DIGITALKONZERNE AN DIE LEINE? WIE DIE HANDELSAGENDA DER EU DIE REGULIERUNG VON BIG TECH GEFÄHRDET

von Deborah James

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

Diese Studie wurde von der Fraktion The Left im Europäischen Parlament in Auftrag gegeben.

März 2023

Die Autorin dankt Bram Vranken, Cecilia Olivet, Cedric Leterme, Christina Colclough, Georgios Altintzis, Jane Kelsey, Kristina Irion, Léa Auffret, Maryant Fernandez, Parminder Jeet Singh, Penny Clarke, Rashmi Banga, Roland Kulke, Sanya Reid Smith, Theo Morrissey, Nicolas Strauch und anderen für ihre sorgfältige Analyse, ihre Anmerkungen und ihre Änderungsvorschläge. Die Verantwortung für alle Fehler und Lücken liegt bei der Autorin.

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

B-1047 Brussels, Belgium
+32 (0)2 283 23 01
left-communications@europarl.europa.eu
www.left.eu

VORWORT

Lehrer*innen, Ärzt*innen, Politiker*innen und Journalist*innen haben vor kurzem einen gemeinsamen Grund zur Besorgnis ausgemacht: ChatGPT. Sie alle entdeckten die potenziell schädlichen – und noch weithin unbekannten – Auswirkungen der sich schnell entwickelnden Technologien der künstlichen Intelligenz (KI).

Lehrer*innen haben Bedenken, dass Schüler*innen KI nutzen, um Aufsätze zu schreiben, die nicht als Plagiate erkannt werden können, was ihre analytische Entfaltung ernsthaft beeinträchtigen könnte. Ärzt*innen sind besorgt über Patient*innen, die einer über KI erstellten Diagnose Folge leisten, ohne dass diese fachärztlich bestätigt worden wäre. Politiker*innen befürchten, dass ChatGPT die wahre Substanz ehrlicher demokratischer Diskussionen in Frage stellen und ihren Dialog mit den Bürger*innen beeinträchtigen könnte, auch in Entscheidungsprozessen. Journalist*innen beobachten mit Sorge, dass mit KI erstellte Artikel als Journalismus präsentiert werden ohne jegliche Überprüfung der Richtigkeit oder der Quellen, was eine Zunahme von Fake News zur Folge haben könnte.

Alle weisen auf dieselben Fallstricke hin. Zum einen lernt KI, indem sie enorme Datenmengen aus dem Internet zieht, aber sie kann nicht zwischen Fakten und Fakes unterscheiden. Zum anderen sind die im Internet vorhandenen Daten inhärent rassistisch, geschlechtsspezifisch und klassenspezifisch voreingenommen, sodass das KI-System diese Voreingenommenheiten, auf die es sich stützt, wahrscheinlich reproduzieren und so bestehende Ungleichheiten verschärfen wird.

KI verbreitet sich wie ein Lauffeuer. Die Vorteile der KI sind zwar leichter zu erkennen, aber **die potenziellen Schäden von KI-Anwendungen sind noch nicht vollständig bekannt**, und es gibt auch noch keine ausreichenden Schutzmaßnahmen, um sie abzuwenden. Zurzeit sind Big-Tech-Unternehmen den Rechts- und Regulierungsvorschriften weit voraus und operieren in einem der am wenigsten regulierten Sektoren der Weltwirtschaft. **Die Regierungen haben begonnen, mögliche Risiken zu ermitteln, die sich aus dieser mangelnden Regulierung ergeben, und sind dabei, Lösungen zu entwickeln**. So treibt zum Beispiel die EU Rechtsvorschriften wie das Gesetz über digitale Dienste, das Gesetz über den digitalen Markt, das Datengesetz, das Daten-Governance-Gesetz und das Gesetz über künstliche Intelligenz voran, die alle darauf abzielen, die Macht von US-amerikanischen und chinesischen Unternehmen, die den Sektor dominieren, zu beschränken.

Dennoch sind die **Big-Tech-Unternehmen bestrebt, die Regulierungsbemühungen der Regierungen zu verhindern, um weiter Daten anzuhäufen. Eines der wirksamsten Instrumente, die ihnen zur Verfügung stehen, sind internationale Handelsabkommen**. Klauseln, die den freien Datenverkehr, das Verbot der Datenlokalisierung und die Geheimhaltung von Algorithmen vorschreiben, verschaffen multinationalen Unternehmen ein vollständiges Datenmonopol und nehmen Regierungen und anderen Akteuren der Gesellschaft jegliche Möglichkeit zur Aufsicht über Algorithmen und die Datennutzung.

Es scheint widersprüchlich, dass die EU einerseits Gesetze zur Regulierung der globalen Digitalwirtschaft und Big-Tech-Unternehmen erlässt und andererseits Handelsabkommen fördert, die den Einfluss von Big Tech gegen staatliche Regulierung zwangsläufig stärken.

Aufgrund dieses Widerspruchs wurde in der Fachwelt die Forderung laut, ein internationales Governance-System für die digitale Ökonomie zu entwickeln.[1] Hierfür könnte eine Kerngruppe von Nationen geschaffen werden, die neue Abkommen über digitalen Handel vorantreiben, um durch die Festlegung von Normen und Regeln ein vertrauenswürdiges digitales Umfeld zu fördern. Im Rahmen dieses Systems könnten auch grundlegende Kriterien auf der Grundlage gemeinsam vereinbarter

1 Peter F. Cowhey und Jonathon D. Aronson, „Digital DNA: disruption and the challenges for global governance", Oxford University Press, New York, 2017.

Werte entwickelt werden – im demokratischen Sinne, indem alle die Chance und das Recht erhalten, an der Entwicklung digitaler Ökonomien und deren Auswirkungen auf das tägliche Leben mitzuwirken.

Es wird zunehmend erkannt, dass digitale Technologien das Welthandelssystem verändern und die Grenzen zwischen den Sektoren unserer Makro- und Mikroökonomien verwischen, indem sie die Trennung zwischen traditionellen und neuen Wirtschaftszweigen aufbrechen. Vor diesem Hintergrund wird der Markt allein die entstehenden Konflikte und Auseinandersetzungen nicht lösen. Eine Governance der digitalen Wirtschaft ist erforderlich - in Zukunft und schon jetzt.

Shoshana Zuboff zufolge wird die digitalisierte Gesellschaft durch die Institutionalisierung einer „pathologischen" Teilung des Wissens definiert. Big-Tech-Unternehmen aus den USA und China erhalten Zugriff auf und verarbeiten immer mehr Informationen, die in ihre Entscheidungen über Einzelpersonen – und folglich – Gesellschaften einfließen.

Es ist notwendig, die Gestaltung von Regeln und Governance-Strukturen neu zu überdenken und einen globalen Prozess in Gang zu setzen, der den Bedürfnissen und Rechten der Bevölkerungen im globalen Süden Rechnung trägt und ihre Teilhabe an der Festlegung neuer Normen sicherstellt.

Die Wechselbeziehungen zwischen den neuen Gesetzesvorschlägen der EU für die Digitalwirtschaft und der aktuellen EU-Politik im Bereich des digitalen Handels sind nur in sehr geringem Maße untersucht worden. Vor diesem Hintergrund hat die Fraktion Die Linke im Europäischen Parlament diese Studie in Auftrag gegeben, um diesen Zusammenhang zu untersuchen und die möglichen Auswirkungen der EU-Abkommen über digitalen Handel auf die europäische Gesellschaft aufzuzeigen.

Wenngleich die vorläufigen Ergebnisse besorgniserregend sind, so hoffe ich doch, dass sie eine produktive Mitwirkung an der kollektiven Aufgabe der Neugestaltung der Handelsregeln und Governance-Strukturen der digitalen Ära bewirken. Die Feststellungen dieser Studie lassen auf einen Mangel an politischer Kohärenz schließen, da die EU demnach mit der einen Hand zunichtemacht, was sie mit der anderen tut.

Wir laden Abgeordnete, die Europäische Kommission, nationale Regulierungsbehörden, Aufsichtsbehörden, Wissenschaftskreise, Gewerkschaften und zivilgesellschaftliche Organisationen dazu ein, diese Studie zu lesen, und hoffen, dass er zur Festlegung neuer Normen und Vorschriften führen wird, die der gesamten Gesellschaft zugutekommen.

Helmut Scholz

INHALT

ZUSAMMENFASSUNG

In dieser Studie wird aufgezeigt, wie Big-Tech-Unternehmen versuchen, rechtsverbindliche und langfristige „Handelsabkommen" zu nutzen, um den Spielraum der Institutionen der Europäischen Union (EU) zur Regulierung ihrer Geschäftstätigkeit im öffentlichen Interesse zu begrenzen.

Die Digitalisierung ist der prägende wirtschaftliche Wandlungsprozess unserer Zeit. Der Nutzen für die Gesellschaft ist bekannt, aber die Schäden, die durch die Ausbreitung von Big Tech verursacht werden, werden erst allmählich erkannt. Die EU begreift allmählich die dringende Notwendigkeit, einige der gefährlichsten Praktiken von Big Tech einzudämmen. Das Gesetz über digitale Dienste (DSA), das Gesetz über den digitalen Markt (DMA) sowie das Datengesetz, das Daten-Governance-Gesetz (DGA) und das Gesetz über künstliche Intelligenz (KI-Verordnung) sind erste Schritte, um zu gewährleisten, dass der digitale Wirtschaftssektor denselben Bedingungen des Fairplay und des öffentlichen Interesses unterliegt wie die übrige Wirtschaft.

Dieselbe EU, die neue Gesetze zur Regelung der digitalen Wirtschaft vorantreibt, betreibt gleichzeitig eine Politik für den digitalen Handel, die die gegenwärtige und künftige Politikgestaltung im öffentlichen Interesse in der EU und darüber hinaus konterkariert und erheblich einschränken würde.

Über eine Reihe von bilateralen und regionalen Handelsabkommen versucht Big Tech, ein politisches Umfeld aufrechtzuerhalten, das die private Kontrolle von technologischen Ressourcen und Praktiken sowie von Daten zugunsten von übermäßigen Gewinnen begünstigt. Die Kontrolle von Daten – insbesondere die Möglichkeit zur grenzüberschreitenden Datenübermittlung – und die Geheimhaltung ihrer Algorithmen oder Quellcodes sind die wichtigsten Ziele von Big Tech in allen Abkommen über den „digitalen Handel".

Die EU hat Handelsabkommen mit einem eigenen Kapitel zum digitalen Handel mit Kanada, Singapur, Vietnam, Japan, Großbritannien, Mexiko, Chile, Mercosur und Neuseeland abgeschlossen. Sie verhandelt derzeit ferner über Kapitel zum digitalen Handel mit Indonesien, Australien, Indien, der Region des östlichen und südlichen Afrikas sowie plurilateral im Rahmen der Welthandelsorganisation (WTO).

Diese Untersuchung analysiert die gefährlichsten Klauseln in der EU-Agenda für den digitalen Handel („freier" Datenverkehr, Verbot der Datenlokalisierung und Geheimhaltung von Quellcode). Sie nenn **10 GRÜNDE, WARUM SIE DER EUROPÄISCHEN GESELLSCHAFT, DER GRÜNEN AGENDA EUROPAS UND DER DEMOKRATIE IM ALLGEMEINEN SCHADEN WIRD:**

1. DIE MÖGLICHKEITEN DER EU, DIE PROFITABELSTEN UNTERNEHMEN IN DER GESCHICHTE DER WELT ZU BESTEUERN, WÜRDEN DURCH DIE REGELN FÜR DIGITALEN HANDEL EINGESCHRÄNKT

Die Gewinne digitaler Unternehmen sind in den letzten Jahren aufgrund der starken Zunahme grenzüberschreitender digitaler Aktivitäten in die Höhe geschossen. Dennoch zahlen sie weiterhin extrem niedrige Steuern, auch in Europa. Ein Unternehmen wie Uber kann beispielsweise seine „höchste Wertschöpfung" problemlos aus dem Land seiner Geschäftstätigkeit in eine Steueroase wie Irland verlagern, wo laut seinen Angaben die Backend-Software und die Analysefunktionen bereitgestellt werden. Die Europäische Kommission schlug bereits im Jahr 2018 vor, die ungerechte Besteuerung der digitalen Wirtschaft zu verbessern. Im Jahr 2021 ist die EU dann dem im Rahmen der OECD verabschiedeten globalen Steuerabkommen beigetreten. Dennoch werden die Bemühungen der EU zur Besteuerung von Big Tech möglicherweise durch ihre eigene Politik im Bereich des digitalen Handels konterkariert.

Fast alle Handelsabkommen der EU mit digitalen Bestimmungen beinhalten ein Verbot von Zöllen auf elektronische Übertragungen. Das bedeutet, dass Importeure von Produkten wie Autos, Uhren und

landwirtschaftlichen Erzeugnissen zwar Zöllen oder Handelssteuern unterliegen, aber die Staaten auf elektronische Versionen derselben Waren – z. B. von Büchern, Filmen oder Musik – keine Steuern erheben dürfen. Ein zentrales Argument der Verfechter dieses Verbots lautet, dass es kleinen und mittleren Unternehmen (KMU) der EU im Bereich des digitalen Exports Vorteile bringt. Aber große Unternehmen mit Sitz in den USA, wie Apple (Musik), Netflix (Filme) und Amazon (Bücher), profitieren von dem Moratorium wesentlich stärker als alle KMU in der EU.

Es sind zudem nicht nur die direkten Steuern, die Big Tech durch Handelsabkommen zu verhindern sucht. Eine Bestimmung, die es den Regierungen untersagt, die lokale Vorhaltung einer Datenkopie zu verlangen, erschwert es den Regierungen, Steuern auf Unternehmensgewinne zu erheben. Steueroasen werden von Big Tech zunehmend als „Datenoasen" genutzt, um den staatlichen Zugriff auf Daten zu verhindern, die sonst steuerliche Auswirkungen haben könnten.

2. QUALITATIV HOCHWERTIGE, ZUGÄNGLICHE ÖFFENTLICHE DIENSTLEISTUNGEN WÜRDEN DURCH DIE KONTROLLE VON BIG TECH ÜBER DIE DIGITALISIERUNG VON DIENSTLEISTUNGEN BEEINTRÄCHTIGT

Die Aufrechterhaltung eines starken Sektors öffentlicher Dienstleistungen in Europa erfordert die Stärkung der Rechenschaftspflicht für Algorithmen und den Ausbau der digitalen Kompetenzen der Beschäftigten im öffentlichen Dienst. Sie setzt des Weiteren die Nutzung großer Datensätze durch den öffentlichen Sektor zur Verbesserung von Bildung, Gesundheit, Verkehr, Wasser- und Stromversorgung und anderen öffentlichen Dienstleistungen voraus. Die Digitalisierung öffentlicher Dienste ist häufig Gegenstand öffentlich-privater Partnerschaften mit Big-Tech-Unternehmen. Wenn die Datenerhebung im Bereich des öffentlichen Dienstes oder die Erbringung der Dienstleistung selbst privatisiert ist, gilt dies auch für die Daten. Um Daten für die Verbesserung öffentlicher Dienste zu erhalten, sollten die öffentlichen Dienste das Recht auf Zugang zu und Kontrolle der Daten behalten, die im Rahmen von Partnerschaften mit privaten Unternehmen erzeugt werden. Laut den vorgeschlagenen Regeln der EU für digitalen Handel, wonach es Staaten verboten ist, die Lokalisierung von Daten im Hoheitsgebiet der Vertragspartei zur Speicherung oder Verarbeitung zu verlangen, könnte die den Unternehmen auferlegte Offenlegung im Rahmen von Handelsabkommen angefochten werden.

3. DIE DATEN- UND VERBRAUCHERSCHUTZRECHTE VON EU-BÜRGER*INNEN KÖNNTEN DURCH DIE REGELN FÜR DIGITALEN HANDEL AUSGEHÖHLT WERDEN

Die im Jahr 2016 veröffentlichte bahnbrechende Datenschutz-Grundverordnung (DSGVO) setzte den globalen Standard für das Grundrecht auf Datenschutz und Datensicherheit. Neuere Handelsabkommen, wie die mit Großbritannien und Neuseeland, enthalten eine Klausel, die den Schutz personenbezogener Daten und der Privatsphäre gewährleisten soll. Es bestehen jedoch starke Zweifel daran, ob diese „Schutzklausel" die Privatsphäre wirklich schützt. Nach der Veröffentlichung des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich (HKA EU-VK) erklärte der Europäische Datenschutzbeauftragte (EDSB), dass das Handels- und Kooperationsabkommen Rechtsunsicherheit in Bezug auf die Position der EU zum Schutz personenbezogener Daten im Rahmen von Handelsabkommen schaffe und zu Konflikten mit dem EU-Rechtsrahmen für den Datenschutz führen könne.

4. DIE BESTREBUNGEN DER EUROPÄER, DIE RECHTE VON MINDERHEITEN GEGEN DISKRIMINIERUNG ZU GEWÄHRLEISTEN, WÜRDEN DURCH DIE REGELN FÜR DIGITALEN HANDEL UNTERGRABEN

Es gibt immer mehr Belege dafür, dass künstliche Intelligenz (KI) Diskriminierung verschlimmern und Schäden verursachen kann, sei es durch fehlerhafte Algorithmen, die auf der Grundlage früherer Ungleichbehandlungen bestimmte Muster „lernen", oder durch die Verschärfung von Ungleichheiten in den für das Training von KI verwendeten Datensätzen. Im Jahr 2019 veröffentlichte die Europäische Kommission ein Weißbuch zur Künstlichen Intelligenz, in dem anerkannt wurde, dass die zunehmende Verwendung von Algorithmen in Europa mit besonderen Risiken für die Grundrechte einhergeht, insbesondere das Recht auf Gleichstellung und Diskriminierungsfreiheit. Aus neueren Studien geht ferner hervor, dass Quellcodes und Algorithmen, die

miteinander verbunden sind und von sich selbst lernen (maschinelles Lernen), zu vielen unerwünschten Ergebnissen führen können, darunter Diskriminierung aufgrund von Einkommen, Hautfarbe und Geschlecht.

Nach den vorgeschlagenen Regeln für digitalen Handel ist es den Staaten jedoch untersagt, die Offenlegung von Quellcode zu verlangen. Sie sehen allerdings Ausnahmen vor, die die Offenlegung von Quellcode und Algorithmen gegenüber ersuchenden Justiz- oder Regulierungsbehörden zum Zwecke von Ermittlungen erlauben, was sich im Freihandelsabkommen zwischen der EU und Neuseeland ausdrücklich auch auf Diskriminierung und Voreingenommenheit bezieht. Auf der Konferenz der Gleichstellungsministerinnen und -minister Deutschlands wurde jedoch festgestellt, dass es aufgrund der Komplexität des Themas unrealistisch erscheine, dass die Betroffenen in der Lage sein würden, algorithmische Diskriminierung zu erkennen und zu verfolgen. Außerdem müssen Transparenz-Instrumente auch Betroffenen, Forschenden, kritischen Ingenieur*innen, Anwält*innen, Gewerkschaftsvertreter*innen und der breiten Öffentlichkeit zur Verfügung stehen – nicht nur den Regierungen. Wenn algorithmische Systeme das Grund- und Menschenrecht auf Diskriminierungsfreiheit verletzen könnten, müsste für KI-Systeme nachgewiesen werden, dass sie dies nicht tun – und zwar vor ihrer Einführung und nicht erst, wenn bereits Schaden angerichtet wurde.

5. DIE EU-AGENDA FÜR DEN GRÜNEN DEAL, DIE FÜR DIE SICHERUNG EINER LEBENSWERTEN ZUKUNFT ENTSCHEIDEND IST, WÜRDE DURCH DIE REGELN FÜR DIGITALEN HANDEL UNTERGRABEN

Der europäische Grüne Deal fördert neue technologische Innovationen für die Lösung der weltweiten Klimakrise. Doch damit der notwendige Wandel auf der ganzen Welt vollzogen werden kann, ist der Transfer klimaschonender Technologieinnovationen zur Gewährleistung ihrer globalen Nutzung erforderlich. Ein Verbot der Offenlegung von Quellcode und anderer Formen des Technologietransfers wird die Verwirklichung des Pariser Klimaschutzübereinkommens für viele Länder unmöglich machen.

Länder brauchen außerdem Steuereinnahmen (zum Beispiel aus der Besteuerung von Big Tech), um ihren Übergang zu finanzieren. Die Vorschläge von Big-Tech-Unternehmen zur Beschränkung der Möglichkeiten von Staaten, ihre Tätigkeiten zu besteuern, werden eine Reduzierung der hierfür erforderlichen Investitionen zur Folge haben. Die hochkonzentrierte und datenhungrige digitale Wirtschaft, die von Big Tech vorangetrieben wird, und die vorgeschlagenen Regeln für digitalen Handel laufen auch dem Kampf gegen die Erderwärmung radikal zuwider. Auf die digitale Wirtschaft entfallen 10 Prozent des weltweiten Stromverbrauchs und fast 4 Prozent der globalen CO2-Emissionen, fast doppelt so viel wie auf den Zivilluftverkehr. Nachhaltige Digitalisierung ist nicht mit riesigen digitalen Monopolen vereinbar, die auf eine immer weitergehende Erhebung, Speicherung und Verarbeitung von Daten auf globaler Ebene drängen.

6. DIE EU-AGENDA FÜR DEN DIGITALEN HANDEL WÜRDE DIE BEFUGNISSE DER POLITISCHEN ENTSCHEIDUNGSTRÄGER UND DER REGULIERUNGSBEHÖRDEN EINSCHRÄNKEN, DIE MARKT-DOMINANZ DER BIG-TECH-RIESEN EINZUDÄMMEN UND GLEICHE WETTBEWERBSBEDINGUNGEN DURCHZUSETZEN

Europäische Regulierungsbehörden und Gesetzgeber sind sich der negativen Auswirkungen der monopolistischen Praktiken und Macht von Big Tech inzwischen sehr bewusst. Europa führt weitreichende Durchsetzungsmaßnahmen durch, um die Marktdominanz von Big Tech einzuschränken und gleiche Rahmenbedingungen für einen fairen Wettbewerb zu schaffen, insbesondere für KMU. Bestimmte Regelungen in Abkommen über digitalen Handel, insbesondere die Vereinbarung über Computer- und verwandte Dienstleistungen (Understanding on Computer and Related Services, UCRS), Verbote der Offenlegungsanforderungen für Quellcode, Interoperabilitätsbestimmungen und Verbote von Anforderungen hinsichtlich der lokalen Präsenz könnten diese Bemühungen untergraben.

Die UCRS würde Unternehmen der digitalen Infrastruktur praktisch ungehinderten Zugang zu Ländern geben und Rechte garantieren, um dort mit sehr begrenzter Regulierung tätig zu sein. Länder, die der UCRS der EU zustimmen, gehen damit Verpflichtungen in Bezug auf den Marktzugang für Computersysteme, die Programmierung einschließlich von Quellcodes und Algorithmen, die Wartung von Computersystemen und Software sowie die

Verarbeitung und Speicherung von Daten ein. Dies würde sich aber auch auf solche Dienstleistungen beziehen, die noch gar nicht erfunden sind. Sie könnten den Umfang oder die Reichweite der Geschäftstätigkeit eines ausländischen Unternehmens nicht begrenzen. Die Anwendung offener Regelungen, die wettbewerbspolitische Abhilfemaßnahmen im Hinblick auf alle digitalen Dienste beschränken, würde den monopolistischen Praktiken von Big Tech Vorschub leisten.

Wettbewerbsfeindliche Praktiken unter Einsatz von Algorithmen sind im Online-Einzelhandel gang und gäbe, wo Unternehmen wie Amazon dafür sorgen, dass ihre Suchalgorithmen ihre eigenen Produkte oder Dienstleistungen gegenüber denen anderer Anbieter begünstigen. Die in den Regeln für digitalen Handel enthaltenen Ausnahmen werden nicht ausreichen, um diese Praktiken zu ändern. Diese Regeln setzen nach wie vor einen Verdacht voraus, da sie sich auf bestimmte Fälle beziehen, und können keine generelle Offenlegung verlangen – die Betroffenen müssen wissen, dass sie geschädigt werden, den Verdacht haben, dass dies mit dem Algorithmus zusammenhängt, und die Regulierungsbehörde davon überzeugen.

7. KLEINE UNTERNEHMEN IN DER EU WÜRDEN DURCH DIE EU REGELN FÜR DIGITALEN HANDEL STARK BENACHTEILIGT

Im Jahr 2021 waren 99,8 Prozent aller Unternehmen in der EU-27 im nichtfinanziellen Sektor der gewerblichen Wirtschaft KMU. Sie beschäftigten 83 Millionen Menschen. Die große Mehrheit der KMU in der EU, die Online-Handel betreiben, nutzen die Online-Plattformen von Big Tech, um die Verbraucher*innen zu erreichen. Im Hinblick darauf, wie ihre Produkte in den Suchergebnissen platziert oder auf sonstige Weise beworben werden, sind KMU von den Algorithmen der Plattformen abhängig. Unternehmen, die Big-Tech-Plattformen nutzen, haben keinen Zugang zu den Daten ihrer eigenen Kund*innen, die aus ihren eigenen Aktivitäten auf der Plattform des Gatekeepers resultieren, was ihre Konkurrenzfähigkeit auf einem fairen Markt zunichtemacht, wohingegen die Big-Tech-Plattform diese Daten für ihre eigenen Geschäftszwecke verwenden können. Bestimmungen für den digitalen Handel, die Staaten daran hindern, algorithmische Transparenz oder die lokale Speicherung von Datenkopien zu verlangen, schränken die Abhilfemöglichkeiten für solche Probleme ein.

Die europäischen Vorschläge im Rahmen von Handelsabkommen sehen außerdem vor, den Marktzugang für Computer- und verwandte Dienstleistungen vollständig zu liberalisieren, sodass Unternehmen der digitalen Infrastruktur praktisch ungehinderten Zugang zu Ländern haben und Rechte erhalten, um dort mit sehr begrenzter Regulierung tätig zu sein. Manche sehen darin zwar eine Chance, europäischen Unternehmen den Zugang zu ausländischen Märkten zu eröffnen, aber die in den USA ansässigen Big-Tech-Unternehmen werden ihre Dominanz dank ihrer Erstanbieter- und Größenvorteile wahrscheinlich eher festigen als die KMU. Vor diesem Hintergrund lässt sich ein Spielraum für den Schutz oder die Unterstützung europäischer KMU nur schwerlich erkennen.

8. DIE EU-AGENDA FÜR DIE DIGITALE INDUSTRIALISIERUNG WÜRDE UNTERGRABEN, WENN DIE BIG-TECH-RIESEN IHRE INTERESSEN IN ABKOMMEN ZUM DIGITALEN HANDEL FESTSCHREIBEN KÖNNEN

Die Strategie Europas für die digitale Industrialisierung stützt sich auf die Verbesserung des Zugangs zu Daten, die Entwicklung von Technologie und Infrastruktur und entsprechende Regulierung. Die Strategie für den digitalen Handel steht jedoch im Widerspruch zu den Zielen Europas. Ein Großteil der in Europa generierten Daten ist im Besitz von ausländischen Unternehmen. Europäische Fahrer*innen und Kurier*innen produzieren Daten für Uber und europäische Verbraucher*innen treffen Kaufentscheidungen auf Amazon, die die in den USA beheimateten Unternehmen dann für ihre eigenen Geschäftsstrategien nutzen. Digitale Regeln würden Regierungen daran hindern, Unternehmen zur Weitergabe oder lokalen Speicherung dieser Daten zu verpflichten. Infolgedessen werden die Möglichkeiten Europas eingeschränkt, auf die großen Datenbestände zuzugreifen, die für die Ausweitung der digitalen Industrialisierung erforderlich sind.

Die Schaffung digitaler Infrastrukturen, insbesondere von für das Cloud Computing genutzten Rechenzentren, ist von zentraler Bedeutung für die europäische Strategie für die digitale Industrialisierung. Derzeit kontrollieren US-amerikanische Unternehmen fast 72 Prozent des europäischen Cloud-Speicher-Markts. Frankreich und Deutschland fördern lokale Infrastrukturen für Rechenzentren, und die EU schlug die Schaffung einer europäischen Cloud im Rahmen der Initiative Gaia-X vor. Aber die Regeln der EU für

digitalen Handel bezüglich der Datenlokalisierung verbieten es den Staaten, zur Speicherung oder Verarbeitung die Nutzung von Rechenanlagen oder Netzwerkelementen im Gebiet der Vertragspartei zu verlangen. Wenn die EU nicht sicherstellen kann, dass in der EU befindliche Dateninfrastrukturen genutzt werden, werden Cloud-Betreiber wie Amazon, Google und Microsoft ihren Bedarf an Datenspeicherung und -verarbeitung in billigeren Datenparadiesen decken und nicht in Europa.

9. DIE DIGITALEN HANDELSREGELN WÜRDEN DIE FÄHIGKEIT DER EUROPÄISCHEN BEHÖRDEN UNTERGRABEN, DIE STABILITÄT DES FINANZSYSTEMS, DIGITALE INTEROPERABILITÄT SOWIE CYBERSICHERHEIT ETWA IM BEREICH DES „INTERNET DER DINGE" SICHERZUSTELLEN

Die Erhaltung des politischen Regulierungsspielraums ist von entscheidender Bedeutung für die Sicherstellung eines umfassenden Nutzens der Digitalisierung und die Gewährleistung europäischer Grundrechte im digitalen Raum. Die Regeln für digitalen Handel sind breit gefächert und umfassend. Regulierung im öffentlichen Interesse wäre mit nur wenigen, begrenzten Ausnahmen anfechtbar. Es ist unbedingt erforderlich, die Regulierungsfähigkeit unter Berücksichtigung der sich entwickelnden politischen und wirtschaftlichen Rahmenbedingungen zukunftssicher zu gestalten.

So könnten sich Regeln für digitalen Handel beispielsweise auf Finanzregelungen und die Cybersicherheit auswirken. Entscheidungen im Finanzsektor werden zunehmend von Algorithmen bestimmt, die der Regulierungsaufsicht und öffentlicher Kontrolle unterstellt werden müssen. Entscheidungen wie die, wem ein Kredit für ein Haus gewährt wird oder wer eine Versicherung auf der Grundlage von Kreditrisiken erhält, werden immer häufiger von Daten und Algorithmen getroffen. Die zunehmende Automatisierung von Börsenvorgängen bringt ebenfalls ein erhebliches Risiko für die finanzielle Stabilität mit sich. Trotz Ausnahmen für aufsichtsrechtliche Maßnahmen würden Handelsbestimmungen Regierungen daran hindern, die Offenlegung von Quellcodes zu verlangen, um die Sicherheit des Finanzsektors zu gewährleisten, und die für die Gewährleistung der finanziellen Sicherheit erforderliche Regulierungsaufsicht ausschließen.

Der Markt für das Internet der Dinge (IoT) für digital verbundene Geräte bereitet Fachleuten im Bereich der Cybersicherheit zunehmend Sorge. Europäische Regierungen weiten derzeit die Rechtsvorschriften zur Cybersicherheit auf IoT-Geräte aus, um sensible Daten (einschließlich Finanzdaten) und die Sicherheit der Verbraucher*innen zu schützen. Für die Regulierung der Cybersicherheit werden Standards wie die Zwei-Faktor-Authentifizierung (TFA) sowie die Offenlegung von Quellcode erforderlich sein, um hochriskante Algorithmen und Maßnahmen zur Cybersicherheit zu bewerten. Aber die von der EU im Rahmen der Regeln für digitalen Handel vorangetriebenen Bestimmungen würden Staaten die Möglichkeit nehmen, die notwendige Offenlegung von Quellcodes zu verlangen. Die Ausnahmen – unter anderem im jüngsten FHA zwischen der EU und Neuseeland – werden der enormen und dringenden Notwendigkeit verstärkter öffentlicher Aufsicht bei weitem nicht gerecht.

10. DAS KRÄFTEUNGLEICHGEWICHT ZWISCHEN DEN BIG-TECH-GIGANTEN UND BESCHÄFTIGTEN WÜRDE SICH NOCH WEITER ZU UNGUNSTEN DER ARBEITNEHMER*INNEN VERSCHIEBEN

Mit den Regelvorschlägen für digitalen Handel in Handelsabkommen versucht Big Tech, die Aufwärtsverteilung des Einkommens von der Arbeit zum Kapital weiter zu festigen. In Diskussionen über die Zukunft der Arbeit kann die Betonung von Umschulung und qualifikationsbasiertem technologischem Wachstum nützlich sein, sollte aber nicht vom eigentlichen Thema ablenken. Der wichtigste Aspekt bei der Festlegung, wer von einer erweiterten Nutzung von Technologien profitieren wird, ist das politische Umfeld, in dem die betreffende Technologie eingesetzt wird. Wenn den Beschäftigten ihre Grundrechte, ihre Freiheit und ihre Autonomie an digitalisierten Arbeitsplätzen nicht garantiert werden und wenn Beschäftigte nicht über die Verwaltung der von ihnen produzierten Daten mitbestimmen dürfen, sondern diese Daten stattdessen dem erhebenden Unternehmen „gehören" dürfen, wird sich das Kräftegleichgewicht auf Dauer zugunsten der Unternehmen verschieben. Über die Frage, ob Beschäftigte wirtschaftliche Rechte an den von ihnen mitproduzierten Daten haben sollten, wird derzeit diskutiert. Wenn datenbezogene Verpflichtungen in Handelsabkommen verankert werden, wird eine solche Möglichkeit ausgeschlossen, was wahrscheinlich zur dauerhaften

Unterdrückung der kollektiven Verhandlungsmacht der Beschäftigten im digitalen Zeitalter führen wird.

Big Tech übt in Europa hohen politischen Druck aus und es sieht so aus, als ob seine Lobbytätigkeit eine Agenda zur Deregulierung des Handels auf den Weg gebracht hat, von der in erster Linie Silicon Valley profitiert.

Es wäre falsch anzunehmen, dass mehr digitaler Handel mit Regeln für diesen Handel einhergehen muss. Handelsabkommen schränken per se die Rechte der Staaten zur Regulierung wirtschaftlichen Verhaltens ein. Regierungen sollten jedoch die Möglichkeit haben, Vorschriften zu erlassen, um Menschen- und Grundrechte in der digitalen Wirtschaft zu gewährleisten, die Nutzung von Daten und Digitalisierung zum Wohle der Allgemeinheit zu fördern und die digitale Industrialisierung voranzutreiben. Die EU muss sicherstellen, dass ihre Handelsabkommen nicht ihre Fähigkeit einschränken, Big Tech stärker zu regulieren, um Beschäftigte, Verbraucher*innen, KMU, Minderheiten, Nachhaltigkeit und Grundrechte im digitalen Umfeld zu schützen.

1.

EINLEITUNG: DIE EU-AGENDA FÜR DEN DIGITALEN HANDEL: WARUM IST SIE WICHTIG?

Die Digitalisierung ist der prägende wirtschaftliche Wandlungsprozess unserer Zeit. Der Nutzen für die Gesellschaft durch erhöhte digitale Effizienz und verbesserten Zugang ist wohlbekannt. Aber die Schäden, die der Gesellschaft durch die Ausweitung der Entscheidungsmacht von Big Tech über unser Leben als Beschäftigte, Verbraucher*innen, kleine Unternehmen und Bürger*innen sowie unseren Demokratien in ihrer Gesamtheit entstehen, werden nicht mehr übersehen.

Aus diesem Grund haben Regulierungsbehörden und Gesetzgeber in der EU einen langen Prozess eingeleitet, um im öffentlichen Interesse angemessene Aufsichtsmechanismen für die Tätigkeit der Big-Tech-Giganten und die digitale Ökonomie im Allgemeinen zu entwickeln.

Technologische Verbesserungen sind zwar begrüßenswert, aber das politische Umfeld, in dem die Technologien eingesetzt werden, bestimmt, wer gewinnt und wer auf lange Sicht das Nachsehen haben wird. Dieses politische Umfeld hängt von den Entscheidungen der Gesetzgeber und Regulierungsbehörden ab und nicht von einer unsichtbaren Macht, die schicksalhaft Gewinner und Verlierer schafft.

Bislang haben politische Entscheidungsträger zugelassen, dass Technologieunternehmen das Eindringen der Technologie in unsere Lebenswelt ohne vorherige Regulierung beschleunigen. Big Tech sind zwar die größten und mächtigsten Unternehmen der Weltgeschichte, aber auch die am wenigsten regulierten aller Sektoren.

Big-Tech-Unternehmen vertreten seit langem die These, dass Regulierung Innovation hemmt. Die heutige Realität sieht jedoch so aus, dass die größten und einflussreichsten Technologieunternehmen nicht als Innovatoren auftreten, sondern als Monopolisten, die Wettbewerb verhindern und Märkte dominieren wollen. Sie erreichen das mit einem Geschäftsmodell, dass sich auf die Massenüberwachung von Nutzer*innen stützt, indem sie Daten und Datenverarbeitung sowie digitale Infrastrukturen monopolisieren und die Technologienutzung durch ihre firmeneigenen Algorithmen kontrollieren.

Insbesondere sind sie bestrebt, die Produktion, die Erfassung und die Nutzung von Daten für den privaten Profit zu kommerzialisieren und zu kontrollieren, statt der Allgemeinheit die Möglichkeit zu geben, Digitalisierung und Daten für das gemeinsame soziale, ökologische und wirtschaftliche Wohl zu nutzen, und versuchen, die Geltung von Menschen- und Grundrechten und gemeinwohlorientierte Regulierung im Bereich der Technologie zu umgehen.

Gesetzgeber, Strafverfolgungsbehörden, Medien, Gewerkschaften, Interessenvertreter für digitale Rechte und die Gesellschaft als Ganzes haben eine substanzielle Debatte über die negativen Auswirkungen von Big-Tech-Unternehmen auf die Gesellschaft angestoßen. Insbesondere die EU hat diese Schäden erkannt und begonnen, neue Gesetze auf den Weg zu bringen, um einige der gefährlichsten Praktiken von Big Tech einzudämmen. Das Gesetz über digitale Dienste (DSA), das Gesetz über den digitalen Markt (DMA) sowie das Datengesetz, das Daten-Governance-Gesetz (DGA) und das Gesetz über künstliche Intelligenz (KI-Verordnung) sind erste Schritte, um zu gewährleisten, dass der digitale Wirtschaftssektor denselben Bedingungen des Fairplay und des öffentlichen Interesses unterliegt wie die übrige Wirtschaft.

Die großen Technologiekonzerne sehen diesem wachsenden Regulierungsinteresse nicht tatenlos zu. Sie unternehmen massive Anstrengungen, um den Umfang und den Geltungsbereich dieser neuen Rechtsvorschriften in der EU und weltweit zu begrenzen.

Ihr Lobbymaßnahmen sind zwar hinreichend bekannt, weniger bekannt ist hingegen, dass sie parallel dazu darauf hinarbeiten, jetzt und für alle Zeiten die Freiheit und die Verpflichtung des Gesetzgebers einzuschränken, sie im öffentlichen Interesse zu regulieren, indem sie Regierungen dazu bewegen, verbindliche internationale „Handelsabkommen" zu schaffen, die ihren Interessen dienen.

Unternehmen nutzen internationale „Handelsabkommen" für die Erreichung ihrer Ziele, da sie der Politikgestaltungsprozess sind, der am stärksten der Wirtschaft verpflichtet und am wenigsten offen für andere Interessengruppen ist (wie Gewerkschaften, Datenschützer, Antidiskriminierungsgruppen und andere). Sie sind rechtsverbindlich, anders als die Empfehlungen der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) oder die Erklärungen der G20. Big Tech nutzt Handelsabkommen auch gerne für die Festlegung von Vorgaben für die nationale Gesetzgebung, denn Länder können zwar ihre Regierungen ändern, aber es ist doch nahezu unmöglich, Handelsabkommen zu ändern, da sie auf zwischenstaatlicher Ebene ausgehandelte dauerhafte Verträge sind. Während sich „Handelsabkommen" früher auf Zölle konzentrierten, geht es heute in der überwiegenden Mehrheit der Bestimmungen um die Gewährung von Handelsrechten, die von Handelsunternehmen ausgeübt werden, während die Möglichkeiten der Staaten eingeschränkt werden, die betreffenden Unternehmen in den festgelegten Bereichen zu regulieren.

Konkret hat Big Tech die Europäische Kommission erfolgreich davon überzeugt, seine langfristigen Business-Ziele zur EU-Agenda für den digitalen Handel zu machen. Viele der Bestimmungen dieser Agenda wirken sich auf die Politikgestaltung in unzähligen, über den „Handel" hinausgehenden Bereichen aus, wie im Folgenden gezeigt werden soll.

Diese Agenda wird jedoch von Gesetzgebern, Medien oder der allgemeinen Öffentlichkeit kaum diskutiert oder durchblickt. Dennoch dient sie als Blaupause für die Bemühungen der EU, im Rahmen von bilateralen Vereinbarungen mit Zielländern sowie auf globaler Ebene im Rahmen der Welthandelsorganisation (WTO) Abkommen über „digitalen Handel" abzuschließen.

Diese „Handels"-Agenda steht in direktem Widerspruch zu den aktuellen Anstrengungen europäischer Entscheidungsträger und Gesetzgeber, Menschen- und Grundrechte im digitalen Umfeld zu wahren, von Big Tech verursachte Schäden einzudämmen und sicherzustellen, dass Technologien der gesamten Gesellschaft dienen. Angesichts des Erfordernisses, dass die Außenpolitik der EU mit ihren Grundsätzen, Dokumenten und bestehenden Rechtsvorschriften im Einklang stehen muss, ist es dringend notwendig, den Ansatz der EU für Abkommen über digitalen Handel grundlegend zu überdenken.

In den letzten fünf Jahren wurden von entwicklungspolitischen und wissenschaftlichen Akteur*innen ungeahnte entwicklungshemmende Auswirkungen der Bestimmungen dieser vorgeschlagenen Abkommen ermittelt. Dabei stehen vor allem die Bestimmungen im Fokus, die Unternehmen die grenzüberschreitende Datenübermittlung ermöglichen, während gleichzeitig den Staaten die Möglichkeit genommen wird, die Nutzung lokaler Datenserver oder die lokale Speicherung von Datenkopien vorzuschreiben. Kritiker*innen führen ins Feld, dass diese Bestimmungen Entwicklungsländern die Möglichkeit nehmen, die von Beschäftigten, Verbraucher*innen, Unternehmen und Angehörigen ihrer eigenen Staaten erzeugten Daten für ihre eigene Entwicklung zu nutzen, und daher die digitale Industrialisierung in Entwicklungsländern verhindern. Sie beanstanden, dass diese Bestimmungen stattdessen vor allem Big-Tech-Unternehmen in den USA dienen.[2] Sie schadeten daher den Beschäftigten und KMU und entmachteten die Gesetzgeber und Regulierungsbehörden in Entwicklungsländern.[3]

Entwicklungspolitische Organisationen und UN-Agenturen haben ferner dargelegt, dass Bestimmungen wie das Verbot für Regierungen, die Offenlegung von Quellcode zu verlangen, die Wissensakkumulation in Industrieländern auf Kosten des technologischen Fortschritts in den Entwicklungsländern begünstigen.[4] Außerdem

2 Rashmi Banga, 'Joint Statement Initiative on E-Commerce (JSI): Economic and Fiscal Implications for the South,' *UNCTAD* Research Paper No. 58 (February 2021), https://www.twn.my/announcement/UNCTAD%20Re%20Paper%2058_022021.pdf. See also UNCTAD DITC and DTL, 'What is at Stake for Developing Countries in Trade Negotiations on E-commerce?: The Case of the Joint Statement Initiative,' UNCTAD (2021), https://unctad.org/webflyer/what-stake-developing-countries-trade-negotiations-e-commerce; and Jane Kelsey, 'How a TPP-style E-commerce outcome in the WTO would endanger the development dimension of the GATS acquis (and Potentially the WTO)', Journal of International Economic Law 21, no. 2 (June 2018): 273-295, https://doi.org/10.1093/jiel/jgy024.

3 Renata Ávila Pinto, „Digital Sovereignty or Digital Colonialism? New Tensions of Privacy, Security and National Policies", Sur *International Journal on Human Rights 15, Nr. 27* (Juli 2018): 15-27, https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-renata-avila-pinto.pdf

4 Rashmi Banga und Richard Kozul-Wright, „South-South Digital Cooperation for Industrialization: A Regional Integration Agenda", *UNCTAD* (April 2018), https://unctad.org/system/files/official-document/gdsecidc2018d1_en.pdf.

wurden Bedenken im Hinblick auf Probleme bezüglich der Geheimhaltung von Quellcode erhoben, die zur Aushöhlung der Demokratie führen, z. B. in Bezug auf die Fähigkeit böswilliger Akteure, die Algorithmen von Facebook zu nutzen, um die Ergebnisse zahlreicher Wahlen in unzulässiger Weise zu beeinflussen.[5]

Weniger beachtet wird die Tatsache, dass viele dieser Bestimmungen über „Handel" enorme negative Auswirkungen auf Beschäftigte, Verbraucher*innen, Staatsbürger*innen und Regierungen innerhalb Europas haben würden.

Diese vorläufige Studie soll daher ein Schlaglicht auf die EU-Agenda für den digitalen Handel und ihre potenziellen Auswirkungen auf die europäische Gesellschaft werfen, insbesondere im Hinblick auf die jüngsten regulatorischen Vorgaben des neuen Gesetzespakets für die digitale Wirtschaft.

5 Sanya Reid Smith, „Some Preliminary Implications of WTO Source Code Proposal", *Third World Network* WTO MC11 Briefing Paper (Dezember 2017), https://www.twn.my/MC11/briefings/BP4.pdf und Banga, „JSI on E-Commerce", UNCTAD (2021).

2.

DIE EU-ABKOMMEN ÜBER DIGITALEN HANDEL

Die USA haben einen Top-Lobbyisten aus dem Bereich Big Tech mit der Gestaltung ihrer digitalen Handelspolitik beauftragt. Daraufhin brachten sie im Jahr 2016 die ersten Vorschläge zum digitalen Handel in die WTO ein, die weitgehend der Wunschliste der Unternehmen entsprachen. Die EU zog nach. Die EU und die USA scheiterten mit ihrem Versuch, die WTO-Mitglieder generell zu überzeugen, auf dem Ministertreffen in Buenos Aires im Dezember 2017 neue Verhandlungen über den digitalen Handel einzuleiten, gaben aber später ihre Absicht bekannt, dies trotzdem zu tun.[6]

Im März 2019 nahmen weniger als die Hälfte der WTO-Mitglieder untereinander „plurilaterale" Verhandlungen über den digitalen Handel auf.[7] Die EU ist ein aktiver Teilnehmer und hat mehrere Vorschläge vorgelegt.[8] Die Verhandlungen werden in enger Abstimmung mit den Lobbygruppen der Wirtschaft auf regelmäßiger Basis fortgesetzt.[9] Entgegen der WTO-Praxis werden die Verhandlungstexte geheim gehalten, aber Textentwürfe sind durchgesickert.[10] Die Verhandlungen werden mit Blick auf die nächste WTO-Ministerkonferenz, die im Februar 2024 anberaumt ist, beschleunigt.[11]

Parallel dazu hat die EU ihre Politik im Bereich des digitalen Handels[12] über eine Reihe von bilateralen und regionalen Verträgen und Verhandlungen vorangetrieben.[13]

Die EU hat Handelsabkommen mit einem eigenen Kapitel zum digitalen Handel mit Kanada, Singapur, Vietnam, Japan, Großbritannien, Mexiko, Chile, Mercosur und Neuseeland abgeschlossen. Von diesen sind bislang nur die ersten fünf in Kraft getreten.

In wissenschaftlichen Untersuchungen wurde festgestellt, dass die EU-Bestimmungen für den digitalen Handel sich im Laufe der Zeit erweitert haben.[14] Anfangs bestand die digitale Agenda im Wesentlichen aus einem Moratorium für Zölle auf elektronische Übertragungen. Ab dem Jahr 2016 wurden immer mehr regulatorische Aspekte aufgenommen, darunter Bestimmungen zur grenzüberschreitenden Datenübermittlung und Quellcodes,[15] die ein wesentlicher Bestandteil von algorithmischen Systemen sind.[16]

Die EU verhandelt derzeit bilateral über Handelsabkommen mit einem eigenen Kapitel zum

6 Craig Silverman, Ryan Mac und Pranav Dixit, „I Have Blood on My Hands: A Whistleblower Says Facebook Ignored Global Political Manipulation", BuzzFeed News (September 2020), https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo.

7 Kelsey, „How a TPP-Style E-commerce Outcome in WTO…", Journal of IntlEcon Law (2018).

8 Dieses Unterfangen steht in Anbetracht der multilateralen Struktur der WTO auf einer wackeligen Rechtsgrundlage. Siehe Jane Kelsey, „The Illegitimacy of Joint Statement Initiatives and Their Systemic Implications for the WTO", *Journal of International Economic Law 25*, Nr. 1 (März 2022): 2– 24, https://doi.org/10.1093/jiel/jgac004.

9 Siehe den Vorschlag der EU im Rahmen der Joint Statement Initiative (JSI) on E-Commerce, EU-Delegation, „Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce (Document # 19-2880)", WTO INF/ECOM/22 (April 2019), https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=253794,253801,253802,253751,253696,253697,253698,253699,253560,252791&CurrentCatalogueIdIndex=6&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.

10 „WTO Electronic Commerce Negotiations: Updated Consolidated Negotiating Text – September 2021", WTO INF/ECON/62/Rev.2 (September 2021), https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text_september_2021.pdf.

11 Welthandelsorganisation (WTO), „E-commerce talks resume following summer break, Mauritius joins the initiative", WTO-Pressemitteilung, (September 2022), https://www.wto.org/english/news_e/news22_e/ecom_16sep22_e.htm.

12 Europäische Kommission, Generaldirektion Handel, „Mitteilung: Überprüfung der Handelspolitik – Eine offene, nachhaltige und entschlossene Handelspolitik", Europäische Kommission COM/2021/66 final (Februar 2021), https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM:2021:66:FIN. Siehe auch Europäische Kommission, „Gestaltung der digitalen Zukunft Europas", EU-Flyer (Februar 2020): Abschnitt 3, https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278 und Europäische Kommission, „Mitteilung: Digitaler Kompass 2030: der europäische Weg in die digitale Dekade", Europäische Kommission COM/2021/118 final (März 2021), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

13 Sofia Scasserra und Carolina Martínez Elebi, „Digital Colonialism: Analysis of Europe's trade agenda", TransNational Institute (Oktober 2021), https://www.tni.org/en/publication/digital-colonialism.

14 Michele Fink, „Legal analysis of international trade law and digital trade", Briefing des Europäischen Parlaments PE 603.517, angefordert vom Ausschuss für internationalen Handel (INTA) (November 2020), https://op.europa.eu/en/publication-detail/-/publication/18173e33-2954-11eb-9d7e-01aa75ed71a1/language-en/format-PDF/source-172804686.

15 Pierre Sauvé und Marta Soprana, „Chapter 11 The Evolution of the EU Digital Trade Policy", in *Law and Practice of the Common Commercial Policy. The first 10 years after the Treaty of Lisbon* (Leiden: Brill | Nijhoff, Dezember 2020): 290, https://doi.org/10.1163/9789004393417_013; Scasserra und Elebi, „Digital Colonialism: Europe's trade agenda", TransNational Institute (2021).

16 Dorobantu et al. schreibt: "Als Quellcode werden die von Programmierern geschriebenen Codezeilen bezeichnet, mit denen eine Maschine angewiesen wird, eine bestimmte Aufgabe auszuführen. Quellcode wird in der Regel in einer Textdatei geschrieben, ist für Menschen lesbar und verwendet eine Programmiersprache", und: „Codestücke, die eine Reihe von Schritten enthalten, die zur Lösung eines Rechenproblems befolgt werden müssen, werden oft als Algorithmen bezeichnet". Cosmina Dorobantu, Florian Ostmann und Christina Hitrova, „Source code disclosure: A primer for trade negotiators", in Addressing Impediments to Digital Trade (London: CEPR Press, April 2021): 105-140, https://ssrn.com/abstract=3877039.

digitalen Handel mit Indonesien, Australien, Indien, der Region des östlichen und südlichen Afrikas sowie plurilateral im Rahmen der Welthandelsorganisation (WTO). [17]

Darüber hinaus wird die EU demnächst Verhandlungen über digitale Partnerschaften mit Singapur und Südkorea aufnehmen.[18] Im Oktober 2022 trat sie mit Japan in Verhandlungen über die Aufnahme von Bestimmungen zur grenzüberschreitenden Datenübermittlung in das Kapitel über digitalen Handel ein, ein Thema, das aus dem im Jahr 2018 unterzeichneten Vertrag ausgeklammert war.[19]

17 Europäische Kommission, „Overview of FTA and other Trade Negotiations", Entwurfsfassung der Kommission 1.15 (Januar 2023), https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/a7aab8e0-085d-4e36-826f-cbe8e913cf13/details, Europäische Kommission, „Overview of Economic Partnership Agreements", Entwurfsfassung der Kommission 1.9 (Januar 2023), https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/10ca1b54-d672-430b-aed4-8b25b4b9c2ee/details.

18 Europäische Kommission, „Overview of FTA and other Trade Negotiations" (Januar 2023).

19 Europäische Kommission, Generaldirektion Handel, „EU and Japan start negotiations to include rules on cross-border data flows in their Economic Partnership Agreement", European Commission Trade News (Oktober 2022), https://policy.trade.ec.europa.eu/news/eu-and-japan-start-negotiations-include-rules-cross-border-data-flows-their-economic-partnership-2022-10-07_de.

3.

DIE GEFÄHRLICHSTEN EU-REGELN FÜR DIGITALEN HANDEL: DATENVERKEHR, DATEN-LOKALISIERUNG UND GEHEIMHALTUNG VON QUELLCODEE

Frühe Abkommen zum digitalen Handel konzentrierten sich im Wesentlichen auf Handelssteuern und zielten darauf ab, Staaten die Möglichkeit zu nehmen, Zölle auf elektronische Übertragungen zu erheben. Es gibt in der WTO keine Übereinkunft darüber, was eine elektronische Übermittlung ist,[20] aber in einer WTO-Mitteilung aus dem Jahr 2016 wurden digitalisierte Filme, Musik, Druckerzeugnisse, Computer-Software und Videospiele aufgeführt.[21] Andere haben versucht, dies auf digitale Dienstleistungen auszuweiten.[22]

Die neueren Abkommen der EU gehen jedoch weit über traditionelle Handelsaspekte hinaus. Im Mittelpunkt der neuen Agenda steht der Wunsch von Big-Tech-Unternehmen, Daten zu monopolisieren und ihre Nutzung zu kontrollieren. Die Kontrolle von Daten – insbesondere die Möglichkeit zur grenzüberschreitenden Datenübermittlung – und die Geheimhaltung ihrer Algorithmen oder Quellcodes sind die vorrangigen Ziele von Big Tech in allen Abkommen über den „digitalen Handel".

Der Einsatz von künstlicher Intelligenz (KI) hat in den letzten Jahren exponentiell zugenommen. KI beinhaltet die Verwendung großer Datensätze, um Computer zu trainieren, Entscheidungen zu treffen. Computer treffen die Entscheidungen auf der Grundlage der ihnen übermittelten Daten, basierend auf den Anweisungen der Algorithmen, die wiederum auf Quellcodes basieren. Größere Datensätze erweitern die Möglichkeiten von Unternehmen, Computer für die Nutzung der algorithmischen Systeme zur Erzielung weitaus genauerer Ergebnisse zu trainieren. Das Unternehmen, das eine Branche in Zukunft dominieren wird, ist also dasjenige, das den größten Zugang zu riesigen Datenmengen und die Fähigkeit hat, sie zu verwalten, und gleichzeitig über firmeneigene Algorithmen verfügt, die maximalen Gewinn erzeugen.

Der weltweite Markt für KI wurde im Jahr 2020 auf 35 Milliarden Euro beziffert. Diese Zahl sollte bis 2021 auf 45,5 Milliarden Euro steigen und bis 2028 die schwindelerregende Summe von 349 Milliarden Euro erreichen, mit einer jährlichen Wachstumsrate von 33,6 Prozent.[23] In den USA wurden von November 2016 bis November 2021 über 58.000 KI-bezogene Patente angemeldet, was sie zum weltweiten Marktführer im Bereich KI macht.[24] Im Fokus der Unternehmen steht daher, von ihren eigenen Tochterunternehmen riesige Datenmengen zu

20 Indonesien hat auf der 11. Ministerkonferenz (MC11) eine Definition durchgesetzt, von der Inhalt ausgenommen ist. Entwicklungsländer haben den Definitionsbereich des Begriffs elektronische Übertragungen in der WTO angefochten, weil es verheerende Auswirkungen auf ihre Einnahmen haben könnte, wenn er digitalisierte Inhalte mit einbezieht. Aber Freihandelsabkommen vertuschen das Problem und verstetigen es, z. B. in Artikel X.6 des Freihandelsabkommens zwischen der Europäischen Union und Neuseeland.

21 Allgemeiner Rat der WTO, „Fiscal implications of the customs moratorium on electronic transmissions: the case of digitisable goods (Doc # 16-6961)", WTO JOB/GC/114 (Dezember 2016). Eine ausführlichere Erörterung dieses Themas findet sich in der bereits zitierten Veröffentlichung von Banga „JSI on E-Commerce", UNCTAD (2021).

22 Siehe Hosuk Lee-Makiyama und Badri Narayanan Gopalakrishnan, „The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions", *European Centre for International Political Economy*, Policy Brief No. 3 (August 2019), https://ecipe.org/publications/moratorium/.

23 Zahlen ausGlobal Newswire, „Artificial Intelligence (AI) Market to Hit USD 360.36 Billion by 2028; Surging Innovation in Artificial Internet of Things (AIoT) to Augment Growth: Fortune Business Insights™", Fortune Business Insights (September 2021), https://www.globenewswire.com/news-release/2021/09/16/2298078/0/en/Artificial-Intelligence-AI-Market-to-Hit-USD-360-36-Billion-by-2028-Surging-Innovation-in-Artificial-Internet-of-Things-AIoT-to-Augment-Growth-Fortune-Business-Insights.html, Währungsumrechnung am 14. November 2022 unter Verwendung von https://www.bloomberg.com/quote/USDEUR:CUR.

24 Naomi Davies, „Index shows US is winning the AI race – but for how long?", Investment Monitor (November 2021), https://www.investmentmonitor.ai/ai/ai-index-us-china-artificial-intelligence.

sammeln, zu erfassen, zu speichern und zu verarbeiten und Daten aus anderen Quellen zu kaufen.

Die neuere Generation von „Handelsabkommen" enthält die folgenden Top-Regelungen von der Wunschliste der Unternehmenslobby:

- Einschränkung der Möglichkeit für Staaten, die grenzüberschreitende Datenübermittlung von Unternehmen zu begrenzen;
- Verbot der Möglichkeit für Staaten, von ausländischen Unternehmen die lokale Verarbeitung und/oder Speicherung von Daten zu verlangen;
- Verbot für Staaten, von Unternehmen die Offenlegung von Quellcodes zu verlangen, die wesentlicher Bestandteil von algorithmischen Systemen sind.[25]

GRENZÜBERSCHREITENDE DATENÜBERMITTLUNGEN

Big Tech verwendet häufig den Euphemismus „freier Datenverkehr" für die Beschreibung seiner Zielsetzungen im Hinblick auf die grenzüberschreitende Datenübermittlung. Es ist aber klar, dass ein „freier" Verkehr nicht beabsichtigt ist. Die Absicht von Big Tech besteht vielmehr in der Aneignung und Kontrolle aller Formen von Daten durch private Unternehmen – ganz gleich, wer sie erzeugt hat, wer sie verarbeitet hat, aus welchem Staat sie stammen oder wie sie der Allgemeinheit nutzen könnten – für rein private Interessen. Der erste Artikel des horizontalen Texts, auf den sich die EU zur Verwendung in Abkommen über digitalen Handel verständigt hat, besagt zum Thema Datenverkehr: „Die Vertragsparteien verpflichten sich, den grenzüberschreitenden Datenverkehr zu gewährleisten, um den Handel in der digitalen Wirtschaft zu erleichtern."[26]

Vier der fünf größten Unternehmen der Welt nach Marktkapitalisierung sind heute Big-Tech-Unternehmen.[27] Apple, Microsoft, Alphabet (Google) und Amazon werden von Investoren unter anderem wegen ihres Datenbesitzes und ihres Ertragspotenzials so hoch bewertet. Der Economist kam 2017 zu dem berühmten Schluss, dass Daten die wertvollste Ressource der Welt sind.[28] Dementsprechend hatte Apple im November 2022 eine Marktkapitalisierung von 2 Billionen Euro. Deutschland (4 Billionen Euro), Frankreich (2,8 Billionen Euro) und Italien (2 Billionen Euro)[29] sind die einzigen drei Länder in der EU, deren BIP im Jahr 2021 höher war als die Marktkapitalisierung von Apple. Die Marktkapitalisierung von Apple ist somit höher als die Jahresleistung von 24 EU-Ländern.

Seit der Verabschiedung der wegweisenden Datenschutz-Grundverordnung (DSGVO)[30] hat die EU das Primat der Privatsphäre und des Datenschutzes als wesentliches Element der EU-Politik im Bereich des digitalen Handels konkretisiert.[31] Datenschutzexpert*innen beklagen die unzureichende Durchsetzung der DSGVO und fordern immer wieder ihre Verschärfung. Dennoch markiert sie einen Wendepunkt im Hinblick auf die uneingeschränkte Befugnis von Unternehmen zur grenzüberschreitenden Datenübermittlung.

Die Auswirkungen der Möglichkeit für Unternehmen, Daten ohne Einschränkungen über Grenzen hinweg zu übermitteln, gehen weit über die Frage der persönlichen Privatsphäre hinaus. Seit etwa 40 Jahren hat sich die Nutzung digitaler Technologien dramatisch ausgeweitet. Das Produktivitätswachstum in Industrieländern war in den letzten Jahrzehnten zwar langsamer als in der Nachkriegszeit, aber das vorhandene Wachstum ist wahrscheinlich zum großen Teil auf digitale Technologien zurückzuführen. Allerdings haben Kapitaleigner, und nicht arbeitende Menschen, in den letzten vierzig Jahren einen immer

25 Ein Beispiel für die Wunschliste von Unternehmen ist die Erklärung über die empfohlenen Schwerpunkte für die WTO-Beratungen über den elektronischen Handel „Recommended Priorities for the WTO E-Commerce Discussions" vom 16. Juli 2018, unterzeichnet von Australian Information Industry Association, DIGITALEUROPE, Information Technology Association of Canada, Information Technology Industry Council, Internet Association, Japan Electronics and Information Technology Industries Association und National Foreign Trade Council (NFTC). Abrufbar hier: Information Technology Industry Council, „Business and Tech Groups Release Priorities for WTO E-Commerce Meetings", ITI-Pressemitteilung (Juli 2018), https://www.itic.org/news-events/news-releases/business-and-tech-groups-release-priorities-for-wto-e-commerce-meetings.

26 Auszug aus dem horizontalen Vorschlag „Provisions on cross-border data flows and protection of personal data and privacy", EU-Vorschlag (Juli 2018), http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf, siehe auch das „Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits", abgekürzt HKA EU-VK (April 2021): Titel III, Artikel 201, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:22021A0430(01)&from=EN.

27 Matthew Johnston, „Biggest Companies in the World by Market Cap", Investopedia (September 2022), https://www.investopedia.com/biggest-companies-in-the-world-by-market-cap-5212784.

28 „The world's most valuable resource is no longer oil, but data", *The Economist* (Mai 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Andere mögen dem entgegenhalten, dass beispielsweise Wasser oder Luft wertvollere Ressourcen für die Menschheit seien.

29 Datenquelle von der Weltbank, „World Development Indicators", WB Datenbank, https://databank.worldbank.org/reports.aspx?source=2&series=NY.GDP.MKTP.CD&country=, Währungsumrechnung am 14. November 2022 unter Verwendung von https://www.bloomberg.com/quote/USDEUR:CUR.

30 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [2016] Abl. L 119/1 (nachstehend „DSGVO").

31 Titel III, Artikel 201 des HKA EU-VK.

größeren Anteil des aus dem Wachstum stammenden Einkommens abgeschöpft.[32]

In den heutigen Gesellschaften gibt es eine große Quelle von Ungleichheit. Im Jahr 2021 verfügten die oberen 10 Prozent aller Haushalte über fast das sechsfache Einkommen der unteren 50 Prozent – und zwar nach Steuern und Transferzahlungen, die die Einkommensverteilung weniger regressiv machen. Dies ist ein Anstieg im Vergleich zu 1990, als die oberen 10 Prozent das Fünffache des Einkommens der unteren Hälfte erzielten.[33] Auch die Ungleichheit bei der Vermögensverteilung hat zugenommen – das reichste Dezil besaß im Jahr 1995 das 62-fache des Nettovermögens der unteren 50 Prozent der Bevölkerung, im Jahr 2021 das 86-fache.[34]

Wenn dieser Trend umgekehrt oder zumindest aufgehalten werden soll und stattdessen die Beschäftigten an den Produktivitätsgewinnen aus der Digitalisierung teilhaben sollen, muss dafür gesorgt werden, dass die Kontrolle über eine der wertvollsten wirtschaftlichen Ressourcen in der Geschichte der Menschheit nicht vom Kapital gekapert wird, sondern generell unter den arbeitenden Menschen, den Einwohner*innen, den Bürger*innen und der Gesellschaft als Ganzes aufgeteilt wird.

In Anbetracht des wirtschaftlichen Werts von Daten ist es wichtig, nicht nur den Datenschutz zu erörtern und zu regulieren, sondern auch die wirtschaftliche Verwaltung von Daten. Sollen die von den Bewohner*innen eines Landes erzeugten Daten zur Nutzung für die lokale Förderung von digitaler Industrialisierung, Arbeitsplätzen und KMU zur Verfügung stehen? Oder sollten sie ausschließlich von Big Tech kontrolliert werden? Privatpersonen haben das Menschen- und Grundrecht auf Privatsphäre und Datenschutz, aber der Internationale Pakt über wirtschaftliche, soziale und kulturelle Rechte (IPwskR) erteilt Menschen auch ein kollektives Recht auf Kontrolle und Nutzung ihrer Ressourcen.[35]

Datenverkehr unterscheidet sich im internationalen Handel grundlegend vom Waren- und Dienstleistungsverkehr. Im Digital Economy Report 2021 der UN-Konferenz für Handel und Entwicklung (UNCTAD)[36] wird zu Recht darauf verwiesen, dass angesichts der Multidimensionalität von Daten ein großer Teil der Daten nicht mit dem Handel verbunden ist, was die Regulierung von Daten durch Handelsabkommen problematisch macht. Der Datenverkehr erfordert auch eine andere Behandlung als der Güter- und Dienstleistungsverkehr, da Daten nicht wie Güter und Dienstleistungen gehandelt werden können. So können beispielsweise Nutzer*innen einen ausländischen Online-Service kostenlos nutzen (z. B. Suchmaschinen, Social Media usw.), aber während dieses Prozesses können die von ihnen und über sie erzeugten Daten extrahiert, verarbeitet und vermarktet werden.

Da die Übermittlung von Daten auch nicht handelbare Aspekte, wie das Recht auf Personenschutz und Privatsphäre sowie Menschenrechte beinhaltet, wäre ihre Behandlung im Rahmen der Handelsregelungen eine Einschränkung. Bei Handelsverhandlungen werden keine unterschiedlichen Interessengruppen einbezogen, wie es für eine gemeinsame Verständigung über nicht handelsbezogene Aspekte besonders vonnöten wäre. Darüber hinaus sind Handelsverhandlungen eher von Bedeutung, wenn es um die gegenseitige Behandlung von Themen wie Zöllen und Kontingenten usw. geht. Aber die Berücksichtigung von nicht handelsbezogenen Aspekten wie Privatsphäre und Menschenrechten insbesondere im Kontext von digitalen Technologien wie Gesichtserkennung und Rassendiskriminierung können Handelsgespräche erschweren und führen mit hoher Wahrscheinlichkeit zu deren Scheitern.

Abgesehen von den oben genannten Gründen für die Ausklammerung des Datenverkehrs aus Handelsgesprächen unterscheiden sich Datenströme unter eher praktischen Erwägungen in vielerlei Hinsicht von internationalen Handelsströmen. Governance und Verhandlungen im internationalen Handelsverkehr stützen sich in hohem Maße auf Statistiken über die Art der Handelsströme sowie die Werte und die Herkunfts- und Bestimmungsländer der gehandelten Waren und Dienstleistungen. Ein solcher Ansatz für den Datenverkehr ist extrem schwierig, wenn nicht gar unmöglich, da es keine

32 Dies lässt sich am rückläufigen Anteil der Arbeit am Einkommen in vielen Volkswirtschaften in diesem Zeitraum ablesen. Aus einer Studie von OECD-Forscher*innen geht hervor, dass der Anteil der Arbeit in der gesamten OECD im Zeitraum von 1995 bis 2014 um durchschnittlich 2,5 Prozentpunkte sank und in zwei Drittel der untersuchten Länder ein Rückgang zu verzeichnen war. Cyrille Schwellnus, Andreas Kappeler und Pierre-Alain Pionnier, „Decoupling of wages from productivity: Macro-level facts", Arbeitspapier Nr. 1373 der Abteilung Wirtschaft der OECD (Januar 2017), https://www.oecd-ilibrary.org/content/paper/d4764493-en.

33 Gewichtet nach der Bevölkerung der einzelnen Staaten; "rdiinc_992_j" und "npopul_999_i" für 27 EU-Länder (Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechien, Ungarn und Zypern) anhand von Daten der: World Inequality Database (abgerufen am 11. November 2022), https://wid.world/data.

34 "rhweal_992_j_QY" aus der World Inequality Database (abgerufen am 11. November 2022).

35 Im Rahmen des Nagoya-Protokolls zum Übereinkommen über die biologische Vielfalt machen Entwicklungsländer beispielsweise Rechte im Hinblick auf die Verwertung von Daten aus der Gensequenzierung ihrer Flora und Fauna geltend.

36 UNCTAD, „Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow", Vereinte Nationen (September 2021), https://unctad.org/system/files/official-document/der2021_en.pdf

offiziellen Statistiken zur Verfolgung von Datenströmen und deren Quantifizierung auf Länderebene gibt.

Es gibt keine einfachen Lösungen für das Problem, wer Daten besitzen und kontrollieren sollte. Das zeigt sich sehr klar in den Diskussionen und Debatten über die aktuellen Legislativprojekte in der EU.[37] Klar ist aber auch, dass es inakzeptabel ist, wenn Big Tech das faktische Eigentum an der wertvollsten Ressource der Geschichte ohne demokratische Debatte oder Vereinbarung für sich reklamiert.

VERBOT DER DATENLOKALISIERUNG

Neben der Möglichkeit, Daten in einen Rechtsraum zu verlagern, der seinen privaten Profitinteressen und seinen bevorzugten Regulierungssystemen am besten entspricht, will Big Tech auch erreichen, dass Regierungen keine lokale Speicherung von Datenbeständen, noch nicht einmal von Datenkopien, verlangen dürfen. Die auf den oben genannten Artikel über den grenzüberschreitenden Datenverkehr folgende Bestimmung im horizontalen Text lautet:

„Zu diesem Zweck darf der grenzüberschreitende Datenverkehr zwischen den Vertragsparteien nicht durch eine Vertragspartei eingeschränkt werden, indem diese:

a) die Nutzung von Rechenanlagen oder Netzelementen im Gebiet der Vertragspartei für die Verarbeitung vorschreibt, auch durch die Vorgabe der Nutzung von Rechenanlagen oder Netzelementen, die im Gebiet einer Vertragspartei zertifiziert oder zugelassen sind;

b) *die Lokalisierung von Daten im Gebiet der Vertragspartei zur Speicherung oder Verarbeitung verlangt;*

c) die Speicherung oder Verarbeitung im Gebiet der anderen Vertragspartei verbietet;

d) die grenzüberschreitende Übermittlung von Daten von der Nutzung von Rechenanlagen oder Netzelementen im Gebiet der Vertragsparteien oder von Lokalisierungsanforderungen im Gebiet der Vertragsparteien abhängig macht.[38] (Kursivsetzung eingefügt. Derselbe Wortlaut findet sich in Artikel 201 des Handels- und Kooperationsabkommens (HKA) zwischen der EU und dem Vereinigten Königreich und in Artikel X.4 des Freihandelsabkommens zwischen der Europäischen Union und Neuseeland (EU-NZ FTA)[39].)

Diese Bestimmungen gegen die Datenlokalisierung treffen das Potenzial der Gemeinschaften, Daten zum Wohle der Allgemeinheit zu nutzen, ins Mark. Abgesehen davon, dass eine Person Rechte an den von ihr erzeugten Daten haben sollte, gibt es Gründe, warum die Öffentlichkeit ein Interesse daran hat, dass kollektive Daten für das Gemeinwohl verfügbar sind, z. B. für die Beendigung von Pandemien oder die Eindämmung des Klimawandels, warum eine Gemeinde oder Behörde (z. B. eine Verkehrsbehörde) Rechte an Daten geltend machen möchte (z. B. die von privaten Ridesharing-Apps) oder warum Bevölkerungsgruppen wie Beschäftigte Rechte an Daten z. B. über ihre eigene Arbeit anmelden könnten, Fragen, die nachstehend weiter ausgeführt werden.[40]

Rechenzentren sind die Fabriken der digitalen Wirtschaft, und Regierungen sollten das Recht haben, digitale Fabriken innerhalb ihrer eigenen Staatsgrenzen über politische Richtlinien für die Datenlokalisierung zu fördern. Die Handelsregeln, die eine Datenlokalisierung verbieten, führen zu einem Wettlauf nach unten, da sich die Länder bemühen, durch Subventionen und Anreize zugunsten von Big-Tech-Unternehmen Investitionen in ihr Land zu locken. Die UNCTAD hat eine Liste von Industrie-Subventionen und -Anreizen zusammengestellt, mit denen US-amerikanische Bundesstaaten Investitionen in Rechenzentren anziehen wollen.[41] Dazu gehören unter anderem Steuerbefreiungen, Steuervergünstigungen, Grundsteuerbefreiungen, Zuschüsse und vergünstigte Darlehen.

Bei all diesen Diskussionen ist es daher wichtig, den sozialen, kulturellen und anderweitigen Wert von Daten zu berücksichtigen. Die UNCTAD hat vor kurzem anerkannt, dass Daten nicht nur eine wirtschaftliche Ressource darstellen, sondern ganzheitliche kulturelle und soziale Aspekte haben, und daher nicht nur von einer wirtschaftlichen

37 Joan Lopez Solano et al, „Governing data and artificial intelligence for all: Models for sustainable and just data governance", Europäisches Parlament, Studie PE 729.533 (Juli 2022), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf.

38 Titel III, Artikel 201 des HKA EU-VK.

39 Freihandelsabkommen zwischen der Europäischen Union und Neuseeland", abgekürzt FHA EU-Neuseeland (Juni 2022). Der Wortlaut von Artikel X.4 ist hier abrufbar: „Consolidated text of all chapters, including the Preamble", (Juni 2022): 168, https://circabc.europa.eu/rest/download/1a0e0689-f705-47f3-88e1-09103b88b58d.

40 Siehe Parminder Jeet Singh und Anita Gurumurthy, „Economic Governance of Data: Balancing individualist-property approaches with a community rights framework", *IT for Change* Entwurf zur Diskussion beim vierteljährlichen Rundtischgespräch des Data Governance Network (Januar 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873141

41 Banga, „JSI on E-Commerce", UNCTAD (2021).

Institution[42] wie der WTO oder sonstigen Handelsabkommen geregelt werden sollen.

Der IPwskR verlangt ferner den Schutz weiterer Grundrechte wie der Freiheit von Diskriminierung. Es gibt eine Bestimmung über das „Regelungsrecht", z. B. im Freihandelsabkommen zwischen der EU und Neuseeland (Art. X.2), die eine Reihe „legitimer politischer Ziele" „bekräftigt", wie Sozialdienstleistungen, Klimawandel und kulturelle Vielfalt. Diese Bestimmung ist deklaratorisch, kann also nur über die allgemeinen Ausnahmen umgesetzt werden.[43] Der Ansatz der EU stützt sich für den Schutz dieser Rechte im Wesentlichen auf die unzureichenden allgemeinen Ausnahmen.[44] Nur für den Schutz personenbezogener Daten gibt es eine eigene Ausgleichsbestimmung, die auf einem Kompromiss für horizontale Bestimmungen über den grenzüberschreitenden Datenverkehr und den Schutz personenbezogener Daten in den im Jahr 2018 geschlossenen Handels- und Investitionsabkommen basiert.[45]

Unternehmen sollten in einer Zeit, in der Bürger*innen, Beschäftigte, Regulierungsbehörden und Gesetzgeber über den Wert von Daten und die erste notwendige Regulierungswelle für diesen Sektor debattieren, nicht die Möglichkeit haben, demokratische Prozesse zu umgehen, insbesondere wenn sie das Ziel verfolgen, die Regierungen daran zu hindern, den breiten Zugang zu Daten und ihren Nutzen für alle sicherzustellen.

GEHEIMHALTUNG VON QUELLCODES

Genauso wächst auch das Bewusstsein über die zunehmende Nutzung und Macht der algorithmischen Entscheidungsfindung. Das aktuelle Geschäftsmodell des „Surveillance Advertising", das zunehmend von digitaler Überwachungswerbung geprägt ist und bei dem Facebook und Google „mehr Klicks" (und damit höhere Einnahmen) durch hetzerische und ungenaue Informationen[46] erhalten, statt durch verlässliche, dokumentierte Fakten und eine vernünftige Debatte, ist untragbar.[47]

Aber algorithmische Systeme, einschließlich der vom Menschen lesbaren Quellcodes, bestimmen zunehmend wichtige Aspekte unseres Arbeitslebens, unseres sozialen Lebens, unseres finanziellen Lebens und unseres politischen Lebens. Sie werden genutzt, um Entscheidungen darüber zu treffen, wer eingestellt wird, wer einen Kredit erhält, zu welchen Preisen uns Waren angeboten werden und welche Wahlwerbung wir sehen. In die Privatsphäre eingreifende Überwachung von Beschäftigten in Betrieben mit Wearables und Spionage-Software werden immer alltäglicher. Diese Systeme verschärfen oftmals Rassen- und Geschlechterdiskriminierung sowie Diskriminierung in Beschäftigung und können die Ausgrenzung von ohnehin schon benachteiligten Gruppen weiter verfestigen.[48] Die „AI Incidents Database" der Organisation „Partnership on AI" enthält fast vierhundert Schadensereignisse, die weltweit durch den Einsatz algorithmischer Systeme verursacht wurden, wobei Facebook, Tesla, Google, Amazon, YouTube und TikTok die schlimmsten Wiederholungstäter sind.[49] Algorithmische Systeme, die Auswirkungen auf die Gesellschaft haben, müssen öffentlicher Aufsicht unterliegen.[50]

Algorithmische Systeme können mittels „White-Box"-Tests, bei denen auch auf den Quellcode zugegriffen wird, oder mittels „Black-Box"-Tests untersucht werden, bei denen verschiedene Techniken zur Anwendung kommen, für die keine Analyse des Quellcodes der Algorithmen erforderlich ist.[51] Für „Black-Box"-Tests ist der Zugang zu Daten erforderlich, die von algorithmischen Systemen aufgenommen oder erzeugt werden, wofür wiederum Softwareschnittstellen für die Prüfung benötigt werden, die als Quellcode ausgedrückt werden. Bei

42 UNCTAD, „Digital Economy Report 2021", Vereinta Nationen (2021).

43 Der emeritierten Professorin für Recht Jane Kelsey zufolge hat die Bestimmung über das Regelungsrecht interpretatorische Relevanz, wenn es um Angelegenheiten geht, bei denen sich die Regierungen auf ein Argument für das Regelungsrecht stützen würden. Der Wortlaut der Bestimmung über das Regelungsrecht hat eine gewisse unmittelbare Auslegungsrelevanz für den verfolgten Ansatz, beispielsweise im CPTPP (Comprehensive and Progressive Agreement for Trans-Pacific Partnership), in dem die Datenvorschriften eine Ausnahmeregelung für legitime Ziele der öffentlichen Ordnung enthalten (aber weiterhin vorbehaltlich der am wenigsten restriktiven und Chapeau-Prüfungen). Das Freihandelsabkommen zwischen der EU und Neuseeland enthält keine solche Bestimmung, lediglich einen Querverweis auf die Allgemeinen Ausnahmen und die "die dort genannten Gemeinwohlziele", die laut Art. X.1 des Kapitels über Ausnahmen begrenzt sind. Es ist zu beachten, dass sich die Allgemeinen Ausnahmen von dem viel strengeren Wortlaut des Artikels X.5 über den Schutz personenbezogener Daten und der Privatsphäre unterscheiden.

44 Daniel Rangel, „WTO General Exceptions: Trade Law's Faulty Ivory Tower", *Public Citizen* (Februar 2022), https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/.

45 Svetlana Yakovleva und Kristina Irion, „Pitching trade against privacy: reconciling EU governance of personal data flows with external trade", *International Data Privacy Law10*, No. 3 (August 2020): 201–222, https://doi.org/10.1093/idpl/ipaa003.

46 Yael Eisenstat, „I Worked on Political Ads at Facebook. They Profit By Manipulating Us", *Washington Post* (November 2019), https://www.washingtonpost.com/outlook/2019/11/04/i-worked-political-ads-facebook-they-profit-by-manipulating-us/.

47 Matt Stoller, „Ad Tech and the News: Background on the Rise of Surveillance Advertising and Its Effects on Journalism", *Center for Journalism & Liberty* (September 2020), https://static1.squarespace.com/static/5efcb64b1cf16e4c487b2f61/t/5f75107ef21702786068d8a3/1601507762535/adtech-cjl-sept2020.pdf.

48 Siehe Cathy O'Neil, *„Angriff der Algorithmen. Wie sie Wahlen manipulieren, Berufschancen zerstören und unsere Gesundheit gefährden"* (Hanser Verlag, 2017); und Safiya Umoja Noble, *„Algorithms of Oppression: How Search Engines Reinforce Racism"* (New York University Press: 2018).

49 Abrufbar unter „AI Incident Database", *Responsible AI Collaborative* (abgerufen am 13. Januar 2022), https://incidentdatabase.ai/entities.

50 Frederick Mostert und Alex Urbelis, „Social media platforms must abandon algorithmic secrecy", *Financial Times* (Juni 2021), https://www.ft.com/content/39d69f80-5266-4e22-965f-efbc19d2e776.

51 Kristina Irion, „AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?", Gutachten im Auftrag der *Verbraucherzentrale Bundesverband (vzbv)* (Januar 2021), https://doi.org/10.2139/ssrn.3786567.

wissenschaftlichen Untersuchungen wurde ferner festgestellt, dass es zahlreiche komplexe Situationen gibt, in denen es genauer oder effizienter ist, Tests zu verwenden, bei denen nicht nur das Ergebnis des maschinellen Lernens, sondern der Quellcode selbst analysiert wird.[52] Für solche Situationen müssen Rechtsvorschriften erlassen werden, die den vorherigen und nachträglichen Zugang zu den in Quellcode ausgedrückten Algorithmen zur notwendigen Bedingung machen, um zu bewerten, ob algorithmische Systeme die regulatorischen und rechtlichen Erfordernisse erfüllen, unter anderem im Hinblick auf das Wettbewerbsrecht, das Gleichstellungsrecht, Datenschutz, finanzielle Absicherung und Verbraucherschutz; für die Vergabe öffentlicher Aufträge (einschließlich der Sorgfaltspflicht, beispielsweise für die im Rahmen kritischer nationaler Infrastrukturen wie Wahlen genutzte Software; für Transparenz und Rechenschaftspflicht oder andere strategische Aspekte) oder für die Förderung von Innovation und wirtschaftlicher Entwicklung.[53]

Im Kapitel über den digitalen Handel des Freihandelsabkommens zwischen der EU und Neuseeland, dessen Wortlaut dem vieler EU-Abkommen entspricht,[54] heißt es: „Eine Vertragspartei darf die Weitergabe des Quellcodes von Software, die Eigentum einer natürlichen oder juristischen Person der anderen Vertragspartei ist, oder den Zugang dazu nicht als Voraussetzung für die Einfuhr, die Ausfuhr, den Vertrieb, den Verkauf oder die Verwendung solcher Software oder von Produkten, die eine solche Software enthalten, in oder aus ihrem Gebiet vorschreiben."[55] Diese Klausel enthält zwar eine Reihe von maßgeschneiderten Ausnahmen für die behördliche und gerichtliche Durchsetzung und sogar für Konformitätsbewertungen, aber die Rechtsvorschriften, die den Zugriff auf den Quellcode für diese Ziele erlauben, sind von dieser Regel nicht ausgenommen.

Befürworter*innen bringen vor, dass diese Regelungen zum Schutz des Quellcodes wichtig für den Schutz vor erzwungenem Technologietransfer sind (in der Regel unter Verweis auf China). Die meisten Staaten, die Vertragsparteien von Abkommen über digitalen Handel sind, sehen darin jedoch kein Problem.

Im Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich sind Ausnahmen für Wettbewerbsauflagen und in Artikel 207 „eine Auflage einer Regulierungsbehörde gemäß den Gesetzen oder Vorschriften einer Vertragspartei im Hinblick auf den Schutz der öffentlichen Sicherheit in Bezug auf die Nutzer online" vorgesehen.[56] Frühere Abkommen enthielten sogar noch weniger Ausnahmen für die die Offenlegung von Quellcode, was darauf hindeutet, dass die Regulierungsbehörden möglicherweise feststellten, dass Handelsbeamt*innen dabei waren, den notwendigen politischen Spielraum für die Behandlung der zunehmenden algorithmischen Entscheidungsfindung zu begrenzen.[57] Diese Ausnahmen wurden im Freihandelsabkommens zwischen der EU und Neuseeland auf die Diskriminierungsfreiheit und die Verhinderung von Voreingenommenheit ausgeweitet. Ausnahmen für zahlreiche weitere soziale Übel, die oft eine Folge von algorithmischer Voreingenommenheit sind, wie Falschinformation, emotionale Manipulation und weitere Aspekte, die von Verbraucherorganisationen genannt werden,[58] werden im Text jedoch nicht erwähnt.

Zivilgesellschaftliche Sachverständigenorganisationen kritisieren, dass die vorgesehenen Ausnahmen nicht ausreichen, um die Konformität von Algorithmen und digitalen Technologien mit EU-Recht zu gewährleisten. Um eine wirkliche Aufsicht im öffentlichen Interesse zu ermöglichen, dürfen die Handelsabkommen der EU nach Meinung der Sachverständigen der Zivilgesellschaft[59] sowie Wissenschaftler*innen, Medien, kritische Ingenieur*innen[60] und Gewerkschaften[61] nicht den politischen Handlungsspielraum für die öffentliche Kontrolle von Algorithmen entziehen.

Die Möglichkeit der Aufsicht über algorithmische Systeme darf auch nicht der Überprüfung durch ein Handelsgericht unterliegen, das handelspolitischen

52 Ibid; auch Dorobantu et al, „Source code disclosure", in Addressing Impediments (2021). Siehe auch: Magdalena Słok-Wódkowska und Joanna Mazur, „Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code", *Journal of International Economic Law 25*, Nr. 1 (März 2022): 91–109, https://doi.org/10.1093/jiel/jgac005.
53 Dorobantu et al, „Source code disclosure", in Addressing Impediments (2021).
54 Scasserra und Elebi, „Digital Colonialism", Transnational Institute (2021).
55 Kapitel XX Digitaler Handel des Freihandelsabkommens zwischen der Europäischen Union und Neuseeland, abrufbar unter https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/0fa614a2-7365-4f91-9bd0-88822fc9a16e/details.
56 Titel III, Kapitel 3, Artikel 207: Quellcode, HKA zwischen der EU und dem Vereinigten Königreich
57 Kristina Irion, „Algorithms Off-limits? If digital trade law restricts access to source code of software then accountability will suffer", ACM 2022 Conference on Fairness, Accountability, and Transparency (Juni 2022): 1561-1570, https://doi.org/10.1145/3531146.3533212.
58 Maryant Fernandez und Sebastien Pant, „Why it's time to ban surveillance ads", *BEUC (Europäische Verbraucherorganisation)* Blog (November 2021), https://www.beuc.eu/blog/why-its-time-to-ban-surveillance-ads/.
59 BEUC, „EU-New Zealand Trade Agreement: BEUC reaction to the concluded agreement", *BEUC* Positionspapier (August 2022), https://www.beuc.eu/position-papers/eu-new-zealand-trade-agreement-beuc-reaction.
60 Irion, „Algorithms Off-limits?", ACM (2022).
61 Christina Colclough, „Union Brief: G7 Digital Policy Priorities 2022", *Why Not Lab* (2022), https://www.thewhynotlab.com/post/reminding-the-g7-workers-rights-are-human-rights.

Erwägungen mehr Gewicht beimisst als Menschen- und Grundrechten.[62] Wissenschaftler*innen haben festgestellt, dass für Vertragsparteien durch das gegenwärtige Fehlen internationaler Normen und eines Konsens über algorithmische Governance ein höheres rechtliches Risiko besteht, dass ein Versuch, eine nicht konforme Maßnahme auf der Grundlage der allgemeinen Ausnahmen zu rechtfertigen, scheitert.[63]

Ein Blick auf die Geschichte der Rechtsprechung zu den Ausnahmen im allgemeinen öffentlichen Interesse im Rahmen der WTO zeigt, dass Handelsgerichte Erwägungen des öffentlichen Interesses oder Menschenrechtsaspekten keine Priorität einräumen würden. In einer jüngsten Analyse wurde in Bezug auf das Allgemeine Zoll- und Handelsabkommen (GATT) festgestellt, dass in den 26 Jahren des Bestehens der WTO die allgemeinen Ausnahmen des GATT (Artikel XX) und des Allgemeinen Abkommens über den Handel mit Dienstleistungen (GATS, Artikel XIV) nur zweimal erfolgreich geltend gemacht wurden, bei insgesamt 48 Versuchen zur Verteidigung innerstaatlicher Politiken, die nach WTO-Regeln als illegal angefochten wurden.[64]

Darüber hinaus wird Quellcode bereits durch Rechte an geistigem Eigentum einschließlich Urheberrechten und in einigen Fällen im Rahmen von Patenten und Geschäftsgeheimnissen geschützt.[65] Das Recht des geistigen Eigentums folgt einer bestimmten Logik, wenn es darum geht, ausschließliche Rechte zu gewähren, und im Falle des Urheberrechts und des Patentschutzes unterliegt es gesetzlichen Beschränkungen, und muss veröffentlicht werden. Das Geschäftsgeheimnisrecht macht bereits einen Großteil des erreichten Gleichgewichts zunichte, da es potenziell unbegrenzt ist und keine Freigabe des geschützten Gegenstands für die Wissensallmende bewirkt. Die neuen Verbote der Offenlegung von Quellcode stellen eine zusätzliche Schutzebene für Algorithmen in Abkommen dar und betreffen einen breiten Bereich menschlicher Aktivitäten, in denen kaum andere ausgleichende menschliche, soziale, wirtschaftliche oder kulturelle Rechte zugesichert werden.[66] Aus diesem Grund ist auch das Argument, dass Unternehmen diesen zusätzlichen Schutz von Quellcode brauchen, weil sie sonst die neueste Technologie nicht in Entwicklungsländern einsetzen würden, nicht stichhaltig.[67]

Darüber hinaus berücksichtigen die Ausnahmen, wenn auch unzureichend, nur *bekannte* Risiken von KI-Systemen. Mit dem Bekanntwerden neuer Risiken und Schäden wird es für Regierungen noch wichtiger werden, die Befugnis zur Regulierung solcher Algorithmen zu behalten, um sicherzustellen, dass Menschen- und Grundrechte eingehalten und Schäden an der Gesellschaft verringert werden.

Angesichts der nachfolgend dargelegten unzähligen Schäden für die europäische Gesellschaft lässt sich kaum etwas anderes schlussfolgern, als dass es keine zwingenden Gründe für, aber eine Fülle von Argumenten gegen die Aufnahme von Bestimmungen gibt, die Regierungen daran hindern, die Offenlegung von Quellcode in „Handelsabkommen" zu verlangen.

Es gibt weitere gefährliche Bestimmungen in den Regeln für digitalen Handel, die derzeit bei der WTO verhandelt werden, auf die unten näher eingegangen wird.[68]

Alle diese Bestimmungen sind miteinander und mit den bestehenden Handelsvorschriften verknüpft, wie dem GATS, dem Übereinkommen über das öffentliche Beschaffungswesen, dem Übereinkommen über technische Handelshemmnisse und dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS Übereinkommen) der WTO sowie weiteren bilateralen Handelsabkommen und Regelungen zum Investitionsschutz. Daher gehen die potenziellen Auswirkungen dieser vielfachen, sich überschneidenden Bestimmungen und Abkommen in einer sich entwickelnden digitalen und wirtschaftlichen Landschaft weit über das hinaus, was dieses Dokument abdecken kann, und bedürfen weiterer Untersuchungen.

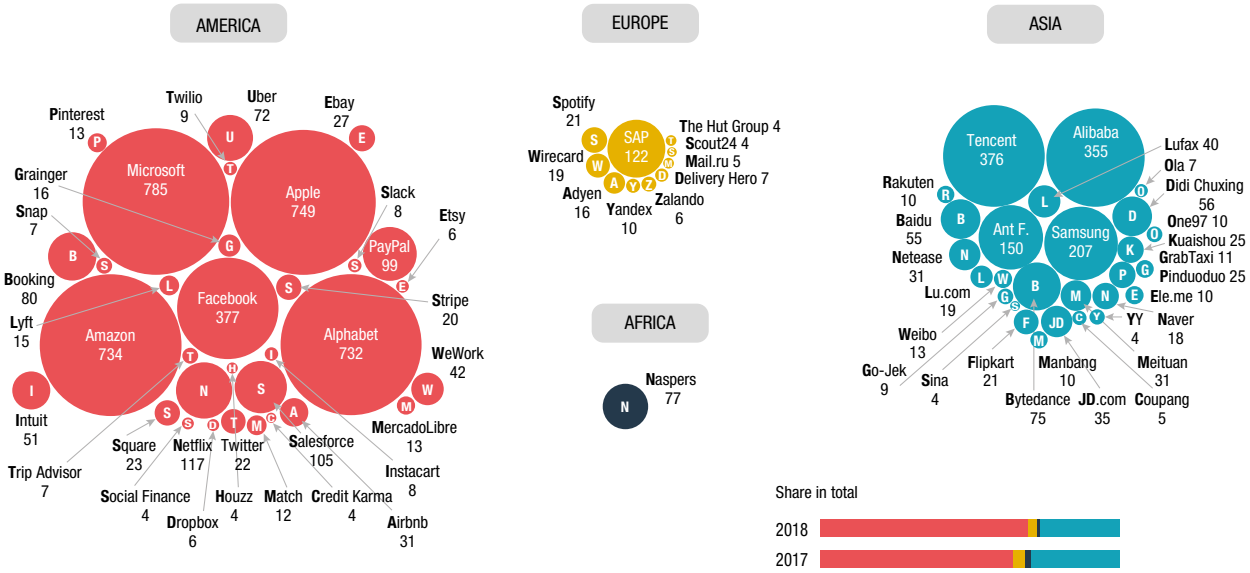
62 Irion, Kristina, „AI Regulation in the EU", vzbv (2021).
63 Irion, „Algorithms Off-limits?", ACM (2022).
64 Rangel, „WTO General Exceptions", Public Citizen (2022). Bei den beiden erfolgreichenVersuchen handelt es sich um die Fälle USA – Garnelen und USA – Thunfisch-Delfin.
65 Słok-Wódkowska und Mazur, „Secrecy by Default", *Journal of IntlEcon Law* (2022).
66 Ich danke Kristina Irion für diese Feststellung.
67 In einem Gespräch, das die Autorin am 22. November 2022 mit Aitor Montesa Lloreda, dem Leiter des Bereichs Digitaler Handel der Generaldirektion Handel der EU-Kommission, führte, brachte er dieses Argument vor.
68 Deborah James, „Digital Trade Rules: A Disastrous New Constitution for the Global Economy, by and for Big Tech", *Rosa-Luxemburg-Stiftung* (Juli 2020), https://www.rosalux.eu/en/article/1742.digital-trade-rules.html.

4.

DIE EU IST NICHT IN DER LAGE, VON DIESEN REGELN ZU PROFITIEREN

Es gibt zwei Wirtschaftsmächte, die den digitalen Handel ökonomisch dominieren, natürlich die USA und China.[69] Während die digitale Kluft in Bezug auf den Zugang zur Digitalisierung und zum Internet kleiner wird, vergrößert sich die wirtschaftliche Kluft zu den Entwicklungsländern in Afrika, Asien und Lateinamerika. Es mag aber viele schockieren, dass sich auch die digitale und wirtschaftliche Kluft zwischen Europa und den USA/China vergrößert. Der UNCTAD zufolge entfallen auf die beiden Länder etwa 90 Prozent der Marktkapitalisierung der größten digitalen Plattformen der Welt, und während der Covid-19-Pandemie stiegen ihre Profite und ihre Marktkapitalisierungen sprunghaft an.[70] Tatsächlich ist in der Plattform-Landschaft nur das deutsche Softwareunternehmen SAP als wichtiger Akteur zu registrieren, wie der folgenden Grafik der UNCTAD zu entnehmen ist.

Figure I.17. Geographical distribution of the main global platforms in the world, 2018
(Market capitalization in billions of dollars)



Source: Holger Schmidt (https://www.netzoekonom.de/vortraege/#tab-id-1).

Quelle: UNCTAD[71]

69 UNCTAD, „Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries", Vereinte Nationen (September 2019): xvi, https://unctad.org/system/files/official-document/der2019_en.pdf
70 UNCTAD, „Digital Economy Report 2021", UN (2021).
71 Siehe Abbildung in UNCTAD, „Digital Economy Report 2019", UN (2019): 19.

Der UNCTAD zufolge müssen Länder die digitale Industrialisierung vorantreiben, um von der Digitalisierung zu profitieren. Digitale Industrialisierung bezeichnet die Nutzung von Daten und nationalen digitalen Infrastrukturen zur Wertschöpfung in der digitalen Wirtschaft. Aufbauend auf IKT-Fähigkeiten und Konnektivität erfordert die digitale Industrialisierung die (lokale) Datenerfassung, die (lokale) Datenspeicherung und (lokale) Datenserver, um große Datensätze in Informationen umzuwandeln, die für den Einsatz von KI genutzt werden können.

Um die von Europa angestrebte digitale Industrialisierung zu erreichen, wird es notwendig sein, Strategien für die digitale Industrialisierung zu verfolgen, wie nachfolgend dargelegt wird. Die Mitteilung der Europäischen Kommission „2030 Digital Compass: The European way for the Digital Decade"[72] befasst sich mit den vier Kardinalpunkten Kompetenzerweiterung, Sicherstellung sicherer und nachhaltiger digitaler Infrastrukturen, digitale Unternehmenstransformation und Digitalisierung öffentlicher Dienstleistungen. Für diese Digitalstrategie erarbeitet die EU derzeit eine Reihe neuer Vorschläge, darunter eine Europäische Datenstrategie[73], eine Europäische Industriestrategie[74], das Gesetz über digitale Dienste (DSA)[75], das Gesetz über den digitalen Markt (DMA)[76], einen Rechtsakt zur Cybersicherheit[77] und das Gesetz über Künstliche Intelligenz[78] sowie weitere Regulierungsprojekte.

Gleichzeitig ist Europa, wenn man es aus der Rechtsperspektive betrachtet, in einer führenden Position im Hinblick auf die Festlegung von Normen auf der Grundlage des europäischen Sozialmodells und der EU-Grundrechtecharta. Europäische Gesetzgeber haben weniger Angst vor der Regulierung von Big Tech als ihre amerikanischen Kollegen. Aufgrund des sozialen Dialogs und der stärkeren Rolle der Gewerkschaften und der Zivilgesellschaft bei der Politikgestaltung genießen Europäer*innen mehr digitale Rechte und Freiheiten als die Bürger*innen anderer Länder wie der USA und China. Dort „profitieren" eher die Wirtschaftstitanen als die Normalbürger*innen von der marktbeherrschenden Stellung ihrer Länder

Die von den Verhandlungsführer*innen der EU verfolgte Agenda für den digitalen Handel beinhaltet die Kommodifizierung von Beschäftigten und digitalen Nutzer*innen zugunsten von (meist) in den USA ansässigen Big-Tech-Unternehmen und steht in fundamentalem Widerspruch zu den jüngsten Bemühungen der europäischen Gesetzgeber und Regulierungsbehörden.

72 Europäische Kommission, „Communication: 2030 Digital Compass: the European way for the Digital Decade", *Europäische Kommission* COM(2021) 118 final (März 2021), https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf; siehe auch Europäische Kommission, „Ein Europa für das digitale Zeitalter: Eine neue Generation von Technologien für die Menschen", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_de.

73 Europäische Kommission, „Europäische Datenstrategie", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

74 Europäische Kommission, „Europäische Industriestrategie", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_de.

75 Europäische Kommission, „Gesetz über digitale Dienste: mehr Sicherheit und Verantwortung im Online-Umfeld", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de.

76 Europäische Kommission, „Das Gesetz über digitale Märkte: für faire und offene digitale Märkte", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de.

77 Europäische Kommission, „Das EU-Cybersicherheitsgesetz", EU-Website, https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-act.

78 Europäische Kommission, „Ein europäischer Ansatz für künstliche Intelligenz", EU-Website, https://digital-strategy.ec.europa.eu/de/policies/european-approach-artificial-intelligence.

5.

ZEHN GRÜNDE, WARUM DIE EU-REGELN FÜR DIGITALEN HANDEL NICHT IM INTERESSE DER BÜRGER*INNEN, BESCHÄFTIGTEN ODER KLEINEN UNTERNEHMEN IN DER EU SIND

Inwiefern gefährden die EU-Regeln für digitalen Handel ...

1- ... DIE EU-AGENDA FÜR DIE DIGITALE INDUSTRIALISIERUNG?

Die europäischen Staatsoberhäupter haben eine Gesetzgebungs- und Investitionsinitiative für eine neue Industriestrategie für Europa auf den Weg gebracht, deren Kernstück die Digitalisierung ist.[79] Das Hauptziel besteht darin, China und die USA im technologischen Wettlauf einzuholen, die Praktiken von Big Tech innerhalb der EU zu regulieren, um unlauteren Wettbewerb zu verhindern, und die strategische Abhängigkeit von Rohstoffen, Energie und Halbleitern abzubauen, die zur Erreichung der Ziele für die digitale Industrialisierung benötigt werden. Die Strategie Europas für die digitale Industrialisierung stützt sich auf die Verbesserung des Zugangs zu Daten, die Entwicklung von Technologie und Infrastruktur und entsprechende Regulierung.[80]

Viele dieser Maßnahmen gehen auf den stärker werdenden Ruf nach technologischer Souveränität zurück. Insbesondere der EU-Kommissar für Binnenmarkt Thierry Breton unterstreicht die Bedeutung der Geopolitik von Technologie und technologischer Souveränität. "In dieser neuen geopolitischen Ordnung handelt Europa eher wie ein Stratege als wie ein bloßer Markt. Es bleibt offen, aber zu seinen eigenen Bedingungen. Es trifft seine eigenen Entscheidungen und stellt seine eigenen Regeln auf, und es hat keine Angst davor, sie seinen Partnern aufzuerlegen," so Breton in einer Rede im Jahr 2021.[81]

Manche der erklärten Ziele der EU stehen jedoch im Konflikt mit ihrer Strategie für den digitalen Handel, erstens im Hinblick auf das europäische Eintreten für einen Rahmen, der es den Unternehmen, insbesondere KMU, ermöglicht, Daten zu erzeugen, zu sammeln und zu nutzen, um Produkte zu verbessern und international wettbewerbsfähig zu sein, und zweitens im Hinblick auf die Verbesserung nationaler oder EU-weiter digitaler Infrastrukturen wie Cloud Computing.

Europäische Daten für die digitale Industrialisierung

Die EU hat die europäische Datenstrategie[82] auf den Weg gebracht, um Daten in strategischen Sektoren zu erzeugen und zu sammeln, sowohl im Bereich des Datenaustauschs zwischen Unternehmen und Behörden (B2G) als auch zwischen den Unternehmen

79 Europäische Kommission, „Mitteilung: Eine neue Industriestrategie für Europa", Europäische Kommission COM(2020) 102 final (März 2020), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020DC0102&from=EN; Europäische Kommission, „Communication: Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery", Europäische Kommission COM(2021) 350 final (Mai 2021), https://commission.europa.eu/system/files/2021-05/communication-industrial-strategy-update-2020_en.pdf

80 Europäische Kommission, „Europäische Industriestrategie", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_de

81 Luca Bertuzzi, „Mastery of technology is central to the 'new geopolitical order', Breton says", *Euractiv* (Juli 2021), https://www.euractiv.com/section/industrial-strategy/news/mastery-of-technology-is-central-to-the-new-geopolitical-order-breton-says/.

82 Europäische Kommission, „Europäische Datenstrategie", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

(B2B). Damit soll ein gemeinsamer europäischer Datenraum für den Datenverkehr innerhalb des Binnenmarktes geschaffen werden, um ihn im Einklang mit der Datenschutz-Grundverordnung und anderen europäischen Gesetzen sowie mit klaren Mechanismen der Daten-Governance für Innovationen verfügbar zu machen. Als Teil dieser Strategie hat die EU das Daten-Governance-Gesetz (DGA)[83] und das Datengesetz[84] angenommen. Auch das Gesetz über den digitalen Markt (DMA) bietet gewerblichen Nutzern größerer Plattformen – beispielsweise Händlern bei Amazon – wesentliche datenbezogene Rechte. In bestimmten Fällen werden öffentliche Daten zur Weiternutzung durch öffentliche und private Stellen im Einklang mit Datenschutzvorschriften und weiteren Governance-Regeln verfügbar sein. Gewerbliche Nutzer großer Plattformen können ihre Daten von den Plattformen zurückerhalten (gemäß DMA), gleiches gilt für IoT-Nutzer wie KMU gegenüber Datensammlern (gemäß Datengesetz). Sie können dann die Bestimmungen des DGA für die Entwicklung von Datenkooperationen zur Anwendung bringen, um ihre Daten auf die für sie bestgeeignete Weise zu nutzen. Darüber hinaus gibt es Anreize für private Einrichtungen, im öffentlichen Interesse Daten für die gemeinsamen Datenräume bereitzustellen. Das Datengesetz eröffnet auch Möglichkeiten für öffentlichen Stellen, auf Daten im Besitz des privaten Sektors zuzugreifen und diese zu nutzen, wenn sie für außergewöhnliche Situationen gebraucht werden, insbesondere bei öffentlichen Notfällen wie Überschwemmungen und Bränden, oder um einem gesetzlichen Auftrag nachzukommen, wenn anderweitig keine Daten verfügbar sind. Der Entwurf des Datengesetzes gibt den Nutzer*innen von IoT-Geräten auch das Recht, auf ihre Daten zuzugreifen, die von verschiedenen Plattformen und Apps gesammelt werden können, und sie weiterzugeben.

Ein Großteil der in Europa generierten Daten ist jedoch im Besitz von ausländischen Unternehmen, die ebenfalls verpflichtet werden sollten, Daten im Interesse der Europäer*innen weiterzugeben.[85] Europäische Fahrer*innen produzieren Daten für Uber, die Uber dann nutzt, um weitere Gewinne aus der europäischen Gesellschaft zu ziehen, während das Unternehmen gleichzeitig von öffentlichen Investitionen Europas in Straßen und Infrastruktur profitiert. Öffentliche europäische Wetterdaten werden von der globalen Versicherungsbranche genutzt, um aus der Vorhersage von schweren Wetterereignissen Kapital zu schlagen. Europäische Verbraucher*innen treffen Kaufentscheidungen auf Amazon, die das US-amerikanische Unternehmen dann nutzt, um europäische KMU herabzustufen und seine eigenen Produkte besser zu platzieren. In all diese Fällen werden europäische Daten von transnationalen Unternehmen (TNU), viele davon aus dem Ausland, für private, meist ausländische, Gewinne erfasst.[86]

Nach dem DGA hätten diese TNU Zugriff auf europäische öffentliche Daten. Gleichzeitig sind sie offenbar nicht dazu verpflichtet, Daten an europäische KMU oder den öffentlichen Raum weiterzugeben. Regeln für digitalen Handel, nach denen Staaten die Übermittlung von Daten ins Ausland zulassen müssen und Regierungen die Befugnis genommen wird, die lokale Speicherung eines Datenbestands zu verlangen, würden die Möglichkeiten Europas beschränken, Gegenseitigkeit beim Datenaustausch zu verlangen. Die großen Datenbestände, die für die Ausweitung der digitalen Industrialisierung erforderlich sind, wären infolgedessen gefährdet,

Europäische digitale Infrastrukturen

Zur effizienten Verwaltung großer Datenbestände für die digitale Industrialisierung bedarf es der Schaffung digitaler Infrastrukturen, insbesondere von Rechenzentren für das Cloud Computing. Deshalb stellt die Europäische Industriestrategie die Bedeutung der Förderung von Dateninfrastruktur, einschließlich des Cloud Computing, als notwendige Voraussetzung heraus. Die US-amerikanischen Unternehmen Amazon Web Services, Microsoft Azure und Google Cloud dominieren jedoch gemeinsam 65 Prozent des globalen Cloud-Marktes.[87] Einer jüngsten Studie zufolge sind die Einnahmen europäischer Cloud-Hosting-Provider seit 2017 zwar um 167 Prozent gestiegen, aber ihr Marktanteil ist im selben Zeitraum von 27 Prozent auf 15 Prozent geschrumpft, weil die drei oben genannten US-amerikanischen Unternehmen inzwischen fast 72

83 Europäische Kommission, „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz)" Europäische Kommission COM/2020/767 final (November 2020), https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:52020PC0767.

84 Europäische Kommission, „Datengesetz", EU-Website, https://digital-strategy.ec.europa.eu/de/policies/data-act.

85 Die derzeit geltenden bzw. vorgeschlagenen Bestimmungen des Gesetzes über den digitalen Markt und des Datengesetzes (in Verbindung mit dem Daten-Governance-Gesetz) sind zwar hilfreich, reichen aber nach dem Urteil von Sachverständigen im Bereich der digitalen Industrialisierung nicht aus. Es sollte mehr Nachdruck auf kollektive Daten und kollektive Stellen gelegt werden, die diese Daten auf sinnvolle Weise weitergeben und verwenden können. Siehe Parminder Jeet Singh und Anita Gurumurthy, „A Primer on Data and Economic Justice", *Global Partnership on Artificial Intelligence* (November 2022), https://gpai.ai/projects/data-governance/primer-on-data-and-economic-justice.pdf.

86 Rosie Collington, „Digital Public Assets: Rethinking value and ownership of public sector data in the platform age", Common Wealth (November 2019), https://www.researchgate.net/publication/337110612_Digital_Public_Assets_Rethinking_value_access_and_control_of_public_sector_data_in_the_platform_age.

87 Felix Richter, „Top Cloud Market Share Leaders: AWS, Microsoft, Google Lead Q2 2022", *Statista (Dezember 2022)*, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

Prozent des europäischen Cloud-Storage-Marktes kontrollieren.[88]

Um die Abhängigkeit von in den USA ansässigen Rechenzentren zu vermeiden, fördert die französische Regierung eine lokale Rechenzentrums-Infrastruktur. Frankreich hat vorgeschrieben, dass alle Daten aus öffentlichen Verwaltungen als Archive zu betrachten sind und deshalb in Frankreich gespeichert und verarbeitet werden müssen.[89] Im Mai 2021 machte es Frankreich den Anbietern von Cloud-Diensten zur Auflage, die mit dem SecNumCloud-Referenzsystem verbundenen Sicherheitsanforderungen zu erfüllen, die Infrastrukturen in Europa anzusiedeln und die Systeme in Europa zu betreiben und die operative und kommerzielle Unterstützung des Angebots durch eine europäische Einrichtung zu gewährleisten, die sich im Besitz europäischer Akteure befindet.[90]

Im Rahmen ihres Plans NextGenerationEU[91] unterstützt die EU die Schaffung einer europäischen Cloud, Gaia-X, um der zunehmenden Sorge über die Abhängigkeit einheimischer Unternehmen, Behördendienste und sogar Sicherheitsdienste von ausländischen Cloud-Hosts Rechnung zu tragen.[92] Trotz einer Governance-Struktur, die an europäische Unternehmen gebunden ist, sind die führenden US-amerikanischen Cloud-Anbieter jedoch schon jetzt ein untrennbarer Bestandteil von Gaia-X.[93]

Deutschland hat ähnliche Beschränkungen von Souveränitätsanforderungen in Bezug auf das europäische Zertifizierungssystems für Cybersicherheit für Cloud-Dienste vorgeschlagen, die von Frankreich, Italien und Spanien unterstützt werden.[94] Sie werden jedoch von mehreren europäischen Ländern sowie US-amerikanischen Big-Tech-Anbietern von Cloud-Diensten abgelehnt. Lobbygruppen der Wirtschaft, die vor allem in den USA ansässige Big-Tech-Unternehmen vertreten, stellen sich gegen die Strategien zur digitalen Industrialisierung und beschweren sich seit langem über diese Politik, die digitale Kapazitäten in Europa fördern soll.[95]

Aber die EU-Regeln für digitalen Handel in Bezug auf die Datenlokalisierung verbieten es den Staaten: die Nutzung von Rechenanlagen oder Netzelementen im Gebiet der Vertragspartei für die Verarbeitung vorzuschreiben, auch durch die Vorgabe der Nutzung von Rechenanlagen oder Netzelementen, die im Gebiet einer Vertragspartei zertifiziert oder zugelassen sind; die Lokalisierung von Daten im Gebiet der Vertragspartei zur Speicherung oder Verarbeitung zu verlangen und die grenzüberschreitende Übermittlung von Daten von der Nutzung von Rechenanlagen oder Netzelementen im Gebiet der Vertragsparteien oder von Lokalisierungsanforderungen im Gebiet der Vertragsparteien abhängig zu machen.[96] Wenn die EU nicht sicherstellen kann, dass in der EU befindliche Dateninfrastrukturen genutzt werden, können Cloud-Betreiber wie Amazon, Google und Microsoft ihren Bedarf an Datenspeicherung und -verarbeitung in billigeren Datenparadiesen decken und nicht in Europa.

Einige Wissenschaftler*innen haben sich einfach für eine Ausweitung der Abkommen über digitalen Handel ausgesprochen, um den Zugang Europas zu ausländischen Märkten zu verbessern, ohne darüber nachzudenken, ob der ausländische Zugang zum europäischen Markt in einem strategischen Sektor wie der Dateninfrastruktur die digitale Industrialisierung beeinträchtigen könnte.[97] Wenn der europäische Cloud-Markt von in den USA ansässigen Big-Tech-Unternehmen beherrscht wird, ist nicht klar, welchen Nutzen Europäer*innen aus einem erweiterten Marktzugang dieser Unternehmen zu den Daten von Drittländern ziehen könnten.

Dies sind komplexe Fragen, die sich darauf auswirken, wer von Daten wirtschaftlich profitiert, und die politische Abhängigkeit Europas von ausländischen Unternehmen betreffen. Sie müssen erörtert und demokratisch entschieden werden. Sie sollten nicht von den in Handelsabkommen enthaltenen Verpflichtungen in Bezug auf den Marktzugang

88 Will McCurdy, „European cloud market is being dominated by three big players", TechRadar (September 2022), https://www.techradar.com/news/european-cloud-market-is-being-dominated-by-three-big-players.
89 Regierung der Französischen Republik, Stratégie Nationale Pour Le Cloud (Mai 2021), https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/.
90 Matteo Quartieri, „France: The new national cloud strategy - data transfers and localisation implications", DataGuidance (Mai 2021), https://www.dataguidance.com/opinion/france-new-national-cloud-strategy-data-transfers.
91 „Präsidentin von der Leyens Rede zur Lage der Union bei der Plenartagung des Europäischen Parlaments", Europäische Kommission (September 2020), https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_20_1655.
92 Janosch Delcker, „Germany's plan to control its own data", *Politico EU* (September 2019), https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/.
93 Louis Westendarp und Peter O'Brien, „Gaia-X board member blames lobbying for project's gridlock", *Politico EU* (Juli 2022), https://www.politico.eu/article/eu-lobbying-cloud-project-gaia-x-board-member-says-cloud-project-must-neuter-lobbies-role-to-get-on-track/.
94 Luca Bertuzzi, „Germany calls for political discussion on EU's cloud certification scheme", Euractiv (September 2022), https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/.
95 BusinessEurope, „Free Flow of Data is at the essence of a true European Digital Single Market", Rundschreiben der Vereinigung der Industrie- und Arbeitgeberverbände in Europa (November 2016), https://www.businesseurope.eu/sites/buseur/files/media/public_letters/imco/2016-11-29_ffd_joint_statement.pdf.
96 Kapitel XX Artikel X.4 des FHA zwischen der EU und Neuseeland, auch Titel III Artikel 201 des HKA EU-VK.
97 Georgios Petropoulos et al, „Data flows, artificial intelligence and international trade: impacts and prospects for the value chains of the future", Analyse des Europäischen Parlaments, angefordert vom Ausschuss für internationalen Handel (INTA) (November 2020), https://www.europarl.europa.eu/thinktank/de/document/EXPO_IDA(2020)653617.

bestimmt werden, und die Debatten sollten auch nicht übermäßig von der Lobbymacht ausländischer Unternehmen oder der von ihnen finanzierten Denkfabriken beeinflusst werden.[98]

Die EU-Politik im Bereich des digitalen Handels steht also offensichtlich in fundamentalem Widerspruch zu der in jüngster Zeit verbreitet aufkommenden Besorgnis über die Dominanz von in den USA beheimateten Big-Tech-Giganten und die Art und Weise, wie sie europäische Daten zum Schaden der europäischen Gesellschaft kontrollieren und missbrauchen, sowie zum allgemeinen Einvernehmen über die Notwendigkeit von Schadensbegrenzungsstrategien, die die wirtschaftlichen Vorteile der Digitalisierung in Europa verstärken.

2- ... DIE MÖGLICHKEITEN DER EU ZUR BESTEUERUNG VON BIG TECH?

Die Gewinne digitaler Unternehmen sind in den letzten Jahren aufgrund der starken Zunahme grenzüberschreitender digitaler Aktivitäten infolge der Covid-19-Pandemie in die Höhe geschossen. Dennoch zahlen sie weiterhin extrem niedrige Steuern, auch in Europa.[99] Niedrige Steuerzahlungen von Big-Tech-Unternehmen sind das Ergebnis von Steuerhinterziehung und Steuerflucht sowie der übermäßigen steuerlichen Anreize mancher Regierungen, aber auch der Tatsache, dass das derzeitige Steuersystem für digitale Transaktionen nicht ausgelegt ist.[100] Dies gilt insbesondere für den digitalen Raum, wo die Wertschöpfung je nach Niveau leicht zwischen verschiedenen Bereichen der Wertschöpfungskette verschoben werden kann, die sich in unterschiedlichen Gebieten befinden können. Ein Unternehmen wie Uber kann beispielsweise seine „höchste Wertschöpfung" problemlos aus dem Land seiner Geschäftstätigkeit in eine Steueroase wie Irland verlagern, wo laut seinen Angaben die Backend-Software und die Analysefunktionen bereitgestellt werden.[101] Big-Tech-Unternehmen machen sich in hohem Maße Steueroasen zunutze, um Gewinne zu verlagern, Steuern zu hinterziehen, Vermögen zu verwahren und Regulierungsvorschriften zu unterlaufen.[102] Im Jahr 2019 berichtete Fair Tax Mark, dass Google, Facebook, Apple, Microsoft, Netflix und Amazon von 2011 bis 2020 zusammen über 100 Milliarden US-Dollar an Steuern hinterzogen.[103]

Big-Tech-Unternehmen nutzen einen zweigleisigen Ansatz, um diese günstige Situation aufrechtzuerhalten. Sie betreiben Lobbyarbeit gegen Änderungen des Steuersystems. Parallel dazu treiben sie Regeln für digitalen Handel voran, die die Befugnisse der Staaten zu ihrer Besteuerung einschränken.

Im Jahr 2016 hatte die EU die ungerechte Besteuerung der digitalen Wirtschaft bereits erkannt. Als Erstes warf die Kommission Apple[104] und Amazon[105] die Nutzung unzulässiger Steuervergünstigungen vor. Im Jahr 2018 legte sie in einer Mitteilung Vorschläge für eine Umstrukturierung des Steuersystems für die Digitalwirtschaft vor,[106] ein Projekt, das später auf Druck der USA und von Big-Tech-Unternehmen verworfen wurde.[107]

Das im Jahr 2021 im Rahmen der OECD verabschiedete globale Steuerabkommen ist derzeit die einzige Vereinbarung, die dazu beitragen könnte, dass digitale Unternehmen einen gerechteren Anteil an den Steuern zahlen,[108] obwohl kritisiert wird, dass es für eine Wiederherstellung der Steuerverteilung zugunsten der Länder, in denen die digitalen Giganten

98 Siehe zum Beispiel: Nigel Cory, „Sovereignty Requirements' in France—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners" , Information Technology and Innovation Foundation (ITIF) (Dezember 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/. Zu den Geldgebern der ITIF gehören laut einer unter https://itif.org/our-supporters/ veröffentlichten Liste unter anderem Amazon, Meta, Microsoft, Uber, Visa und Walmart.

99 In der EU unterlagen grenzüberschreitende digitale Aktivitäten einer Studie aus dem Jahr 2017 zufolge einem durchschnittlichen Steuersatz von nur 9,5 Prozent. Europäische Kommission, „Commission Staff Working Document Impact Assessment, Accompanying the document 'Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence,' and 'Proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services", Europäische Kommission SWD(2018) 81 final/2 (März 2018): 18, https://taxation-customs.ec.europa.eu/document/download/89deda55-f8a7-40f1-a767-46d58f500518_en?filename=fair_taxation_digital_economy_ia_21032018.pdf.

100 Europäische Kommission, „Commission Staff Working Document Impact Assessment", Europäische Kommission SWD (2018) 81 final/2 (2018).

101 Scilla Alecci, „Uber shifted scrutiny to drivers as it dodged tens of millions in taxes: Executives agreed to share driver data to 'contain' a tax audit and deflect from the tech giant's use of European and Caribbean tax havens, new leak shows", *International Consortium of Investigative Journalists* (Juli 2022), https://www.icij.org/investigations/uber-files/uber-tax-havens-dodge-drivers/. Siehe auch Brian O'Keefe und Marty Jones, „How Uber plays the tax shell game", *Fortune* (Oktober 2015), https://fortune.com/2015/10/22/uber-tax-shell/.

102 Rodrigo Fernandez et al, „Engineering Digital Monopolies: The financialisation of Big Tech", Zentrum für Forschung über multinationale Unternehmen (SOMO) (Dezember 2020), https://www.somo.nl/the-financialisation-of-big-tech/.

103 Fair Tax, „Tax gap of Silicon Six over $100 billion so far this decade", Pressemitteilung von Fair Tax (Dezember 2019), https://fairtaxmark.net/tax-gap-of-silicon-six-over-100-billion-so-far-this-decade/.

104 Europäische Kommission, „Kommission erklärt irische Steuervergünstigungen für Apple für unzulässig", Pressemitteilung der Europäischen Kommission (August 2016), https://ec.europa.eu/commission/presscorner/detail/de/ac_16_3727.

105 Europäische Kommission, „Staatliche Beihilfen: Kommission stellt fest, dass Luxemburg Amazon unzulässige Steuervergünstigungen von rund 250 Mio. EUR gewährt hat", Pressemitteilung der Europäischen Kommission (Oktober 2017), https://ec.europa.eu/commission/presscorner/detail/de/IP_17_3701.

106 Europäische Kommission, „Faire Besteuerung der digitalen Wirtschaft", EU-Website, https://taxation-customs.ec.europa.eu/fair-taxation-digital-economy_de.

107 Mark Scott und Emily Birnbaum, „How Washington and Big Tech won the global tax fight", Politico EU (Juni 2021), https://www.politico.eu/article/washington-big-tech-tax-talks-oecd/.

108 Siehe „Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy – 8 October 2021", OECD/G20 Base Erosion and Project Shifting Project (Oktober 2021), https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.htm.

tatsächlich tätig sind, nicht ausreicht.[109] Außerdem ist seine Annahme, insbesondere durch die USA, ziemlich ungewiss.[110]

Dieses neue Abkommen könnte durch zahlreiche unterschiedliche Bestimmungen in Abkommen über digitalen Handel untergraben werden, die darauf abzielen, die Möglichkeiten der Staaten zur Besteuerung des elektronischen Handels einzuschränken.[111] Eine Sachverständigengruppe kam im Rahmen einer eingehenden Untersuchung[112] zu dem Schluss, dass Regeln für digitalen Handel der Besteuerung in den Entwicklungsländern im Wege stehen würden. Für die europäische Steuerpolitik steht eine solche Untersuchung noch aus. Eine erste Analyse zeigt jedoch, dass die Bemühungen der EU zur Besteuerung von Big Tech möglicherweise durch ihre eigene Politik im Bereich des digitalen Handels konterkariert werden.

Verbot von Zöllen auf elektronische Übermittlungen

Fast alle Handelsabkommen der EU mit digitalen Bestimmungen beinhalten ein Verbot von Zöllen auf elektronische Übermittlungen. Das bedeutet, dass Importeure von Produkten wie Autos, Uhren und landwirtschaftlichen Erzeugnissen zwar Zöllen oder Handelssteuern unterliegen, aber die Staaten auf elektronische Versionen derselben Waren – z. B. von Büchern, Filmen oder Musik – keine Abgaben erheben dürfen. Dieses Verbot benachteiligt die Importeure und Einzelhändler von analogen Versionen derselben Produkte, bei denen es sich eher um lokale Unternehmen handelt und nicht um digitale Giganten wie Amazon, Netflix oder Apple.[113]

Die EU ist seit jeher Nettoimporteur von elektronisch übermittelten Produkten (wie in der WTO-Notiz aus dem Jahr 2016 festgestellt).[114] Im Laufe der Zeit sind die Importe der EU viel schneller gewachsen als ihre Exporte, wobei der Wert der Nettoimporte dieser Produkte von 2,2 Mrd. USD im Jahr 2020 auf 4,4 Mrd. USD im Jahr 2021 gestiegen ist. Der Wert der Nettoimporte von Videospielen hat von 3,5 Mrd. USD im Jahr 2020 auf 5,3 Mrd. USD im Jahr 2021 zugelegt. Die gebundenen Zölle in der EU auf diese elektronisch übermittelten Produkte betragen durchschnittlich 6,5 Prozent, was in vielen EU-Ländern zur Regulierung der Einfuhr dieser Produkte beitragen kann.[115]

Ein zentrales Argument der Verfechter dieses Verbots oder Moratoriums lautet, dass es für KMU der EU im Bereich des digitalen Exports Vorteile bringt. Aber große Unternehmen mit Sitz in den USA, wie Apple (Musik), Netflix (Filme) und Amazon (Bücher), profitieren von dem Moratorium wesentlich stärker als alle KMU in der EU, die mit viel größerer Wahrscheinlichkeit für normale Zölle und andere Abgaben aufkommen müssen, die Bestandteil des unternehmerischen Geschäfts sind.

Diese Bestimmung ist inzwischen Gegenstand einer äußerst kontroversen Diskussion bei der WTO, wo ein Moratorium auf solche Zölle seit 1998 auf jeder Ministerkonferenz verlängert wird. Es gibt jedoch zunehmend Anhaltspunkte dafür, dass diese fraglichen Steuerbefreiungen für Big Tech den Wachstumsperspektiven der Entwicklungsländer schaden, die auf der 12. Ministerkonferenz (MC12) im Juni 2022 daher auf deren Aufhebung drängten. Auf massiven Druck von Big Tech wurde das Moratorium letztlich um ein weiteres Jahr verlängert, aber der Kampf wird bis zur nächsten Ministerkonferenz weitergehen. Armen Ländern die Einnahmen zu entziehen, die sie für ihre eigene Entwicklung benötigen, um Amazon Steuererleichterungen zu verschaffen, ist nicht im Interesse der europäischen Öffentlichkeit.

Es gibt darüber hinaus Bestrebungen, das Moratorium für die Besteuerung des elektronischen Handels auf digitale Dienste auszuweiten. Viele europäische Länder erheben jedoch Digitalsteuern. Nach Angaben der Tax Foundation hat etwa die Hälfte aller europäischen Länder in den letzten Jahren Digitalsteuern entweder angekündigt, vorgeschlagen

109 „South Centre Comments on the 'Progress Report on the Administration and Tax Certainty Aspects of Amount A of Pillar One", South Centre Vorlage bei der OECD-Taskforce Digitale Wirtschaft zum „Progress Report on the Administration and Tax Certainty Aspects of Amount A of Pillar One" (November 2022), https://www.southcentre.int/south-centre-comments-on-progress-report-on-administration-and-tax-certainty-aspects-of-amount-a-11-november-2022/.

110 Mary McDougall, „Biden Tax proposals fall short of OECD standards for minimum rate", Financial Times (August 2022), https://www.ft.com/content/ff0c15b7-2e34-469f-8c5e-9168bbb30c51.

111 Deborah James, „Anti-development Impacts of Tax-Related Provisions in Proposed Rules on Digital Trade in the WTO", *Development* 62 (2019): 58-65, https://doi.org/10.1057/s41301-019-00205-4.

112 Jane Kelsey et al, „How 'Digital Trade' Rules Would Impede Taxation of the Digitalised Economy in the Global South", *Third World Network* (August 2020), https://twn.my/title2/latestwto/general/News/Digital%20Tax.pdf

113 Richard Kozul-Wright und Rashmi Banga, „Moratorium on Electronic Transmissions: Fiscal Implications and the Way Forward", *UNCTAD* Forschungspapier Nr. 47 (Juni 2020), https://unctad.org/system/files/official-document/ser-rp-2020d6_en.pdf

114 Allgemeiner Rat der WTO, „Fiscal implications of the customs moratorium on electronic transmissions: the case of digitisable goods (Doc # 16-6961)", WTO JOB/GC/114 (Dezember 2016).

115 Berechnungen auf der Grundlage von Daten von COMTRADE, World Integrated Trade Solutions, UNCTAD und der Weltbank, auf Anfrage bei der Autorin erhältlich.

oder erhoben.[116] Da die profitabelsten Unternehmen, die von den Steuern betroffen wären, ihren Sitz in den USA haben, bezeichnet die US-amerikanische Regierung sie als diskriminierend, obwohl sie allgemein gelten, und droht mit Vergeltungszöllen. Im Oktober 2021 verständigten sich Österreich, Frankreich, Italien, Spanien und Großbritannien auf eine Aufhebung der Digitalsteuern, und die USA erklärten sich bereit, die angedrohten Vergeltungszölle zurückzunehmen, wenn die neuen Regelungen der ersten Säule des OECD-Übereinkommens in Kraft treten.[117] Aber für den Fall, dass die USA oder andere Handelspartner die Regelungen der ersten Säule nicht umsetzen oder diese nicht zu den erwarteten Einnahmen führen, werden die europäischen Länder sicherlich daran interessiert sein, ihre Möglichkeiten zur Besteuerung von digitalen Diensten aufrechtzuerhalten.

Verbot der Datenlokalisierung

Es sind aber nicht nur die direkten Steuern, die Big Tech durch Handelsabkommen zu verhindern sucht. Eine Bestimmung, die es den Regierungen untersagt, die lokale Vorhaltung einer Datenkopie zu verlangen, erschwert es den Regierungen, Steuern auf Unternehmensgewinne zu erheben, ein Thema, das Gesetzgebern und Regulierungsbehörden ernste Sorgen bereitet. Viele Länder verlangen, dass die Daten ausländischer Unternehmen lokal gespeichert werden, damit die Steuerbehörden im Falle einer Revision oder erforderlichen Prüfung darauf zugreifen können. So müssen beispielsweise Unternehmen in Dänemark nach dem dänischen Buchhaltungsgesetz ihre Rechnungslegungsdaten fünf Jahre lang speichern.[118]

Steueroasen werden von Big Tech zunehmend als „Datenoasen" genutzt, um den staatlichen Zugriff auf Daten zu verhindern, die sonst steuerliche Auswirkungen haben könnten.[119] Verbote der Datenlokalisierung in Abkommen über digitalen Handel leisten dieser Praxis Vorschub.

Die EU-Richtlinie über die länderbezogene Berichterstattung, die die öffentliche Kontrolle der Körperschaftssteuern verbessern soll, dürfte die Rechnungslegung verbessern,[120] aber die Regeln für digitalen Handel laufen diesem Ziel zuwider. Margrethe Vestager sagte dazu: „Selbst wenn wir es schaffen, diese mögliche Vereinbarung perfekt umzusetzen, wird meiner Meinung nach immer noch die Aufgabe zu bewältigen sein, diejenigen aufzuspüren, die Energie, Kreativität und Anwaltskosten aufwenden, um sich der Entrichtung ihrer Steuern zu entziehen."[121]

Wissenschaftler*innen haben noch viele weitere Bestimmungen für den digitalen Handel ermittelt, die die staatlichen Möglichkeiten zur Besteuerung von Big Tech beschränken könnten.[122] Es gibt auch Ausnahmen in den Steuervorschriften, die mehr Flexibilität und Handlungsspielraum ermöglichen. Diese stützen sich jedoch häufig auf überholte WTO-Ausnahmen, die für das digitale Zeitalter ungeeignet sind, z. B. im Freihandelsabkommens zwischen der EU und Neuseeland, oder unglaublich komplex sind,[123]
Big Tech sollte keine weiteren Bestimmungen in „Handelsabkommen" durchsetzen können, die die Hinterziehung gerechter Steuern ermöglichen.

3- ... DIE MACHT DER EU-AGENTUREN ZUR REGULIERUNG VON BIG TECH?

Europa setzt auch auf die Chance, mit der Festlegung globaler Normen für das Internet wieder eine führende Position einzunehmen. Wie in der Digitalstrategie der EU dargelegt, umfasst das Bemühungen um den Schutz der Menschen vor Cyberbedrohungen (Hacking, Ransomware, Identitätsdiebstahl); die Gewährleistung, dass künstliche Intelligenz so entwickelt wird, dass die Rechte der Menschen geachtet werden und sie ihr Vertrauen verdient; die Verbesserung des Zugangs zu hochwertigen Daten bei gleichzeitiger

116 „Austria, France, Hungary, Italy, Poland, Portugal, Spain, Turkey, and the United Kingdom have implemented a digital services tax. Belgium, the Czech Republic, Denmark, and Slovakia have published proposals to enact a digital services tax, and Latvia, Norway, and Slovenia have either officially announced or shown intentions to implement a digital tax." Daniel Bunn und Elke Asen, „What European Countries Are Doing about Digital Services Taxes", *Tax Foundation* (August 2022), https://taxfoundation.org/digital-tax-europe-2022/.

117 „Joint Statement from the United States, Austria, France, Italy, Spain, and the United Kingdom, Regarding a Compromise on a Transitional Approach to Existing Unilateral Measures During the Interim Period Before Pillar 1 is in Effect", Pressemitteilung des Finanzministeriums der Vereinigten Staaten (Oktober 2021), https://home.treasury.gov/news/press-releases/jy0419.

118 Unter bestimmten Bedingungen können Unternehmen von der dänischen Behörde für Handel und Unternehmen die Genehmigung zur Aufbewahrung ihrer Buchhaltungsunterlagen im Ausland erhalten. Dies wird in der Praxis jedoch relativ restriktiv gehandhabt, sodass diese Genehmigung selten erteilt wird. Matthias Bauer et al, „Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", European Centre for International Political Economy Policy Brief (März 2016), https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

119 Sofia Scasserra und Adriana Foronda, „Banking on data: How the world's tax havens became the data centres for the digital economy", Transnational Institute (November 2022), https://www.tni.org/en/publication/banking-on-data

120 „Richtlinie (EU) 2021/2101 des Europäischen Parlaments und des Rates vom 24. November 2021 zur Änderung der Richtlinie 2013/34/EU im Hinblick auf die Offenlegung von Ertragsteuerinformationen durch bestimmte Unternehmen und Zweigniederlassungen (Text von Bedeutung für den EWR)", Europäisches Parlament PE/74/2021/INIT (November 2021), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021L2101&from=DE.

121 Interview mit Molly Wood und Stephanie Hughes, „Big Tech dodged one tax bullet, but another one is coming", *Marketplace Radio* (Juli 2021), https://www.marketplace.org/shows/marketplace-tech/big-tech-dodged-one-tax-bullet-but-another-one-is-coming/.

122 Kelsey et al, „How 'Digital Trade' Rules Would Impede", *TWN* (2020).

123 Ibid: 41-44.

Gewährleistung des Schutzes personenbezogener und sensibler Daten; den Zugang zu Finanzmitteln und Möglichkeit der Expansion für eine lebendige Gemeinschaft innovativer und rasch wachsender Start-ups und KMU und zahlreiche weitere am Menschen orientierte Ziele.[124]

Aufkommende Probleme bestätigen, dass die Erhaltung des politischen Regulierungsspielraums viel entscheidender für die Wiederherstellung der europäischen Führungsposition ist, indem ein umfassender Nutzen der Digitalisierung sichergestellt und europäische Grundrechte im digitalen Raum garantiert werden. Die Regeln für digitalen Handel sind breit gefächert und umfassend. Regulierung im öffentlichen Interesse wäre anfechtbar, wobei zur Verteidigung nur das schmale Fenster begrenzter Ausnahmen für die Regulierung im öffentlichen Interesse herangezogen werden könnte. Die Zukunftssicherheit der Regulierungsfähigkeit im Einklang mit der sich entwickelnden politischen und wirtschaftlichen Landschaft überwiegt daher bei weitem alle von Big Tech vorgebrachten Behauptungen über angebliche Vorteile der Regeln für digitalen Handel. Dauerhafte, verbindliche Vorschläge für Verträge, die der Wunschliste US-amerikanischer Big-Tech-Unternehmen im Hinblick auf die Behinderung europäischer Regulierung entsprechen, sind angesichts des sich herausbildenden politischen Konsens in der EU über die digitale Industrialisierung und all der nachfolgend beschriebenen Bedenken offensichtlich keine Lösung.

Unzählige Aspekte der dringend erforderlichen Regulierung von Big Tech wären von den Regeln für digitalen Handel betroffen. Dieser Abschnitt konzentriert sich auf zwei Aspekte: Finanzregulierung und Cybersicherheit.

Regulierung des Finanzsektors

Entscheidungen wie die, wem ein Kredit für den Kauf eines Hauses oder eines Autos gewährt wird oder wer eine Versicherung auf der Grundlage von Kreditrisiken erhält, werden immer häufiger von Daten und Algorithmen getroffen. Aber algorithmische Systeme sind anfällig für Diskriminierung.[125] Wenn eine Maschine „lernt", dass Menschen mit bestimmten Namenstypen, einem bestimmten Flüchtlingsstatus oder einer bestimmten aktuellen Adresse ein höheres Risiko darstellen, könnten solche Algorithmen einen höheren Zinssatz anzeigen, als er auf der Grundlage rechtlicher Kriterien, wie Einkommensniveau und Kredithistorie, zugewiesen würde. Es gibt unzählige Gründe dafür, warum eine Regierung dazu in der Lage sein muss, für die Regulierung finanzieller Transaktionen auf Quellcode zuzugreifen, um Grundrechtsverletzungen auszuschließen.

Neben der Gerechtigkeit bei der Regulierung des Finanzsektors ist auch die finanzielle Stabilität eine zentrale Frage. Hochfrequenzhandel und die zunehmende Automatisierung des Börsenbetriebs gehen aufgrund der Verstärkung von Volatilität, Dominoeffekten, Unsicherheit und fehlgeleiteten Algorithmen mit enormen Risiken für die finanzielle Stabilität einher.[126] Ähnliche Argumente werden nach Angaben des Europäischen Ausschusses für Systemrisiken (ESRB) im Hinblick auf Kryptowährungen, Ransomware[127] und Geldwäsche vorgebracht,[128] was den Europäischen Rat im Oktober 2022 dazu veranlasste, die Verordnung über Märkte für Kryptowerte zu verabschieden.[129] Entscheidungen im Finanzsektor werden zunehmend von Algorithmen bestimmt, die der Regulierungsaufsicht und öffentlicher Kontrolle unterstellt werden müssen. Für den Finanzsektor gilt eine Ausnahmeregelung für aufsichtsrechtliche Maßnahmen, die jedoch recht umstritten ist.[130]

Handelsbestimmungen, die es Regierungen verbieten, die Offenlegung von Quellcode zur Gewährleistung der Sicherheit des Finanzsektors zu verlangen, würden die für die Garantie der finanziellen Sicherheit erforderliche Regulierungsaufsicht in einer Situation verhindern, in der der algorithmische Handel einen wachsenden Anteil der Finanzmärkte erobert und die finanzielle Stabilität beeinflusst.

Elektronische Authentifizierung

Mit den Regeln würde den Staaten auch die Möglichkeit genommen, die Authentifizierungsmethode für eine Online-Transaktion festzulegen. In Artikel X.9 des Abkommens zwischen der EU und Neuseeland über elektronische

124 Europäische Kommission, „Gestaltung der digitalen Zukunft Europas", Factsheet FS/20/278 (Februar 2020), https://ec.europa.eu/commission/presscorner/detail/de/fs_20_278.
125 Adair Morse und Karen Pence, „Technological Innovation and Discrimination in Household Finance", *National Bureau of Economic Research Arbeitspapier Nr. 26739* (Februar 2020), https://www.nber.org/system/files/working_papers/w26739/w26739.pdf
126 Elvis Picardo, „4 Big Risks of Algorithmic High-Frequency Trading", Investopedia (Januar 2022), https://www.investopedia.com/articles/markets/012716/four-big-risks-algorithmic-highfrequency-trading.asp.
127 Weltwirtschaftsforum, „The Global Risks Report 2022: 17th Edition", Weltwirtschaftsforum (Januar 2022), https://wef.ch/risks22.
128 Jack Schickler, „Crypto Popularity Could Pose Stability Risk, EU Watchdog Warns, as It Ponders New Powers", *CoinDesk* (März 2022), https://www.coindesk.com/policy/2022/03/31/crypto-popularity-could-pose-stability-risk-eu-watchdog-warns-as-it-ponders-new-powers/.
129 Issam Hallak, „Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets", in „A Europe Fit for the Digital Age", Legislative Train (Dezember 2022), https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1.
130 Kelsey et al, „How 'Digital Trade' Rules Would Impede", TWN (August 2020): 48.

Authentifizierung heißt es: „Eine Vertragspartei darf keine Maßnahmen einführen oder aufrechterhalten, die die an einer elektronischen Transaktion Beteiligten daran hindern würden, im gegenseitigen Einvernehmen geeignete Methoden der elektronischen Authentifizierung für ihre Transaktion festzulegen." Diese Regel besagt im Wesentlichen, dass eine Regierung kein höheres Maß an Sicherheit verlangen kann.[131] In der Geschichte gibt es jedoch zahlreiche Beispiele dafür, dass Staaten es versäumt haben, die Sicherheit von Finanztransaktionen zu regulieren und dafür den Preis zahlten.

Nur durch Regulierung haben Finanzdienstleister und andere Unternehmen die Sicherheit ihrer Transaktionen verbessert. Zwei-Faktor-Authentifizierung (TFA) entwickelt sich zum globalen Standard für Finanz- und andere risikobehaftete Transaktionen Die zweite Zahlungsdiensterichtlinie der EU enthält die Anforderung einer starken Kundenauthentifizierung[132], wofür TFA die wichtigste Methode ist. Dies könnte allerdings von einem ausländischen Diensteanbieter unter Verweis auf sein in Handelsabkommen verankertes „Recht" auf Bestimmung der elektronischen Authentifizierungsmethode angefochten werden. Natürlich ist elektronische Authentifizierung auch für ein breiteres Spektrum von Bereichen wichtig, wie das Internet der Dinge (IoT).

Regulierung der Cybersicherheit im Internet der Dinge (IoT)

Die Anzahl von Produkten für den Alltagsgebrauch, die mit dem Internet verbunden sind, nimmt exponentiell zu. Der IoT-Markt für digital vernetzte Geräte ist für Fachleute im Bereich der Cybersicherheit ein wachsendes Problem, da IoT-Geräte regelmäßig von Cyberattacken und Datenlecks betroffen sind. Laut einem Folgenabschätzungsbericht der Europäischen Kommission belaufen sich die jährlichen Kosten von Datenschutzverletzungen auf mindestens 10 Milliarden Euro und die jährlichen Kosten böswilliger Versuche zur Störung des Internetverkehrs auf mindestens 65 Milliarden Euro.[133]

Abgesehen von den Kosten und der Sicherheit von Daten ist dies auch von großem Belang für die menschliche Gesundheit und Sicherheit. Vernetzte Fahrzeuge könnten gehackt werden und zu gefährlichen Fahrmanövern veranlasst werden; böswillige Hacker von medizinischen Geräten wie Herzschrittmachern könnten die Gesundheit von Menschen schädigen; das Hacken von Babyfonen könnte Kinder gefährden. In Anbetracht des weltweit unzureichenden Stands der Regulierung von Cybersicherheit weiten europäische Regierungen derzeit die Rechtsvorschriften zur Cybersicherheit auf IoT-Geräte aus, um sensible Daten (einschließlich Finanzdaten) und die Sicherheit der Verbraucher*innen zu schützen.

Am 22. März 2022 verabschiedete die Europäische Kommission zwei neue Vorschläge für eine Verordnung über Cybersicherheit[134] und eine Verordnung über Informationssicherheit[135], mit denen der bestehende Rahmen von 2019 aktualisiert wurde. Diese Verordnungen, die derzeit noch das Gesetzgebungsverfahren durchlaufen, stützen sich auf die EU-Strategie für eine Sicherheitsunion und die EU-Cybersicherheitsstrategie für die digitale Dekade.[136]

Im September 2022 schlug die Europäische Kommission neue Bestimmungen speziell für intelligente Geräte vor, das Cyberresilienzgesetz.[137] Die neuen Vorschriften werden das bestehende Netz- und Informationssystem (NIS-Richtlinie)[138], die NIS2-Richtlinie[139] (für Anbieter von Cloud-Diensten und Software as a Service) und das EU-Cybersicherheitsgesetz[140] ergänzen.

Für die Regulierung der Cybersicherheit im Hinblick auf das IoT werden Standards wie die Zwei-Faktor-

131 Sanya Reid Smith, „Electronic Authentication: Some Implications", *Third World Network* (August 2018), https://ourworldisnotforsale.net/2018/esignatures2018-9.pdf.
132 Europäische Bankaufsichtsbehörde, „Question on delegation of 2-Factor Authentication (2FA) to PISP, AISP or other third party", EBA Question ID 2020_5643 und Legal Act Directive 2015/2366/EU (PSD2), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5643.
133 Europäische Kommission, „Commission Staff Working Document Impact Assessment Report Accompanying the document: Commission Delegated Regulation supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive", Europäische Kommission SWD(2021) 302 final (Oktober 2021), https://single-market-economy.ec.europa.eu/system/files/2021-10/SWD%282021%29%20302_EN_impact_assessment_part1_v3.pdf.
134 Europäische Kommission Generaldirektion Informatik, „Proposal for Cybersecurity Regulation", Vorschlag für eine Verordnung der Europäischen Kommission (März 2022), https://ec.europa.eu/info/publications/proposal-cybersecurity-regulation_en.
135 Europäische Kommission, „Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union", Europäische Kommission COM(2022) 119 final (März 2022), https://ec.europa.eu/info/files/proposal-regulation-information-security-institutions-bodies-offices-and-agencies-union_en.
136 Sarah O'Brien und Cynthia O'Donoghue, „European Commission adopts two proposals for cybersecurity and information security regulations", ReedSmith Technology Law Dispatch (April 2022), https://www.technologylawdispatch.com/2022/04/privacy-data-protection/european-commission-adopts-two-proposals-for-cybersecurity-and-information-security-regulations/.
137 Europäische Kommission, „EU Cyber Resilience Act: New EU cybersecurity rules ensure safer hardware and software", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
138 Europäische Kommission, „NIS2-Richtlinie" EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/nis2-directive.
139 Europäische Kommission, „Kommission begrüßt politische Einigung über neue Vorschriften für die Cybersicherheit von Netz- und Informationssystemen", Pressemitteilung der Europäischen Kommission (Mai 2022), https://ec.europa.eu/commission/presscorner/detail/de/IP_22_2985.
140 Europäische Kommission, „Das EU-Cybersicherheitsgesetz", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-act.

Authentifizierung (TFA) sowie die Offenlegung von Quellcode gegenüber maßgeblichen Behörden erforderlich sein, um hochriskante Algorithmen und Maßnahmen zur Cybersicherheit zu bewerten. Aber die von der EU im Rahmen der Regeln für „digitalen Handel" vorangetriebenen Bestimmungen würden Staaten die Befugnis nehmen, die notwendige Offenlegung von Quellcode zu verlangen, selbst bei bestimmten Ausnahmen.

Diese Einschränkungen sind angesichts der bisherigen Praxis und der aktuellen Notwendigkeit einer verstärkten Aufsicht über die Cybersicherheit im öffentlichen Interesse inakzeptabel. Wie schon oben erwähnt, werden die Ausnahmen der Bestimmungen über die Offenlegung von Quellcode– unter anderem im jüngsten FHA zwischen der EU und Neuseeland – der enormen und dringenden Notwendigkeit verstärkter öffentlicher Aufsicht bei weitem nicht gerecht.

Einige Vertreter*innen der Unternehmensperspektive argumentieren, dass Handelsbestimmungen genutzt werden können, um auszuschließen, dass Cybersicherheitsregeln zu Protektionismus werden, indem internationale Normen favorisiert werden, die nicht handelsbeschränkend sind.[141] Die Europäer haben allerdings klare Ziele zur Festlegung von Normen aufgestellt, die höher sind als die derzeit international geltenden Normen.[142] Der Gedanke, dass Staaten durch Handelsabkommen in ihren Möglichkeiten eingeschränkt werden sollten, höhere Normen festzulegen, macht angesichts der wachsenden Bedrohungen für die Cybersicherheit und der anhaltenden Notwendigkeit erhöhter Sicherheitsstandards keinen Sinn.

Cybersicherheit ist vielmehr eine grundlegende Frage der öffentlichen Sicherheit und Gefahrenabwehr und der Grundrechte. Normen sollten über demokratische Kanäle im Rahmen öffentlicher Debatten und auf der Grundlage von einem hohen Maß an qualifiziertem technischem Input festgelegt werden, Die wirtschaftlichen Interessen ausländischer Unternehmen wie Big Tech sollten in Anbetracht der Tragweite der Probleme und der bisherigen Bilanz derselben Unternehmen im Hinblick auf missbräuchliche Datenpraktiken und Lücken bei der Cybersicherheit keine Rolle spielen.

4- ... DIE ÖFFENTLICHEN DIENSTE DER EU?

Qualitativ hochwertige und zugängliche öffentliche Dienste sind ein Eckpfeiler europäischen Lebens und eine wesentliche Grundlage des Gesellschaftsvertrags, die für die Erhöhung der Lebensqualität und Lebenserwartung der europäischen Bevölkerung sorgt. Öffentliche Dienste könnten allerdings durch die von Big Tech vorgeschlagenen Regeln für digitalen Handel beeinträchtigt werden. Die potenziellen Auswirkungen auf die Besteuerung und die staatlichen Einnahmen, die für die Ausrechterhaltung erschwinglicher und qualitativ hochwertiger öffentlicher Dienste unverzichtbar sind, stellen in dieser Hinsicht nur eines der Probleme dar. Menschenrechtsorganisationen haben Bedenken hinsichtlich der übermäßigen Abhängigkeit von algorithmischen Entscheidungssystemen bei der Festlegung sozialer und wirtschaftlicher Rechte wie dem Anspruch auf Sozialleistungen und andere öffentliche Dienste erhoben,[143] weshalb KI einer angemessenen Aufsicht unterliegen muss.

Die vorgeschlagenen Regeln könnten eine weitere Privatisierung öffentlicher Dienste zur Folge haben und damit zu Arbeitsplatzverlusten und einer Aushöhlung von Arbeitnehmerrechten führen. Die Digitalisierung öffentlicher Dienste ist häufig Gegenstand öffentlich-privater Partnerschaften mit Big-Tech-Unternehmen, was der Privatisierung von Arbeitsplätzen Vorschub leistet. Privatisierung führt nachweislich zur Reduzierung guter Arbeitsplätze, da Unternehmen miteinander konkurrieren, indem sie die Löhne und Sozialleistungen senken und Gewinne aus staatlichen Zuwendungen abschöpfen.[144]

Gleichzeitig entzieht Privatisierung ein breites Spektrum von Teilbereichen dieser Dienste der öffentlichen Aufsicht. So umfasst die Digitalisierung im Gesundheitswesen „Telemedizin", aber auch die Digitalisierung von Patientenakten, Diagnosen, Entscheidungen über Personalfragen und die Zuteilung von Ressourcen und Algorithmen zur Ermittlung des Versicherungsschutzes. Dies alles

141 Joshua P. Meltzer und Cameron F. Kerry, „Cybersecurity and digital trade: Getting it right", Brookings-Bericht (September 2019), https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/.
142 Siehe Europäische Kommission, „Sichere Lösungen für das Internet der Dinge", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/secure-internet-things.
143 Siehe Phillip Alston, „Report of the Special Rapporteur on Extreme Poverty and Human Rights", UN-Menschenrechtsrat A/74/48037 (Oktober 2019), https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx; Lina Dencik und Anne Kaun, „Datafication and the Welfare State: An Introduction", *Global Perspectives* 1, Nr. 1 (2020), https://www.diva-portal.org/smash/get/diva2:1448242/FULLTEXT02.pdf; Human Rights Watch, „UN: Protect Rights in Welfare Systems' Tech Overhaul", HRW Pressemitteilung (Oktober 2019), https://www.hrw.org/news/2019/10/17/un-protect-rights-welfare-systems-tech-overhaul.
144 Christina J. Colclough, „Reshaping the Digitization of Public Services", *New England Journal of Public Policy 34, No. 1* (Oktober 2022), https://scholarworks.umb.edu/nejpp/vol34/iss1/9.

würde den neuen Regeln für digitalen Handel unterliegen und damit weniger reguliert werden.[145]

Die Aufrechterhaltung eines starken Sektors öffentlicher Dienstleistungen in Europa erfordert die Stärkung der Rechenschaftspflicht für Algorithmen und die digitale Weiterqualifizierung der Beschäftigten im öffentlichen Dienst. Sie setzt des Weiteren die Nutzung großer Datensätze durch den öffentlichen Sektor zur Verbesserung von Bildung, Gesundheit, Verkehr, Wasser- und Stromversorgung und anderen öffentlichen Dienstleistungen voraus. Sie erfordert ferner, dass öffentliche Dienste das Recht behalten, auf die Daten zuzugreifen, die im Rahmen von Partnerschaften mit privaten Unternehmen erzeugt werden, und sie zu kontrollieren. Diese Ziele werden nicht zu erreichen sein, wenn Big Tech das Verbot der Offenlegung von Quellcode und die Beibehaltung der Datenerhebung im privaten Raum durchsetzt.

Intelligente Städte

„Intelligente Städte" sind digital vernetzte Städte, die zur Unterstützung der Stadtplanung, auch öffentlicher Dienste, große Datenmengen erheben. In einigen Städten lehnen sich jedoch Bürgerbewegungen gegen die Extraktion ihrer Daten für private Profite auf. In Europa ist Barcelona von der üblichen Praxis abgekehrt. Es hatte lange Zeit eine Vorreiterrolle unter den intelligenten Städten. Sensoren dimmen die Straßenbeleuchtung, wenn keine Menschen in der Nähe sind, wodurch die Stadt Millionen von Dollar an Stromkosten einspart. Wasserzähler messen den Feuchtigkeitsbedarf in öffentlichen Parks, womit mehrere zehn Millionen an Wasserkosten eingespart werden.[146]

Mit der Zeit wehrten sich die Bürger*innen jedoch dagegen, dass die Daten, die sie im Bereich öffentlicher Dienste generierten, privatisiert wurden und im Rahmen von öffentlich-privaten Partnerschaften in den Besitz von Unternehmen gelangten. Mittlerweile steht die Stadt an der Spitze der Bewegung für die Nutzung von Daten für das Gemeinwohl hinsichtlich der Datenautonomie und der Verlagerung der Datenverwaltung. Die naheliegende Lösung lag in der Beschaffungspolitik: Die Stadt verlangt nun in ihren Verträgen mit Technologieunternehmen die Offenlegung von Daten. Francesca Bria, die damalige Leiterin des Amtes für Technologie und digitale Innovation der Stadt Barcelona, erklärte, dass Klauseln über Datenhoheit und öffentliches Dateneigentum in Verträge aufgenommen würden.[147] Im europäischen Projekt Decode (DEcentralised Citizen-owned Data Ecosystems)[148], bei dem die innovatorischen Städte Barcelona und Amsterdam mit gutem Beispiel vorangehen, denken Städte ihre Zukunft neu, indem sie die Technologien und Dateninfrastrukturen an ihre Einwohner*innen anpassen und nicht umgekehrt.

Diese Daten können im Rahmen des Betriebs öffentlicher Dienstleistungen als öffentliche Ressource generiert werden. Wenn aber die Datenerhebung im Bereich öffentlicher Dienste oder die Erbringung der Dienstleistung selbst privatisiert ist, gilt dies auch für die Daten. Um Daten zur Verbesserung öffentlicher Dienste zu erhalten und den zuständigen Behörden wertvolle Steuergelder zu ersparen, müssten die Daten vom privaten Betreiber an den öffentlichen Sektor übermittelt werden.

Die meisten europäischen Städte ergreifen zwar noch keine Maßnahmen zur Gewährleistung der Datenhoheit und des öffentlichen Dateneigentums, täten sie es aber, könnten nach den vorgeschlagenen Regeln der EU für digitalen Handel, wonach es Staaten verboten ist, die Lokalisierung von Daten zur Speicherung oder Verarbeitung im Hoheitsgebiet der Vertragspartei zu verlangen, die Offenlegungspflicht der Unternehmen im Rahmen von Handelsabkommen angefochten werden.

5- ... DATENSCHUTZ UND DATENSICHERHEIT DER EU-BÜRGER*INNEN?

Die im Jahr 2016 veröffentlichte bahnbrechende Datenschutz-Grundverordnung (DSGVO) setzte den globalen Standard für das Grundrecht auf Datenschutz und Datensicherheit. Außerhalb Europas wurde die DSGVO als massives Handelshemmnis kritisiert.[149] Seitdem ist es angesichts der metastasierenden Auswirkungen des Überwachungskapitalismus nur noch dringlicher geworden, das Menschenrecht auf Privatsphäre und das Grundrecht auf Datenschutz zu schützen.[150]

145 Es gibt eine Ausnahmeregelung, u. a. in Artikel 1 des Freihandelsabkommens zwischen der EU und Neuseeland, für Informationen, die einer Vertragspartei vorliegen oder von oder in ihrem Namen verarbeitet werden, oder Maßnahmen im Zusammenhang mit solchen Informationen einschließlich mit deren Erhebung verbundenen Maßnahmen. Die Grenzen sind unklar, insbesondere wenn private Unternehmen die Daten erheben und speichern und sie verlagern und nutzen können.
146 Laura Adler, „How Smart City Barcelona Brought the Internet of Things to Life", Data-Smart City Solutions (Februar 2016), https://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789.
147 Thomas Graham, „Barcelona is leading the fightback against smart city surveillance", Wired (Mai 2018), https://www.wired.co.uk/article/barcelona-decidim-ada-colau-francesca-bria-decode.
148 Mehr zum Projekt DECODE unter: https://decodeproject.eu/what-decode.
149 Philip Thompson, „The International Trade barrier Index 2021", Tholos Foundation (2021), https://atr-tbi19.s3.amazonaws.com/TBI_FullReport_2021_FINAL.pdf
150 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs: Januar 2019).

Trotz alledem enthalten die Vorschläge der EU für den digitalen Handel in bilateralen oder regionalen Abkommen und bei der WTO nach wie vor Bestimmungen, die den Unternehmen Rechte für die grenzüberschreitende Übermittlung von Daten, auch personenbezogener Daten, garantieren.

Als Erstes schlug das Europäische Parlament in Europa Alarm hinsichtlich der Notwendigkeit, personenbezogene Daten aus Freihandelsabkommen auszuklammern.[151] Seit dem Jahr 2018 versucht die EU, die Gewährleistung des uneingeschränkten freien Datenverkehrs durch ein gewisses Maß an Schutz für personenbezogene Daten auszugleichen, um die DSGVO zu erfüllen. Neuere Handelsabkommen, wie die mit Großbritannien und Neuseeland, enthalten eine Klausel, die den Schutz personenbezogener Daten und der Privatsphäre garantieren soll. Es bestehen jedoch starke Zweifel daran, ob diese Schutzklausel die Privatsphäre wirklich schützt.

Nach der Veröffentlichung des HKA zwischen der EU und dem Vereinigten Königreich erklärte der Europäische Datenschutzbeauftragte (EDSB), er bedauere, dass das HKA die horizontalen Bestimmungen der EU für den grenzüberschreitenden Datenverkehr und den Schutz personenbezogener Daten nicht getreu übernehme. Diese Bestimmungen, die die Europäische Kommission wiederholt als nicht verhandelbar bezeichnet habe, ermöglichten es der EU, Maßnahmen zur Erleichterung des grenzüberschreitenden Datenverkehrs in Handelsabkommen aufzunehmen und gleichzeitig die Grundrechte des Einzelnen auf Datenschutz und Privatsphäre zu wahren. Durch die Änderung dieser horizontalen Bestimmungen schaffe das HKA Rechtsunsicherheit bezüglich der EU-Position zum Schutz personenbezogener Daten im Rahmen von Handelsabkommen und könne zu Konflikten mit dem EU-Rechtsrahmen für den Datenschutz führen, so der EDSB.[152]

In einer wissenschaftlichen Untersuchung über die Anwendung der DSGVO im Rahmen der Bestimmungen für grenzüberschreitende Datenübermittlungen in Abkommen über digitalen Handel wurde festgestellt, dass das Handelsrecht bei der Festlegung der Regeln für den grenzüberschreitenden Handel im Zeitalter von Big Data und KI nicht vorpreschen sollte, ohne die Verantwortung der Mitglieder für die Ergreifung von Maßnahmen zu berücksichtigen, die sicherstellen, dass KI und die gesamte Datenverwaltung in vollem Umfang mit dem nationalen Menschenrechtsrahmen im Einklang stehen.[153]

Zivilgesellschaftliche Organisationen haben für den Fall, dass Regeln für den grenzüberschreitenden Datenverkehr Bestandteil des künftigen WTO-Übereinkommens sind, wiederholt gefordert, Sicherheitsklauseln vorzusehen, um zu gewährleisten, dass das Recht der Menschen auf Privatsphäre und Datenschutz immer Vorrang vor den Regeln über den Datenverkehr hat, damit die digitale Wirtschaft gedeihen und die Menschen darauf vertrauen können, dass ihre Grundrechte gewahrt werden. Wenn diese Bedingungen nicht eingehalten werden könnten, müssten die Länder Regeln über den grenzüberschreitenden Datenverkehr aus den Verhandlungen und allen endgültigen Verträgen ausklammern oder dürften sich nicht darauf festlegen. Mit der Annahme anderer verbindlicher internationaler Regeln – insbesondere des Übereinkommens 108+ des Europarates über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten[154] – werde eine größere Ausgewogenheit gewährleistet. Bisher seien bereits 55 Länder dem Übereinkommen 108+ beigetreten.[155]

Es ist interessant, dass die EU sich zwar der Bedeutung des Schutzes personenbezogener Daten bewusst ist und hierzu politische Maßnahmen umsetzt, die digitale Revolution aber gleichzeitig deutlich macht, wie wichtig der Schutz nicht personenbezogener Daten ist. Einer der Gründe für den Schutz nicht personenbezogener Daten ist, dass jüngsten Forschungen zufolge[156] nicht identifizierbare Daten durch den Einsatz von Reverse-Engineering und maschinellem Lernen Einzelpersonen wiedererkennen können, d. h. nicht personenbezogene Daten können

151 Svetlana Yakovleva und Kristina Irion, „Pitching trade against privacy: reconciling EU governance of personal data flows with external trade", International Data Privacy Law 10, No. 3 (August 2020): 201–22, https://doi.org/10.1093/idpl/ipaa003.

152 Europäischer Datenschutzbeauftragter, „Data protection is non-negotiable in international trade agreements", Pressemitteilung des EDSB (Februar 2021), https://edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_de. Die horizontalen EU-Bestimmungen können hier eingesehen werden: Europäische Kommission, „EU proposal for provisions on Cross-border data flows and protection of personal data and privacy", EU-Vorschlag (Juli 2018), http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf.

153 Kristina Irion, „Chapter 11 - Panta Rhei: A European Perspective on Ensuring a High Level of Protection of Human Rights in a World in Which Everything Flows", in „Part III - Safeguarding Privacy and Other Users' Rights in the Age of Big Data" in *Big Data and Global Trade Law*, herausgegeben von Mira Burri (Cambridge University Press: Juli 2021): 231-242, https://www.cambridge.org/core/books/big-data-and-global-trade-law/panta-rhei/B0E5D7851240E0D2F4562B3C6DFF3011#.

154 „Convention 108 + Convention for the protection of individuals with regard to the processing of personal data", Europarat (Juni 2018), https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

155 European Digital Rights, „WTO trade talks must respect privacy: Together with over 40 consumer and digital rights groups, EDRi calls on global governments to place people's fundamental rights to data protection and privacy at the centre of digital trade negotiations", *EDRi* (November 2020), https://edri.org/our-work/wto-trade-talks-must-respect-privacy/.

156 Luc Rocher, Julien M. Hendrickx und Yves-Alexandre de Montjoye, „Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications* 10, Nr. 1 (Juli 2019), https://www.nature.com/articles/s41467-019-10933-3.

in personenbezogene Daten umgewandelt werden. Die Untersuchung zeigt erstmals, wie einfach und exakt dies möglich ist – selbst mit unvollständigen Datensätzen. Im Rahmen der Untersuchung wurden Amerikaner*innen in jedem verfügbaren „anonymisierten" Datensatz zu 99,98 Prozent korrekt wiedererkannt. Wenn also Beschränkungen der grenzüberschreitenden Übermittlung personenbezogener Daten zugelassen werden und digitale Regeln im Hinblick auf „personenbezogene" Daten zum Schutz der Privatsphäre und aus Gründen der nationalen Sicherheit flexibel gestaltet werden, muss dieselbe Flexibilität für den Schutz nicht personenbezogener Daten gelten.

Angemessenheitsbeschlüsse

Die EU erlaubt die freie Übermittlung personenbezogener Daten in Drittländer, mit denen ein Angemessenheitsbeschluss vereinbart wurde, der ein vergleichbares Schutzniveau für personenbezogene Daten wie in der EU gewährleistet.

Der freie Datenverkehr mit den USA wurde in den letzten Jahren eingeschränkt, weil kein Angemessenheitsbeschluss besteht. Im Oktober 2022 verständigten sich die USA und die EU auf das Data-Privacy-Framework.[157] Es soll gewährleisten, dass europäische personenbezogene Daten bei der Übermittlung in die USA sicher sind. Die Vereinbarung wird derzeit geprüft. Da es in den USA kein nationales Datenschutzgesetz gibt, und angesichts der Überwachungspraktiken von Big-Tech-Unternehmen und der Regierung der USA kann es vor dem Europäischen Gerichtshof noch immer angefochten werden. Eine Gruppe von Datenschutzorganisationen hat darum gebeten, die Verhandlungen über ein neues transatlantisches Abkommen über den Datenverkehr auszusetzen, bis der US-Kongress umfassende Datenschutzgesetze verabschiedet und die nationalen Überwachungsgesetze reformiert.[158]

6- ... SCHUTZ DER BESCHÄFTIGTEN IN DER EU?

Verschiebung des Kräftegleichgewichts zwischen Unternehmen und Beschäftigten

Eines der Hauptmerkmale der Hyperglobalisierung besteht darin, dass Unternehmen ihre überdimensionierten Profite nutzen, um die Regeln der Weltwirtschaft zu manipulieren – auch durch Handelsabkommen. Sie tun dies, um Einkommen nach oben umzuverteilen, hin zu sich selbst und ihren hoch bezahlten Führungskräften, weg von den Menschen, durch deren Hände Arbeit die Profite erzeugt werden. Auf diese Weise konnten Unternehmen einen zunehmenden Anteil des durch die Arbeit der Beschäftigten geschaffenen Produktionswerts abschöpfen, deren kollektive Macht eindämmen und einen Teufelskreis von Macht- und Einkommensverlusten in Gang setzen.

Im Klartext stellen die Regelvorschläge für „digitalen Handel" in Handelsabkommen einen Versuch von Big Tech dar, die Aufwärtsverteilung des Einkommens weg von der Arbeit hin zum Kapital weiter zu festigen.

Unternehmen haben in den letzten Jahrzehnten den weitaus überwiegenden Teil der Produktivitätsgewinne eingesteckt, die aus technologischem Fortschritt und dem erweiterten Einsatz von Technologien resultieren. Unternehmen haben in unzulässiger Weise politische Maßnahmen kontrolliert und Branchen umstrukturiert, um den Anteil der Beschäftigten am Gewinn zu reduzieren.[159] In Diskussionen über die Zukunft der Arbeit kann die Betonung von Umschulung und qualifikationsbasiertem technologischem Wachstum nützlich sein, sollte aber nicht vom eigentlichen Thema ablenken. Der wichtigste Aspekt bei der Festlegung, wer von der erweiterten Nutzung von Technologien profitieren wird, ist das politische Umfeld, in dem die betreffende Technologie eingesetzt wird. Diese politischen Maßnahmen werden auf lokaler, branchenbezogener und nationaler Ebene durch Kollektivverhandlungen und/oder auf nationaler Ebene durch Gesetze gestaltet, aber auch auf globaler Ebene durch Handelsabkommen. Wenn den Beschäftigten ihre Grundrechte, ihre Freiheit und ihre Autonomie an digitalisierten Arbeitsplätzen nicht garantiert werden und wenn Beschäftigte nicht über die Verwaltung der von ihnen produzierten Daten mitbestimmen dürfen, sondern diese Daten stattdessen dem erhebenden Unternehmen „gehören" dürfen, wird sich das Kräftegleichgewicht auf Dauer zugunsten der Unternehmen verschieben.[160]

157 Europäische Kommission, „Questions & Answers: EU-U.S. Data Privacy Framework", EU Presseraum Q&A (Oktober 2022), https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.
158 Initiative des Transatlantic Consumer Dialogue (TACD), Brief an Präsident Joseph R. Biden (10. Juni 2021), https://tacd.org/wp-content/uploads/2021/06/20210610-Data-Flows-Negotiations-Coalition-Letter-June2021.pdf.
159 UNCTAD, „Corporate Rent-Seeking, Market Power and Inequality: Time for a Multilateral Trust Buster?" *UNCTAD* Policy Brief Nr. 66 (Mai 2018), https://unctad.org/en/publicationslibrary/presspb2018d3_en.pdf.
160 Parminder Jeet Singh, „Unsere Rechte an Gemeinschaftsdaten: Kollektiver Datenbesitz, Rechte von Arbeitnehmer_innen und die Rolle des öffentlichen Sektors", Friedrich-Ebert-Stiftung und Internationale der Öffentlichen Dienste (Januar 2020), https://library.fes.de/pdf-files/iez/16458.pdf.

Über die Frage, ob Beschäftigte wirtschaftliche Rechte an den von ihnen mitproduzierten Daten haben sollten, wird derzeit diskutiert. Wenn datenbezogene Verpflichtungen in Handelsabkommen verankert werden, wird eine solche Möglichkeit ausgeschlossen, was wahrscheinlich eine dauerhafte Unterdrückung der kollektiven Verhandlungsmacht der Beschäftigten im digitalen Zeitalter zur Folge haben wird.

Arbeitsrechtsverletzungen durch Algorithmen

Unternehmen setzen zunehmend algorithmische Systeme für die Verwaltung ihrer Beschäftigten ein. Der Einsatz von automatisierten Einstellungs-/Entlassungssystemen, Instrumenten für die Einsatzplanung, Systemen zur Steigerung der Produktivität von Beschäftigten wie Bewegungs- und Standortverfolgungssystemen bis hin zu Echtzeit-Überwachungs- und Kontrollsystemen hat zu einer Reihe von Nachteilen für die Beschäftigten geführt. Diese reichen von Diskriminierung, Arbeitsverdichtung, Übergriffen auf die physische und psychische Gesundheit bis zur Aushöhlung grundlegender Arbeitsrechte wie der Vereinigungsfreiheit und des Rechts auf Kollektivverhandlungen. All diese Nachteile können nur korrigiert werden, wenn algorithmische Systeme integrativen Governance-Praktiken unterliegen und angepasst werden können. Wenn Quellcode nicht überprüft werden kann, auch wenn er fehlerhaft ist, gibt es keine Rechenschaftspflicht und keine Abhilfe für die Schäden.

Das gilt insbesondere für „Plattformarbeit", die die EU derzeit mit der Richtlinie zur Plattformarbeit[161] gegen die lautstarke Lobby von Unternehmen wie Uber[162] besser regulieren will. Eine der Hauptforderungen der Gewerkschaften im Hinblick auf Plattformarbeit ist algorithmische Transparenz.[163] So wird in einer Entschließung des Europäischen Gewerkschaftsbunds verlangt, dass der freie Zugang zum Quellcode vor der Einführung des KI-Systems am Arbeitsplatz gewährleistet sein muss.[164] Die bewährte internationale Praxis, auf die in gewerkschaftlichen Verhandlungsleitfäden verwiesen wird,[165] besteht in einer regelmäßigen unabhängigen Prüfung der für das Management genutzten Algorithmen. Das von der EU im Rahmen der Bestimmungen für den digitalen Handel vorangetriebene Verbot der Offenlegung von Quellcode würde eine solche Transparenz untergraben.[166]

Algorithmische Werkzeuge werden zunehmend bei Arbeiter*innen und Angestellten sowie im Dienstleistungsbereich eingesetzt, nicht nur im Bereich der Gig-Ökonomie. Ein bekanntes Beispiel für algorithmische Voreingenommenheit ist die Entwicklung eines automatisierten Einstellungssystems durch Amazon, dessen Nutzung aber wieder beendet wurde, weil es nur Männer einstellte. Da der Algorithmus mit historischen Daten trainiert wurde, lernte er, dass im Technologiebereich mehr Männer als Frauen beschäftigt sind. Männlichkeit wurde also als etwas Positives bewertet, wohingegen das System alle Bewerbungen, die Wörter wie „Frau" oder „weiblich" enthielten, herabstufte.[167]

Gewerkschaftsvertreter*innen, Anwält*innen für Arbeitsrecht und die Beschäftigten selbst sollten Zugang zu den Daten und den Algorithmen haben, auf denen ihr Beschäftigungsverhältnis betreffende Entscheidungen beruhen. Gewerkschaften sollten die Möglichkeit haben, den Einsatz von Technologien, KI und algorithmischen Entscheidungssystemen zum Thema von Kollektivverhandlungen zu machen, wofür der Zugriff auf Quellcode unerlässlich ist. Dies sollte auch im Gesetz als Gegenstand von Kollektivverhandlungen anerkannt (und geschützt) werden. Alle Anwender algorithmischer Systeme sollten gesetzlich dazu verpflichtet sein, auf laufender Basis Governance-Maßnahmen für (halb) automatisierte Systeme umzusetzen, wozu auch die Einbeziehung von Vertreter*innen derjenigen gehören sollte, die vom Einsatz dieser Systeme betroffen sind, in diesem Falle die Beschäftigten. Die Ko-Governance dieser Systeme ist in dieser Hinsicht eine Voraussetzung für die Durchsetzung von Arbeitsrechten.[168] Arbeitsrechtsbehörden sollten

161 Théo Bourgery-Gonse, „EU institutions inch closer to an agreement on platform worker status", Euractiv (September 2022), https://www.euractiv.com/section/economy-jobs/news/eu-institutions-inch-closer-to-an-agreement-on-platform-worker-status/.
162 Ludovic Voet, „Uber's shadow looms over platform workers directive debates", Euractiv (Oktober 2022), https://www.euractiv.com/section/sharing-economy/opinion/ubers-shadow-looms-over-platform-workers-directive-debates/.
163 Aída Ponce Del Castillo und Diego Naranjo, „Regulating algorithmic Management: An assessment of the EC's draft Directive on improving working conditions in platform work", Europäisches Gewerkschaftsinstitut, Policy Brief (August 2022), https://etui.org/publications/regulating-algorithmic-management.
164 Europäischer Gewerkschaftsbund, „Resolution on the European strategies on artificial intelligence and data", Entschließung des EGB-Vorstands (Juli 2020), https://www.etuc.org/en/document/resolution-european-strategies-artificial-intelligence-and-data.
165 Siehe Patrick Briône, „Algorithmisches Management: Ein gewerkschaftlicher Leitfaden", UNI Global Union, Gruppe Fach- und Führungskräfte (September 2020), https://uniglobalunion.org/report/algorithmic-management-a-trade-union-guide/.
166 Anne Dufresne und Cédric Leterme, „App Workers United: The struggle for rights in the gig economy", *Fraktion Die Linke im Europäischen Parlament (Januar 2021)*, https://left.eu/issues/publications/app-workers-united-the-struggle-for-rights-in-the-gig-economy/.
167 Jeffrey Dastin, „Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women", *Reuters* (Oktober 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
168 Siehe Christina Colclough, „Co-Governance of Algorithmic Systems – a guide", *Why Not Lab* Präsentationsfolien (November 2021), https://www.thewhynotlab.com/_files/ugd/aeaf23_62a52b0671c2466e999b2064c0cdb95b.pdf.

alle algorithmischen Systeme und Datenbestände, die auf eine Weise eingesetzt werden, die die Rechte der Beschäftigten am Arbeitsplatz beeinträchtigt, a priori prüfen und genehmigen. Zertifizierungs- und Normungsgremien müssen ausgewogen besetzt sein und Beschäftigtenorganisationen und Wirtschaft paritätisch einbeziehen, und alle Zulassungen müssen an die Verpflichtung geknüpft sein, die angewandten Systeme regelmäßig und umfassend zu überprüfen.[169] Anregungen hierfür finden sich im spanischen Recht, das Beschäftigten Zugang zu Informationen über ihre Merkmale und technischen Spezifikationen gibt,[170] und in der DSGVO-Vorschrift, wonach die Datenschutz-Folgenabschätzung (DPIA) regelmäßig zu überprüfen ist. Diese Regelungen wären nach den Vorschlägen der EU für digitalen Handel verboten, wonach Anforderungen zur Offenlegung von Quellcode und zur Datenlokalisierung unzulässig sein sollen.

Verringerung des Potenzials zur Schaffung von Arbeitsplätzen

Das oberste Ziel von Big Tech besteht darin, Regierungen dazu zu zwingen, ihnen die Erlaubnis zur Erfassung, Nutzung, Übermittlung, Speicherung und Weitergabe von Daten nach eigenem Gutdünken zu erteilen. Die Datenerzeugung ist das zentrale Merkmal der digitalen Wirtschaft der Zukunft, und die meisten Menschen begreifen erst allmählich, welchen Wert Daten haben. Die Unternehmen, die dazu in der Lage sind, die größten Datenbestände zu sammeln, werden ihre KI präziser trainieren und infolgedessen ihre Branchen dominieren. Investor*innen erkennen den Wert von Daten für künftige Gewinne, und die Unternehmen, die die meisten Daten erheben, verfügen über die größte Marktkapitalisierung. Big Tech uneingeschränkte Kontrolle über Daten zu geben, würde politischen Maßnahmen zur Schaffung von Beschäftigung zuwiderlaufen, da die Länder die im Rahmen der digitalen Industrialisierung auf ihrem Staatsgebiet gewonnenen Daten nutzen müssen, um neue Arbeitsplätze zu schaffen und bestehende Arbeitsplätze aufzuwerten. Die Privatisierung von Daten, die im Zentrum der „Regeln für digitalen Handel" steht, würde die Möglichkeiten der Staaten zur Gewährleistung einer breiten Schaffung von Arbeitsplätzen und von Vollbeschäftigung durch Digitalisierung sowie die gerechte Verteilung des erzeugten Einkommens massiv einschränken.

Förderung der Privatisierung

Die Vorschläge der EU für digitalen Handel umfassen Forderungen zur Ausweitung von Liberalisierungsverpflichtungen auf Finanz-, Telekommunikations- und Computerdienstleistungen, insbesondere im Hinblick auf ihre grenzüberschreitende Erbringung.[171] Da ein Großteil der Produktion heute faktisch von Dienstleistungen, namentlich digitalen Dienstleistungen abhängt, würden sich diese neuen Verpflichtungen auch auf die Beschäftigten in der verarbeitenden Industrie, im Verkehr und sogar in der Landwirtschaft und Lebensmittelverarbeitung bis hin zum Einzelhandel auswirken, wie die globalen Gewerkschaftsverbände in diesen Sektoren erklären. Die Erbringung dieser digitalisierten Dienstleistungen im Ausland gefährdet Arbeitsplätze, Löhne und Beschäftigungsbedingungen im Inland.

Die vorgeschlagenen Regeln würden es den Unternehmen ermöglichen, mehr Arbeitsplätze im Dienstleistungssektor auszulagern. Handelsbestimmungen, die Unternehmen das Recht zur grenzüberschreitenden Datenübermittlung garantieren – ohne sie dazu zu verpflichten, in dem Land, in dem sie Gewinne erzielen, eine lokale Präsenz zu unterhalten, Steuern zu zahlen, Technologie zu transferieren, Datenschutz zu gewährleisten oder für jegliche von ihnen verursachten Schäden zu haften – machen es ihnen leichter, Arbeitsplätze weltweit dorthin zu verlagern, wo sie die größten Profite erzielen können. Das bedeutet oft, dass Arbeitsplätze in Niedriglohnländer ausgelagert werden, wo die Verletzung von Arbeitsrechten weitverbreitet ist. Betroffen davon sind Arbeitsplätze in Callcentern, in der Datenverarbeitung, im Bereich von Finanzdiensten und medizinischer Abrechnung, in der Logistik sowie in vielen weiteren Branchen.[172]

Arbeitsrechte: Rechtsverletzende Unternehmen wollen neue Einschränkungen für die Regulierung von Big Tech

Unternehmen, die sich für die Regulierung des digitalen Handels einsetzen, gehören zu dem schlimmsten Verletzern von Arbeitsrechten. Viele der von ihnen geschaffenen Arbeitsplätze sind gering

169 Colclough, „Union Brief: G7 Digital Policy Priorities 2022", Why Not Lab (2022).
170 Carlos del Castillo, „Trabajo lanza una herramienta para facilitar la transparencia de los algoritmos laborales", *El Diario* (Juni 2022), https://www.eldiario.es/tecnologia/trabajo-lanza-herramienta-facilitar-transparencia-algoritmos-laborales_1_9071089.html.
171 Jane Kelsey, „Digital Trade Rules and Big Tech: Surrendering Public Good to Private Power", Friedrich-Ebert-Stiftung und Internationale der Öffentlichen Dienste (Februar 2020), https://publicservices.international/resources/publications/digital-trade-rules-and-big-tech-surrendering-public-good-to-private-power?id=10825&lang=en
172 Kelsey, „Digital Trade Rules and Big Tech", FES und IÖD (2020).

und manchmal untertariflich bezahlt,[173] verstoßen gegen internationale Arbeitsnormen und bieten keine Sozialleistungen. Amazon, dem vorgeworfen wird, amerikanische Beschäftigungsbedingungen nach Europa zu exportieren,[174] steht wegen seiner ausbeuterischen Praktiken weltweit im Visier von Gewerkschaften, unter anderem weil es Beschäftigte bespitzelt, die ihre Arbeitsrechte wahrnehmen,[175] und während der Covid-19-Krise Beschäftigte entließ, die sich organisierten, um bessere Gesundheitsschutzmaßnahmen zu fordern.[176]

Tatsächlich beruht das Geschäftsmodell einiger Big-Tech-Unternehmen auf dem missbräuchlichen Einsatz prekärer und informell beschäftigter Arbeitskräfte, wie z. B. Content-Moderator*innen in Afrika, die für einen Stundenlohn von nicht mehr als 1,50 USD für die Beseitigung gewaltverherrlichender und illegaler Inhalte auf Facebook zuständig sind und unter seelischen Erkrankungen wie posttraumatischer Belastungsstörung (PTSD), Angstzuständen und Depressionen leiden.[177] Noch bekannter ist die Methode von Uber, Arbeitsgesetze der EU zu brechen und dann hochrangige Lobbyisten zu beauftragen und Fahrer*innen zu instrumentalisieren, um Amtspersonen unter Druck zu setzen, die Gesetze zugunsten der Profite des Unternehmens zu beugen, wie von einem Whistleblower enthüllt wurde.[178] Solchen Unternehmen sollten keine weiteren Rechte und Schutzregelungen im Rahmen von „Handelsabkommen" gewährt werden, auch nicht in Bezug auf Bestimmungen, die direkt auf ihre Rechte abzielen.[179]

Generell sollte im Mittelpunkt jeder globalen Vereinbarung über Digitalisierung die Gewährleistung hochwertiger, existenzsichernder und gewerkschaftlich organisierter Arbeitsplätze für Beschäftigte in der digitalen Ökonomie und auf Plattformen stehen. Eine Hauptprofitquelle digitaler Unternehmen ist der „gestörte" Arbeitsmarkt, wo eine ihrer wichtigsten Innovationen darin besteht, Beschäftigung prekärer zu machen. Sie sind bekannt dafür, Plattformbeschäftigte als selbständige Auftragnehmer*innen zu klassifizieren, um die Geltung des Arbeitsrechts auszuhebeln (weil sie unabhängige Unternehmer*innen sind). Aufgrund dieser Einstufung können Beschäftigte, die sich organisieren, als Kartell und nicht als Gewerkschaft betrachtet werden. Seit der Anfangszeit von Uber sind zwar Erfolge im Hinblick auf die Klassifizierung der Beschäftigten erzielt worden, aber die rechtlichen Rahmenbedingungen der meisten Länder müssen noch angepasst werden, um die korrekte Einstufung als Arbeitnehmer*innen sicherzustellen.

Unternehmen machen sich die Digitalisierung zunehmend zunutze, um Arbeitsplätze an Standorten anzusiedeln, wo Beschäftigte den schwächsten Arbeitsschutz genießen und die geringsten Löhne erhalten. Viele Handelsabkommen enthalten Bestimmungen, die Regierungen daran hindern, Unternehmen eine lokale Präsenz zur Auflage zu machen, was die Möglichkeiten der Beschäftigten beschränkt, Kollektivverhandlungen zu führen und Unternehmen für die Verletzung ihrer Rechte zur Verantwortung zu ziehen. Dies hat einen Wettlauf nach unten bei den Arbeitsnormen in Gang gesetzt, durch den die Löhne und Beschäftigungsbedingungen in ganz Europa nach unten gedrückt werden. Gewerkschaften appellieren an die Regierungen, gerechte Regeln für Wettbewerb und Beschäftigungsbedingungen aufzustellen, die die Arbeitsrechte aller Beschäftigten, auch von „Vertragsarbeiter*innen", sicherstellen. Es gibt keinen Weg zu gemeinsamem Wohlstand durch Digitalisierung und technologischen Wandel, bei dem universelle Beschäftigung und qualitativ hochwertige Arbeitsplätze verbunden mit der Freiheit zur gewerkschaftlichen Organisierung nicht im Mittelpunkt stehen.

Gewerkschaftliche Forderungen sind in keinem Vorschlag berücksichtigt

173 Julia Carrie Wong, „Revealed: Google illegally underpaid thousands of workers across dozens of countries: Documents show company dragged feet to correct disparity after learning it was failing to comply with laws in UK, Europe and Asia", *Guardian* (September 2021), https://www.theguardian.com/technology/2021/sep/10/google-underpaid-workers-illegal-pay-disparity-documents.

174 Albert Samaha, „How Amazon Exported American Working Conditions To Europe: After Amazon workers in Germany began striking, the company expanded eastward, where looser labor laws brought record productivity", Buzzfeed News (Juni 2022), https://www.buzzfeednews.com/article/albertsamaha/amazon-poland-slovakia-czechia-germany-labor-laws.

175 Lauren Kaori Gurley, „Secret Amazon Reports Expose the Company's Surveillance of Labor and Environmental Groups: Dozens of leaked documents from Amazon's Global Security Operations Center reveal the company's reliance on Pinkerton operatives to spy on warehouse workers and the extensive monitoring of labor unions, environmental activists, and other social movements", *Vice Motherboard (November 2020)*, https://www.vice.com/en/article/5dp3yn/amazon-leaked-reports-expose-spying-warehouse-workers-labor-union-environmental-groups-social-movements.

176 UNI Global Union, "Global Union Alliance: 'Amazon cannot fire its way out of this crisis'" *UNI Global Union* (April 2020), https://uniglobalunion.org/news/global-union-alliance-amazon-cannot-fire-its-way-out-of-this-crisis/ ; Melissa Heikkilä, „Amazon workers in France, Italy, Spain & Poland strike over labour conditions during COVID-19 pandemic", Politico EU re-upped in Business & Human Rights Resource Centre (März 2020), https://www.business-humanrights.org/en/latest-news/amazon-workers-in-france-italy-spain-poland-strike-over-labour-conditions-during-covid-19-pandemic/.

177 Bill Perrigo, „Inside Facebook's African Sweatshop", *Time* (Februar 2022), https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/.

178 Paul Lewis et al, „The Uber whistleblower: I'm exposing a system that sold people a lie", Guardian (Juli 2022), https://www.theguardian.com/news/2022/jul/11/uber-files-whistleblower-lobbyist-mark-macgann; siehe auch, „Explainer: What are the Uber files? A guide to cab-hailing firm's ruthless expansion tactics", Guardian (Juli 2022), https://www.theguardian.com/news/2022/jul/10/what-are-the-uber-files-guide.

179 Nur ein Beispiel dafür ist die Erklärung von Facebook bei einer Kundenpräsentation seiner Arbeitsplatz-App, dass Arbeitgeber die Posts von Beschäftigten überwachen könnten, beispielsweise daraufhin, ob das Wort „unionize" (gewerkschaftlich organisieren) verwendet wird. Lee Fang, „Facebook Pitched New Tool Allowing Employers to Suppress Words Like 'Unionize' in Workplace Chat Product", *Intercept* (Juni 2020), https://theintercept.com/2020/06/11/facebook-workplace-unionize/.

Die wichtigste Strategie zur Gewährleistung weitreichender und umfassender Vorteile durch Digitalisierung besteht im Streben nach Vollbeschäftigung auf der Grundlage von Gerechtigkeit in Form von starken Arbeitsrechten und menschenwürdigen Arbeits- und Beschäftigungsbedingungen für alle Arbeitnehmer*innen, Rassen- und Geschlechtergleichheit und dem Verbot von Diskriminierung. Dies schließt auch Rechte der Beschäftigten im digitalen Kontext ein, unter anderem auf die eigenen Daten und auf umfassende und übertragbare Sozialschutzleistungen (wie bezahlter Krankenurlaub und Arbeitslosenversicherung), auch für Beschäftigte, die fälschlicherweise als Auftragnehmer*innen eingestuft werden. Es bedeutet ferner, dass öffentliche Aufträge, unter anderem für die Digitalisierung öffentlicher Dienste, an Unternehmen gehen, die das Recht auf Kollektivverhandlungen achten. Keiner der von Gewerkschaften und anderen arbeitnehmerfreundlichen Organisationen vorgelegten Vorschläge wird jedoch in den geplanten Regeln für digitalen Handel aufgegriffen.

Aus diesen und weiteren Gründen rief der Europäische Gewerkschaftsbund die EU und ihre Mitgliedstaaten im März 2020 dazu auf, die plurilateralen Verhandlungen über den elektronischen Handel einzufrieren, unter Verweis auf schwerwiegende Bedenken hinsichtlich der Eignung der WTO als Forum für Verhandlungen über Fragen der Datenverwaltung und für die Gestaltung der Regeln des digitalen Wandels, da die Organisation weder über Fachwissen noch über ein Mandat verfüge, die Gewerkschaften nicht angemessen einbeziehe und bei der Festlegung von Regeln einen reduktiven Ansatz verfolge.[180]

7- ... SCHUTZ VON MINDERHEITEN VOR DISKRIMINIERUNG?

Es häufen sich die Belege dafür, dass künstliche Intelligenz (KI) Diskriminierung verschärfen und Schäden verursachen kann, sei es durch fehlerhafte Algorithmen, die auf der Grundlage früherer Ungerechtigkeiten bestimmte Muster „lernen", oder durch die Verschärfung von Ungleichheiten in den für das Training von KI verwendeten Datensätzen.[181] Je nach Bereich schützt die EU vor Diskriminierung aufgrund persönlicher Merkmale, unter anderem Staatsangehörigkeit und Wohnort, Behinderung, Religion oder Weltanschauung, Rasse und der ethnische Herkunft sowie Geschlecht, sexuelle Orientierung und Alter.

Algorithmen werden in Suchmaschinen und Werbung extensiv genutzt und führen zu schädigender Diskriminierung von Frauen, Mitgliedern von Einwanderergemeinschaften und Menschen mit anderen kulturellen Hintergründen, die häufig zur Zielscheibe von Angriffen werden.[182] Rassistische Voreingenommenheit in Algorithmen wurde dokumentiert im Zusammenhang mit Wähler*innenunterdrückung, Diskriminierung im Wohnungswesen, missbräuchlichen Kreditpraktiken, Versicherungen, Diskriminierung in Beschäftigung[183] sowie staatlicher Überwachung und Polizeiarbeit.[184] Zu den Beispielen gehören auch Suchmaschinenergebnisse, die Stellenangebote nach Maßgabe der vom Algorithmus ermittelten Rasse, ethnischen Zugehörigkeit oder des Geschlechts der suchenden Person anzeigen,[185] und Entscheidungen über Kreditwürdigkeit oder Versicherungsprämien auf Grundlage der ethnischen oder geografischen Herkunft, wie aus einem im Auftrag der Europäischen Kommission erstellten Bericht hervorgeht.[186] Die unglaubliche Fehlerquote von Gesichtserkennungssystemen im Hinblick auf die Unterscheidung von Menschen mit dunklerer Hautfarbe von Menschen mit hellerer Hautfarbe ist gut dokumentiert und ein ernstes Alarmsignal.[187]

Algorithmen, die in der Überwachungswerbung z. B. von Facebook genutzt werden, fördern nachweislich rassistische Hassrede[188] sowie unkorrekte, kontroverse und hetzerische Informationen, was bereits zu gewalttätigen rassistischen Übergriffen beispielsweise auf Immigrant*innen in Deutschland[189] oder auf

180 Europäischer Gewerkschaftsbund, „ETUC position on the plurilateral negotiations on e-commerce", auf der Sitzung des EGB-Exekutivausschusses verabschiedetes Positionspapier (März 2020), https://www.etuc.org/en/document/etuc-position-plurilateral-negotiations-e-commerce.
181 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Polity: 2019).
182 Noble, *Algorithms of Oppression* (2018).
183 Ibid:
184 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press: 2018).
185 Alina Köchling und Marius Claus Wehner, „Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development", Business Research 13 (November 2020): 795–848, https://doi.org/10.1007/s40685-020-00134-w.
186 Janneke Gerards und Raphaële Xenidis, „Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law", Europäische Kommission Generaldirektion Gesundheit und Verbraucher (2020), https://www.equalitylaw.eu/downloads/5361-algorithmic-discrimination-in-europe-pdf-1-975.
187 Siehe zum Beispiel: Patrick Grother, Mei Ngan und Kayee Hanaoka, „Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects", *National Institute of Standards and Technology Report 8280* (Dezember 2019), https://doi.org/10.6028/NIST.IR.8280.
188 Andrew Jakubowicz, „Algorithms of hate: How the Internet facilitates the spread of racism and how public policy might help stem the impact", *Journal & Proceedings of the Royal Society of New South Wales* 151, part 1 (2018): 69–81, https://search.informit.org/doi/10.3316/informit.790571095083969
189 Amanda Taub und Max Fisher, „Facebook Fueled Anti-Refugee Attacks in Germany, New Research Suggests", New York Times (August 2018), https://www.nytimes.com/2018/08/21/world/europe/facebook-refugee-attacks-germany.html

schwarze Fußballspieler in Großbritannien[190] geführt hat, um nur zwei Beispiele aus umfassenden Untersuchungen über die Verschärfung von Rassismus durch sozialen Medien zu nennen.[191]

Dies ist nicht nur im privaten, sondern auch im öffentlichen Sektor ein Problem. Das kürzliche Debakel um den Kinderbetreuungszuschlag in den Niederlanden offenbarte den erheblichen Schaden, den der Einsatz von Algorithmen ohne menschliche Aufsicht in der niederländischen Bevölkerung anrichtete.[192] In diesem gewaltigen Skandal führte die Nutzung von Algorithmen zur Aufdeckung möglichen Betrugs bei Sozialleistungen dazu, dass über 1.000 Kinder in Pflegefamilien untergebracht wurden. Mit einer angemessenen öffentlichen Aufsicht über die Anwendung solcher KI-Systeme hätte die Verwendung schädlicher Datensätze und fehlerhafter Algorithmen verhindert werden können.

Im Jahr 2019 veröffentlichte die Europäische Kommission ein Weißbuch zur Künstlichen Intelligenz, in dem anerkannt wurde, dass die zunehmende Verwendung von Algorithmen in Europa mit besonderen Risiken für die Grundrechte einhergeht, insbesondere für das Recht auf Gleichstellung und Diskriminierungsfreiheit.[193] Diesen Risiken trägt auch die jüngste Gleichstellungsstrategie 2020-2025 der Kommission Rechnung, in der anerkannt wird, dass AI „Ungleichheiten zwischen Frauen und Männern verstärken" kann.[194]

Im Vorfeld der Ausarbeitung des DSA und der KI-Verordnung wurde algorithmische Diskriminierung aufgrund von Rasse oder ethnischer Herkunft und Geschlecht[195] sowie von LGBTQIA+[196] als problematisch eingestuft, Eine Gruppe zivilgesellschaftlicher Organisationen unter der Führung von EDRi, darunter Algorithm Watch, das Europäische Behindertenforum, das Europäische Netzwerk gegen Rassismus, UNI Europa und andere, verlangten rote Linien in der KI-Verordnung im Hinblick auf die Bedrohung von Grundfreiheiten.[197] Dazu gehörten klare Einschränkungen für den Einsatz von KI bei der Migrationskontrolle, den Einsatz von KI für Social Scoring und Entscheidungen über den Zugang zu sozialen Rechten und Leistungen, prädiktive Polizeiarbeit, bei der immer wieder arme, aus der Arbeiterklasse stammende, rassisch determinierte und migrantische Bevölkerungsgruppen mit einer höheren Wahrscheinlichkeit vermuteter künftiger Kriminalität belegt werden, und der Einsatz von Instrumenten zur Risikoermittlung im Strafrechtssystem und im vorgerichtlichen Kontext, die alle eine Bedrohung der Grundrechte insbesondere von rassisch determinierten Gruppen darstellen.

Aus neueren Studien geht ferner hervor, dass Quellcodes und Algorithmen, die miteinander verbunden sind und von sich selbst lernen (maschinelles Lernen)[198] zu vielen unerwünschten Ergebnissen führen können, darunter Diskriminierung aufgrund von Einkommen, Hautfarbe und Geschlecht. Angesichts dessen hat der UN-Ausschuss für die Beseitigung der Rassendiskriminierung betont, dass algorithmenbasierte Profiling-Systeme in vollem Einklang mit den internationalen Menschenrechtsnormen stehen sollten.[199] Er hat die Bedeutung von Transparenz in der Konzeption und Anwendung algorithmenbasierter Profiling-Systeme hervorgehoben, wenn diese zu Strafverfolgungszwecken eingesetzt werden. Wie der Ausschuss in seinen Empfehlungen unterstreicht, beinhaltet dies, die Verwendung solcher Systeme offenzulegen und zu erläutern, wie die Systeme funktionieren, welche Datensätze verwendet werden und welche Maßnahmen vorgesehen sind, um Menschenrechtsverletzungen zu verhindern.[200]

Nach den vorgeschlagenen Regeln für digitalen Handel soll es den Staaten jedoch untersagt sein, die Offenlegung von Quellcode zu verlangen. Sie sehen allerdings Ausnahmen vor, die die Offenlegung von Quellcode und Algorithmen gegenüber

190 Luca Bertuzzi, „Online racial abuses in the UK prompt calls to end anonymity online", Euractiv (Juli 2021), https://www.euractiv.com/section/digital/news/online-racial-abuses-in-the-uk-prompt-calls-to-end-anonymity-online/.
191 Ariadna Matamoros-Fernández und Johan Farkas, „Racism, Hate Speech, and Social Media: A Systematic Review and Critique", *Television & New Media 22*, Nr. 2 (Februar 2021): 205-224, https://doi.org/10.1177/1527476420982230.
192 Melissa Heikkilä, „Dutch scandal serves as a warning for Europe over risks of using algorithms", *Politico EU* (März 2022), https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.
193 Europäische Kommission, „Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen", Europäische Kommission COM(2020) 65 final (Februar 2020): 3 und 11, https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_de.pdf.
194 Europäische Kommission, Mitteilung: „Eine Union der Gleichheit: Strategie für die Gleichstellung der Geschlechter 2020-2025" Europäische Kommission COM(2020) 152 final (März 2020): Abschnitt „Bekämpfung von Geschlechterstereotypen", https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020DC0152.
195 Fabian Lütz, „Gender equality and artificial intelligence in Europe. Addressing direct and indirect impacts of algorithms on gender-based discrimination", *ERA Forum 23* (April 2022): 33-52, https://doi.org/10.1007/s12027-022-00709-6.
196 Christina Dinar, „The state of content moderation for the LGBTIQA+ community and the role of the EU Digital Services Act", *Heinrich-Böll-Stiftung* (Juni 2021), https://eu.boell.org/en/platform-moderation-lgbtiqa-DSA.
197 Von European Digital Rights organisierter offener Brief an die Europäische Kommission, „Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence" (Januar 2021), https://edri.org/our-work/civil-society-call-for-ai-red-lines-in-the-european-unions-artificial-intelligence-proposal/.
198 Harold Feld, „The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms", *Roosevelt Institute* (Mai 2019), https://rooseveltinstitute.org/wp-content/uploads/2020/07/RI-Case-for-the-Digital-Platform-Act-201905.pdf.
199 UN-Ausschuss für die Beseitigung der Rassendiskriminierung, „UN Committee issues recommendations to combat racial profiling", UN General Comments and Recommendations (November 2020), https://www.ohchr.org/en/general-comments-and-recommendations/2020/11/un-committee-issues-recommendations-combat-racial.
200 Ibid:

ersuchenden Justiz- oder Regulierungsbehörden zum Zwecke von Ermittlungen erlauben, was sich im Freihandelsabkommen zwischen der EU und Neuseeland ausdrücklich auch auf Diskriminierung und Voreingenommenheit bezieht. Auf der Konferenz der Gleichstellungsministerinnen und -minister Deutschlands wurde jedoch festgestellt, dass es aufgrund der Komplexität des Themas unrealistisch erscheine, dass die Betroffenen in der Lage sein würden, algorithmische Diskriminierung zu erkennen und zu verfolgen.[201] Wie schon oben festgestellt müssen Transparenz-Instrumente außerdem auch Betroffenen, Forschenden, kritischen Ingenieur*innen, Anwält*innen, Gewerkschaftsvertreter*innen und der breiten Öffentlichkeit zur Verfügung stehen – nicht nur den Regierungen.

Wenn algorithmische Systeme das Grund- und Menschenrecht auf Diskriminierungsfreiheit verletzen könnten, müsste für KI-Systeme nachgewiesen werden, dass sie dies nicht tun – und zwar vor ihrer Einführung und nicht erst, wenn bereits Schaden angerichtet wurde. Politische Maßnahmen zur Wahrung der Menschen- und Grundrechte sollte nicht Gegenstand von Urteilen der Handelsgerichte sein, die Handelsaspekte höher gewichten als die Rechte der betroffenen Bevölkerungsgruppen.

8- ... DIE EU-AGENDA FÜR DEN GRÜNEN DEAL?

Der europäische Grüne Deal legt einen Fahrplan fest, um Europa bis 2050 zum ersten klimaneutralen Kontinent zu machen und dabei die Wirtschaft anzukurbeln, die Gesundheit und Lebensqualität der Menschen zu verbessern und niemanden im Stich zu lassen, so die Europäische Kommission.[202]

Die Handelspolitik der EU soll „den Grünen Deal in all seinen Dimensionen – einschließlich des Ziels, bis 2050 Klimaneutralität zu erreichen – unmissverständlich unterstützen".[203]

Der Grüne Deal fördert neue technologische Innovationen für die Bewältigung der weltweiten Klimakrise. Doch damit der notwendige Wandel auf der ganzen Welt vollzogen werden kann, ist der Transfer klimaschonender Technologieinnovationen erforderlich, um ihre globale Nutzung zu gewährleisten. Ein Verbot der Offenlegung von Quellcode und anderer Formen des Technologietransfers wird die Verwirklichung des Pariser Klimaschutzübereinkommens unmöglich machen.

Länder brauchen außerdem Steuereinnahmen (zum Beispiel aus der Besteuerung von Big Tech), um ihren Übergang zu finanzieren. Die Vorschläge von Big Tech zur Begrenzung der Möglichkeiten von Staaten, ihre Tätigkeiten und die grenzüberschreitende Erbringung von Waren und Dienstleistungen zu besteuern, werden zur Reduzierung der hierfür erforderlichen Investitionen führen.

Der globale elektronische Handel mit Waren führt zu einer weiteren Verdrängung lokaler Produktion zugunsten internationaler Produkte, die aufgrund des transnationalen Transports jedoch möglicherweise klimaintensiver sind.[204]

Die hochkonzentrierte und datenhungrige digitale Wirtschaft, die von Big Tech vorangetrieben wird, und die vorgeschlagenen Regeln für digitalen Handel stehen zudem im radikalen Widerspruch zum Kampf gegen die Erderwärmung. Der CO2-Fußabdruck des Trainings von KI-Systemen oder des Betriebs eines Hyperscale-Rechenzentrums ist deutlich größer als die im Pariser Abkommen geforderten Grenzwerte. Der Fußabdruck der weltweiten Technologiebranche in Bezug auf Energie, Rohstoffe und Wasserverbrauch ist nach den Angaben einer Pariser Denkfabrik dreimal so groß wie der von ganz Frankreich. Auf die digitale Wirtschaft entfallen 10 Prozent des weltweiten Stromverbrauchs und fast 4 Prozent der globalen CO2-Emissionen, fast doppelt so viel wie auf den Zivilluftverkehr.[205]

Die Überbeanspruchung der heimischen Energieversorgung entwickelt sich zu einem solchen Problem, dass Länder wie Irland, das einen Anteil von 25 Prozent am europäischen Markt für Rechenzentren hat, sich mit Forderungen nach einem Moratorium für den Bau neuer Rechenzentren konfrontiert sehen.[206] Zu einer Zeit, in der die europäischen Verbraucher*innen wegen des Kriegs in der Ukraine aufgerufen werden, ihren Energieverbrauch einzuschränken, werden Rechenzentren immer kritischer von Regulierungsbehörden und der

201 Siehe Fußnote 366 in Gerards and Xenidis, „Algorithmic discrimination in Europe", Europäische Kommission (2020): 87.
202 Europäische Kommission, „Europäischer Grüner Deal", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_de.
203 Europäische Kommission, Mitteilung: „Überprüfung der Handelspolitik", Europäische Kommission COM(2021) 66 final.
204 Theresa Kofler et al, „Policy Brief on Digital Trade", *Seattle to Brussels network* (April 2022), http://s2bnetwork.org/wp-content/uploads/2022/04/S2B-DigitalTrade-policybrief.pdf.
205 Hugues Ferreboeuf und Arbeitsgruppe, „Lean ICT: Towards Digital Sobriety", *Shift Project* (März 2019), https://theshiftproject.org/en/article/lean-ict-our-new-report/.
206 Pádraig Hoare, „Energy use of data centres equivalent to powering 200,000 homes", *Irish Examiner* (Mai 2022), https://www.irishexaminer.com/news/arid-40864262.html.

Öffentlichkeit hinterfragt.[207] In einer Studie der Europäischen Kommission wird die Prognose aufgestellt, dass der Stromverbrauch von Rechenzentren von 2018 bis 2030 um 18,5 Prozent steigen wird.[208]

Gleiches gilt für den Wasserverbrauch. Lokale Aktivist*innen in Zeewolde (nahe Amsterdam) zwangen Meta im Juli 2022 zur Aufgabe von Plänen für den Bau eines energieintensiven Rechenzentrums,[209] nachdem bekanntgeworden war, dass der riesige Rechenzentrumskomplex von Microsoft in Nordholland im Jahr 2021, in dem die Hitze einen erheblichen Wassermangel verursachte, 84 Millionen Liter Wasser verbrauchte.[210] Rechenzentren benötigen hohe Mengen an Wasser zu Kühlungszwecken und indirekt durch die Energieerzeugung.[211] Einige Rechenzentren liegen in Gebieten mit prekärer Wassersituation aufgrund der Gefahr von Dürren und Wasserknappheit. Dies führt mancherorts zu Konflikten mit örtlichen Gemeinden oder zu Beschränkungen des Wasserverbrauchs. Diese Risiken werden sogar bei der Untersuchung von Umwelt-, Sozial- und Governance-Aspekten im Rahmen der Beurteilung wirtschaftlicher Risiken berücksichtigt.[212]

Ein jüngster Vorschlag des Climate Neutral Data Centre Pact, bevorstehende gesetzliche Auflagen zur Reduzierung des Wasserverbrauchs bis 2040 auf maximal 400 ml pro kWh Rechenleistung vorwegzunehmen,[213] könnte zu einer Lösung beitragen. Ohne eine Begrenzung der gesamten Rechenleistung bleibt jedoch abzuwarten, wie die Nettoauswirkungen aussehen werden, vor allem weil die Gruppe inzwischen in der Kritik steht, sich zum Vehikel der Lobbyarbeit US-amerikanischer Unternehmen zu entwickeln, statt grüne Ziele zu verfolgen.[214] Stattdessen sollte der Plan der Kommission zu den Umweltauswirkungen von Rechenzentren[215] verbindliche Ziele enthalten.

Neben dem Energie- und Wasserverbrauch hat die Sustainable Digital Infrastructure Alliance Schwerpunkte für die Gestaltung einer nachhaltigen digitalen Ökonomie ermittelt, unter anderem im Hinblick auf Emissionen, Elektronikschrott, den Verbrauch von sonstigen Ressourcen, Verschmutzung und sozioökonomische Aspekte, die alle angesichts des rasanten und unkontrollierten Wachstums digitaler Infrastruktur von Belang sind.[216]

Nachhaltige Digitalisierung ist nicht mit riesigen digitalen Monopolen vereinbar, die auf eine immer weitergehende Erhebung, Speicherung und Verarbeitung von Daten auf globaler Ebene drängen.

9- ... DIE EU-REGULIERUNG VON BIG-TECH-MONOPOLEN?

Europäische Regulierungsbehörden und Gesetzgeber sind sich der negativen Auswirkungen der monopolistischen Praktiken und Macht von Big Tech inzwischen sehr bewusst. Europa ergreift umfangreiche Durchsetzungsmaßnahmen gegen Big Tech. Die Eindämmung der Marktdominanz von Big Tech und die Regulierung seiner Praktiken, um gleiche Rahmenbedingungen für einen fairen Wettbewerb zu schaffen, wird allen Aspekten der europäischen Gesellschaften zugutekommen, insbesondere der digitalen Industrialisierung und KMU, wie bereits in anderen Abschnitten dargelegt.

Big Tech arbeitet jedoch fieberhaft daran, Maßnahmen zur Einschränkung seiner Marktdominanz und wettbewerbsfeindlicher Praktiken im Technologiesektor durch entsprechende Bestimmungen in Abkommen über digitalen Handel zu untergraben und einzudämmen. Dies umfasst die Ausweitung bestehender Regeln über den „Marktzugang" durch die „Vereinbarung über Computer- und verwandte Dienstleistungen", das Verbot von Offenlegungsanforderungen für Quellcode, Inter-

207 April Roach und Ewa Krukowska, „Big Tech Gets Caught Up in Europe's Energy Politics: As the war in Ukraine threatens supplies, some countries are pushing for tighter control over data centers that consume vast amounts of electricity", Bloomberg (Juni 2022), https://www.bloomberg.com/news/articles/2022-06-23/google-facebook-data-centers-face-europe-political-snags-over-in-energy-crisis

208 Europäische Kommission, Generaldirektion Energie, „Green and Digital: study shows technical and policy options to limit surge in energy consumption for cloud and data centres", Europäische Kommission, Presseartikel (November 2020), https://commission.europa.eu/news/green-and-digital-study-shows-technical-and-policy-options-limit-surge-energy-consumption-cloud-and-2020-11-09_de.

209 Georgia Butler, „Meta data center in Zeewolde facing opposition by Dutch Housing Minister: Former Deputy PM Hugo de Jonge hopes stricter requirements for data centers will prevent the development of the hyperscale", DatacenterDynamics (März 2022), https://www.datacenterdynamics.com/en/news/meta-data-center-in-zeewolde-facing-opposition-by-dutch-housing-minister/.

210 Peter Judge, „Drought-stricken Holland discovers Microsoft data center slurped 84m liters of drinking water last year – After the company and local authority said the facility would only need 12 to 20 million liters", DatacenterDynamics (August 2022), https://www.datacenterdynamics.com/en/news/drought-stricken-holland-discovers-microsoft-data-center-slurped-84m-liters-of-drinking-water-last-year/.

211 David Mytton, „Data centre water consumption", *npj Clean Water 4* (Februar 2021), https://doi.org/10.1038/s41545-021-00101-w.

212 Erin Johnson und Kata Molnar, „ESG Risks Affecting Data Centers: Why Water Resource Use Matters to Investors", Sustainalytics (August 2022), https://www.sustainalytics.com/esg-research/resource/investors-esg-blog/esg-risks-affecting-data-centers-why-water-resource-use-matters-to-investors.

213 Peter Judge, „European operators plan to cut water use to 400ml per kWh by 2040", DatacenterDynamics (Juli 2022), https://www.datacenterdynamics.com/en/news/european-operators-plan-to-cut-water-use-to-400ml-per-kwh-by-2040/.

214 Mathieu Pollet, „Alliance for green data centres shows cracks over water consumption target", Euractiv (Juni 2022), https://www.euractiv.com/section/digital/news/alliance-for-green-data-centres-shows-cracks-over-water-consumption-target/.

215 Pieter Haeck und Antonia Zimmermann, „Europe's hidden energy crisis: Data centers: Brussels zones in on digital economy's heavy energy and water use", Politico EU (Oktober 2022), https://www.politico.eu/article/data-center-energy-water-intensive-tech/.

216 Siehe die Website der Sustainable Digital Infrastructure Alliance: https://sdialliance.org/.

operabilitätsbestimmungen und das Verbot von Anforderungen bezüglich einer lokalen Präsenz.

Ausweitung des Marktzugangs durch die Vereinbarung über Computer- und verwandte Dienstleistungen (Understanding on Computer and Related Services - UCRS)

Eines der Hauptziele der EU in den Verhandlungen über digitalen Handel besteht in der Ausweitung der Dienstleistungen, die diesen Regeln für den „Marktzugang" unterliegen, indem weitere Mitglieder ihre vorgeschlagene „Vereinbarung über Computer- und verwandte Dienstleistungen" (UCRS) unterstützen.

Diese Marktzugangsregeln setzen „Maßnahmen", die die Erbringung von Dienstleistungen „beeinträchtigen", einschließlich wettbewerbspolitischer Maßnahmen zur Begrenzung von Größe, Marktanteilen oder Beschränkungen für digitale Dienstleistungen und Anbieter erhebliche Schranken. Die UCRS würde Unternehmen der digitalen Infrastruktur praktisch ungehinderten Zugang zu Ländern und Rechte garantieren, um dort mit sehr begrenzter Regulierung tätig zu sein.[217]

Die UCRS zielt darauf ab, alle computerverwandten Dienstleistungen automatisch diesen Regeln zu unterstellen, selbst wenn sie zu der Zeit, als die Länder die ursprünglichen Verpflichtungen eingingen, noch gar nicht erfunden waren.[218] Länder, die der UCRS der EU zustimmen, gehen damit Verpflichtungen in Bezug auf den Marktzugang für Computersysteme, die Programmierung einschließlich von Quellcodes und Algorithmen, die Wartung von Computersystemen und Software sowie die Verarbeitung und Speicherung von Daten ein. Mit der Vereinbarung wird sichergestellt, dass diese Verpflichtungen für alle Computer- und verwandten Dienstleistungen gelten, einschließlich Suchmaschinen, sozialen Medien, digitalen Marktplätzen, Online-Werbung oder Digital-Unterhaltung.

Sie würde aber auch solche Dienstleistungen einbeziehen, die erst noch erfunden werden müssen. Einer rechtlichen Analyse zufolge wird damit auch für die Zukunft sichergestellt, dass der Begriff Computer- und verwandte Dienstleistungen jegliche neuen Dienstleistungen und Technologien umfasst, die in der Zukunft möglicherweise entwickelt werden, aber ohne irgendwelche Kriterien dafür, welche zusätzlichen Elemente darunterfallen könnten,[219]

Die Anwendung offener Regelungen, die wettbewerbspolitische Abhilfemaßnahmen im Hinblick auf alle digitalen Dienste beschränken, würde den monopolistischen Praktiken von Big Tech zum Nachteil einer gerechten Wettbewerbspolitik bis weit in die Zukunft Vorschub leisten.

Verbot der Transparenz von Quellcode

Wie nachfolgend erläutert, werden im Rahmen der KI-Verordnung weitere Untersuchungen von Algorithmen verlangt, die als „hochriskant" eingestuft werden.

Viele monopolistische Praktiken werden jedoch in einem Umfeld angewandt, das dieser Einstufung nicht entspricht. So mag beispielsweise digitale Werbung nicht als "hochriskant" betrachtet werden, dennoch basiert dieser Sektor weitgehend auf den oligopolistischen Praktiken von Big-Tech-Giganten. Desgleichen sind auch wettbewerbsfeindliche Praktiken unter Einsatz von Algorithmen im Online-Einzelhandel gang und gäbe, wo Unternehmen wie Amazon dafür sorgen, dass ihre Suchalgorithmen ihre eigenen Produkte oder Dienstleistungen gegenüber denen anderer Anbieter begünstigen. Die Einleitung rechtlicher Schritte kann problematisch sein, weil es an Kapazitäten mangelt, die Ursache des Problems zu ermitteln, oder weil es möglicherweise schwierig ist, ohne Zugang die erforderlichen Beweise zu erbringen, oder weil die Behörde nicht über das nötige Fachwissen verfügt, ohne sich an Dritte wenden zu können, was sie aber aufgrund von vorgeschriebenen Maßnahmen zum „Schutz vor unberechtigtem Zugriff" nicht ohne Weiteres tun kann.

Die neuen Ausnahmen erleichtern solche Untersuchungen. Diese Regeln setzen allerdings nach wie vor einen Verdacht voraus, da sie sich auf bestimmte Fälle beziehen, und können keine generelle Offenlegung verlangen, was zum klassischen Henne-Ei-Problem führt – die Betroffenen müssen wissen, dass sie geschädigt werden, den Verdacht haben, dass dies mit dem Algorithmus zusammenhängt, und die Regulierungsbehörde davon überzeugen. Oder die Regulierungsbehörde muss selbst dazu in der Lage sein, eine

217 Jane Kelsey, „Understanding the European Union's Understanding on Computer and Related Services", Third World Network (September 2019), https://www.twn.my/title2/briefing_papers/No101.pdf. Die vollständige Untersuchung unter https://www.twn.my/title2/FTAs/Services/Full%20report%20for%20TD%20series_FORMAT_Ver6-FIN-09012020.pdf.
218 Ibid:
219 Ibid:

Glaubhaftmachung zu erbringen, um den Zugriff auf Quellcode zu rechtfertigen. In früheren Vereinbarungen bezogen sich die Ausnahmen nur auf die Anforderungen an Abhilfemaßnahmen, wobei davon ausgegangen wird, dass die Vertragsparteien ohne Zugriff auf den Code (oder in einigen Vereinbarungen auf Algorithmen, obwohl die Verbindung zwischen beiden manchmal unklar ist) ihre Argumente vorbringen können und das Problem und die Lösung ermitteln können.

Regeln für Interoperabilität

Big Tech schließt häufig die Produkte anderer Unternehmen von seinen Plattformen oder Betriebssystemen aus, um seine Monopolstellung zu behalten. So gewährt z. B. Apple anderen digitalen Zahlungssystemen keinen Zugang zu seinem App Store. Die EU hat im DSA vor kurzem Interoperabilität zur Anforderung erhoben. Big Tech würde gerne das Recht auf diese monopolistische Praxis behalten. Die jüngste durchgesickerte Version der gemeinsamen Initiative zu E-Commerce (Joint Statement Initiative on E-Commerce, JSI), über die derzeit in der WTO verhandelt wird, enthält die folgende Bestimmung: Keine Partei/kein Mitglied darf öffentliche Telekommunikationsnetze oder ihre Diensteanbieter, einschließlich der Anbieter von Mehrwertdiensten, daran hindern, die für ihre Netze und Dienste eingesetzten Technologien und/oder die mit dem elektronischen Geschäftsverkehr verbundenen Netzeinrichtungen und Produkte im Zusammenhang mit den Technologien frei zu wählen.[220] Mit dem Wortlaut dieser Bestimmung wird ausgeschlossen, dass die Staaten Interoperabilität vorschreiben können, z. B. in App-Stores. Sie ist in den EU-Abkommen über den digitalen Handel zwar nicht enthalten, aber ihr Vorhandensein in den plurilateralen Abkommen, die die EU bei der WTO aushandelt, sollte Anlass zur Besorgnis geben.

Vorschriften zum Verbot von Anforderungen an Unternehmen, eine lokale Präsenz zu unterhalten

Big-Tech-Unternehmen wählen die Länder, in denen sie tätig sind, unter dem Gesichtspunkt von Größenvorteilen und Regulierungs- und Steuerarbitrage aus. Wenn sie grenzüberschreitend tätig sind (Modus 1 im GATS-Jargon), ist es äußerst schwierig, sie einer nationalen Gerichtsbarkeit zu unterstellen. Die Regel „keine lokale Präsenz" in den jüngsten Kapiteln über Dienstleistungen, die auf der Wunschliste von Big Tech steht, begünstigt das. Gleiches gilt für die Bestimmung über den Marktzugang, wonach Staaten einer Unternehmenseinheit mit lokaler Präsenz keine bestimmte Rechtsform vorschreiben dürfen, so dass sie für die Handlungen des Unternehmens, dem sie Dienstleistungen erbringt, möglicherweise rechtlich nicht verantwortlich ist. Die Zustellung von juristischen Unterlagen an eine Unternehmenseinheit in einer anderen Gerichtsbarkeit ist äußerst problematisch, wenn sie die Annahme der lokalen Zustellung nicht akzeptiert. Dies kann ein zeitaufwändiger, komplexer und teurer diplomatischer Prozess sein. Nach der Zustellung ist es eine weitere Herausforderung, die Einheit dazu zu bringen, sich der Gerichtsbarkeit zu unterwerfen. Sind diese beiden Schwierigkeiten überwunden, stellt sich das weitere Problem, die Entscheidung durchzusetzen.[221]

Die Vorreiterrolle der EU, wenn es darum geht, Big-Tech-Giganten endlich für ihr wettbewerbswidriges Verhalten zur Rechenschaft zu ziehen und neue Regeln zu erlassen, um monopolistisches Verhalten im Internet einzuschränken, sollte nicht durch verdeckte Versuche von Big Tech ausgehebelt werden, die Regeln der Weltwirtschaft zu seinen eigenen Gunsten zu manipulieren.

10- ... KMU IN DER EU?

Im Jahr 2021 waren 99,8 Prozent aller Unternehmen in der EU-27 im nichtfinanziellen Sektor der gewerblichen Wirtschaft KMU. Sie beschäftigten 83 Millionen Menschen, was 64 Prozent der Gesamtbeschäftigung im nichtfinanziellen Sektor entspricht, und generierten 52 Prozent der gesamten Wertschöpfung des nichtfinanziellen Wirtschaftssektors.[222] Die große Mehrheit der KMU in der EU, die Online-Handel betreiben, nutzen die Online-Plattformen von Big Tech, um die Verbraucher*innen zu erreichen. Das Marktmachtgefälle zwischen KMU und Big Tech in der jüngeren Geschichte ist beispiellos.

Im Hinblick darauf, wie ihre Produkte in den Suchergebnissen platziert oder auf sonstige Weise beworben werden, sind KMU von den Algorithmen der Plattformen abhängig. Unternehmen, die Big-Tech-Plattformen nutzen, haben keinen Zugang zu den Daten ihrer eigenen Kund*innen, die aus ihren eigenen Aktivitäten auf der Plattform des Gatekeepers

220 E(2)(1)5 vom September 2021 WTO-Entwurf.
221 Ich danke Kristina Irion für diese wichtige Feststellung.
222 Patrice Muller et al, „Annual Report on European SMEs 2021/22: SMEs and environmental sustainability", Europäische Kommission (April 2022), https://single-market-economy.ec.europa.eu/smes/sme-strategy/sme-performance-review_en#paragraph_885.

resultieren, was ihnen den Wettbewerb auf einem fairen Markt unmöglich macht, wohingegen die Big-Tech-Plattform solche Daten für ihre eigenen Geschäftszwecke verwenden können.

Bestimmungen für den digitalen Handel, die Staaten daran hindern, algorithmische Transparenz oder die lokale Speicherung von Datenkopien zu verlangen (falls das lokale Unternehmen in einem anderen Land seinen Sitz hat als die Plattform des Gatekeepers), schränken die Abhilfemöglichkeiten für solche Probleme ein.

Aber dies sind nur einige Beispiele dafür, mit welchen Methoden Big-Tech-Giganten versuchen, Regeln für den digitalen Handel zur Errichtung globaler Marktdominanz zu nutzen. Der gesamte Vorschriftenkatalog für den digitalen Handel wurde von Big Tech zugunsten seiner eigenen Interessen erstellt. Statt den größten Unternehmen neue Rechte in verbindlichen, dauerhaften Verträgen einzuräumen, sollte die Rechtsetzung durch diese „Handelsbestimmungen" ausgesetzt werden, bis neue Regeln umgesetzt werden können, die KMU zugutekommen und die Macht von Big Tech, unter anderem zum globalen Absaugen von Daten, einschränken würden.

Die europäischen Vorschläge enthalten darüber hinaus umfassende Verpflichtungen im Hinblick auf „Computer- und verwandte Dienstleistungen", die Unternehmen der digitalen Infrastruktur praktisch ungehinderten Zugang zu Ländern geben und Rechte garantieren, um dort mit sehr begrenzter Regulierung tätig zu sein.[223] Manche sehen darin zwar eine Chance, europäischen Unternehmen den Zugang zu ausländischen Märkten zu eröffnen, aber die Erstanbieter- und Größenvorteile der in den USA ansässigen Big-Tech-Unternehmen lassen vermuten, dass sie ihre Dominanz bei einem solchen Ansatz wahrscheinlich festigen werden.

Bei einer vollständig liberalisierten Marktzugangsregelung für Computer- und verwandte Dienstleistungen, die so breit gefasst ist wie der EU-Vorschlag, lässt sich ein Spielraum für den Schutz oder die Unterstützung europäischer KMU nur schwer erkennen. Angesichts der jüngsten und neu aufkeimenden Besorgnis über den Verlust von Marktanteilen der europäischen KMU, der Begrenzung des politischen Handlungsspielraums im Bereich der digitalen Industrien und der Forderung an die europäische Politik, dass die Vorteile der Digitalisierung in der Region allen Europäer*innen zugutekommen müssen, sind die Regeln für den digitalen Handel, die die EU seit 2016 unterstützt, überholt und nicht zeitgemäß.

223 Kelsey, „Understanding EU Understanding on Computer and Related", TWN (2019).

6.

WEM WIRD DIE EU-AGENDA FÜR DEN DIGITALEN HANDEL NUTZEN?

Man kann sich die Frage stellen, warum die europäische Handelspolitik so sehr darauf ausgerichtet zu sein scheint, statt europäischen Unternehmen die größten transnationalen Technologiekonzerne zu begünstigen, wenn diese doch tatsächlich alle ihren Sitz in den USA (oder in China) haben.

Erstens ist die „europäische" Wirtschaftslobby in großem Maße von US-amerikanischen Big-Tech-Unternehmen dominiert. Die wichtigsten in Europa ansässigen Handelsgruppen, die Lobbyarbeit für den digitalen Handel in der EU betreiben, sind DigitalEurope, Ecommerce Europe und das European Services Forum. So hat DigitalEurope wiederholt in den europäischen Gesetzgebungsprozess für den digitalen Handel eingegriffen, unter anderem mit der Ernennung von Nick Clegg, dem ehemaligen stellvertretenden Premierminister Großbritanniens, zu seinem globalen Cheflobbyisten.[224] Aber es vertritt die Interessen von Amazon, Apple, Meta (Facebook) und Google sowie einiger europäischer Unternehmen. Zu Ecommerce Europe gehören Amazon, eBay und Etsy. Das European Services Forum zählt unter anderem Apple, Google, IBM, Microsoft, Oracle und UPS zu seinen Mitgliedern. Auch die Corporate Advisory and Support Group von BusinessEurope erbringt ihre Dienste für Apple, Meta, Google, Microsoft, Uber, Intel, IBM und Oracle.[225]

Zweitens betreiben neben den „europäischen" Handelsvereinigungen auch in den USA beheimatete Handelsverbände von Big Tech massive Lobbyarbeit im Bereich des digitalen Handels. Dazu gehören die Computer & Communications Industry Association, die inzwischen aufgelöste Internet Association, der Information Technology Industry Council, der U.S. Council for International Business, die Coalition of Services Industries und der National Foreign Trade Council.[226]

Der dritte Grund ist die massive Ausweitung der direkten Lobbyarbeit von US-amerikanischen Big-Tech-Unternehmen bei Amtspersonen der EU. In dem spektakulären Bericht „The Lobby Network: Big Tech's Web of Influence in the EU"[227] geben Corporate Europe Observatory (CEO) und Lobbycontrol Einblick in die Macht der Technologie-Lobby bei der EU. Sie kartierten erstmals das „Universum" der Lobby-Akteure im Bereich der Digitalwirtschaft der EU und entdeckten einen großen, aber sehr aus dem Gleichgewicht geratenen „Kosmos":

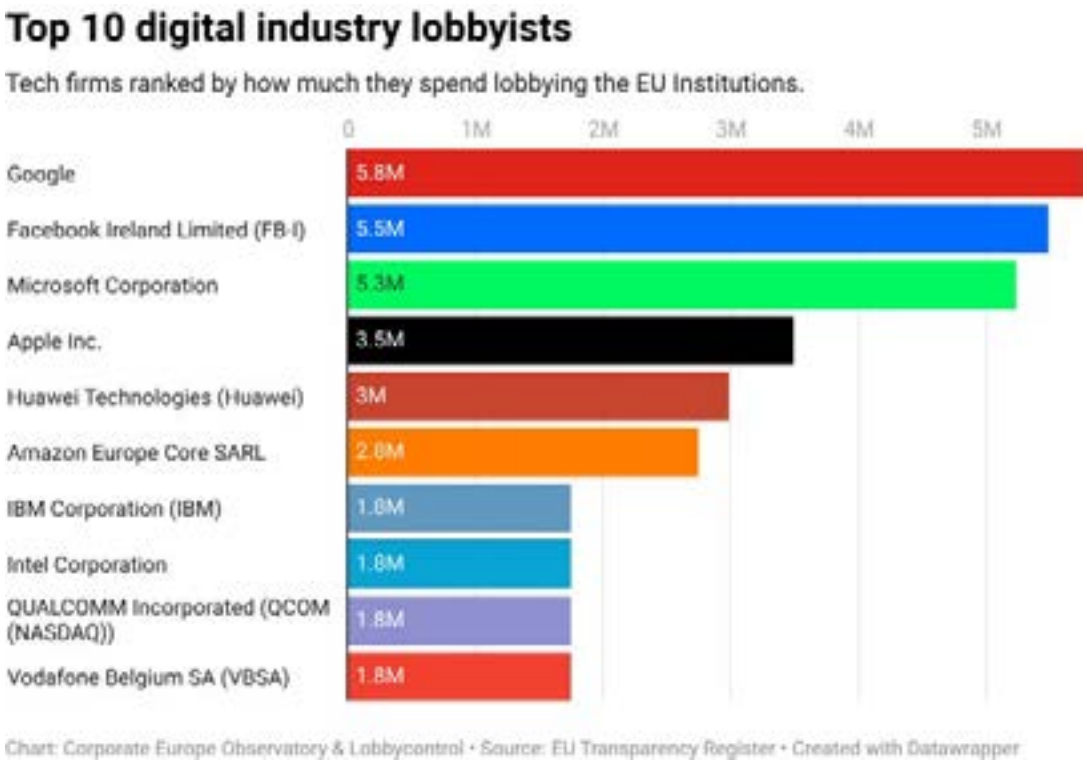
- Dieser besteht aus 612 Unternehmen, Gruppen und Wirtschaftsverbänden, die Lobbyarbeit bei EU-Institutionen betreiben, und jährlich über 97 Millionen Euro dafür aufwenden. Damit ist der Technologiesektor in Bezug auf die Ausgaben die größte Lobbybranche in der EU, noch vor den Bereichen Pharma, fossile Brennstoffe, Finanzwesen und Chemie.

- Trotz der unterschiedlichen Anzahl von Akteuren wird dieser Kosmos von einer Handvoll Unternehmen beherrscht. Auf nur zehn Unternehmen entfällt fast ein Drittel der Gesamtausgaben der Tech-Lobby: Vodafone, Qualcomm, Intel, IBM, Amazon, Huawei, Apple, Microsoft, Facebook und Google geben über 32 Millionen Euro dafür aus, sich in der EU Gehör zu verschaffen.[228]

Die nachstehenden Zahlen stammen aus der Untersuchung und wurden von den Unternehmen

224 Nick Clegg, „The next two years will define the next 20 for Europe's internet economy", Medium (Mai 2021), https://nickclegg.medium.com/the-next-two-years-will-define-the-next-20-for-europes-internet-economy-8e02da6754da.
225 Die zur Corporate Advisory and Support Group von BusinessEurope gehörenden Unternehmen sind auf dieser Website aufgeführt: https://www.businesseurope.eu/about-us/asgroup-our-partner-companies.
226 Daniel Rangel et al, '„Digital Trade' Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies", Rethink Trade (November 2022), https://rethinktrade.org/fact-sheet/digital-trade-doublespeak-big-techs-hijack-of-trade-lingo-to-attack-anti-monopoly-and-competition-policies/.
227 Max Bank et al, „The Lobby Network: Big Tech's Web of Influence in the EU", *Corporate Europe Observatory (CEO) und Lobbycontrol* (August 2021), https://corporateeurope.org/sites/default/files/2021-08/The%20lobby%20network%20-%20Big%20Tech%27s%20web%20of%20influence%20in%20the%20EU.pdf .
228 Bank et al, „The Lobby Network", CEO und LobbyControl (2021).

im Jahr 2021 selbst so angegeben; Google und Facebook sowie einige andere haben ihre Ausgaben erheblich erhöht.



All diese Technologieunternehmen haben ihre Budgets und ihr Personal für die Lobbyarbeit in den letzten Jahren massiv aufgestockt. „Ich habe so etwas noch nie gesehen, zumindest nicht in diesem Ausmaß," so das Zitat von Bernd Meyring, Anwalt für Wettbewerbsrecht, in Politico. „Im Vergleich zu anderen Branchen ist das außergewöhnlich und zeigt, was für diese Unternehmen auf dem Spiel steht."[229] CEO zufolge fanden seit dem Beginn der Ausarbeitung des ersten Rahmens für Legislativvorschläge unzählige Lobby-Treffen dieser Unternehmen mit der Kommission und Parlamentsmitgliedern statt.[230]

Andere Informationsquellen haben diese rege Betriebsamkeit bestätigt, wobei sie insbesondere auf die gezielte Lobbyarbeit von Big Tech bei der EU im Hinblick auf die WTO und den freien Datenverkehr hinweisen.[231] Nach dem Durchsickern der Lobbystrategie von Google, die unter anderem vorsah, „Gegenwind gegen Kommissar Breton zu erzeugen" und „Konflikte zwischen den Abteilungen der Kommission zu schüren" kam es sogar zu einem kleinen Skandal.[232]

US-amerikanische Regulierungsbehörden halten sich mit Kritik an den neuen europäischen Gesetzesinitiativen zurück,[233] möglicherweise weil dieselben Themen im eigenen Land Gegenstand von Debatten im US-Kongress und von Bundesbehörden sind. Der EU-US-Handels- und Technologierat ist jedoch ein klassisches Beispiel dafür, wie unter dem Deckmantel der „regulatorischen Zusammenarbeit" Gesetze blockiert oder geschwächt werden, und dient den Lobbyisten der Branche als Anlaufstelle, wie aus einem weiteren Bericht von CEO hervorgeht.[234]

229 Pietro Lombardi, „Big Tech gears up for tougher regulatory environment in Europe", *PoliticoPro* (März 2022), https://pro.politico.eu/news/147856.
230 „Big Tech brings out the big guns in fight for future of EU tech regulation", *Corporate Europe Observatory* (Dezember 2020), https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation.
231 Alexander Fanta, „Tech industry pushes Europe for WTO data flows deal: Documents reveal the lobbying push by Microsoft, Google and other tech giants to influence secretive trade talks that could change the future of the internet", Netzpolitik.org (Juni 2021), https://netzpolitik.org/2021/digital-trade-tech-industry-pushes-europe-for-wto-data-flows-deal/.
232 Emmanuel Berretta und Guillaume Grallet, „Comment Google veut faire plier Bruxelles", *Le Point* (Oktober 2020), https://www.lepoint.fr/high-tech-internet/exclusif-comment-google-veut-faire-plier-bruxelles-28-10-2020-2398468_47.php.
233 Leah Nylen und Samuel Stolton, „U.S. slow to respond to EU's landmark tech regulation", *Politico* (März 2022), https://www.politico.com/news/2022/03/25/us-eu-digital-markets-act-00020551.
234 'Tech lobby eyes opportunities created by new EU-US Trade and Tech Council,' Corporate Europe Observatory (September 2021), https://corporateeurope.org/en/2021/09/tech-lobby-eyes-opportunities-created-new-eu-us-trade-and-tech-council

Diese Big-Tech-Giganten geben sich jedoch nicht mit direkter lobbyistischer Einflussnahme zufrieden. Sie nutzen für ihre Machtausübung auch Gruppen wie den Pakt für klimaneutrale Rechenzentren (Climate Neutral Data Centre Pact - CNDCP). Europäische Teilnehmer dieser Initiative beschweren sich, dass „große US-amerikanische Datenunternehmen den Pakt als Lobby-Vehikel nutzen. „Es wird nie wirklich ausgesprochen, aber ihr Ziel ist es, die Akteure der Branche zusammenzubringen und in ihrem Namen sprechen zu können,"[235] so der Manager eines von mehreren europäischen Mitgliedern, der anonym bleiben wollte, in einem Gespräch mit Politico. Zu den Unterzeichnern des Pakts gehören Amazon Web Services, Google und Microsoft.[236]

Im Oktober 2002 beantragten führende Parlamentsabgeordnete eine Untersuchung von Google, Meta (Facebook) und Amazon sowie der Computer & Communications Industry Association und weiterer Handelslobbygruppen und forderten, den Unternehmen die Beziehungen zu den EU-Institutionen zu untersagen. In der Beschwerde heißt es, dass die großen Technologieunternehmen *die Gesetzgeber der EU im Rahmen ihrer Lobbymaßnahmen zu DSA und DMA täuschten*, indem sie vorgäben, offizielle Vertreter von KMU zu sein, während sie gleichzeitig die Geschäftsinteressen von Big Tech unterstützten und verteidigten – ohne jedoch ihre Verbindungen offenzulegen.[237]

Angesichts dieser Fakten ist leicht zu erkennen, warum die Handelspolitik der EU noch immer zugunsten von Big Tech gestaltet wird. Und es lässt sich ahnen, dass dies auch für die Handelspolitik in Japan, Australien, Kanada usw. gilt. Von daher ist das Argument, „die gesamte entwickelte Welt" bevorzuge diese oder jene Politik, nicht haltbar, wenn man sieht, dass die betreffende Politik auf die Lobbyarbeit einiger weniger Big-Tech-Unternehmen in den USA zurückzuführen ist.

235 Louise Guillot, „How US tech is using a data center pact to lobby Brussels", *PoliticoPro* (Mai 2022), https://www.politico.eu/article/us-tech-climate-neutral-data-center-pact-eu-lobbying-carbon-footprint-environment/.
236 Die vollständige Liste der Unterzeichner ist hier zu finden: https://www.climateneutraldatacentre.net/signatories/.
237 Clothilde Goujard, „Big Tech accused of shady lobbying in EU Parliament: Lawmakers file complaints against 8 companies and trade groups over alleged shadow lobbying", *Politico EU* (Oktober 2022), https://www.politico.eu/article/big-tech-companies-face-potential-eu-lobbying-ban/.

7.

AGENDA FÜR DEN DIGITALEN HANDEL VS. AKTUELLE EUROPÄISCHE GESETZGEBUNGSAGENDA

In der jüngsten allgemeinen Handelspolitik der EU „Eine offene, nachhaltige und entschlossene Handelspolitik" wird festgestellt: „Die EU sollte bei digitalen Standards und Ansätzen zur Regulierung in diesem Bereich weiterhin eine führende Rolle spielen, insbesondere im Bereich des Datenschutzes, wo die Datenschutz-Grundverordnung der EU häufig als Inspiration dient. Um dies zu erreichen, muss die WTO die Regeln für den digitalen Handel festlegen, und die EU muss dabei eine zentrale Rolle einnehmen."[238]

Die folgende Analyse der aktuellen Legislativvorhaben der EU zeigt jedoch, dass die EU-Handelspolitik den erklärten Zielen und den konkreten Bestimmungen dieser Initiativen de facto fundamental zuwiderläuft und, falls sie nicht grundlegend geändert wird, die Fähigkeit der EU zu ihrer Durchsetzung erheblich beeinträchtigen könnte.

Das Europäische Parlament und die Europäische Kommission haben neben der bekannten DSGVO eine Vielzahl großer Legislativvorhaben, die auf eine Regulierung der digitalen Wirtschaft abzielen, beschlossen oder sind dabei, sie zu prüfen, die mit den Regeln für den digitalen Handel zusammenspielen könnten,.[239] Die relevantesten und bereichsübergreifendsten neben den oben erwähnten spezifischen Projekten werden im Folgenden eingehender betrachtet.

Bevor auf die einzelnen Gesetze eingegangen wird, sei darauf hingewiesen, dass es sich hierbei um einige der ersten großen Schritte der EU zur Regulierung der sich entwickelnden digitalen Wirtschaft handelt, die jedoch nicht die letzten sein dürften. Im Zuge des beschleunigten technologischen Fortschritts, der Erfindung neuer Geschäftsmodelle durch Big Tech und des Auftretens neuer Bedrohungen müssen die Gesetzgeber den politischen Handlungsspielraum für die Bewältigung aktueller und neuer Herausforderungen bewahren. Sie sollten im Rahmen ihrer bereichsübergreifenden gesetzgeberischen Mandate bei der Politikgestaltung in diesem sich schnell verändernden Bereich der digitalen Wirtschaft nicht durch dauerhafte „Handelsbeschränkungen" eingeengt werden.

Das Gesetz über digitale Dienste (DSA) und das Gesetz über den digitalen Markt (DMA) wurden von der EU im Dezember 2020 vorgestellt, in mehreren Ausschüssen beraten und von der Öffentlichkeit eingehend diskutiert. Sie waren Gegenstand intensiver Lobbyanstrengungen der Big Tech-Branche, die sich darum bemühte, die darin enthaltenen Bestimmungen zum Schutz des öffentlichen Interesses zu schwächen. Im Juli 2022 wurden sie vom Europäischen Parlament angenommen, kurz darauf vom Europäischen Rat, und traten am 1. November 2022 (DMA)[240] bzw. 16. November 2022 (DSA)[241] in Kraft.

Beide befassen sich in erster Linie mit Online-Vermittlungsdiensten und Plattformen wie Online-Marktplätzen, sozialen Netzwerken und App-Stores und verfolgen das erklärte Ziel, die Grundrechte aller

238 Europäische Kommission, Generaldirektion Handel, „Mitteilung: Überprüfung der Handelspolitik", Europäische Kommission COM(2021) 66 final (2021).
239 Cristiano Codagnone, Giovanni Liva und Teresa Rodriguez de las Heras Ballell, „Identification and assessment of existing and draft legislation in the digital field: Study Requested by the AIDA Special Committee", Studie des Europäischen Parlaments PE 703.345 (Januar 2022), https://www.europarl.europa.eu/thinktank/de/document/IPOL_STU(2022)703345.
240 Europäisches Parlament, „Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (Text von Bedeutung für den EWR)", EU-Verordnung PE/17/2022/REV/1 veröffentlicht auf EUR-Lex (September 2022), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R1925&from=de.
241 European Parliament,„Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (Text von Bedeutung für den EWR)", EU-Verordnung PE/30/2022/REV/1 veröffentlicht auf EUR-Lex (Oktober 2022), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065&from=en.

Nutzer*innen von digitalen Diensten zu schützen und faire Wettbewerbsbedingungen zur Förderung von Innovation, Wachstum und Wettbewerbsfähigkeit zu gewährleisten.[242] An ihrer Umsetzung werden zahlreiche Akteure beteiligt sein, wobei die Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CNECT) und die Generaldirektion Wettbewerb die Federführung übernehmen werden,

Am 23. Juni 2023 trat dann das Daten-Governance-Gesetz (DGA) in Kraft. Im April 2021 bzw. Februar 2022 legte die Europäische Kommission noch die KI-Verordnung und das Datengesetz vor, die sich noch im Gesetzgebungsverfahren befinden.

Die oben dargelegten Fakten über die negativen Auswirkungen der Bestimmungen der Agenda für den digitalen Handel auf die europäische Gesellschaft werfen die Frage auf, ob die Bestimmungen zu Datenverkehr, Datenlokalisierung und Geheimhaltung von Quellcode mit den neuen Gesetzen vereinbar sind. Die Antwort ist eindeutig: Sie sind keineswegs vereinbar mit den Gesetzen. Sie sind noch weniger vereinbar mit den erklärten Absichten der Gesetzgeber, Regulierungsbehörden und führenden Politiker*innen der EU.

DSA[243]

Mit dem DSA werden neue Verpflichtungen für Online-Vermittlungsdienste eingeführt, insbesondere sehr große Online-Plattformen und sehr große Online-Suchmaschinen,[244] die monatlich 10 Prozent der europäischen Bevölkerung bzw. 45 Millionen Nutzer*innen erreichen. Es verbietet gezielte Werbung für Kinder sowie Werbung, die auf sensiblen Informationen basiert (z. B. über Rasse, ethnische Zugehörigkeit, politische Ansichten, sexuelle Orientierung oder Religion). Es verpflichtet Unternehmen, systemische Risiken zu ermitteln und zu mindern, die sich aus der Gestaltung der algorithmischen Systeme, Funktionsweise und Nutzung ihrer Dienste ergeben. Die Risikobewertungen müssen Aspekte wie rechtswidrige Inhalte, nachteilige Auswirkungen auf die Ausübung zahlreicher Grundrechte, die gesellschaftliche Debatte, Wahlprozesse und die öffentliche Sicherheit sowie die körperliche und geistige Gesundheit einschließlich des Schutzes von Minderjährigen und geschlechtsspezifischer Gewalt aufgreifen. Diese Bewertungen müssten auch Algorithmen wie Werbe- und Empfehlungssysteme sowie Datenpraktiken einbeziehen. Die Anbieter sehr großer Online-Plattformen und Online-Suchmaschinen werden angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen ergreifen müssen.

Laut Amnesty International bedeutet das, dass Hightech-Giganten mehr Verantwortung für die Nutzung von Algorithmen, die toxische Inhalte gestalten und Hassrede, Desinformation oder geschlechtsspezifische Belästigung verstärken, übernehmen und die Funktionsweise und Konzeption dieser Empfehlungssysteme anpassen müssen, um die Verbreitung solcher schädlichen Inhalte zu verhindern.[245]

Algorithmische Transparenz ist ein zentraler Bestandteil des DSA. Die Regulierungsbehörden müssen ein „Europäisches Zentrum für Algorithmische Transparenz" einrichten, um Wissenschaftler*innen im Bereich Daten und Algorithmen für die Unterstützung der Durchsetzung zu gewinnen, wenngleich kritisiert wird, dass die bislang hierfür vorgeschlagenen Gelder unzureichend sind. Mit der Bestimmung in den Abkommen über den digitalen Handel, die es Regierungen mit wenigen Ausnahmen untersagt, die Offenlegung von Quellcode oder Algorithmen zu verlangen, scheint eine umfassende regulatorische Aufsicht über Algorithmen jedoch nicht machbar zu sein und wird sicherlich erschwert. Wie bereits erwähnt, sind in Artikel 207 des HKA zwischen der EU und dem Vereinigten Königreich Ausnahmen zur Verhinderung oder Behebung von Beschränkungen oder Verfälschungen des Wettbewerbs sowie im Hinblick auf den Schutz der öffentlichen Sicherheit vorgesehen,[246] aber nur für spezifische Untersuchungen und ex-post. Im FHA zwischen der EU und Neuseeland ist eine zusätzliche Ausnahme für Befangenheit vorgesehen und die Beschränkung „spezifisch" aufgehoben.

Dennoch sind in den Bestimmungen Ausnahmen für viele andere Ziele des DSA, unter anderem illegale Inhalte, Grundrechte, Wahlmanipulation, nicht enthalten. Wer dies unter Verweis auf die allgemeinen Ausnahmen, die aus Artikel XX des GATT der WTO

242 Europäische Kommission, „Das Paket des Digital Services Act", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package.
243 „Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD)", Europäisches Parlament, angenommener Text P9_TA(2022)0269 zur Abstimmung PV 05/07/2022 - 6.4 zur Aussprache CRE 19/01/2022 - 14 in Bezug auf das Dokument A9-0356/2021 (Juli 2022), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_DE.html.
244 Laut Definition mit einer durchschnittlichen Anzahl von 45 Millionen aktiven Nutzer*innen pro Monat, wozu voraussichtlich auch Google Search und YouTube von Alphabet, Amazon, Facebook und Instagram von Meta, TikTok und möglicherweise Twitter gehören werden.
245 „What the EU's Digital Services Act means for human rights and harmful Big Tech business models", *Amnesty International* Index: POL 30/5830/2022 (Juli 2022), https://www.amnesty.org/en/documents/pol30/5830/2022/en/.
246 Titel III, Kapitel 3, Artikel 207: Quellcode, Handels- und Kooperationsabkommen (HKA) zwischen der EU und dem Vereinigten Königreich.

in die Abkommen über den digitalen Handel übernommen wurden, vielleicht bestreiten will, sollte beachten, dass diese Ausnahmen keinen direkten Bezug zu den meisten dieser politischen Ziele haben und nur zur Verteidigung in einem Rechtsstreit herangezogen werden können, wobei nur zwei von 48 Versuchen, diese Ausnahmen geltend zu machen, in der WTO jemals erfolgreich waren.[247]

Zivilgesellschaftliche Organisationen fordern eine Stärkung des DSA im Hinblick auf die Gewährleistung der Transparenz von Algorithmen und das Verbot für Big Tech, Algorithmen auf eine Weise zu nutzen, die die Verbreitung von Desinformation, Diskriminierung, Manipulation verschlimmern und den Wettbewerb untergraben,[248] sowie die schrittweise Beendigung aller in die Privatsphäre eingreifenden, überwachungsgestützten Werbung.[249]

Nach einer Untersuchung des Todes der 14-jährigen Molly Russel im Jahr 2017 kam der Untersuchungsrichter zu dem Schluss, dass die sozialen Medien eine Mitschuld tragen, und erklärte, dass das Mädchen durch Selbstverletzung gestorben sei, weil sie unter einer Depression und den negativen Auswirkungen von Online-Content litt.[250] Der Vater des Teenagers hat die Gesetzgeber aufgefordert, den Schutz der Gesundheit und Sicherheit von Kindern in den Vordergrund zu stellen und die Verbreitung von Inhalten zu regulieren.

Gesetzgeber und Regulierungsbehörden müssen gegebenenfalls künftig die Instrumente zur Bekämpfung von negativen sozialen Auswirkungen und Grundrechtsverletzungen durch Überwachungswerbung erweitern. Regulierungskompetenzen durch die Hintertür eines Handelsabkommens einzuengen, ist mit den Zielen der EU unvereinbar. Hier geht es um wesentliche Fragen der Gerechtigkeit und der Grundrechte, die keinesfalls Handelsfragen sein sollten.

Was die Haftung betrifft, sieht das DSA Regeln für Technologieunternehmen vor, um sicherzustellen, dass sie gegen illegale Hassreden und Produkte durchgreifen und mehr Transparenz im Hinblick auf ihren Umgang mit Content zeigen. Das Gesetz wird auch dazu beitragen, gegen schädliche Inhalte vorzugehen, die wie politische oder gesundheitsbezogene Desinformation nicht unbedingt illegal sein müssen, und bessere Regeln für die Moderation von Inhalten und den Schutz der Meinungsfreiheit einzuführen.

In den Abkommen der USA über digitalen Handel gibt es jedoch Bestimmungen, die Abschnitt 230 des US-Kommunikationsgesetzes aufgreifen, wo die Haftung der Anbieter von Plattformen für Schäden beschränkt wird, die durch die Aktivitäten Dritter auf ihren Plattformen verursacht wurden. Eine solche Bestimmung ist in den EU-Regelungen für den digitalen Handel zwar nicht enthalten, findet sich aber ohne Klammern in der jüngsten Fassung des Abkommens über den digitalen Handel wieder, über das derzeit bei der WTO verhandelt wird.[251] Je nach Ausgang dieser Verhandlungen wird es daher künftig gegebenenfalls nicht möglich sein, Plattformanbieter für durch Content auf ihren Plattformen verursachte Schäden zur Rechenschaft zu ziehen.

DMA[252]

Die EU ist führend im Hinblick auf die Durchsetzung von Wettbewerbsregeln gegen das wettbewerbswidrige Verhalten von Google, Facebook und anderen US-amerikanischen Unternehmensriesen.[253] Nun geht die EU von der Verhängung von Geldbußen gegen monopolistisches Verhalten dazu über, einige der wettbewerbswidrigen Praktiken von Online-„Gatekeepern" durch das DMA zu verbieten.

Die neuen Vorschriften untersagen bestimmte missbräuchliche Praktiken, wegen derer Big-Tech-Unternehmen in der Vergangenheit in die Kritik gerieten, wie z. B. die Zusammenführung von Nutzerdaten aus einer Reihe unterschiedlicher Quellen ohne ausdrückliche Zustimmung und mögliche Alternativen. Mit den neuen Anforderungen

247 Rangel, „WTO General Exceptions", Public Citizen (2022).
248 Eliska Pirkova, „The Digital Services Act: your guide to the EU's new content moderation rules", AccessNow (Juli 2022), https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/; sowie Asha Allen und Ophélie Stockhem, „A Series on the EU Digital Services Act: Due Diligence in Content Moderation", *Center for Democracy & Technology* (August 2022), https://cdt.org/insights/a-series-on-the-eu-digital-services-act-due-diligence-in-content-moderation/.
249 Siehe zum Beispiel: Geimeinsamer offener Brief der Zivilgesellschaft unter Federführung von Amnesty International, „EU member states urged to curb invasive internet practices" (März 2022), www.amnesty.eu/news/eu-member-states-urged-to-curb-invasive-internet-practices/; Tracking-Free Ads Coalition, unter: https://trackingfreeads.eu; Europäischer Datenschutzausschuss, „Statement on the Digital Services Package and Data Strategy", EDSA (November 2021), https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf.
250 Dan Milmo, „Molly Russell coroner calls for review of children's social media access", *Guardian* (Oktober 2022), https://www.theguardian.com/technology/2022/oct/14/molly-russell-coroner-calls-for-review-of-childrens-social-media-access.
251 „WTO Electronic Commerce Negotiations Updated Consolidated Negotiating Text – September 2021", WTO INF/ECON/62/Rev.2 (September 2021): 23 (siehe Artikel B.1(2) Interactive computer services (limiting liability)), abrufbar unter https://www.bilaterals.org/?-other-292-.
252 Europäische Kommission, „Das Gesetz über digitale Märkte: für faire und offene digitale Märkte", EU-Website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de. Die legislative Entschließung ist abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_DE.html.
253 Europäische Kommission, „Kartellrecht: Kommission leitet Untersuchung zu mutmaßlich wettbewerbswidrigen Verhaltensweisen von Google und Meta im Bereich Display-Werbung ein", Pressemitteilung (März 2022), https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1703.

müssen sich die Betriebssysteme für die Apps von Drittanbietern öffnen, wodurch beispielsweise iPhone-Nutzer*innen flexibler darüber entscheiden können, welche Programme sie auf ihren Telefonen installieren. Darüber hinaus wurden auch Interoperabilitäts-Regeln, die den Nutzer*innen die Kommunikation zwischen unterschiedlichen Messaging-Diensten, wie WhatsApp und Signal, ermöglichen, von Verbraucherorganisationen weithin begrüßt.[254] Big-Tech-Unternehmen wie Apple, Amazon und Facebook haben gegen diese neuen Rechtsvorschriften Lobbyarbeit betrieben, unter anderem über ihre Lobbyorganisation DigitalEurope, werden nun aber gezwungen sein, sie zu erfüllen.

Eine der Kernbestimmungen des DSA lautet, dass gewerbliche Nutzer*innen einer Plattform Zugang zu den Daten haben müssen, die sie bei der Nutzung der Plattform des Gatekeepers generieren. Dies würde wahrscheinlich die grenzüberschreitende Übermittlung von Daten vom Gatekeeper, z. B. Amazon, an den gewerblichen Nutzer, z. B. ein europäisches KMU, erfordern. Das ist ein wesentlicher Schritt zur Schaffung fairer Wettbewerbsbedingungen zwischen Big-Tech-Giganten und KMU, deren Geschäftstätigkeit von diesen großen Marktplätzen abhängt.

Abkommen über digitalen Handel nehmen Staaten jedoch explizit die Befugnis, grenzüberschreitende Datenübermittlung zu beschränken oder zu verlangen, dass Datenkopien vor Ort vorgehalten werden müssen. Es ist unklar, wie die Anforderung, dass Plattformen ihren Geschäftskunden Daten offenlegen müssen, durchgesetzt werden soll, wenn eine Plattform ihre Datenrechte im Rahmen eines Abkommens über digitalen Handel als Rechtfertigung gegen den obligatorischen Datenzugang oder Datenaustausch geltend macht.

DATEN-GOVERNANCE-GESETZ (DGA)

Laut Definition der Europäischen Kommission ist das DGA „ein sektorübergreifendes Instrument, das darauf abzielt, mehr Daten zur Verfügung zu stellen, indem die Weiterverwendung von öffentlich gespeicherten, geschützten Daten geregelt wird, indem der Datenaustausch durch die Regulierung neuer Datenintermediäre gefördert und der Austausch von Daten für altruistische Zwecke gefördert wird."[255] Sowohl personenbezogene als auch nicht personenbezogene Daten fallen in den Anwendungsbereich des DGA, und überall dort, wo personenbezogene Daten betroffen sind, gilt die Datenschutz-Grundverordnung (DSGVO). Zusätzlich zur DSGVO sollen im DGA verankerte Garantien das Vertrauen in den Datenaustausch und die Weiterverwendung stärken, eine Voraussetzung, um mehr Daten auf dem Markt verfügbar zu machen.[256]

Das DGA „wird auch die Einrichtung und Entwicklung gemeinsamer europäischer Datenräume in strategischen Bereichen unterstützen, die sowohl private als auch öffentliche Akteure in Bereichen wie Gesundheit, Umwelt, Energie, Landwirtschaft, Mobilität, Finanzen, verarbeitende Industrie, öffentliche Verwaltung und Kompetenzen einbeziehen."[257]

Das DGA ist offenbar auf die Schaffung einer datengesteuerten europäischen Wirtschaft ausgerichtet. Insofern scheint es das Potenzial zu haben, die Nutzung von Daten im öffentlichen Interesse zu fördern.

Aber neben der Förderung der Weiterverwendung von Daten des öffentlichen Sektors für private Zwecke, unter anderem durch Datentrusts und Datengenossenschaften sowie durch Big Tech,[258] sind offenbar keine Bestimmungen vorhanden, die die Weitergabe oder Weiterverwendung privater Daten (z. B. im Besitz von Big Tech) im öffentlichen Interesse verlangen, ein Gedanke, der künftig von Belang sein könnte. Dieses Erfordernis des öffentlichen Interesses könnte durch Regeln für den „digitalen Handel" eingeschränkt werden, die den Regierungen, abgesehen von den schwachen allgemeinen Ausnahmen, die Befugnis nehmen, die Offenlegung von Daten zu verlangen.

254 Europäische Verbraucherorganisation, „Crucial rules to rein in Big Tech and boost consumer choice to now become EU law", Pressemitteilung der Europäischen Verbraucherorganisation (BEUC) (Juli 2022), https://www.beuc.eu/press-releases/crucial-rules-rein-big-tech-and-boost-consumer-choice-now-become-eu-law.
255 Europäische Kommission, „Data Governance Act erklärt", EU-Webseite Policies, hhttps://digital-strategy.ec.europa.eu/de/policies/data-governance-act-explained.
256 Ibid:
257 Europäische Kommission, „Europäisches Daten-Governance-Gesetz", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/data-governance-act.
258 Collington, „Digital Public Assets", Common Wealth (2019).

DATENGESETZ (DA)

Im Februar 2022 wurde ein Vorschlag für ein neues Datengesetz vorgelegt, um die Vorschriften für den Zugang zu und die Nutzung von Daten zu harmonisieren. Zusammen mit dem DGA ist es Bestandteil der Europäischen Datenstrategie, in deren Fokus die digitale Souveränität Europas steht.[259]

Der Vorschlag für das DA enthält die folgenden Punkte:

- Maßnahmen, die es den Nutzer*innen vernetzter Geräte ermöglichen, Zugang zu den von ihnen generierten Daten zu erhalten und diese Daten an Dritte weiterzugeben, um Aftermarket- oder andere datengesteuerte, innovative Dienstleistungen zu erbringen,

- Maßnahmen zum Ausgleich der Verhandlungsmacht von KMU, indem sie vor unlauteren Vertragsklauseln über den Datenaustausch geschützt werden, die ihnen von einer Partei mit deutlich stärkerer Verhandlungsposition auferlegt werden,

- Maßnahmen, die es öffentlichen Stellen ermöglichen, auf Daten im Besitz des privaten Sektors zuzugreifen und diese zu nutzen, wenn sie unter außergewöhnlichen Umständen benötigt werden, insbesondere bei öffentlichen Notfällen wie Überschwemmungen und Bränden, oder um einem gesetzlichen Auftrag nachzukommen, wenn anderweitig keine Daten verfügbar sind,

- neue Vorschriften, die den Kunden einen effektiven Wechsel zwischen verschiedenen Cloud-Anbietern ermöglichen,

- neue Garantien gegen illegalen Datenverkehr.

Es stellt sich die Frage, wie dies mit EU-Regeln für den digitalen Handel erreicht werden soll, die der datenerhebenden Stelle das exklusive Recht geben, Daten auf beliebige Weise zu sammeln, zu übertragen, zu speichern, zu verwenden, zu verkaufen oder zu nutzen, ohne dass der Staat das Recht hätte, Praktiken wie die gemeinsame Nutzung von Daten im öffentlichen Interesse anzuordnen.

GESETZ ÜBER KÜNSTLICHE INTELLIGENZ (KI-VERORDNUNG) UND KI-HAFTUNGS-RICHTLINIE (AI LIABILITY DIRECTIVE)

Die EU erarbeitet derzeit ferner den Entwurf einer KI-Verordnung[260] mit dem erklärten Ziel, die EU zu einer weltweit führenden Drehscheibe für KI zu machen und sicherzustellen, dass KI menschenzentriert und vertrauenswürdig ist.[261] Die KI-Verordnung würde sich auf einen risikobasierten Ansatz stützen, indem bestimmte Verwendungen von KI verboten, die Nutzung hochriskanter KI-Systeme eingeschränkt und KI-Systeme mit begrenztem oder geringem Risiko reguliert werden. Es geht darum, die führende Position der EU in diesem Bereich zu stärken, um die Vorteile von KI zu nutzen und gleichzeitig rechtswidrige Überwachung oder die Verletzung von Grundrechten einzudämmen.[262] Dies stellt zwar eine Verbesserung gegenüber der derzeit unzureichenden Regulierung dar, Menschen- und Bürgerrechtsgruppen bemängeln jedoch, dass die KI-Verordnung nicht ausreicht, um den lebensrettenden Zugang zu öffentlichen Leistungen und Diensten zu schützen,[263] Grundrechte zu wahren und das Recht auf Entschädigung anzubieten.[264]

Die künftige Regulierung ethischer, vertrauenswürdiger und menschenzentrierter KI erfordert möglicherweise ein gewisses Maß an Transparenz oder Offenlegung der Codes und Algorithmen für maschinelles Lernen, entweder im Zuge des Genehmigungsverfahrens für kritische Anwendungen oder zum Zweck der Ausübung der Regulierungsaufsicht, so das Ergebnis einer wissenschaftlichen Studie im Auftrag des niederländischen Außenministeriums.[265]

Nach den vorgeschlagenen EU-Regeln für digitalen Handel, die Anforderungen an die Offenlegung von Quellcode verbieten, könnten ausländische Beklagte

259 Europäische Kommission, „Eine europäische Datenstrategie", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/strategy-data.
260 Europäische Kommission, „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz" und „Anhänge des Vorschlags", Europäische Kommission COM(2021) 206 final (April 2021), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.
261 Europäische Kommission, „Ein europäischer Ansatz für künstliche Intelligenz", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/de/policies/european-approach-artificial-intelligence.
262 Europäisches Parlament, „Artificial intelligence: MEPs want the EU to be a global standard-setter", Europäisches Parlament Plenarsitzung ITRE Pressemeldung (Mai 2022), https://www.europarl.europa.eu/news/en/press-room/20220429IPR28228/artificial-intelligence-meps-want-the-eu-to-be-a-global-standard-setter.
263 Human Rights Watch, „How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers", HRW Q&A (November 2021), https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net.
264 Zivilgesellschaftliche Erklärung unter der Federführung von European Digital Rights, unterstützt von 123 weiteren zivilgesellschaftlichen Gruppen, an die EU, das Europäische Parlament und alle EU-Mitgliedstaaten, „An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement" (November 2021) https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf.
265 Kristina Irion und Josephine Williams, „Prospective Policy Study on Artificial Intelligence and EU Trade Policy", *Institute for information Law* (Januar 2020), https://www.ivir.nl/publicaties/download/ivir_artificial-intelligence-and-eu-trade-policy.pdf.

möglicherweise vertragliche Rechte gegen die erzwungene Offenlegung von in der KI verwendeten Datensätzen und Quellcodes geltend machen, was die Anwendung der Verordnung auf ausländische, nicht aber auf inländische Beklagte, schwierig macht. In einer Studie des Ausschusses des Europäischen Parlaments für Internationalen Handel (INTA) wird festgestellt, dass Handelsregeln die Regelungskompetenz der EU im Hinblick auf eine vertrauenswürdige und ethische KI erheblich beschränken könnten.[266]

Darüber hinaus wird festgehalten, dass die Verabschiedung einer ähnlichen Bestimmung in einem Abkommen, das auch für die EU verbindlich wäre, die Gefahr berge, dass die derzeitigen Bemühungen der EU um eine Regulierung von KI, z. B. im Hinblick auf seine Transparenz, behindert werden.[267] Auch die Hochrangige EU-Sachverständigengruppe für künstliche Intelligenz nennt der Studie zufolge Transparenz als eine der Anforderungen, die KI erfüllen sollte.[268]

Um also Big Tech und seine Verwendung von Algorithmen zu regulieren, müssen die Länder ihren bestehenden Regulierungsraum bewahren, indem sie keine verbindlichen Verpflichtungen für die Offenlegung von Quellcode eingehen. Da nicht bekannt ist, welche Art von Algorithmen in der Zukunft entwickelt wird, ist dieser Regulierungsraum für alle Regierungen äußerst wichtig.

Im September 2022 veröffentlichte die EU den Entwurf einer KI-Haftungs-Richtlinie, mit der die Haftungsvorschriften für das digitale Zeitalter aktualisiert werden sollen. Der Ansatz der EU unterscheidet sich von dem der USA, wo die Haftung von Plattformen für die Aktivitäten Dritter auf ihren Netzwerken durch Abschnitt 230 des US-Kommunikationsgesetzes begrenzt ist. Die neue KI-Haftungs-Richtlinie würde stattdessen Verbraucher*innen, die durch KI geschädigt wurden, mehr Rechte geben, indem davon ausgegangen wird, dass ein Unternehmen verantwortlich ist, wenn es die rechtlichen Anforderungen nicht erfüllt hat oder sich weigerte, die laut KI-Verordnung verlangten relevanten Informationen offenzulegen.[269] Medienberichten zufolge würde die Richtlinie die Offenlegung der für die Entwicklung des KI-Systems verwendeten Datensätze, der technischen Unterlagen, der Protokolle, des Qualitätsmanagementsystems und aller Korrekturmaßnahmen zur Auflage machen.[270]

Darüber hinaus würde der Haftungsausschluss für Plattformen, der in den Bestimmungen des bei der WTO vorgeschlagenen plurilateralen Abkommens für digitalen Handel vorgesehen ist, Staaten die Möglichkeit nehmen, Plattformen für die Veröffentlichung von Inhalten, die von Dritten erstellt wurden, haftbar zu machen. Die USA selbst befanden die allgemeinen Ausnahmen für so unzureichend, dass sie die Aufnahme einer besonderen Bestimmung in den Entwurfstext vorschlugen, in der ausgeführt wird, dass die Maßnahmen zum Schutz vor Online-Sexhandel, sexueller Ausbeutung von Kindern und Prostitution im Sinne des US Public Law 115-164, des „Allow States and Victims to Fight Online Sex Trafficking Act of 2017" zur Änderung des Kommunikationsgesetzes von 1934, notwendig sind, um die öffentliche Sittlichkeit zu schützen.[271] Dies ist die einzige Ausschlussregelung im US-Recht zum Haftungsverbot gemäß Abschnitt 230.

266 Michele Fink, „Legal Analysis of International Trade Law and Digital Trade: Briefing Requested by the INTA committee", Europäisches Parlament (November 2020), https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2020)603517.
267 Ibid: 13.
268 Europäische Kommission, „High-level expert group on artificial intelligence", EU-Webseite Policies, https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai.
269 Gian Volpicelli und Samuel Stolton, „EU wants to empower courts, victims in fight against harmful AI", *PoliticoPro* (September 2022), https://subscriber.politicopro.com/article/2022/09/eu-wants-to-empower-courts-victims-in-fight-against-harmful-ai-00057225.
270 Luca Bertuzzi, „LEAK: Commission to propose rebuttable presumption for AI-related damages", Euractiv (September 2022), https://www.euractiv.com/section/digital/news/leak-commission-to-propose-rebuttable-presumption-for-ai-related-damages/.
271 'WTO Electronic Commerce Negotiations Updated Consolidated Negotiating Text – September 2021", WTO INF/ECON/62/Rev.2 (September 2021): 24 (siehe Artikel B.1(2) Interactive computer services (limiting liability) provision 7(b)), abrufbar unter https://www.bilaterals.org/?-other-292-.

8.

WELCHE DIGITALEN REGELN SIND ERFORDERLICH?

Die Fürsprecher von Big Tech bringen häufig das solipsistische Argument vor, da es einen umfangreichen digitalen Handel gebe, müsse es auch Regeln für diesen Handel geben. In der Tat sind eine Menge neuer Regeln für Big Tech erforderlich. Die durch die Pandemie verursachte verstärkte Nutzung von Online-Systemen machte die dringende Notwendigkeit innovativer Regulierungsmaßnahmen in vielen Bereichen deutlich. Aber die von Big Tech vorgeschlagenen Regeln würden ihre Vormachtstellung im wirtschaftlichen, sozialen und politischen Leben in Europa und der ganzen Welt faktisch eher verstärken als einschränken und den Schaden, den diese Dominanz verursacht, noch verschlimmern.

Stattdessen sind Maßnahmen erforderlich, um Menschen- und Grundrechte in der digitalen Wirtschaft zu gewährleisten, die Nutzung von Daten und Digitalisierung zum Wohle der Allgemeinheit zu fördern und die digitale Industrialisierung voranzutreiben.

Alle Länder brauchen Daten als öffentliches Gut. Alle Länder müssen den Wert der Daten für das öffentliche Interesse nutzbar machen, indem sie z. B. den Zugang zu qualitativ hochwertigen öffentlichen Dienstleistungen ausweiten, Gerechtigkeit und Diskriminierungsfreiheit gewährleisten und Daten für die Suche nach Lösungen für drängende soziale Probleme, wie den Klimawandel, nutzen. So sollten öffentliche Einrichtungen das Recht auf entpersonalisierte, privat gesammelte Daten für Zwecke des öffentlichen Interesses haben, beispielsweise Daten von Ride-Share-Apps für die Verkehrsplanung. Daten sollten der Gemeinschaft gehören, die sie erzeugt, und ihr zugutekommen, und nicht nur dem Big-Tech-Unternehmen, das sie erhebt. Erforderlich sind Anstrengungen zum Aufbau einer öffentlichen Dateninfrastruktur für das Gemeinwohl.

„Daten sollten die grundlegende öffentliche Infrastruktur des 21. Jahrhunderts sein, so wie bisher Straßen, Straßenbeleuchtung und sauberes Trinkwasser. Als Partner des Projekts Decode wünschen wir uns von Stadtverwaltungen, dass sie Daten allmählich als eine neue Art von Gemeingut begreifen,“[272] so Tom Symons, Mitautor von „Reclaiming the Smart City: Personal Data, Trust and the New Commons“.

Eine der Schlüsselstrategien zur Nutzung von Daten und Digitalisierung für das Gemeinwohl ist eine digitale Industrialisierung mit Regeln und Verfahren, die innovative Kleinunternehmen fördern, die Schaffung von Arbeitsplätzen unterstützen, die Entstehung von Monopolen verhindern, menschenwürdige Arbeit und Rechte für die Beschäftigten im digitalen Raum gewährleisten und sicherstellen, dass die Gemeinschaften von der Digitalisierung wirtschaftlich profitieren. Wir brauchen eine Politik für digitale Industrialisierung, die der Mehrheit nutzt und den seit Jahrzehnten andauernden Trend umkehrt, dass das Kapital den gesamten Gewinn aus dem Produktivitätswachstum abschöpft.

Dies würde einen Ansatz erfordern, der den von Big Tech verfochtenen Regeln diametral entgegensteht, da er Maßnahmen zur Einschränkung der Macht von Big Tech voraussetzt. Hier eine kurze, nicht erschöpfende Aufstellung der erforderlichen neuen Regeln für den digitalen Handel:

- neue Steuervorschriften, um sicherzustellen, dass Big Tech seinen gerechten Anteil zahlt,
- neue Antidiskriminierungsvorschriften, um gegen grassierende Diskriminierung und daraus entstehende Schäden durch KI anzugehen,
- neue Haftungsvorschriften, um zu verhindern, dass Unternehmen von Schäden profitieren,
- neue Cybersicherheitsregeln, um wiederholte Leaks und Hackerangriffe zu verhindern,
- neue Rechte für Gig-Worker – und die Geltung geltender Arbeitnehmer*innenrechte in der digitalen Wirtschaft,

272 Theo Bass, Emma Sutherland und Tom Symons, „Reclaiming the Smart City: Personal data, trust and the new commons“, *Nesta* (Juli 2018), https://www.nesta.org.uk/report/reclaiming-smart-city-personal-data-trust-and-new-commons/.

- neue kartellrechtliche Regelungen, um vertikal integrierte Riesenmonopole aufzubrechen,
- neue Regeln zur Verbesserung der Wettbewerbspolitik und Beendigung monopolistischen Missbrauchs,
- neue Regeln, um die faire Teilhabe von KMU und Start-ups an der Wirtschaft sicherzustellen,
- neue Regeln für die Datenfreigabe, um die Nutzung von Daten für das Gemeinwohl zu fördern,
- neue Regeln, um die digitale Wirtschaft ökologisch nachhaltiger zu machen,
- Durchsetzung und Stärkung hart erkämpfter Regeln für die Gewährleistung der digitalen Privatsphäre und des Datenschutzes.

Nichts von alledem kann jedoch durch ein „Handelsabkommen" erreicht werden. Dies hängt damit zusammen, dass Handelsabkommen per se die Rechte der Staaten zur Regulierung wirtschaftlichen Verhaltens einschränken, während sie gleichzeitig Handelsrechte gewähren, die von Handelsunternehmen wahrgenommen werden. Ein weiterer Grund ist, dass der Apparat für Handelsverhandlungen stärker auf die Interessen von Unternehmen ausgerichtet ist und weniger auf andere Aspekte von öffentlichem Interesse wie Arbeits- oder Persönlichkeitsrechte.

Zur Erreichung dieser im Interesse der Allgemeinheit liegenden Ziele sind Entscheidungen erforderlich, die über demokratische Kanäle unter Einbeziehung von Gesetzgebern, Regulierungsbehörden, Sachverständigen, der Zivilgesellschaft, Gewerkschaften und Vertreter*innen betroffener Gemeinschaften getroffen werden. Der private Sektor ist nur eine dieser Gemeinschaften. Er war bislang die Entscheidungsinstanz für nahezu alle Fragen, die sich auf die digitale Wirtschaft und die Digitalisierung im Allgemeinen über den Handelsraum auswirken. Sein Einfluss auf Entscheidungen, die das Leben und die Rechte aller betreffen, muss beendet werden. Die Agenda für den digitalen Handel ist ein Vorstoß, die Regulierungsfähigkeit im öffentlichen Interesse generell einzuschränken.

Bürger*innen und gesetzgebende Instanzen müssen sicherstellen, dass die Staaten den politischen Handlungsspielraum für die oben genannten Aspekte behalten, indem sie dafür sorgen, dass Abkommen für den „digitalen Handel" ihn NICHT im Rahmen der Vereinbarungen der WTO oder bilateraler Abkommen einschränken.

It has heretofore been the arbiter of nearly all decisions affecting the digital economy and digitalization more generally through the trade space. Their rein over decisions that affect the lives and rights of all must end. The digital trade agenda is an effort to constrain the ability of regulation in the public interest across the board.

Citizens and legislators must ensure that states maintain policy space for the above by NOT having "digital trade" agreements restricting it in the WTO or in bilateral agreements.

9.

SCHLUSSFOLGERUNG

Die negativen Auswirkungen der aktuellen Gesetzlosigkeit von Big Tech in der EU sind derzeit Gegenstand zahlreicher öffentlicher Debatten. Das Parlament und die Kommission erörtern und verabschieden gerade weitere Rechtsvorschriften, die die regulatorische Landschaft grundlegend verändern werden. Big-Tech-Unternehmen, insbesondere mit Sitz in den USA, wollen diesen demokratischen Beratungsprozess umgehen, indem sie über die „Handelspolitik" versuchen, die Regulierungsfähigkeit auf Dauer einzuengen. Big Tech will sein „Recht" auf Datenkontrolle jetzt und in Zukunft festschreiben, bevor Aufsichtsorgane sich des enormen Werts dieser Daten bewusst werden. Mit fadenscheinigen Begründungen wollen sie Mechanismen zur Geheimhaltung von Geschäftspraktiken – Algorithmen – sichern, die eine immer größere Zahl von Entscheidungen über zahllose Aspekte des menschlichen Lebens bestimmen, indem Anforderungen zur Offenlegung von Quellcode verboten werden.

Wer von der Digitalisierung profitieren wird, hängt wie bei jeder Technologie von der politischen Landschaft ab, in der diese Technologie angewandt wird, und dazu gehören in Handelsabkommen verankerte globale Regeln.

Damit Digitalisierung und Daten sich positiv auf unsere Gesellschaft und unsere gemeinsame Umwelt auswirken, statt ihnen zu schaden, müssen die entsprechenden politischen Maßnahmen im öffentlichen Interesse gestaltet werden. Aus diesem Grund muss die von Big Tech vorangetriebene Abschottung des politischen Raums durch „Handelsregeln" verhindert werden.

Es könnte für EU-Gesetzgeber, Regulierungsbehörden, Medien und die Öffentlichkeit von Vorteil sein, dies zu berücksichtigen, wenn mit dem Handel befasste Amtspersonen behaupten, die Agenda für den digitalen Handel sei in ihrem Interesse. Weitere Untersuchungen der potenziellen Konflikte dieser Bestimmungen und anderer bestehender Handelsregeln mit den neuen EU-Rechtsvorschriften sowie mit geltenden Grund- und Menschenrechten sind dringend angezeigt.

ANHANG - TABELLE ZUM VERGLEICH DER WICHTIGSTEN KLAUSELN FÜR DIGITALEN HANDEL IN DEN FREIHANDELSABKOMMEN ZWISCHEN DER EU UND GROSSBRITANNIEN UND ZWISCHEN DER EU UND NEUSEELAND

	HKA zwischen der EU und dem Vereinigten Königreich[273]	FHA zwischen der EU und Neuseeland[274]
Freier Datenverkehr und Datenlokalisierung	*ARTIKEL 201* **Grenzüberschreitender Datenverkehr** 1. Die Vertragsparteien verpflichten sich, den grenzüberschreitenden Datenverkehr zu gewährleisten, um den Handel in der digitalen Wirtschaft zu erleichtern. Zu diesem Zweck darf der grenzüberschreitende Datenverkehr zwischen den Vertragsparteien nicht durch eine Vertragspartei eingeschränkt werden, indem diese (a) die Nutzung von Rechenanlagen oder Netzelementen im Gebiet der Vertragspartei für die Verarbeitung vorschreibt, auch durch die Vorgabe der Nutzung von Rechenanlagen oder Netzelementen, die im Gebiet einer Vertragspartei zertifiziert oder zugelassen sind; (b) die Lokalisierung von Daten im Gebiet der Vertragspartei zur Speicherung oder Verarbeitung verlangt; (c) die Speicherung oder Verarbeitung im Gebiet der anderen Vertragspartei verbietet oder (d) die grenzüberschreitende Übermittlung von Daten von der Nutzung von Rechenanlagen oder Netzelementen im Gebiet der Vertragsparteien oder von Lokalisierungsanforderungen im Gebiet der Vertragsparteien abhängig macht. 2. Die Vertragsparteien überprüfen die Durchführung dieser Bestimmung und bewerten ihr Funktionieren innerhalb von drei Jahren nach dem Inkrafttreten dieses Abkommens. Eine Vertragspartei kann der anderen Vertragspartei jederzeit vorschlagen, die Liste der in Absatz 1 aufgeführten Beschränkungen zu überprüfen. Eine solche Anfrage ist wohlwollend zu prüfen.	*ARTIKEL 12.4* **Grenzüberschreitender Datenverkehr** 1. Die Vertragsparteien sind der Sicherstellung des grenzüberschreitenden Datenverkehrs verpflichtet, um den Handel in der digitalen Wirtschaft zu erleichtern und sie erkennen an, dass jede Vertragspartei in dieser Hinsicht ihre eigenen regulatorischen Anforderungen haben kann. 2. Zu diesem Zweck darf eine Vertragspartei den grenzüberschreitenden Datenverkehr, der zwischen den Vertragsparteien im Zusammenhang mit einer in den Anwendungsbereich dieses Kapitels fallenden Tätigkeit erfolgt, nicht einschränken, indem sie (a) die Nutzung von Rechenanlagen oder Netzelementen für die Datenverarbeitung in ihrem Gebiet, einschließlich der Nutzung von im Gebiet der Vertragspartei zertifizierten oder genehmigten Rechenanlagen oder Netzelementen verlangt, (b) die Verortung von Daten in ihrem Gebiet verlangt, (c) die Speicherung oder Verarbeitung von Daten im Gebiet der anderen Vertragspartei verbietet oder (d) die grenzüberschreitende Datenübertragung von der Nutzung von Rechenanlagen oder Netzelementen in ihrem Gebiet oder von Verortungsanforderungen in ihrem Gebiet abhängig macht. 3. Zur Klarstellung sei angemerkt, dass die Vertragsparteien sich darüber im Klaren sind, dass dieser Artikel die Vertragsparteien nicht daran hindert, Maßnahmen nach Artikel 25.1 (Allgemeine Ausnahmen) einzuführen oder aufrechtzuerhalten, um die dort genannten Gemeinwohlziele zu erreichen, welche für die Zwecke dieses Artikels, soweit relevant, auf eine Weise auszulegen sind, die den evolutionären Charakter der digitalen Technologien berücksichtigt. Der vorstehende Satz berührt die Anwendung anderer, in diesem Abkommen vorgesehener Ausnahmen von diesem Artikel nicht. 4. Sofern die Vertragsparteien nichts anderes vereinbaren, überprüfen die Vertragsparteien die Umsetzung dieses Artikels fortlaufend und bewerten dessen Funktionieren innerhalb von drei Jahren nach Inkrafttreten dieses Abkommens. Zudem kann eine Vertragspartei der anderen Vertragspartei vorschlagen, diesen Artikel zu überprüfen. Ein solches Ersuchen wird wohlwollend geprüft. 5. Im Kontext der Überprüfung nach Absatz 4 und nach der Veröffentlichung des Berichts Wai 2522 des Gerichts Waitangi vom 19. November 2021 (a) bekräftigt Neuseeland, dass es auch im Rahmen dieses Abkommens die Interessen der Māori weiter unterstützen und fördern kann und (b) bestätigt Neuseeland seine Absicht zur Beteiligung der Māori, um sicherzustellen, dass die in Absatz 4 genannte Überprüfung der Tatsache Rechnung trägt, dass Neuseeland die Māori weiterhin unterstützen muss, damit sie ihre Rechte und Interessen wahrnehmen können, sowie zur Erfüllung seiner Verantwortlichkeiten aus dem Vertrag von Waitangi/te Tiriti o Waitangi und zur Einhaltung seiner Grundsätze.

273 Abkommen über Handel und Zusammenarbeit zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, Dokument 22021A0430(01), 01/12/2021 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:22021A0430(01)&from=EN

274 EU-Neuseeland: Wortlaut des Abkommens https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en

	HKA zwischen der EU und dem Vereinigten Königreich[273]	FHA zwischen der EU und Neuseeland[274]
Schutz personenbezogener Daten und der Privatsphäre	*ARTIKEL 202* **Schutz personenbezogener Daten und der Privatsphäre** 1. Jede Vertragspartei erkennt an, dass Einzelpersonen ein Recht auf den Schutz personenbezogener Daten und der Privatsphäre haben und dass hohe Standards in dieser Hinsicht zum Vertrauen in die digitale Wirtschaft und zur Entwicklung des Handels beitragen. 2. Dieses Abkommen hindert eine Vertragspartei nicht daran, Maßnahmen zum Schutz personenbezogener Daten und der Privatsphäre, auch im Hinblick auf den grenzüberschreitenden Datenverkehr, zu erlassen oder beizubehalten, sofern das Recht der Vertragspartei Instrumente vorsieht, die Übermittlungen unter allgemein geltenden Bedingungen (34) zum Schutz der übermittelten Daten ermöglichen. 3. Jede Vertragspartei unterrichtet die andere Vertragspartei über jede in Absatz 2 genannte Maßnahme, die sie ergreift oder beibehält. (34) Zur Klarstellung sei angemerkt, dass sich der Ausdruck „allgemein geltende Bedingungen" auf objektiv formulierte Bedingungen bezieht, die horizontal für eine unbestimmte Anzahl von Wirtschaftsteilnehmern gelten und somit eine Reihe von Situationen und Fällen abdecken.	*ARTIKEL 12.5* **Schutz personenbezogener Daten und der Privatsphäre** 1. Jede Vertragspartei erkennt an, dass der Schutz personenbezogener Daten und der Privatsphäre zu den Grundrechten zählt und dass hohe Standards in diesem Bereich einen Beitrag zur Stärkung des Vertrauens der Verbraucher in den digitalen Handel leisten. 2. Jede Vertragspartei kann unter anderem durch die Einführung und Anwendung von Regeln für die grenzüberschreitende Übertragung personenbezogener Daten Maßnahmen einführen oder aufrechterhalten, die sie für geeignet hält, um den Schutz personenbezogener Daten und der Privatsphäre zu gewährleisten. Der durch die jeweiligen Maßnahmen der Vertragsparteien gewährte Schutz personenbezogener Daten und der Privatsphäre wird durch dieses Abkommen nicht berührt. 3. Jede Vertragspartei unterrichtet die andere Vertragspartei über in Absatz 2 genannte Maßnahmen, die sie einführt oder aufrechterhält. 4. Jede Vertragspartei veröffentlicht Informationen über den Schutz personenbezogener Daten und der Privatsphäre, den sie Nutzern des digitalen Handels bereitstellen, unter anderem (a) Informationen, wie Personen einen Rechtsbehelf aufgrund eines Verstoßes gegen den Schutz personenbezogener Daten und der Privatsphäre anstrengen können, und (b) Leitlinien und sonstige Informationen bezüglich der Einhaltung geltender Rechtsvorschriften zum Schutz personenbezogener Daten und der Privatsphäre durch Unternehmen.

	HKA zwischen der EU und dem Vereinigten Königreich[273]	FHA zwischen der EU und Neuseeland[274]
Access to source code	*ARTIKEL 207* **Übertragung von oder Zugriff auf Quellcode** 1. Eine Vertragspartei verlangt nicht die Übertragung von oder den Zugriff auf den Quellcode von Software, die einer natürlichen oder juristischen Person der anderen Vertragspartei gehört. 2. Zur Klarstellung: (a) Die in Artikel 199 genannten allgemeinen Ausnahmen, Ausnahmen zur Wahrung der Sicherheit und aufsichtsrechtlichen Ausnahmeregelungen gelten für Maßnahmen einer Vertragspartei, die im Rahmen eines Zertifizierungsverfahrens angenommen oder beibehalten werden, und (b) Absatz 1 des vorliegenden Artikels gilt nicht für die freiwillige Weitergabe von Quellcode oder die Gewährung des Zugangs zu diesem auf kommerzieller Basis durch eine natürliche oder juristische Person der anderen Vertragspartei, beispielsweise im Rahmen eines öffentlichen Auftragsvergabevorgangs oder eines frei ausgehandelten Vertrags. 3. Dieser Artikel berührt nicht (a) eine Auflage eines Gerichts oder Verwaltungsgerichts oder eine Auflage einer Wettbewerbsbehörde nach dem Wettbewerbsrecht einer Vertragspartei, um eine Beschränkung oder Verfälschung des Wettbewerbs zu verhindern oder zu beheben; (b) eine Auflage einer Regulierungsbehörde gemäß den Gesetzen oder Vorschriften einer Vertragspartei im Hinblick auf den Schutz der öffentlichen Sicherheit in Bezug auf die Nutzer online, vorbehaltlich von Schutzmaßnahmen gegen eine unbefugte Weitergabe; (c) den Schutz und die Durchsetzung von Rechten des geistigen Eigentums und (d) das Recht einer Vertragspartei, Maßnahmen gemäß Artikel III GPA – wie übernommen durch Artikel 277 dieses Abkommens – zu ergreifen.	*ARTIKEL 12.11* **Weitergabe von oder Zugang zu Quellcodes** 1. Die Vertragsparteien erkennen die zunehmende gesellschaftliche und wirtschaftliche Bedeutung des Einsatzes digitaler Technologien sowie die Bedeutung der sicheren und verantwortungsvollen Entwicklung und Nutzung solcher Technologien an, auch in Bezug auf Quellcodes von Software, um das Vertrauen der Öffentlichkeit zu stärken. 2. Eine Vertragspartei darf die Weitergabe des Quellcodes von Software, die Eigentum einer natürlichen oder juristischen Person der anderen Vertragspartei ist, oder den Zugang dazu nicht als Voraussetzung für die Einfuhr, die Ausfuhr, den Vertrieb, den Verkauf oder die Verwendung solcher Software oder von Produkten, die eine solche Software enthalten, in oder aus ihrem Gebiet vorschreiben.1 3. Zur Klarstellung sei angemerkt, dass Absatz 2 (a) nicht für die freiwillige, auf wirtschaftlicher Grundlage erfolgende Weitergabe von oder Gewährung des Zugangs zu Quellcodes von Software durch eine Person der anderen Vertragspartei gilt, beispielsweise im Rahmen eines öffentlichen Beschaffungsvorhabens oder eines frei ausgehandelten Vertrags, und (b) das Recht der Regulierungs-, Verwaltungs-, Strafverfolgungs- oder Justizbehörden einer Vertragspartei unberührt lässt, die Änderung des Quellcodes von Software zu verlangen, damit er ihren Gesetzen und sonstigen Vorschriften entspricht, die nicht im Widerspruch zu diesem Abkommen stehen. 4. Dieser Artikel berührt nicht (a) das Recht der Regulierungs-, Strafverfolgungs- sowie Justizbehörden oder Konformitätsbewertungsstellen einer Vertragspartei vor oder nach der Einfuhr, der Ausfuhr, dem Vertrieb, dem Verkauf oder der Verwendung von Software, vorbehaltlich des Schutzes vor unbefugter Weitergabe, für Ermittlungs-, Kontroll-, Prüf- oder Strafverfolgungsmaßnahmen oder zu Zwecken von Gesichtsverfahren Zugang zu Quellcodes von Software zu erhalten, um die Konformität mit ihren Gesetzen und sonstigen Vorschriften, auch solcher in Bezug auf Gleichbehandlung und die Verhinderung von Voreingenommenheit, festzustellen, (b) Anforderungen einer Wettbewerbsbehörde oder einer anderen maßgeblichen Stelle einer Vertragspartei, um eine Verletzung des Wettbewerbsrechts zu beheben, (c) den Schutz und die Durchsetzung der Rechte des geistigen Eigentums oder (d) das Recht einer Vertragspartei, Maßnahmen nach Artikel 14.1 (Übernahme bestimmter Bestimmungen des GPA) Absatz 2 Buchstabe a, gemäß dem Artikel III des GPA sinngemäß Bestandteil dieses Abkommens ist, zu ergreifen. [1 Dieser Artikel hindert eine Vertragspartei nicht daran, vorbehaltlich des Schutzes vor unbefugter Weitergabe zu verlangen, dass Zugang zu Software, die für kritische Infrastrukturen eingesetzt wird, gewährt wird, soweit dies für die Gewährleistung des wirksamen Funktionierens kritischer Infrastrukturen erforderlich ist.]

	HKA zwischen der EU und dem Vereinigten Königreich[273]	FHA zwischen der EU und Neuseeland[274]
Zölle auf elektronische Übertragungen	*ARTIKEL 203* **Zölle auf elektronische Übertragungen** 1. Elektronische Übertragungen gelten als Erbringung von Dienstleistungen im Sinne von Titel II dieses Teilbereichs. 2. Die Vertragsparteien erheben keinen Zoll auf elektronische Übertragungen.	*ARTIKEL 12.6* **Zölle auf elektronische Übertragungen** 1. Eine Vertragspartei darf keine Zölle auf elektronische Übertragungen zwischen einer Person einer Vertragspartei und einer Person der anderen Vertragspartei erheben. 2. Zur Klarstellung sei angemerkt, dass Absatz 1 eine Vertragspartei nicht daran hindert, inländische Steuern, Gebühren oder sonstige Abgaben auf elektronische Übertragungen zu erheben, sofern diese Steuern, Gebühren oder Abgaben in einer Weise erhoben werden, die mit diesem Abkommen im Einklang steht.
Keine vorherige Genehmigung	*ARTIKEL 204* **Keine vorherige Genehmigung** 1. Eine Vertragspartei verlangt weder eine vorherige Genehmigung für die Erbringung einer Dienstleistung auf elektronischem Wege allein aufgrund der Tatsache, dass eine Dienstleistung online erbracht wird, noch nimmt sie andere Vorschriften mit gleicher Wirkung an oder behält sie bei. Eine Dienstleistung wird online erbracht, wenn sie auf elektronischem Wege und ohne gleichzeitige Anwesenheit der Parteien erbracht wird. 2. Absatz 1 gilt nicht für Fernmeldedienste, Rundfunkdienste, Glücksspieldienste, Rechtsvertretungsdienste oder für die Dienstleistungen von Notaren oder gleichwertigen Berufen, soweit sie in einem unmittelbaren und spezifischen Zusammenhang mit der Ausübung öffentlicher Gewalt stehen.	*ARTIKEL 12.7* **Verzicht auf eine vorherige Genehmigung** 1. Jede Vertragspartei ist bestrebt, auf vorherige Genehmigungen oder die Erfüllung sonstiger Anforderungen mit gleichen Auswirkungen auf die Erbringung von Dienstleistungen auf elektronischem Wege zu verzichten. 2. Genehmigungsregelungen, die nicht speziell und ausschließlich auf elektronischem Wege erbrachte Dienstleistungen betreffen, sowie Regelungen im Bereich der Telekommunikation bleiben von Absatz 1 unberührt.

The Left in the European Parliament
Rue Wiertz 43 B-1047 Brussels
www.left.eu