalisierungs- und Datenschutzgesetze erlassen, die den Transfer und die Verwendung von Daten einschränken. Nicht zuletzt kann z.B. über Haftungsregeln auch Kontrolle über Nutzerinnen und Nutzer ausgeübt werden.

Wo hierarchische Mittel wie Gesetze und deren justizielle und polizeiliche Durchsetzung nicht ausreichen, greifen Staaten zu anderen Mitteln. Eins davon ist die Herrschaft über Intermediäre, welche für die Umsetzung einer Entscheidung zuständig sind. In Bezug auf das Internet sind das oft große Firmen, die zur Durchsetzung von Gerichtsentscheidungen verpflichtet werden, indem sie z.B. justiziable Äußerungen in sozialen Medien löschen oder Softwarepiraterie bekämpfen. Ein anderes ist die stärkere Beteiligung an der Governance des Internet, indem sich Staaten in etablierten Foren der Regel- und Standardsetzung einbringen und dort mit Unternehmen, zivilgesellschaftlichen Organisationen sowie Expertinnen und Experten zusammenarbeiten.

In letzter Konsequenz betrifft die erwähnte Entgrenzung nicht nur soziale Sphären innerhalb von Gesellschaften, sondern auch die Grenzen zwischen Gesellschaften. Das Territorium löst sich damit ein Stück weit vom Territori-

alstaat, dessen untrennbarer Bestandteil es in Vorstellungen territorialer Souveränität lange Zeit war. Räume werden dadurch dynamischer, beweglicher, anpassungsfähiger. Damit entstehen aber auch Möglichkeiten, Einfluss weit jenseits dessen auszuüben, was wir als nationales Territorium verstehen. So wird die Europäische Datenschutzrichtlinie nahezu auf der ganzen Welt umgesetzt. Solche funktionalen Regulierungsräume greifen weit über nationales Territorium hinaus. So gewinnen Staaten unter Umständen sogar Kontrollmöglichkeiten hinzu.

Eine derartig gestaltungsfähige Politik ist derzeit von besonderer Notwendigkeit. Angesichts von Globalisierung, Entgrenzung und Digitalisierung haben viele Bürgerinnen und Bürger das Gefühl eines Kontrollverlustes. Zukunfts- und Verlustängste prägen den sozialen und politischen Diskurs. Gerade jetzt sollte also der Staat als Gestalter der neuen digital-realen Welt auftreten, um die Legitimation der Demokratie zu erhalten und den Bürgerinnen und Bürgern zu zeigen, dass sie in der komplexen neuen Welt nicht anonymen Kräften schutzlos ausgeliefert sind. Besonderen Handlungsbedarf gibt es zum Beispiel beim Datenschutz. Erstens ist die internationale Kooperation auf diesem Feld noch unterentwickelt, da es in vielen Ländern stark abweichende Gesetze gibt. Zweitens leben viele Internetkonzerne von der Monetarisierung von Nutzerdaten – „if you are not paying for the product, you are the product" heißt es aus der Wirtschaft. Drittens fallen immer größere Datenmengen über Bürgerinnen und Bürger an, die mittels big data-Verfahren kombiniert und ausgewertet werden können. Hier müssen insbesondere stärkere Regeln zu Geolokationsdaten entwickelt werden. Wie detailliert die Aktivitätsprofile sind, hat bereits 2009 die ZEIT gezeigt, als sie von der Telekom gesammelte Bewegungsdaten des Grünenpolitikers Malte Spitz mit anderen frei zugänglichen Daten kombinierte (https://www.zeit.de/datenschutz/malte-spitz-vorratsdaten). Dieses bereits zehn Jahre alte Bild würde heute noch sehr viel detaillierter ausfallen – ohne dass es dafür bereits hinreichende Kontrollen gäbe.