

3.1 Mehrebenensystem

Digitalpolitik von technischen Standards über staatliche Normen bis zum digitalen Völkerrecht

Matthias C. Kettemann

Zur Verortung der Digitalpolitik

Zunächst müssen wir Digitalpolitik lokalisieren. Wo wird Digitalpolitik betrieben? Die einfachere Frage wäre inzwischen: Wo nicht? Digitalisierung ist phänomenologisch so breit und diffus geworden wie die Globalisierung. Ähnlich begrifflich konturlos, häufig missverstanden, manchmal dämonisiert. Das Buch, in dem dieser Beitrag erscheint, zeigt die Vielfalt der Digitalisierung, aber auch ihre Wirkkraft auf gesellschaftliche Realitäten und Werte. Die Beiträge in diesem Buch betonen die Gestaltungsnotwendigkeit der Digitalisierung, die Bedeutung des *Primats des Rechts*. Hier knüpft dieser Beitrag an und zeigt auf, wie vielfältig die Produktion von Recht im Kontext der Digitalisierung ist und wie Normen gesellschaftliche Gestaltungsansprüche erheben – und dies sind nicht nur und nicht einmal vor allem Rechtsnormen.

Staaten, Individuen, privatwirtschaftliche Unternehmen, die Zivilgesellschaft und technische Standardsetzer – sie alle schaffen und vollziehen, bestreiten und bekräftigen in verschiedenen Konstellationen Normen. Deren Entstehung, Legitimität und Durchsetzbarkeit variiert stark: von privaten Normen durch normgebende Gremien und nationale Verfassungen bis hin zu bindenden Normen des Völkerrechts. Nur durch eine sorgfältige Analyse der Faktizität und Normativität der Regeln für das Netz und die digitale Welt kann ein Modell einer umfassenden und nuancierten Ordnung der

Digitalpolitik – einer normativen Ordnung des Internets¹ – herausdestilliert werden. Diese Ordnung speist sich aus privaten Normen und öffentlichen Regeln (Gesetzen), ist also hybrider Natur. Sie setzt sich zusammen aus internationalen Rechtsnormen, nationalem Recht und transnationalen Regelungsarrangements unterschiedlicher Art.

Dieser Beitrag stellt beispielhaft einige Akteurskonstellationen vor, in denen Digitalisierungspolitik stattfindet, Normen mit Digitalbezug gesetzt und normative Konflikte verhandelt werden. Eine Einordnung nach Ebenen (international, regional, national, lokal) kann nicht trennscharf erfolgen, da Akteur*innen in Foren zusammenwirken, die diese Ebenen gerade durchbrechen. Nicht zwingend, aber doch aufschlussreicher erscheint daher eine Einteilung auf Ebene der normativen Instrumente, die das Ergebnis der digitalpolitischen Arbeit verschiedener Akteurskonstellationen sind: darunter Verträge, Gesetze, Prinzipien, Standards.

Häufig liegen indes Mischformen vor: Technische Standardsetzung findet auf nationaler wie internationaler Ebene statt, mal als Versuch, qua Normierung nationale technologische Souveränität zu projizieren (wenn etwa China und Huawei einen neuen Internet Protocol-Standard vorschlagen), mal durch technisch dominierte globale Institutionen ohne vordergründig politische Agenden (wie die Standards der Internet Engineering Task Force [IETF]). Dabei ist jede technische Standardisierung immer auch politisch, da sie sowohl kontingent als auch normativ ist. Das dynamische Mehrebenensystem der Digitalpolitik charakterisiert aber auch, dass Akteur*innen gleichermaßen Normunternehmer (also Normenschaffer und -promoter), Normanwender und Normdurchsetzer sein können.

Internetvölkerrecht und Internet Governance

Das Konzept der *digitalen Welt* impliziert eine neue Lebensrealität jenseits des staatlichen Territoriums, in der Recht beziehungsweise Menschenrechte keine Gültigkeit hätten. Das ist falsch. Der Cyberspace ist keine rechtliche *ter-*

1 Vgl. Kettemann, Matthias: *The Normative Order of the Internet. A Theory of Online Rule and Regulation* (Oxford: Oxford University Press, 2020).

ra nullius.² Natürlich entstehen mit den neuen »Territorialitäten«³ neue normative Herausforderungen, aber die Normativität des Rechts wird nicht vor grundlegend neue Herausforderungen gestellt.⁴ Recht gilt online wie offline. Menschenrechte gelten online wie offline.⁵ Völkerrecht gilt offline wie online. In der Tat hat die Regulierung internationaler Informations- und Kommunikationsflüsse durch das Völkerrecht eine lange Tradition. Das Völkerrecht ist das einzige Rechtsgebiet, mit dem globale öffentliche Güter verwaltet werden, das globale öffentliche Interessen schützt und über Verteilungsfragen entscheiden kann.⁶

Der Konsens der Staaten der Welt, dass sich das Internet nur mit einem globalen Ansatz gestalten lässt, wird schon in den Schlussfolgerungen der Weltgipfel zur Informationsgesellschaft 2003 (Genf) und 2005 (Tunis) sichtbar. Die Staatengemeinschaft verpflichtete sich, mitzuwirken am Aufbau einer »den Menschen in den Mittelpunkt stellende[n], inklusive[n] und entwicklungsorientierte[n] Informationsgesellschaft [...] gestützt auf die Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus sowie unter voller Achtung und Einhaltung der Allgemeinen Erklärung der Menschenrechte«⁷, wobei bekräftigt wurde, dass »Menschenrechte und Grundfreiheiten, einschließlich des in der Erklärung von Wien verankerten Rechts auf Entwicklung, allgemein gültig und unteilbar sind, einander bedingen und miteinander verknüpft sind«⁸.

2 Vgl. Hobe, Stephan: Cyberspace – der virtuelle Raum, in: Isensee/Kirchhof (Hg.), HStR XI, 2013, 3. Auflage.

3 Sassen, Saskia: Territory, Authority, Rights. From Medieval to Global Assemblages (Princeton: Princeton University Press, 2006), 346: »[T]erritorialities [...] entail specific political, operational, or subjective encasements, including some that might be formalized and some that might remain informal.« Die Formalisierung dieser »Encasements« ist ein normativer Prozess. Vgl. auch instruktiv: Daniel Lambach, The Territorialization of Cyberspace, International Studies Review, vizo22, <https://doi.org/10.1093/isr/vizo22>.

4 Siehe hierzu auch den Beitrag von Ulf Buermeyer und Malte Spitz in diesem Band.

5 Siehe Kettemann, Matthias: Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015), <http://library.fes.de/pdf-files/akademie/12068.pdf>

6 Ebd.

7 World Summit on the Information Society (WSIS), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E vom 18.11.2005, Ziff. 2. Cf. auch WSIS, Geneva Declaration of Principles (2003), Ziff. 1.

8 Tunis Commitment (Fn. 2), Ziff. 3.

Deutlicher und verbindlicher wurde erstmals ein Bericht von 2013,⁹ in dem ein staatenbesichtigtes Gremium der Vereinten Nationen, die Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), festhielt, dass die Anwendung von Normen, die aus dem bestehenden Völkerrecht abgeleitet werden, »essenziell« ist, um Risiken für den Weltfrieden und die internationale Sicherheit und Stabilität zu minimieren.¹⁰ Dies gelte auch für den völkerrechtlichen Schutz der Souveränität und der Verantwortung, die dieser entfließe, sowie für die Menschenrechte.¹¹

2015 bestätigte die GGE erneut, dass Völkerrecht einen essenziellen Rahmen für die nationale Nutzung von Informations- und Kommunikationstechnologien darstelle.¹² Für die Gewährleistung der Integrität des Internets besonders relevant sind die angesprochenen völkerrechtlichen Grundsätze,¹³ die teils in der Satzung der UNO in die Form von Vertragsrecht gegossen wurden, teils völkergewohnheitsrechtlich (also durch Anwendung und übereinstimmende gemeinsame Rechtsüberzeugung etabliertes Recht) geschützt sind und teils als Allgemeine Prinzipien des Völkerrechts auftreten: souveräne Gleichheit, Gewaltverbot, Interventionsverbot, friedliche Streitbeilegung, Menschenrechtsschutz, Kooperationsprinzip (das sich speist aus dem Grundsatz der guten Nachbarschaft) und Präventionsprinzip [*due diligence*].¹⁴ Diese Prozesse wurden auch in der jüngsten Vergangenheit fortgesetzt. Russland schlug in einer Resolution die Schaffung einer Open-ended Working Group

9 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 vom 24.6.2013.

10 Ebd., Rz. 16.

11 Perspektiven darauf bei Kettemann, Matthias C./Kleinwächter, Wolfgang/Senges, Max: »Implementing Sustainable Digital Cooperation: Towards Next Generation Internet Governance«, in: Kettemann, Matthias C./Kleinwächter, Wolfgang/Senges, Max (Hg.): Towards a Global Framework for Cyber Peace and Digital Cooperation. An Agenda for the 2020s, BMWi: Berlin 2019, S. 31-46.

12 Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, A/70/174 vom 22.7.2015, retrieved 15.2.2020 from https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

13 Ebd., Abs. 26.

14 Vergleiche dazu auch Kettemann, Matthias C.: »Die Weltordnung des Digitalen, Vereinte Nationen«. Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen/German Review on the United Nations 5/2019, 195-200.

(OEWG) der Generalversammlung vor, die USA bevorzugten die Weiterführung der Group of Governmental Experts.

Neben dem klassischen Völkerrecht ist die zweite internationale Grundordnung des Internets das normativ weniger stringente, aber dennoch einflussreiche Internet-Governance-Regime.¹⁵ Die Governance des Internets (oder »Internet Governance«) umfasst die »Entwicklung und Anwendung durch Regierungen, den Privatsektor und die Zivilgesellschaft, in ihren jeweiligen Rollen, von gemeinsamen Prinzipien, Normen, Regeln, Entscheidungsfindungsprozessen und Programmen, die die Weiterentwicklung und Verwendung des Internets gestalten«.¹⁶ Die Bedeutung der Teilhabe aller Stakeholdergruppen (Staaten, Privatsektor, Zivilgesellschaft)¹⁷ wird schon in der Definition deutlich. Die Realisierung demokratischer Partizipationsansprüche im Rahmen transnationaler Steuerungsprozesse ist indes schwierig.

Der Multistakeholderprozess als inklusiver Ansatz, die Internet-Governance-Policy zu gestalten, ist mit wenigen Ausnahmen (ordnungspolitische Initiativen souveränitätsbewusster bis autoritärer Regierungen) unumstritten. Da sich Staaten, der Privatsektor und die Zivilgesellschaft (Input-Legitimität) an dem Legitimationsprozess beteiligen und dabei eine gleichberechtigte Interaktion ermöglicht wird (Throughput-Legitimität), sind auch die Regelungsergebnisse besonders legitim (Output-Legitimität).¹⁸ Diese Regelungsergebnisse sind aufgrund ihrer Legitimität auch im Großen und Ganzen effektiv, was wiederum ihre Legitimität befördert.

Die in den normativen Prozessen der Internet Governance entwickelten Normen gehören zur Kategorie der *transnationalen Regulierungsarrangements*. Hier ist als Ort der Diskussion besonders das Internet Governance Forum der Vereinten Nationen zu nennen, eine jährliche Konferenz, die Tausende

15 Vgl. Kettemann, Matthias: »Internet Governance«, in: Jahnel et al. (Hg.): Internetrecht, 4. Auflage Wien: Springer 2020, S. 47-73.

16 Arbeitsgruppe über Internet Governance (WGIG), Bericht der Arbeitsgruppe (2005), Abs. 10.

17 Zur Rolle der Zivilgesellschaft und Stärkung der Vielfalt siehe auch den Beitrag von Julia Kloiber und Elisa Lindinger, für Ideen zur Reform der nationalen Governance siehe den Beitrag von Stefan Heumann in diesem Band.

18 Vgl. die gute Übersicht über die Prozeduralisierung von Legitimation in transnationalen Konstellationen bei Michael Zürn, Michael/Binder, Martin/Ecker-Ehrhardt, Matthias/Radtke, Katrin: »Politische Ordnungsbildung wider Willen«, Zeitschrift für Internationale Beziehungen 14 (2007) 1, S. 129-164 (154ff, 157).

Akteure der Digitalpolitik versammelt, ohne konkrete Entscheidungsbefugnis zu haben. Internet Governance ist eine normativ wertvolle Ergänzung des Völkerrechts, da sie in einer nicht-binären Logik (legal/illegal) mit variierender, flexibler Normativität die *weicheren* Themen der Internetregulierung, wie zum Beispiel Rechenschaftspflicht, normativ rahmt.

Demokratie ist begrifflich die Herrschaft des Volkes, der Normunterworfenen, die sich selbst Normen geben. Im Kontext des Internets verlieren Grenzen an Bedeutung, trotz Tendenzen der Souveränitätsrückgewinnung in Russland und China. »Das Volk« des Internets diffundiert. Einzelne haben keine effektive Möglichkeit, Regeln von großen Plattformen zu beeinflussen. Mark Zuckerberg lässt sich nicht wählen. Dabei haben alle Menschen ein demokratisches Teilhabeinteresse am Internet und dessen Regulierung. Insofern haben sie ein wertefundiertes Interesse nicht nur am Regulationsergebnis, sondern auch am Regelungsprozess an sich, der voraussetzt, dass alle Akteur*innen in alle Phasen des normativen Prozesses eingebunden sind. Dieses wird auch (wenn auch primär hinsichtlich von technischen Grundfragen der Internet Governance) durch den Multistakeholderansatz durchgesetzt, der durch Regierungen (Staaten), den Privatsektor (Unternehmen) und die Zivilgesellschaft (Individuen) in ihren jeweiligen Rollen verwirklicht wird.

Multistakeholderansätze und technische Standards

Internet-Governance-Prozesse leiden unter einer vagen Sprache, wiederholten normativen Mantras (»Multistakeholderismus«) und intellektueller Dürrtigkeit. Prinzipien, die innerhalb dieser Prozesse entwickelt werden, neigen dazu, aus wenigen Quellen zu schöpfen (wie den Ergebnisdokumenten des Prozesses zum World Summit on the Information Society und dem NetMundial-Treffen 2014). Dennoch sind diese Prozesse wichtig, weil sie Normen hervorbringen und Verfahren legitimieren, in denen diese Normen entwickelt werden. Diese wiederum sind Teil der hybriden normativen Ordnung des Internets. Viele von ihnen sind weder internationales noch nationales Recht, sondern bilden eine dritte Kategorie des normativen *Tertiums*. Als transnationale regulatorische Arrangements müssen sie sodann entweder durch ihre Genese (etwa in fairen Prozessen, an denen alle relevanten Akteur*innen beteiligt waren) oder die Ergebnisse, die sie hervorbringen, legitimiert werden.

So wie die Ausarbeitung und Akzeptanz von Internet-Governance-Mechanismen wichtige Beispiele für die staatliche Praxis sind, können neue rechtliche Instrumente, einschließlich Gerichtsentscheidungen, Governance-Entscheidungen und -Prozesse stark beeinflussen. So wurde die Global Commission on the Stability of Cyberspace beauftragt, die Internet Governance weiterzuentwickeln, um ein stabiles Internet zu gewährleisten. Die Kommission schlug Ende 2017 eine Norm vor, die speziell den öffentlichen Kern des Internets schützen und ein Prinzip der Nichteinmischung in diesen etablieren soll: »Unbeschadet ihrer Rechte und Pflichten sollten staatliche und nichtstaatliche Akteure keine Handlungen vornehmen oder wissentlich zulassen, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des Internets und damit die Stabilität des Cyberspace absichtlich und erheblich beeinträchtigen.«¹⁹ Dies ist offensichtlich eine präzisere Formulierung des Nichteinmischungsprinzips, die sich an dem öffentlichen Kern des Internets orientiert, dessen Schutz im gemeinsamen Interesse liegt. Da die Staaten durch das Völkergewohnheitsrecht angehalten sind, die für die Gewährleistung der Integrität des Internets wesentliche Infrastruktur nicht zu beschädigen (weil deren Schutz im gemeinsamen Interesse liegt), beinhaltet die Norm keine neue Pflicht, sondern rückt eine bestehende stärker in den Fokus und fördert so normkonformes Verhalten.

Doch angesichts der Vielzahl politischer und rechtlicher Fragen, mit denen das Internet konfrontiert ist, hinterlässt selbst die Kombination der beiden Regime von *Recht* und *Governance* erhebliche Regelungslücken und normative Brüche. Obwohl Recht und Governance des Internets ineinander verwoben sind, treten diese Brüche bei einer kritischen Betrachtung der Ordnung des Internets leicht zutage.

Ein Kohärenzfaktor sind technische Normen. Ohne Regeln im weitesten Sinne (in ihrer Ausprägung als technische Spezifikationen), ohne einige Normen zur Zusammenarbeit und zum Austausch von Informationen, wären die Informations- und Kommunikationsflüsse über das Internet nicht möglich gewesen. Dass die eher technischen Spielregeln für das frühe Internet in informellen Rundschreiben (Requests for Comments; RFCs) veröffentlicht und *bottom-up* in Meetings von Ingenieur*innen entwickelt wurden, ändert nichts an der Tatsache, dass einige (hauptsächlich technische) Normen von

19 Global Commission on the Stability of Cyberspace, Norm to Protect the Core of the Internet, <https://cyberstability.org/norms>

den Normsubjekten als höchst legitim angesehen wurden. Aber Ingenieur*innen haben auch verhaltensorientierte Normen formuliert, wie beispielsweise der US-amerikanische Informatiker Jon Postel: »Sei liberal in dem, was du akzeptierst, und konservativ in dem, was du sendest.«²⁰ Darüber hinaus findet die Tätigkeit von Ingenieur*innen und Unternehmen in einem Rahmen nationaler und internationaler Normen statt, die ihr Handeln beeinflussen. Diese Normen, die im Kraftfeld von Technik und Recht entstehen, mögen hybridisiert und weitgehend privatisiert sein, bleiben aber innerhalb der Grenzen, die das nationale und internationale Recht setzt.

Konturen einer digitalen Wertordnung

Ziel einer gelungenen Gestaltung der Digitalisierung muss es sein, zentrale Werte in allen Teilen der normativen Ordnung zu verankern. So muss dem Mehrebenensystem der Internet Governance mit dessen vielen Akteur*innen und der nötigen Vielfalt im normativen Vokabular ein Anker gegeben werden: gemeinsame, geteilte Werte und insbesondere der Schutz des Gemeinwohls, die Gemeinwohlbindung der Ausübung von Gestaltungsmacht und die Gemeinwohlorientierung von Policymacht.

Jeder Internetuser kann menschenverachtende Kommentare melden. Jede Plattform kann sich menschenrechtssensible Standards geben. Jeder Staat kann sich zu einer menschenrechtswahrenden Cyberaußenpolitik verpflichten. Aufsichtsbehörden spielen zunehmend eine wichtige Rolle, um die Werte und Rechte in der digitalen Welt zu bewahren. International sind auch Ombudspersonen²¹ von Bedeutung, ebenso bewusste Konsultationen von Expert*innen im Kontext von Rechtssetzungsverfahren,²² verpflichtende Algo-

20 Braden, R. (Hg.): RFC 1222, Requirements for Internet Hosts -- Communication Layers, October 1989, <https://www.ietf.org/rfc/rfc1122.txt>, 1.2.2. October 1989.

21 Z. B. Australian Competition and Consumer Commission, »Digital Platforms Inquiry – Final Report«, Australian Competition and Consumer Commission, 2019.

22 »Assessment for German Parliament's Commission on Artificial Intelligence: Technology-Driven Disinformation by Bots«, Botswatch Technologies, 2020 <https://www.botswatch.io/assessment-sb/>

rithmenfolgenabschätzungen (Kanada²³) sowie Modelle verstärkter Transparenz im Kampf gegen Hate Speech.²⁴ Zahlreiche hochspezialisierte Nichtregierungsorganisationen im Digitalbereich wie Access Now²⁵, Amnesty International²⁶ und AlgorithmWatch²⁷ zeigen beispielsweise beim Monitoring von Algorithmen, wie man effektiv in digitalen Konstellationen für Menschenrechte eintreten kann.

Das Recht ist (oder besser: die Normen und ihre Gefüge sind) das wichtigste Medium der Gesellschaft, um Ordnung zu schaffen, Herrschaft zu konstituieren und zu begrenzen und Gerechtigkeit zu gewährleisten.²⁸ Oben habe ich gezeigt, dass verschiedene Normen auf verschiedenen Ebenen für die Gestaltung der Digitalpolitik relevant sind. Wie können diese disparaten Prozesse zusammengeführt werden? Dafür bietet sich das Modell der *normativen Ordnung* der digitalpolitischen Gestaltung des Internets an.

Die normative Ordnung des Internets ist dezidiert kein hierarchisches System expliziter Normen. Es gibt keine Grundnorm. Sie ist vielmehr ein Komplex von Normen, Werten und Praktiken, die sich auf die Nutzung und Entwicklung des Internets beziehen. Durch die Ordnung werden die Aktivitäten und die Interaktionen verschiedener Akteur*innen, einschließlich Staaten, privater Unternehmen und der Zivilgesellschaft, die sich auf das Inter-

23 Treasury Board of Canada Secretariat Government of Canada, Algorithmic Impact Assessment (Archived) – Government of Canada Digital Playbook (Draft) <https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/automated-decision-auditomatisation/en/algorithmic-impact-assessment.html>

24 Vgl. Wagner, Ben et al.: »Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act«, in: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, FAT* '20 (Barcelona, Spain: Association for Computing Machinery, 2020), S. 261-271.

25 Experts Are Finished, Politicians to Deliver – the Council of Europe Publishes Expert Recommendations on the Human Rights Impacts of Algorithmic Systems, Access Now, 2019 <https://www.accessnow.org/experts-are-finished-politicians-to-deliver-the-council-of-europe-publishes-expert-recommendations-on-the-human-rights-impacts-of-algorithmic-systems/>

26 Amnesty International, Schütze deine Daten und deine Menschenrechte: Drei Schritte zum Datenschutz, <https://www.amnesty.de/informieren/aktuell/schuetze-deine-daten-und-deine-menschenrechte-drei-schritte-zum-datenschutz>

27 States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights, AlgorithmWatch, 2020 <https://algorithmwatch.org/en/joint-statement-pandemic-surveillance-tech-and-human-rights>

28 Vgl. Kettmann, Matthias: The Normative Order of the Internet. A Theory of Online Rule and Regulation (Oxford: Oxford University Press, 2020).

net beziehen oder durch dieses vermittelt werden, geregelt. Ebenso werden die Ausübung privater oder öffentlicher Autorität und die Verteilung gemeinschaftlicher Güter, einschließlich des Internetzugangs und des Zugangs zu Internetinhalten, normativ gerahmt. Die normative Ordnung des Internets ist somit die Menge an Normen, normativen Erwartungen und Legitimationsnarrativen, die die Nutzung und Entwicklung des Internets prägen. Sie ist im Kern das, woran sich die Digitalpolitik abarbeitet, der Regelungsgehalt des Politikfelds Digitalisierung.

Das Internet hat sich in der Tat zu einem lebenswichtigen Kommunikationsmedium entwickelt, durch das jede Person ihre Menschenrechte ausüben kann, insbesondere durch das ihr zustehende Recht auf freie Meinungsäußerung, das das Recht einschließt, Informationen und Ideen aller Art zu suchen, zu empfangen und weiterzugeben, und zwar über das Medium ihrer Wahl und ohne Rücksicht auf Grenzen. Das Internet ist jedoch kein ätherisches Subjekt utopischer normativer Projekte und Projektionen, sondern lediglich eine hardwarebasierte Datenübertragungsmöglichkeit, auf der Software läuft, die auf Protokollen basiert, die Interkonnektivität gewährleisten.

Beides – der öffentliche Kern des Internets und die dafür notwendigen Server – sind für das Funktionieren kritischer Infrastrukturen (z.B. Stromnetze) unabdingbar und stellen selbst kritische (Informations-)Infrastrukturen dar. Daher hat sich der Schutz der Integrität des Internets (seine Sicherheit, Stabilität, Robustheit, Widerstandsfähigkeit und Funktionalität) im gemeinsamen Interesse zu einer völkerrechtlichen Verpflichtung der Staaten entwickelt, sowohl einzeln als auch als Mitglieder der globalen Gemeinschaft. Wir sehen auch hier wieder, wie im Mehrebenensystem unterschiedliche Normen zusammenwirken.

Die flexible normative Geometrie der Digitalpolitik

Die normativen Akteure im Internet haben die Zusammensetzung des Mediums Recht beeinflusst und es in Richtung einer flexibleren Geometrie der Normativität bewegt. Unverbindliche Normen und Prinzipien, Standards und Codes haben sich zu einer dritten Art von relevanten Regeln neben den internationalen und nationalen Normen etabliert. Sie entstehen im umkämpften Raum zwischen technischer Notwendigkeit und sozialen und rechtlichen Werten und weisen eine variable normative Dichte und Bindungswirkung auf. Doch diese nicht-rechtliche Normativität muss (und wird) durch einen

wertebasierten normativen Ansatz neu ausgerichtet werden, der gleichwohl Normsetzungsverfahren einbezieht.

Jeder Bereich von Normen innerhalb der Ordnung – internationales Recht, nationales Recht, transnationale normative Arrangements – wird entweder durch traditionelle normative Prozesse oder durch seine Integration in nationale Rechtsordnungen legitimiert. Jede Akteur*innengruppe ist direkt oder indirekt legitimiert und überträgt dieses Legitimationspotenzial auf das normative Ergebnis, das oft – zusätzlich – epistemisch legitimiert ist. Die normative Ordnung selbst ist legitim als eine notwendige Ordnung, um den Schutz des Internets und den Schutz vor digital vermittelter oder mit digitalen Tools amplifizierter Gefahren zu gewährleisten.

Diese normative Ordnung des Internets integriert Normen, die materiell und normativ mit der Nutzung und Entwicklung des Internets verbunden sind, auf drei verschiedenen Ebenen (national, regional, international)²⁹, von zwei Typen (privat und öffentlich verfasst) und von wesentlich unterschiedlichem Charakter (von bindendem Völkerrecht bis zu technischen Standards). Wie eben erwähnt, handelt es sich um eine Rechtsordnung, die durch die Form des Rechts und in Analogie zu ihr funktioniert. Ihre Akteur*innen – Staaten, juristische Personen, natürliche Personen – erfüllen vielfältige Funktionen als Normunternehmer, Normanwender und Normdurchsetzer. Mit den Rechtfertigungsnarrativen werden technische Konsistenz und rechtlich-kulturelle Übereinstimmung bewertet. Die normative Ordnung des Internets ist durch Legitimationsbeziehungen mit nationalen und internationalen Rechtsordnungen verflochten.

Rules rule

Normen herrschen (vor). Eine normative Ordnung des Internets hat sich etabliert. Mit dem Recht als System sollen gemeinsame Werte realisiert, Autorität kontrolliert und grundlegende Güter und Rechte verteilt werden. Nur ein alle Akteur*innen in den Blick nehmender, für Regeln unterschiedlichster Art offener, ganzheitlicher und systematischer Ansatz zur normativen Ordnung im Internet kann zu gerechten Regeln in der (und über die) Digitalisierung führen. Diese Regeln schützen Rechte und Werte in der Strukturierung des

29 Zur Frage einer europäischen Strategie siehe auch den Beitrag von Tyson Barker in diesem Band.

Digitalen, legitimieren die Ausübung privater und öffentlicher Autorität und gewährleisten die gerechte Verteilung grundlegender Güter und Rechte, einschließlich des Internetzugangs.

Logiken der Technizität sind nicht zwingend beherrschend in normativen Debatten. Code ist Recht, indem er normativ ist, aber nicht Recht in dem Sinne, dass er Rechtsnormen verdrängt oder hierarchisch übergeordnet oder praktisch beherrschend ist. Code taucht nicht einfach auf, er wird in Prozessen geschrieben, die reguliert werden können, die an der normativen Ordnung des Internets gemessen werden können. *Protocols have politics* und Normen müssen konsequent auf ihre Entwicklung und Implementierung angewendet werden. Dieser Befund gilt für Algorithmen und algorithmische Entscheidungsfindung,³⁰ einschließlich Selektions- und Empfehlungslogiken, die klare Auswirkungen auf Rechte und Freiheiten haben, indem sie beispielsweise die Gestaltung und den Inhalt der informatorischen Diskursgrundlage beeinflussen, die für jede demokratische Gesellschaft in algorithmisierten Medienmärkten wesentlich ist.³¹

Digitalpolitik geht uns alle an. Die gesellschaftlichen Mehrwerte der Digitalisierung zu realisieren und die Risiken für individuelle Schutzgüter sowie für den gesellschaftlichen Zusammenhalt zu minimieren, ist die zentrale politische Aufgabe im Mehrebenensystem der Digitalisierung und ihrer Politik. Um die Zukunft gestalten zu können, müssen digitalisierungstheoretische und -praktische Erwägungen sowohl in die Wahl der Steuerungsinstrumente wie auch in das Objekt der Steuerung einfließen. Angesichts der Vielfalt möglicher Regulierungsebenen und -objekte ist es einfach, den Blick für das Wesentliche zu verlieren: den Schutz der Werte und Rechte. Digitalisierungsregulierung droht so zum Selbstzweck zu verkommen und ihren wichtigen Gestaltungsanspruch in dem Maße einzubüßen, in dem sie zunehmend diffundiert.

Wer glaubt, dass die Regulierung der Digitalisierung alle Probleme löst, hat weder Regulierung noch Digitalisierung noch die damit verbundenen Probleme verstanden. Wer Digitalisierungspolitik mit Sicherheitsagenden überfrachtet, wird sie zum Erstarren bringen; wer wiederum emanzipatorischen Freiheitshoffnungen folgend auf Utopien blickt, die durch Technologie realisiert werden sollen, läuft Gefahr, konkrete Probleme zu übersehen. Gera-

30 Siehe hierzu auch die Beiträge von Eric Hilgendorf und von Lorena Jaume-Palásí in diesem Band.

31 Siehe hierzu den Beitrag von Christian Stöcker in diesem Band.

de in Mehrebenensystemen mit einer Vielfalt an Akteur*innen und Normenformen muss Klarheit herrschen darüber, wer im Mittelpunkt zu stehen hat: der Mensch. Menschenrechte schützen, Menschenwürde sichern, menschliche Sicherheit wahren, menschliche Entwicklung fördern – das muss Gestaltungsziel der Digitalpolitik bleiben.

