

## Arbeitspapier

Arbeitspapiere sind Online-Veröffentlichungen der Forschungsgruppen.  
Sie durchlaufen kein förmliches Gutachterverfahren wie SWP-Studie,  
SWP-Aktuell und SWP-Zeitschriftenschau.

FORSCHUNGSGRUPPE EU / EUROPA | AP NR. 01, MÄRZ 2021

# Integrationspolitische Bedeutung des Digital Service Act (DSA) und Digital Markets Act (DMA)

Digitalmarktregulierung als eines von fünf digitalpolitischen Großprojekten der EU<sup>1</sup>

*Annegret Bendiek*

<sup>1</sup> Dieses Papier erschien als Schriftliche Stellungnahme für das deutsch-französische Fachgespräch des Europaausschusses des Deutschen Bundestages am 11.2.2021 (Ausschussdrucksache 19(21)135).

## **Inhalt**

<b>1</b>	<b>Das Problem: Öffentliche Räume in der Hand von Oligopolen</b>	<b>3</b>
<b>2</b>	<b>Europäische Re-Souveränisierung: 5 digitalpolitische Großprojekte der EU</b>	<b>6</b>
<b>3</b>	<b>DSA-E und DMA-E als ein integrationspolitisches Souveränitätsprojekt</b>	<b>8</b>
3.1	DSA-E und DMA-E sind komplementär (positive und negative Integration)	9
3.2	Plattformregulierung nach den Prinzipien der Rechtsgemeinschaft	10
<b>4</b>	<b>Umsetzungsschwierigkeiten</b>	<b>15</b>
4.1	Transatlantisches Konfliktpotential	15
4.2	Die soziale und ethische Herausforderung	17

# 1 Das Problem: Öffentliche Räume in der Hand von Oligopolen

Europa ist zum Schauplatz intensiver politischer und ökonomischer Auseinandersetzungen um seine Selbstbehauptung in der digitalen Welt geworden.<sup>2</sup> Die Allgegenwart US-amerikanischer Digitalkonzerne, die Abhängigkeit Europas von chinesischer Kommunikationstechnologie und die Einflussnahme Washingtons auf den Boykott von Huawei's 5G Technologie haben gerade in der globalen Pandemie deutlich gemacht, wie stark Europa von asiatischen Hard- und US-amerikanischen Softwareprodukten abhängig ist. Der bisherige Ansatz der EU gegenüber multinationalen Konzernen der Digitalwirtschaft wird derzeit grundsätzlich überdacht.<sup>3</sup> Mit einem globalen Marktanteil von Google in der Größenordnung von 80 Prozent aller Suchanfragen und einem Social Media-Marktanteil von 70 Prozent für Facebook und Youtube befinden wir uns inmitten eines beispiellosen Konzentrationsprozesses der kommunikativen Infrastrukturen der Demokratie.

Mit der zunehmenden Relevanz digitaler Öffentlichkeiten verlagert sich die Kommunikation in der Gesellschaft in Richtung eines marktorientierten Bereichs, in dem jeder Sprechakt seinen Preis hat. Öffentliche, digitale Diskursräume werden von privaten Unternehmen bereitgestellt und der Zugang zu ihnen wird entsprechend kontrolliert. Nur wer ein privates Vertragsverhältnis eingeht und seinen Beitrag entweder monetär oder in Form von wirtschaftlich nutzbaren Daten leistet, hat ein Nutzungs- bzw. Mitspracherecht. Eine bedingungslose demokratische Beteiligung, die nur an den Bürgerstatus gebunden ist, ist in diesen für Vermarktungszwecke entwickelten sozialen Netzwerken nicht vorgesehen.<sup>4</sup> Dies wäre in etwa vergleichbar mit einer Situation, in der nicht nur das Parlamentsgebäude im Besitz eines privaten Anbieters ist und der Zugang zu ihm nach wirtschaftlichen Kriterien geregelt wird, sondern auch die Lautstärke der Lautsprecher und die Übertragung von Reden nach außen marktgerecht bewertet werden. Diese Risiken für die Demokratie sind zuletzt mit der Sperrung des Twitter- und Facebook Accounts von @realDonaldTrump deutlich geworden.<sup>5</sup>

Da digitale Netzwerkeffekte wirken, also sinngemäß die großen Plattformen die kleinen verdrängen, kann man davon ausgehen, dass das Problem auch in anderen sozialen Bereichen zunehmen wird (z.B. beim Medienstreaming, digitaler Bildung). Die kartellrechtlichen Verfahren der Kommission gegen Google hängen seit Jahren in der Rechtsprechung, die Abhilfemaßnahmen im Fall von Google Search (Shopping) gelten als

<sup>2</sup> Als „digital“ lässt sich diese Selbstbehauptung insofern verstehen, als wir es heute in der Politik mit einer umfassenden algorithmischen Erfassung und Verarbeitung von Sachverhalten zu tun haben. Siehe hierzu ausführlicher: Armin Nassehi, *Muster: Theorie der digitalen Gesellschaft*, München: C.H. Beck Verlag, 2019.

<sup>3</sup> Florence Chédotal, »Thierry Breton, commissaire européen au Marché intérieur: «Pour l'Europe, c'est la fin de la naïveté»«, in: *L'Echo Républicain*, 25.1.2021.

<sup>4</sup> Annegret Bendiek et al., *Digitale Selbstbehauptung der EU*, Berlin: Stiftung Wissenschaft und Politik (SWP), August 2015 (SWP-Aktuell 2015/A 71); Annegret Bendiek/Matthias Schulze, *Desinformationen und Wahlen zum Europäischen Parlament*, Berlin: Stiftung Wissenschaft und Politik (SWP), Februar 2019 (SWP-Aktuell 2019/A 10), doi:10.18449/2019A10.

<sup>5</sup> Vgl. Christoph Schmutz/Daniel Steinvorth, »Die EU sagt der „digitalen Oligarchie“ den Kampf an«, in: *Neue Zürcher Zeitung*, 13.1.2021.

wenig hilfreich.<sup>6</sup> Die Übernahme von WhatsApp durch Facebook ist bereits von der EU-Kommission 2014 genehmigt worden. Facebook war in erster Linie ein Soziales Netzwerk. Der eigene Messenger Service war deutlich abgeschlagen hinter dem werbefreien und die Privatsphäre schonenden WhatsApp. Mittlerweile ist Facebook bei Kurznachrichtendiensten marktbeherrschend. Forscher fanden selbst am Wahltag in den USA Hunderttausende Facebook-Kommentare, die zu politisch motivierter Gewalt aufriefen. Entgegen des Konzerns wurden die Kontakt- und Nutzungsdaten von WhatsApp komplett ins Facebook-Ökosystem integriert, die Öffnung für (Wahl-)Werbung wurde umgesetzt.<sup>7</sup> Dieser Machtkonzentration werden die bisherigen Regulierungsansätze der EU, wie z.B. das Setzen auf freiwillige Selbstverpflichtungen, nicht gerecht. Der „Code of Practice“ wurde in Zivilgesellschaft, Wissenschaft, Medien und Fakt-Checkern eher kritisch bewertet. Im Rahmen der deutschen „Doxing-Affäre“ im Dezember 2018/Januar 2019 reagierte die online-Plattform Twitter trotz der Selbstverpflichtung des Codes nur schleppend. Der Sturm auf das Kapitol in Washington im Januar 2021 ist ein „Weckruf“ für Europa (Hohe Vertreter Josep Borrell).

Große Plattformenanbieter haben aufgrund von Netzwerkeffekten in Europa kaum Konkurrenz zu befürchten, so dass als verbleibendes Mittel entweder eine grundsätzliche Reform des Kartell- und Wettbewerbsrechts oder eine behutsame Fortentwicklung des Wettbewerbsrechts bleibt. Die bisherigen kartellrechtlichen Verfahren zu Bewertung und Kontrolle von Monopolen, etwas das Konzept des „consumer harm“ greifen oftmals zu kurz. Als zentrales Problem wird oftmals angeführt, dass die großen Firmen aufkeimende, kleinere Konkurrenz Start-ups regelmäßig vom Markt kaufen, bevor diese zu einer Bedrohung des Geschäftsmodells werden können (Killerakquisitionen). Der Einkauf von WhatsApp und Instagram durch Facebook sind hier exemplarisch. Ein effizienter und schon gar nicht fairer Wettbewerb ist in vielen Bereichen nicht mehr gegeben.

Die EU-Kommission mit der Vizepräsidentin Margarethe Vestager und dem Kommissar Thierry Breton hat mit dem Digital Service Act (DSA-E) und Digital Markets Act (DMA-E) am 15. Dezember 2020 zwei Verordnungsentwürfe zur Regulierung digitaler Dienste und digitaler Märkte veröffentlicht, „die vor allem die Gatekeeper des Internets ins Visier nehmen“<sup>8</sup>. Vieles aus der e-Commerce-Richtlinie wird in den Rang der Verordnung gehoben. DSA-E und DMA-E wollen stärkere Rechenschafts- und Sorgfaltspflichten über digitale Dienste und digitale Märkte einführen, um Transparenz in den Netzwerken zu erzwingen und Desinformation und Hetze zum Risikogeschäft werden zu lassen.<sup>9</sup> Als Verordnungen wären sie künftig unmittelbar in den Mitgliedstaaten anwendbar. Dieses Regulierungspaket wird in den Medien sehr positiv rezeptiert, weil mit dieser Neuordnung der Digitalwirtschaft in Europa und weltweit, Schaden an der Demokratie abgewendet werden kann.<sup>10</sup> Es soll die

<sup>6</sup> Vgl. Dennis Brouwer, »A non-discrimination principle for rankings in app stores«, in: *Internet Policy Review*, 9(2020)4; Dennis Brouwer, »Towards a ban of discriminatory rankings by digital gatekeepers? Reflections on the proposal for a Digital Market Act«, in: *Internet Policy Review*, 11.1.2021.

<sup>7</sup> Während der Präsidentschaftswahl vergangenen Jahres gab es zum ersten Mal (mit zeitlicher Beschränkung) ein Verbot von Wahlwerbung, siehe Oliver Bunte, »Facebook: Polit-Anzeigen für weiteren Monat ausgesetzt«, in: *Heise Online*, 12.11.2020, <<https://www.heise.de/news/Facebook-Polit-Anzeigen-fuer-weiteren-Monat-ausgesetzt-4957557.html>>.

<sup>8</sup> Rupprecht Podszun/Sarah Langenstein, »Gatekeeper im Visier«, in: *Legal Tribune Online*, 16.12.2020, <<https://www.lto.de/recht/hintergruende/h/eu-digital-wirtschaft-regulierung-plattformen-intermediaere-dsa-dma-kommission-datenschutz-kartellrecht/>>.

<sup>9</sup> Felix Karrrte, »Resilient gegen Trump und Twitter. Die EU-Gesetzesinitiative zu Tech-Konzernen stärkt Grundrechte und Gesellschaften«, in: *Der Tagesspiegel*, 13.1.2021, S. 6.

<sup>10</sup> Vgl. Guillaume Klossa, »Les média, premier pilier de la souveraineté numérique de l'Europe face aux GAFAs«, in: *Le Figaro*, 1.12.2020; Agieszal Kumor, »Digital Act: l'Europe veut limiter la toute-puissance des géants du numérique«, in: *RFI*, 15.12.2020; Jan Penfrat, »L'Europe a besoin de lois qui limitent le pouvoir des grandes entreprises du numérique sur nos vies«, in: *Le Monde*, 15.12.2020.

zentralen Spielregeln der Digitalwirtschaft neu bestimmen und es ist bei weitem nicht das einzige Gesetzespaket, um diesem Ziel näher zu kommen.

## 2 Europäische Re-Souveränisierung: 5 digitalpolitische Großprojekte der EU

Souveränität muss heute neu gedacht werden.<sup>11</sup> Sie kann weder bei der überholten Vorstellung von Volkssouveränität (*la volonté générale*), noch bei der rechtlichen Anforderung legaler Regelsetzungsautorität oder gar der von Carl Schmitt stammenden Vorgabe, letztlich Herrschaftsgewalt stehen bleiben. Souveränität ist heute angemessener als eine politische Mehrebenenpraxis in Europa zu verstehen. Der Europäischen Union kommt hier die delegierte Funktion zu, mitgliedstaatliche öffentliche und private Interessen zusammen zu bringen und in den einschlägigen internationalen Standardsetzungsgremien mit angemessenen Haftungs- und Sicherheitsvorkehrungen für die Plattformökonomie und sozialen Medien zu versehen. Unternehmensexpertise gilt es hier mit Konsumenteninteressen und ethischen Überlegungen im europäischen Gesamtinteresse zusammen zu bringen. Damit wären einzelstaatliche Regierungen überfordert. Europa, insbesondere Frankreich und Deutschland sind heute zunehmend weniger bereit, den Preis eines Verlusts über die Kontroll- und Steuerungsfähigkeit der europäischen Daseinsvorsorge und Demokratie zu bezahlen.

Die Globalisierung der europäischen Datenschutzbestimmungen, die Förderung einer rechtsstaatlich orientierten, vorsorgenden Technologie-Governance im Bereich der künstlichen Intelligenz, die Cloudentwicklung wie GAIA-X, das Cybersicherheitsgesetz und ihre neuen Zertifizierungsanforderungen für Hard-, Soft aber auch für die digitale Netzinfrastruktur wie 5G und das Screening von Auslandsinvestitionen in digitalen Schlüsseltechnologien sind deutliche Reaktionen, die in der aktuellen Kommission unter der Kommissionspräsidentin Ursula von der Leyen zur Schaffung technologischer Souveränität verwirklicht werden sollen.<sup>12</sup> Die deutsche Regierung hatte für ihre (Trio-)Ratspräsidentschaft das Ziel ausgesprochen, Europa „technologisch und digital souverän“ werden zu lassen.<sup>13</sup> 20 Prozent der Gelder des Aufbauprogramms Next Generation EU sollen in digitale Projekte fließen.<sup>14</sup>

Die französische Ratspräsidentschaft in 2022 mit der Zukunftskonferenz wird alle Maßnahmen der 5 digitalpolitischen Großprojekte mit konkreten Ergebnissen zu einem erfolgreichen Abschluss bringen müssen. Denn: In allen diesen Feldern geht es nicht nur um die ökonomisch motivierte Internationalisierung eigener Standards, sondern um die Aufrechterhaltung des europäischen Gesellschaftsmodells (*un nouveau contrat social*). Das Problem ist erkannt: Marktmacht ist aufs Engste mit politischer Gestaltung verbunden.

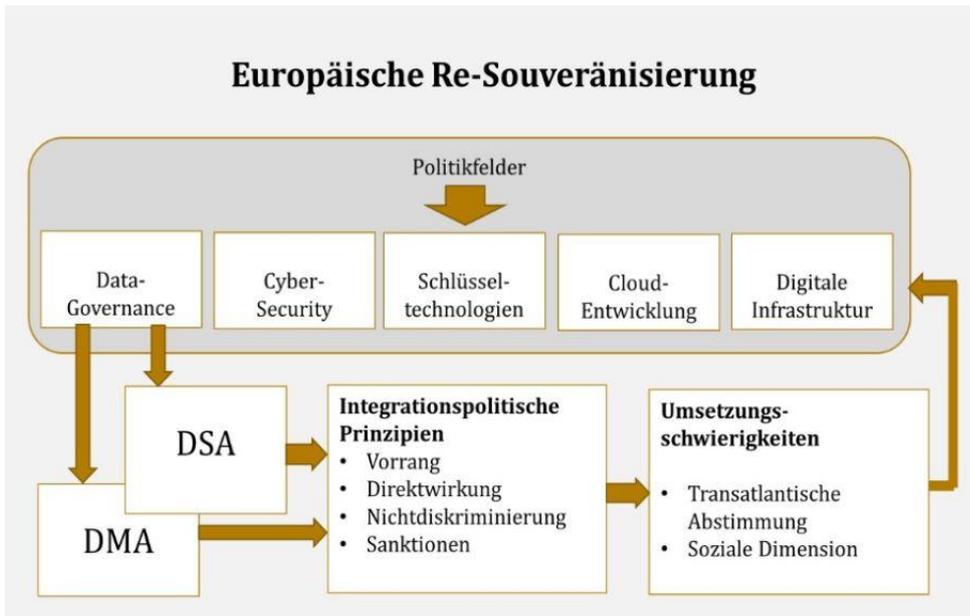
<sup>11</sup> Siehe auch aus französischer Perspektive Guillaume Klossa, »Pas de souveraineté numérique pour l'Europe sans souveraineté médiatique«, in: *Les Echos*, 29.12.2020.

<sup>12</sup> Siehe hierzu auch Ursula von der Leyen, *A Union that strives for more. My agenda for Europe. Political Guidelines for the next European Commission 2019-2024*, Brussels, 2019.

<sup>13</sup> „Das ist auch eine Priorität unserer deutschen EU-Ratspräsidentschaft. Wir brauchen eine eigene kluge und ambitionierte europäische Strategie des Digitalen, mit der wir Außen-, Wirtschafts- und Technologiepolitik konsequent zusammenbringen und ein starkes, souveränes und innovatives Europa schaffen“, siehe Auswärtiges Amt, »Europa muss digitale Macht sein. Staatsminister Michael Roth in der FAZ«, Berlin, 4.10.2020, <<https://www.auswaertiges-amt.de/de/newsroom/roth-faz/2402136>>.

<sup>14</sup> Ursula von der Leyen, »Wir müssen die Macht der Internetkonzerne demokratisch einhegen«, in: *Die Welt*, 28.1.2021.

Gesichtserkennungssoftware, Social Scoring und andere Überwachungsinstrumente werden bereits heute auf dem europäischen Markt für die Kontrolle und Unterdrückung von Dissidenz angeboten. Chinesische Infrastruktur impliziert die Möglichkeit chinesischer Einflussnahme. Mit US-amerikanischen Cloud- und Videokonferenzanbietern sind angelsächsische Vorstellungen von beschränkter Datenprivatheit verbunden. Der Kampf um die technologische Vorherrschaft sei insofern auch ein „Kampf der Narrative“ (Josep Borrell), in dem das europäische Gesellschaftsmodell selbst zur Disposition stünde. Um in diesem neuen Umfeld bestehen zu können, so der weit verbreitete Tenor, müsse Europa „digitale Souveränität“ entwickeln und wie eine geopolitische Macht denken.



### 3 DSA-E und DMA-E als ein integrationspolitisches Souveränitätsprojekt

Souverän ist, wer innerstaatliche private und öffentliche Meinungsbildungsprozesse zusammenführen und in europäischen und internationalen Gremien so artikulieren kann, dass das europäische Gesellschaftsmodell Bestand hat. Strittig ist eben, ob Binnenmarktpolitiken auf dieses Ziel hin ausgerichtet werden sollten. Die Proteste gegen Uploadfilter haben „einen Sinneswandel in Brüssel“<sup>15</sup> herbeigeführt, so Julia Reda. Digitale Souveränität bezieht sich nicht länger bloß auf einen rechtlich definierten Zustand, sondern muss auf die Moderationsfähigkeit der EU-Akteure bezogen werden, vertreten durch die EU-Kommission und den Ministerrat, ihre Positionierungen durch transparente interne Meinungsbildungsprozesse zu legitimieren und diese international effektiv auszuüben. Der Begriff der digitalen Souveränität ist analytisch hilfreich, bietet er Orientierungshilfe für die Skizzierung der Herausforderungen der digitalen Transformation und der Entwicklung europäischer Handlungsfähigkeit. Komplexe digitale Souveränität unterliegt einem korporatistischen Willensbildungsprozess und dafür hat die EU-Kommission seit Juni 2020 eine öffentliche Konsultation zum DSA-E eingeleitet, so dass bis zum 8.9.2020 Stellungnahmen eingebracht werden konnten. Diese Gesetze sind einem hohen Lobbydruck ausgesetzt. In der Top 5 der Unternehmen mit den höchsten Lobbyausgaben in Brüssel stehen laut Lobbycontrol Google, Microsoft und Facebook. Eine Koordination zwischen den Digitalministerien und parlamentarischen Ausschüssen wie am 11. Februar 2021 durch eine gemeinsame Sitzung der Europaausschüsse des Bundestags und der Assemblée Nationale praktiziert, ist eine wichtige Voraussetzung für den Willensbildungsprozess. Bis zum Inkrafttreten dieser Verordnungen wird es bis 2022 dauern. Dieser politische Prozess ist beispielgebend für andere digitalpolitische Vorhaben.

DSA-E und DMA-E sind ein Baustein der insgesamt 5 digitalpolitischen Großprojekte einer europäischen Re-Souveränisierung (Schaubild: Europäische Re-Souveränisierung). Als Unterbau sind bereits viele Einzelregelungen, vom Verbraucherrecht über das Immaterialgüterrecht bis zur Geoblocking-Verordnung in Kraft. Darüber hinaus gibt es eine „B2B-Plattformisierung“ und „Datafizierung“ in der Digitalwirtschaft, die auch traditionelle Industrieunternehmen umfasst, die aber nicht Gegenstand der DSA-E sind (Siehe unten Schaubild „Daten“).<sup>16</sup> Die EU-Kommission hat am 25.11.2020 eine Daten-Governance-Initiative vorgestellt.<sup>17</sup> 2021 soll dann der Data Act folgen. Wettbewerbs- und Datenschutzrecht konnten aber bisher die wachsende Marktmacht der Konzerne nicht zügeln. Mit den Rechtsakten DSA-E und DMA-E werden wie bei der Umsetzung der DSGVO politische Ressourcen supranational unter parlamentarischen Mitentscheidung

<sup>15</sup> Julia Reda, »Der Digital Service Act steht für einen Sinneswandel in Brüssel«, in: *Edit Policy*, 5.1.2021, <<https://www.heise.de/hintergrund/Edit-Policy-Der-Digital-Services-Act-steht-fuer-einen-Sinneswandel-in-Bruessel-5002121.html>>.

<sup>16</sup> Amtsblatt der Europäischen Union, *Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (Text von Bedeutung für den EWR)*, L 186/5, Brüssel, 11.7.2019,

<sup>17</sup> Europäische Kommission, *Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTES UND DES RATES über europäische Daten-Governance (Daten-Governance-Gesetz)*, COM(2020) 767 final, 2020/0340 (COD), Brüssel, 25.11.2020.

konzentriert, um das bloße Akkumulieren von zu vielen Daten in einer Hand zu unterbinden: „Ein Anti-Datendominanzgesetz, welches eine Entflechtung von zu großen Daten(blöcken) sicherstellt – selbst, wenn kein nachweisbar Marktmissbrauch vorliegt.“<sup>18</sup>

### **3.1 DSA-E und DMA-E sind komplementär (positive und negative Integration)**

DAS-E und DMA-E stehen komplementär zueinander, um inhaltliche und rechtliche Widersprüche möglichst zu vermeiden. Negative Integration bedeutet, dass Beschränkungen des freien Handels beseitigt werden. Sie wirken marktschaffend. Der DSA-E soll somit eine europaweit einheitliche Plattformregulierung schaffen, weil nationale Alleingänge wie das deutsche Netz-DG den europäischen Binnenmarkt immer weiter behindern, wenn sich Online-Plattformen an unterschiedliche teils widersprüchliche Regelwerke halten müssen. Haftung und Verantwortlichkeiten der digitalen Dienste sollen klarer und vor allem EU-weit einheitlicher geregelt werden.

Positive Integration bedeutet den Einsatz wirtschaftspolitischer und regulatorischer Kompetenzen auf EU-Ebene, um Marktergebnisse zu korrigieren und Marktversagen zu überwinden. Mit der Meldung und Löschung von illegalen Inhalten sollen demokratiepolitische Risiken vermieden und Grundrechte der Nutzer gewährleistet werden. Der DSA-E integriert aber auch negativ, da er Haftungsprivilegien begründet. Genauso dient der DMA-E einerseits der Bekämpfung von übermäßiger Marktmacht, andererseits der Etablierung von positiven Verhaltenspflichten.

Der DSA-E baut auf der e-Commerce-Richtlinie (2000/31/EG) auf, so dass der Verbraucherschutz, verbesserte Transparenz und Content-Fragen modernisiert und zur Datenschutz-Grundverordnung Ergänzungen vorgenommen werden.<sup>19</sup> Beim DSA-E soll ein modernes System der Zusammenarbeit bei der Compliance (Kontrolle und Durchsetzung) großer Plattformen Anwendung finden. Ergänzend soll der DMA-E die sogenannten Gatekeeper-Plattformen stärker schon im Vorfeld einer marktbeherrschenden Stellung in den Blick nehmen, um gleiche Wettbewerbsbedingungen auf den digitalen Märkten des Binnenmarkts zu schaffen. Hier zeigt EU-Recht sogar Wirkungen über den eigenen Markt hinaus, indem in die Geschäftsmodelle der großen internationalen Internetkonzerne hineinregiert wird, zumindest wenn sie sich mit ihren Dienstleistungen gezielt an Menschen in der EU richten. Die EU ist aufgrund der Größe des Binnenmarkts nicht nur ein wichtiger Ort der Regulierung, sondern gleichzeitig auch ein starker wirtschaftlicher Akteur mit einer globalen Ambition zur digitalen Selbstbehauptung, womit neue Konflikte im transatlantischen Datentransfer einhergehen können.<sup>20</sup>

Im EU-Parlament sei hiermit die Ambition verbunden, „die Verfassung des Internets auf eine moderne Basis zu stellen“. Erklärtes Ziel des DSA-E ist es, allen Menschen „die Ausübung der ihnen durch die Grundrechtecharta garantierten Rechte zu ermöglichen, insbesondere das Recht auf Meinungs- und Informationsfreiheit, unternehmerische Freiheit und Freiheit von Diskriminierung“. In Art. 1 des DSA-E definiert die Kommission ihr Vorhaben: Die Verordnung soll die Regeln für Intermediäre, also Online-Plattformen, die Vermittlungsleistungen erbringen vereinheitlichen, indem vor allem Ausnahmen von der Haftung, besondere Sorgfaltspflichten für bestimmte Plattformbetreiber und die

<sup>18</sup> Lucia Puttrich, »Wir können Google entflechten«, in: *Frankfurter Allgemeine Zeitung*, 10.12.2020.

<sup>19</sup> Siehe hierzu Laura Ziegler et al, »Digital Service Act (DSA) et Digital Markets Act (DMA): l'Europe vise une régulation équilibrée du Net«, in: *Edition Multimédi*, No. 248, 25.1.2021.

<sup>20</sup> Vgl. Dan Clark, »US General Counsel are watching as EU prepares for new data privacy laws«, in: *New York Law Journal*, 24.12.2020.

Durchsetzung geregelt werden. Kapitel II des Entwurfs definiert Haftungsfragen für digitale Dienste. Kapitel III des DSA-E enthält klar umrissene Sorgfaltspflichten, die einzuhalten sind. „Das Providerprivileg bleibt erhalten. Upload-Filter [...] soll es nicht geben. Dafür werden Notice-and-Action-Regeln für illegalen Content vorgesehen, aber auch viele andere Vorgaben, etwa zur Suspendierung von Nutzerkonten oder zur Transparenz bei der Werbung.“<sup>21</sup> Die Verordnungsentwürfe zielen auf große Tech-Konzerne als „very large online platforms“, indem ihre Marktmacht eingeengt werden soll. Konkret gemeint sind Plattformen mit mindestens 45 Mio. monatlich aktiven Nutzern in der EU und einer Marktkapitalisierung von 65 Milliarden (Art. 25 Abs. 1, DSA-E, Art. 3 Abs. 2 lit b DMA-E). Nur ein einziger europäischer Konzern - der deutsche Softwareentwickler SAP - erreicht diese Marktgröße. Der DMA-E ist die Antwort der Kommission auf eine faktische Machtlosigkeit gegenüber den Infrastrukturanbietern des Internets. Laut Art. 1 sollen die Regeln „contestable and fair markets“ im Digitalsektor sichern.

## 3.2 Plattformregulierung nach den Prinzipien der Rechtsgemeinschaft

Die Neuausrichtung des europäischen digitalen Binnenmarktes greift weit über einen bloßen Ordnungsrahmen für den Markt hinaus. Sie berührt wesentliche Grundrechte und hat hohe Relevanz für den Charakter der EU als einer demokratischen und freiheitlichen Ordnung. Die digitale Binnenmarktregulierung muss zusätzlich den Bedingungen des internationalen Wettbewerbs und der wachsenden Systemkonkurrenz mit China sowie den unterschiedlichen transatlantischen Regelungstraditionen Rechnung tragen. Bislang atmen die europäischen Regeln den Geist einer Zeit, in der Facebook nicht einmal gegründet war. Die Wettbewerbsregeln sind aus der Gründungszeit des europäischen Projekts, die e-commerce Richtlinie wurde 2000 verabschiedet.

Dass ein Update auch im Hinblick auf die Prinzipien der Rechtsgemeinschaft notwendig ist, ist unstrittig. Im Gegenteil: Die neuen Rechtsgrundlagen bestärken die Prinzipien der europäischen Rechtsgemeinschaft und stehen damit in einem direkten Zusammenhang zu dem Bemühen um eine Re-souveränisierung der EU. Diese sind u.a. der Vorrang und die Direktwirkung europäischen Rechts, das Prinzip der Nichtdiskriminierung sowie bindende Sanktionsmechanismen.

### 3.2.1 Vorrang und Direktwirkung

In der Kompetenzordnung steht Europarecht vor nationalem Recht. Mit der Zustimmung des Rats und dem Europäischen Parlament zu den beiden Verordnungen werden alle ihre Bestimmungen mit dem Inkrafttreten unmittelbar. Plattformen können sich dann nicht mehr nur auf nationales materielles Recht berufen, sondern müssen alle Inhalte löschen, die im Widerspruch zu europäischen Bestimmungen stehen.<sup>22</sup> Diese Vorgabe ist politisch durchaus brisant. Sie würde beispielsweise Plattformen dazu verpflichten, Inhalte von Politikern zu entfernen wenn diese offensichtliche Falschbehauptungen, Lügen oder Hate Speech enthalten, je nach mitgliedstaatlicher Rechtslage. Artikel 20 der DSA-E schreibt vor, dass ein Unternehmen wie Twitter<sup>23</sup> einen Account unter bestimmten Voraussetzungen

<sup>21</sup> Eine prägnante Zusammenfassung liefern hier Podszun/Langenstein, »Gatekeeper im Visier« [wie Fn. 8].

<sup>22</sup> Der DSA-E tritt an die Seite einer Vielzahl von Bestimmungen des EU-Rechts; zudem verdrängt er auch staatliches Recht nicht vollständig, vor allem was die materiellen Standards angeht. Siehe hierzu ausführlicher Prof. Dr. Martin Nettesheim, *Die unionsrechtliche Regulierung großer Internet-Plattformen. Die Kommissionentwürfe für einen Digital Market Act und einen Digital Service Act*, Stellungnahme für das deutsch-französische Fachgespräch des Europaausschusses des Deutschen Bundestages, Berlin, 11.2.2021.

<sup>23</sup> Siehe hierzu Karthe, »Resilient gegen Trump und Twitter« [wie Fn. 9].

„suspendieren“ muss, wenn der Nutzer „häufig offensichtlich illegale Inhalte bereitstellt“. Gemäß Artikel 21 müssen Online-Plattformen die Strafverfolgungsbehörden verständigen, wenn sie Verdacht auf eine „schwere Straftat“ schöpfen, die „das Leben oder die Sicherheit von Personen gefährdet“.

Brüssel könnte somit zu einer Kontrollinstanz für den politischen Raum in den Mitgliedstaaten werden. Zur Gewährleistung des Grundrechtsschutzes von Nutzern sieht die DSA-E vor, dass die jeweilige Plattform, die Inhalte entfernt oder Accounts suspendiert, ihre Handlung erklären und ein Beschwerdesystem einrichten muss. Der Fall kann schließlich zu einer unabhängigen außergerichtlichen Rekurs-Instanz weitergeleitet werden. Dort, wo sicherheitsrelevante Verordnungen zur Terrorismusbekämpfung bestehen, soll es auch künftig die Möglichkeit zu Uploadfiltern geben, auch wenn der DSA-E diese eigentlich ausschließt. Eine neue Verordnung soll Internetplattformen dazu verpflichten, terroristische Inhalte in weniger als einer Stunde nach einer behördlichen Anordnung zu löschen. Der Verordnungsentwurf geht ferner davon aus, dass diese Plattformen von Unternehmen betrieben werden, jedoch müssen nichtkommerzielle Projekte wie die Wikipedia diese Regeln ebenfalls umsetzen. Hier müssen Rat und Europäisches Parlament sicherstellen, dass gemeinnützige große Unternehmen eine besondere Berücksichtigung finden.

Die materielle Reichweite des DSA-E ist nicht auf politische Inhalte beschränkt, sondern umfasst ebenfalls Vorgaben für Kinderpornographie, Terrorismus oder andere strafrechtlich relevante Tatbestände. Das DSA-E ist damit insgesamt als eine Art „europäisches NetzDG“ zu verstehen, das zusätzlich um strengere Vorgaben für Werbung und einen einheitlichen Umgang mit illegalen Inhalten erweitert ist. Entgegen den Forderungen von Verbraucherschützern ist zwar kein generelles Verbot von Microtargeting, also personalisierter Werbung und Tracking, vorgesehen. Gleichwohl werden die Transparenzpflichten für Plattformen gestärkt, was Unternehmen direkt bindet und im Verbraucherinteresse ist:<sup>24</sup>

1. Hosting-Provider müssen ihre Sperr-Entscheidungen gegenüber den Nutzern begründen. In zentralen Datenbanken soll veröffentlicht werden, welche Begründungen hierfür herangezogen werden. Die EU hat hierfür die Lumen-Datenbank in den USA als Vorbild genommen um Transparenz für Journalismus und Wissenschaftsinteressen zu bewahren.
2. Online Marktplätze müssen die Identität aller Händler überprüfen und gegenüber Verbrauchern offenlegen. Bei Nichtoffenlegung dieser Informationen können Marktplätze ihr Haftungsprivileg verlieren und für Produktschäden haften.
3. Plattformen mit mehr als 45 Millionen monatlichen Nutzern in der EU müssen eine öffentliche Datenbank aller geschalteten Werbung inklusive deren Reichweite und Zielgruppen anbieten. Außerdem sollen diese Plattformen regelmäßige Risikoanalysen vorlegen, um Phänomenen wie Wahlmanipulation oder Desinformationskampagnen vorzubeugen. Verbraucher sollen darüber entscheiden können, ob sie Adressat von Empfehlungsalgorithmen sein wollen.

DMA-E steht im Gegensatz zum DSA-E in einem vergleichsweise liberalen ordnungspolitischen Kontext. Seine Kompetenzgrundlage ist nicht das von der Kommission ausgeübte Wettbewerbs-, sondern das stärker mitgliedstaatlich bestimmte Binnenmarktrecht, da eine Reihe von Mitgliedstaaten Bedenken haben, bei der Kontrolle großer Plattformen Kompetenzen an Brüssel abzugeben.

<sup>24</sup> Hierzu ausführlicher Reda, »Der Digital Service Act steht für einen Sinneswandel in Brüssel« [wie Fn. 15].

Das DMA-E ist gleichwohl nicht ohne Biss.<sup>25</sup> Zu den automatisch verbotenen, bußgeldbewehrten Praktiken gehört das Zusammenführen von personenbezogenen Daten von zwei Diensten, wenn dieses ohne ordentliches Einverständnis der Nutzer geschieht, auch wenn dahinter derselbe Gatekeeper steht.<sup>26</sup> Unternehmen sollen zudem die Wahlfreiheit garantiert bekommen, auf anderen Plattformen ihre Produkte oder Leistungen zu anderen Konditionen anzubieten. Eingriffe der EU in den Markt sollen nur dann erfolgen, wenn sie für die Funktionsweise eines freien Marktes unabdingbar sind. Das DMA-E steht damit neben dem europäischen und dem nationalem Kartellrecht, ohne diese abzulösen. Hiermit soll den unterschiedlichen marktwirtschaftlichen Traditionen der Mitgliedstaaten Rechnung getragen werden. In der politischen Praxis ist es gleichwohl nicht ausgeschlossen, dass die EU-Kommission das Bundeskartellamt und andere nationale Behörden mehr und mehr verdrängen wird.

Es bleibt abzuwarten, wie das Regulierungspaket mit dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. C DSGVO) vereinbar ist. Online-Plattformen sollen verpflichtet werden, einen umfassenden Zugang zu aufgebahrten Daten zu gewähren. So kann bspw. die Forschung auf Archive zurückgreifen dürfen, um Desinformationen und illegale Werbeinhalte zu untersuchen. Eine einheitliche Durchsetzung ist herausfordernd, da auch die bisherige Vollzugspraxis im Datenschutz sehr unterschiedlich in Deutschland, Frankreich oder Irland ist.

### 3.2.2 Nichtdiskriminierung

Nichtdiskriminierung beinhaltet in der Internet Governance der EU das Verbot jeglicher illegitimer Schlechterstellung nicht nur von öffentlichen, sondern auch von privaten Wettbewerbern.<sup>27</sup> Im DSA-E sollen alle Intermediäre, die User-Inhalte moderieren, diese Moderationsregeln und die Maßnahmen zu ihrer Durchsetzung künftig in ihren allgemeinen Geschäftsbedingungen öffentlich machen.

Das bedeutet, dass beispielsweise eine Rezeptplattform grundsätzlich auch weiterhin alle Uploads verhindern darf, die sich nicht auf Kochrezepte beziehen. Gleichzeitig muss sie allerdings offenlegen, wie sie den Begriff des Kochrezeptes operationalisiert. Alles das, was unter diesen Begriff subsumierbar ist, muss dann gleich („nicht-diskriminierend“) behandelt werden. Unklar ist das DSA-E bisher noch hinsichtlich der Frage, unter welchen Bedingungen Plattformen eigene Produkte hervorgehoben darstellen dürfen. Gleiches gilt für das Verhindern der Deinstallation von beim Kauf bereits installierter Software.

<sup>25</sup> Ebenfalls empfehlenswert »Das „Digital Services Act“-Paket - Europas Antwort auf die Macht der großen Tech-Konzerne?«, in: *Noerr*, 22.12.2020, <<https://www.noerr.com/de/newsroom/news/das-digital-services-act-paket>>.

<sup>26</sup> Eine Direktwirkung des EU-Rechts würde sehr interessant, wenn die Facebook-Entscheidung des Bundeskartellamts nun künftig auf EU-Ebene einheitlich geregelt wird. Demzufolge musste Facebook die Zusammenführung von Nutzerdaten stoppen. Facebook nutze seine Marktmacht aus, indem es seine Nutzer vor die Wahl stelle, entweder die Nutzungsbedingungen von Facebook zu akzeptieren und der Verwendung ihrer externen Daten zuzustimmen oder Facebook überhaupt nicht nutzen zu können (vgl. BGH setzt Facebook Grenzen für die Datennutzung). Zum GWB, dem deutschen Rechtsakt, siehe hierzu: Philipp Bongartz, »Happy New GWB!«, in: *D’Kart Blog*, 14.1.2021, <<https://www.d-kart.de/blog/2021/01/14/happy-new-gwb/>>.

<sup>27</sup> Nichtdiskriminierung meint “comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified“, in: *Open Internet Access Regulation*, recital 8.

Der DMA-E enthält ebenfalls einen kartellrechtlichen regulierungsrechtlichen Ansatz, die die EU-Kommission bereits im Juni 2020 zur Diskussion gestellt hat.<sup>28</sup> Das „New Competition Tool“ beinhaltet die Möglichkeit von Vorabkontrollen von Unternehmen.<sup>29</sup> Diese können nach Art. 3 DMA-E bereits dann greifen, wenn ein übergeordnetes Interesse an der „Entflechtung“ von Unternehmen besteht, die „core platform services“ bereitstellen, ohne dass auch bereits ein Verstoß gegen das Kartellrecht festgestellt werden konnte.

Die neuen Bestimmungen sehen ebenfalls vor, dass es Nutzern erlaubt sein soll, vorinstallierte Software-Anwendungen zu deinstallieren (vg. Art. 6 Abs. 1 lit.b und c DMA-E): „To enable end user choice, gatekeepers should not prevent end users from un-stalling any pre-installed software applications on its core platform service and thereby favour their own software applications“. Provider werden ebenfalls darauf verpflichtet, alternative App-Stores zuzulassen. Die Implikation dieser Regelung wäre, dass App-Stores in ihrer bisherigen exklusiven Form so nicht mehr zulässig wären, sondern für alle Anbieter geöffnet werden müssen, unabhängig von ihrer Vertragsbeziehung zu der jeweiligen Plattform.

Grundsätzlich gilt, dass die Adressaten des DMA-E alle sozialen Netzwerke, Suchmaschinen, Clouddienste, Videoplattformen, Betriebssysteme und Werbenetzwerke sind. Faktisch sind die Bestimmungen allerdings an außerordentliche anspruchsvolle Kriterien gekoppelt. Dazu gehören: erheblicher Einfluss auf den Binnenmarkt, die Rolle als Vermittler eines Gateways sowie eine gefestigte und dauerhafte Stellung, mit Kennzahlen wie 6,5 Milliarden Euro Jahresumsatz oder eine Marktkapitalisierung von 65 Milliarden Euro. Aktuell würden diese Kriterien wohl nur von vergleichsweise wenigen US-amerikanischen Anbietern erfüllen, während europäische Start-up Plattformen ausgenommen blieben. Die Regelungen sollen der EU die Möglichkeit geben, bereits ex ante gegen einen möglichen Missbrauch vorgehen zu können.

### 3.2.3 Compliance und Sanktionen

Die Durchsetzung der Verordnung (geregelt in Kapitel IV, DSA-E) obliegt grundsätzlich mitgliedstaatlichen Behörden. Kollektive Rechtsschutzmechanismen werden nur dann aktiviert, wenn die oben genannten Bestimmungen erfüllt sind. Zur Umsetzung des DSA-E ist zudem vorgesehen, dass die Mitgliedstaaten „Koordinatoren für digitale Dienste“ (Digital Services Coordinators, Art. 38ff DSA-E) ernennen, die die Durchsetzung der EU-Vorgaben überwachen und in einem gemeinsamen Ausschuss darauf achten sollen, dass die Durchsetzung der Bestimmungen einheitlich praktiziert wird. Die Mitgliedstaaten müssen bestenfalls einen Beauftragten für Verbraucherschutz benennen. Verfehlungen können zu Geldbußen führen. Die Höhe legt der Mitgliedstaat fest, sie dürfen aber die Höchstbeträge der Kommission nicht überschreiten. Zuständig ist das Land, wo der Intermediär seine Hauptniederlassung hat. Der Kommission soll bei Verfahren gegen große Plattformen ein Interventionsrecht haben, indem sie selbst Strafen verhängen kann. Als Hüterin der Verträge müssen ihr dazu genügend finanzielle und personelle Kompetenzen zur Verfügung gestellt werden.

Bei den Sanktionen sind im DSA-E Zahlungen von bis zu 6 Prozent und im DMA-E von bis zu 10 Prozent des gesamten weltweit erzielten Konzernjahresumsatzes möglich. Im Vergleich dazu sind in der DSGVO (Art. 83) nur Geldbußen von bis zu 4 Prozent des Konzernvorjahresumsatzes möglich. Der DMA-E sieht in letzter Konsequenz sogar den Ausschluss von Unternehmen aus dem europäischen Markt vor. Konzerne können ebenfalls

<sup>28</sup> Vgl. »Das „Digital Service Act“-Paket« [wie Fn. 25].

<sup>29</sup> Vgl. Europäische Kommission, »Impact Assessment for a possible New Competition Tool. Policy field«, <[https://ec.europa.eu/competition/consultations/2020\\_new\\_comp\\_tool/index\\_en.html](https://ec.europa.eu/competition/consultations/2020_new_comp_tool/index_en.html)>.

im Wiederholungsfall gezwungen werden, sich von einzelnen Geschäftsbereichen zu trennen.

Interessant dürfte in der Praxis das Notice-and-Take-down-Verfahren werden, also die Prozedur, über die Plattformen Informationen über etwaige illegale Inhalte auf ihren Diensten sammeln. Hosting-Provider müssen Systeme vorhalten, wo Nutzer mutmaßliche illegale Inhalte melden können. Ab einer gewissen Größe des Geschäftsmodells sind Beschwerdeverfahren gegen widerrechtliche Sperrungen vorzuhalten. Der DAS-E unterscheidet aber bislang nur unzureichend zwischen unterschiedlichen Arten von illegalen Inhalten. Verbraucherschützer sehen die Gefahr, dass eine Wiedereinführung von Uploadfiltern durch die Hintertür gegeben sei, weil die vollautomatische Sperrung von Inhalten erlaubt ist, solange die Plattform den Einsatz solcher Filtersysteme transparent macht.

## 4 Umsetzungsschwierigkeiten

### 4.1 Transatlantisches Konfliktpotential

Fragen der Regulierung von Daten in der EU gehen weit über die DSA-E und DMA-E hinaus und betreffen unmittelbar auch den Datentransfer zwischen Staaten und Wirtschaftsräumen. Der EuGH hat das Privacy Shield Abkommen über den ökonomischen Datentransfer mit den USA am 16.7. für ungültig erklärt.<sup>30</sup> Das Urteil hat nicht nur Folgen für die rund 6.000 Unternehmen, die aktuell unter diesem Datenschutz-Schild ihre Daten in die USA transferieren. Dieses Urteil hat ebenfalls Folgen für alle Unternehmen die unter den gängigen EU-Standardvertragsklauseln (SVV) arbeiten und Daten in Drittstaaten transferieren. Die EU-Kommission hat hierfür bisher gültige Musterverträge für die Datenübermittlung bereitgestellt. Verbraucheranwälte, Prozessfinanzierer und Legal-Tech Unternehmen erarbeiten Datenschutzklagen, dass auch die SVV nach ihrer Auffassung keine adäquate Rechtsgrundlage für Datenübertragungen darstellen können. Wenn es keine Lösungen für die SVV gibt, verlieren europäische und internationale Unternehmen ihre rechtmäßige Geschäftsgrundlage. Der wirtschaftliche Schaden wäre immens, die Unternehmen müssen ihre Dienste einstellen, die Entkoppelung von Wirtschaftsräumen sowie die Fragmentierung des Internets würden fortschreiten.

Eine ungleich größere Herausforderung stellen Datentransfers mit chinesischen Serviceanbietern wie Bytedance dar, die ihren Hauptsitz in China haben und der Kontrolle durch chinesische Sicherheitsbehörden unterliegen. Aber auch für diese Transfers gilt es Lösungen zu finden. Bytedance mit der Videoplattform Tiktok ist zwar keine klassische Sicherheitsbedrohung, aber es kann von einer nicht vorhandenen Komplementarität mit der DSGVO und dem europäischen Kinder- und Jugendschutz ausgegangen werden. Bytedance Tiktok arbeitet mit Gesichtserkennungssoftware und KI-Anwendungen, die in der EU nach noch ausstehender eingehender Prüfung nicht erlaubt sind. Die irische Datenschutzbehörde hat im Juni 2020 den Auftrag von Tiktok erhalten, die Datenverarbeitung zu prüfen und Lösungen vorzustellen. Die irische Datenschutzbehörde sieht sich damit aber überfordert. In Irland ist die Datenschutzbehörde auch gegen Facebook aktiv geworden.<sup>31</sup> Es erging die Aufforderung, keine Datentransfers gemäß den Standardvertragsklauseln mehr durchzuführen. Europäische Datenschutzbehörden arbeiten an Lösungsvorschlägen. Drei Lösungswege werden diskutiert:

1. Anpassung der Standardvertragsklauseln (SVV): Die EU-Kommission hatte beabsichtigt, die SSV im Jahr 2020 anzupassen und eine „broad toolbox“ für den Datenverkehr erarbeiten. Hierbei müssen Datenexporteur und Datenimporteur plausibel rechtfertigen, dass Daten nach der Datenschutz-Grundverordnung (DSGVO) verarbeitet werden. Hierfür können *appropriate supplementary measures* zu den SSV definiert werden. Aktuell behelfen sich die Unternehmen mit ad-hoc Risikoprüfungen, die auch dokumentiert werden. Teil einer solchen

<sup>30</sup> The ruling in the case »Data protection Commissioner v. Facebook Ireland and Maximilian Schrems«, 16.7.2020 (Case No. C-311/18); Vgl. weiter Björn Vollmuth, »Personal Data Transfer to the US and other non-EEA Countries«, in: *Mondaq Business briefing*, 14.9.2020; Sven Venzke- Caprarese/Dennis-Kenji Kipker, »Neusortierung des internationalen Datentransfers«, in: *Weser Kurier*, 1.9.2020; Commerce Department, »U.S. Surveillance Law Doesn't Threaten EU Privacy«, in: *Cybersecurity Policy Report*, 28.9.2020.

<sup>31</sup> Vgl. »Facebook's EU-US data transfer mechanisms 'cannot be used«, in: *EurActiv*, 10.9.2020.

Bewertung ist die Sensibilität der übermittelten Daten. Hier sind Prüfkriterien zu berücksichtigen: Sind die Daten interessant für ausländische Geheimdienste? Kann die Verschlüsselung von Daten ermöglicht werden? SSV können durch zusätzliche vertragliche Regelungen abgesichert werden, durch Informationspflichten und Sonderkündigungsrechte.

2. Transatlantische Abstimmung: Datenschützer wie Maximilian Schrems vertreten die Meinung, solange der US Surveillance Act die Europäische Grundrechtecharta aushebelt, gibt es keine Lösung. Europarat und Committee of Convention 109 Human Rights Organization plädieren für einen internationalen Vertrag mit Schutzklauseln. Problematisch ist Section 5 of the Federal Trade Commission Act (FTCA), der unfaire and deceptive Handelshemmnisse unterbinden soll und wofür es nunmehr eine Lösung geben müsse, so Reynders.<sup>32</sup> Der Regierungswechsel in den USA ermöglicht den Rückgriff auf den Exekutive Order, um den Foreign Intelligence Surveillance Act (FIISA) zu reformieren und einen Privacy Agreement Ombudsperson ernennen, so dass das gleiche Datenschutzniveau und die Möglichkeit der Rechtshilfe von Drittstaatsangehörigen in den USA und ebenbürtigen Datenschutzbestimmungen auf beiden Seiten des Atlantiks wieder möglich werden.
3. Datenlokalisierung in der EU: Tiktok, Facebook sind der Push für die europäische Cloudentwicklung und damit für die europäische Dateninfrastruktur Gaia-X.<sup>33</sup> Sie soll als internationale Vereinigung ohne Gewinnerzielungsabsicht nach belgischem Recht operieren. Zu den 22 Gründungsunternehmen zählen u.a. Atos, Dt. Telekom, Bosch, SAP etc. Teilnahme erfordert Akzeptanz von Leitlinien entsprechend der europäischen Verträge. Es verspricht eine KI-Anwendung, die den Kriterien wie Datensicherheit, Datenschutz oder ökologische Nachhaltigkeit berücksichtigt. Amerikanische und chinesische Unternehmen seien zwar auf dem Markt willkommen aber nicht bei der Gaia-X Initiative. Unternehmen wie Amazon Web Service taucht als Cloud-Provider in den Demos von Gaia-X auf. Das wirft wieder Fragen einer Ungleichbehandlung auf.

Die EU-Kommission versucht mit dem Digital Service Act durch die neu zu schaffende Aufsichtsbehörde für Verbraucherschutz europäische Datenschutzbehörden unter die Arme zu greifen. Aber nicht alle EU-Staaten ziehen an einem Strang: der Europäische Rechnungshof mahnte am 10. September 2020, dass 15 EU-Staaten die gleichzeitig Mitglieder der Belt-and-Road-Initiative sind, durch ihre jeweiligen bilateral ausgehandelten Verträge mit China gegen europäische Richtlinien handeln.

Will Europa „technologisch und digital souverän“ werden, müssen die Mitgliedstaaten die EU-Kommission unterstützen. Neue Spielregeln für das Netz sind eine Sache. Dadurch entstehen aber nicht automatisch europäische Wettbewerber, die mithalten können. Alle fünf digitalpolitischen Großprojekte sind wichtig und müssen parallel verwirklicht werden. So wird die Kommission im Frühjahr weitere wichtige Rechtsakte bspw. für KI-Systeme vorlegen.<sup>34</sup>

<sup>32</sup> Brookings Institution holds Webinar on EU-US Privacy Shield, 10.9.2020, Political Transcript; Vgl. Auch Samuel Stolton, »Don't expect new EU-US data transfer deal anytime soon, Reynders says«, in: *EurActiv*, 4.9.2020.

<sup>33</sup> Vgl. Timo Hoppe et al., »GAIA-X, Altmaiers Cloud wird europäisch«, in: *Handelsblatt*, 23.9.2020; Catherine Stupp, »Europe's Cloud Project Mandates Security, Privacy Compliance« in: *The Wall Street Journal*, 8.6.2020.

<sup>34</sup> Christine Lambrecht, »Wehrhaft gegen Algorithmen. Auch KI muss Menschenrechte achten. Was die künftigen EU-Regeln zu leisten haben«, in: *Der Tagesspiegel*, 18.12.2020.

## 4.2 Die soziale und ethische Herausforderung

Wenn Mitgliedstaaten versuchen die europäische Digital- und Technologiepolitik dafür zu nutzen, um eigene Abhängigkeiten zu reduzieren und das ‚Gleichgewicht des Schadens‘ in Richtung des Gegners zu verändern, um sich selbst größere Handlungsspielräume zu eröffnen,<sup>35</sup> dann beginnt ein Weg, der sich schon in der europäischen Politik als verhängnisvoll erwiesen hat. Nicht die Zerschlagung von Tech-Konzernen, die Abschottung und Autonomie, sondern bewusst gestaltete „strategische“ Interdependenz bzw. Offenheit wie es die EU-Kommission formuliert, muss das erklärte Ziel sein. Eine kluge Politik digitaler Souveränität identifiziert nicht nur gefährdete Bereiche von strategischer Bedeutung für Europas Daseinsvorsorge, sondern nutzt gleichzeitig auch die Gelegenheiten internationaler Arbeitsteilung im Rahmen einer weiter vertieften transnationalen Vernetzung vor allem aber nicht nur mit anderen großen Demokratien. Es muss die Einsicht einkehren, „dass europäische Nutzer und Unternehmen nicht automatisch davon profitieren, wenn man die Macht großer ausländischer Tech-Konzerne beschränkt.“<sup>36</sup> Umgekehrt gedacht: Die Globalisierung lässt sich in der digitalen Konstellation aus der Perspektive Chinas nur mit autoritären Mitteln und um den Preis der offenen Gesellschaft aufhalten. Diese Alternative zu einem Denken in den Begriffen einer europäischen Re-Souveränisierung wäre ein Rückfall in die internationale Fragmentierung und die innereuropäische nationalstaatliche Spaltung. Beides ist mit dem Versprechen Europas „Frieden durch Integration“ unvereinbar und würde entweder in eine technologische Dystopie führen oder den Rückfall Europas in einen digitalen und technologischen Stellungskrieg bedeuten. Für Europa kann das keine Option sein. Souveränität ist komplex und mehr Prozess als Status. Es liegt besonders an Deutschland und Frankreich, Vertrauen in uns als Europäer zu wecken und das digitale Europa dazu zu ermächtigen, seine Souveränität verantwortungsvoll und gemeinschaftlich, kontinuierlich neu herzustellen. Diese Rechtsakte werden von entscheidender Bedeutung dafür sein, ob die liberale Demokratie und die europäische Integration ihre Glaubwürdigkeit als probate Instrumente auf dem Weg zu einer inklusiven Wohlfahrtsgesellschaft in Europa behalten werden. Ihre Legitimität hängt davon ab, dass sie nicht nur Innovationen, sondern auch ein solides Maß an innerer sozialer Stabilität und gleichzeitig internationaler Offenheit liefern. Die hierfür notwendige interne Einigkeit hat in Europa zumindest zwei Vorbedingungen, die von der Digitalisierung direkt betroffen sind und sich als die soziale und die ethische Herausforderung der Digitalisierung beschreiben lassen. Datenschutz, Content-Moderation, Zertifizierung, ethische Richtlinien für die Verwendung von künstlicher Intelligenz und ökologische und faire Produktstandards sind von wesentlicher Bedeutung, um die globale Entwicklung anspruchsvoller digitaler Technologien im Einklang mit den politischen Werten und kulturellen Traditionen Europas zu halten. Sie sind eine notwendige Voraussetzung, um die soziale Akzeptanz einer potenziell disruptiven Technologie zu sichern. Diese Regulierungen sind aber nicht auf Europa beschränkt, sondern können auch weltweit Nachahmer finden und Geltung erlangen.

Die Plattformökonomie und damit verbundenem Aufstieg der künstlichen Intelligenz (KI) signalisiert eine neue große Transformation des Kapitalismus mit potentiell erheblichen sozialen Verwerfungen. Eine Studie des World Economic Forum (WEF) schätzt, dass bis 2025 die von Maschinen geleistete Arbeit von 29% auf über 50% steigen wird. In ähnlicher Weise schätzt das McKinsey Global Institute, dass etwa dreißig bis sechzig Prozent der Arbeitsplätze vollständig automatisiert werden können. Die KI lernt zunehmend,

<sup>35</sup> Vgl. Mark Leonard/ Jeremy Shapiro, *Strategic Sovereignty. How Europe Can Regain the Capacity To Act*, London: European Council on Foreign Relations (ECFR), 25.6.2019 (Policy Brief).

<sup>36</sup> Jenni Thier, »Big Tech misstrauen – nicht dem Markt. Neue EU-Regeln für digitale Plattformen«, in: *Neue Zürcher Zeitung*, 17.12.2020.

anspruchsvolle intellektuelle Aufgaben zu erfüllen, wie das Erkennen komplexer Muster, das Synthetisieren von Informationen, das Ziehen von Schlussfolgerungen und die Erstellung von Prognosen, von denen vor nicht allzu langer Zeit angenommen wurde, dass sie menschliche Kognition erfordern. Für den politischen Zusammenhalt der Mitgliedstaaten könnten derartige Entwicklungen verheerend wirken. Eine Gesellschaft, in der Menschen ökonomisch ‚überflüssig‘ werden, gerät schnell in Schwierigkeiten, den sozialen Zusammenhalt zu bewahren. Technische Innovationen wie die Blockchain und virtuelle Realitäten könnten es Unternehmen ermöglichen, sich der Regulierungsautorität auf allen Ebenen der Politik zu entziehen, Firmengewinne in Offshore-Oasen zu deponieren und demokratische Regulierungen wie in der DSA-E und DMA-E zu umgehen. Ein europäischer Wirtschaftsraum, in dem die ökonomischen Disparitäten in der Folge noch weiter zunehmen und Regierungen die Fähigkeit verlieren könnten, Umverteilung zu organisieren, würde schnell zu enormen politischen Fliehkräften führen. Nur ein soziales Europa wird seine Fähigkeit zur inneren Einigung aufrechterhalten können.

Dr. Annegret Bendiek ist  
Stellvertretende  
Forschungsgruppenleiterin  
der Forschungsgruppe  
EU/Europa.

© Stiftung Wissenschaft  
und Politik, 2021  
**Alle Rechte vorbehalten**

Das Arbeitspapier gibt die  
Auffassung des Autors bzw.  
der Autorin wieder.

**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](http://www.swp-berlin.org)  
[swp@swp-berlin.org](mailto:swp@swp-berlin.org)

doi: 10.18449/2021AP01