Schmalenbach IMPULSE 3(1):1-10
https://doi.org/10.54585/BSQI8377

Die „Balkanisierung“ der Digitalwirtschaft

Luka Mucic*

1 Grenzüberschreitender Datenfluss als Chance des Internets

Im Jahr 1996 veröffentlichte der Internetpionier John Perry Barlow die Unabhängigkeitserklärung des Cyberspace. Das Internet, so Parlow, sei ein Akt der Natur und wachse durch die kollektiven Handlungen der Nutzer. Daher gebe es dort keine staatliche Souveränität. Aus der Sicht eines Internetaktivisten formulierte er damals: „Ich erkläre den globalen sozialen Raum, den wir aufbauen, für natürlich unabhängig von den Tyranneien, die ihr uns aufzwingen wollt.“ (Barlow 1996) Regierungen hätten, so das Manifest, weder das moralische Recht über das Internet zu regieren noch verfügten sie über Durchsetzungsmethoden (Barlow 1996).

Heute, mehr als 25 Jahre später, ist offensichtlich, dass Barlows Vision nicht Wirklichkeit geworden ist. Entgegen der Vorhersage haben nationale Grenzen aufgrund der digitalen Vernetzung ihre Bedeutung nicht verloren. Ein möglichst freier Zugang zum Internet und ein ungehinderter, weltweiter Datenaustausch sind jedoch heute noch wertvoller als damals.

1.1 Digitalisierung als Wettbewerbsfaktor

Für Unternehmen sind die Digitalisierung und der Zugang zum globalen Datenfluss längst zu einem entscheidenden Wettbewerbsfaktor geworden. Eine Umfrage der Unternehmensberatung PwC unter mehr als 650 amerikanischen Führungskräften aus den Bereichen Technologie und Wirtschaft ergab, dass 60 Prozent der Manager Initiativen zur digitalen Transformation auch im Hinblick auf die eigene Geschäftsstrategie für sehr wichtig halten (PwC 2022). Es ist daher nicht verwunderlich, dass Investitionen in die Digitalisierung weltweit weiter anwachsen: Bis 2022 sol-

* Luka Mucic | Mitglied des Vorstands | SAP SE

len 65 Prozent des globalen Bruttoinlandsprodukts „digitalisiert“ sein (Kindle 2020).

1.2 Die Entwicklung der Digitalwirtschaft

Der globale Datenstrom ist in unvorstellbarem Tempo gewachsen: Im Jahr 1990 öffnete die National Science Foundation der USA das Internet für kommerzielle Zwecke. Drei Jahre später – das erste „Touchphone“ von IBM war gerade auf den Markt gekommen – fand bereits ein Prozent des weltweiten Informationsflusses im Internet statt. Schon im Jahr 2007 stieg dieser Anteil auf 97 Prozent. Auch die Anzahl vernetzter Geräte und Maschinen schnellt seit Jahren in die Höhe: 2021 waren bereits mehr als 11 Milliarden smarte Geräte im Einsatz. Bis 2025 könnte die Marke von 19 Milliarden vernetzter Geräte überschritten werden (Kroker 2019). Parallel dazu steigt die Menge an Daten an. Schätzungen zufolge betrug die weltweite Datenmenge im Jahr 2020 ungefähr 64,2 Zettabyte. Hinter dieser unscheinbaren Zahl verbirgt sich eine kaum vorstellbare Datenmenge: Ein Zettabyte ist 1.125.899.906.842.620 Gigabyte. Prognosen gehen davon aus, dass die globale Datasphäre bis zum Jahr 2025 auf 181 Zettabyte anwachsen wird (Taylor 2022).

1.3 Digitalisierte Geschäftsprozesse und grenzüberschreitende Datenströme sind ein Muss

Der grenzüberschreitende internationale Datenfluss prägt die Wirtschaft und die Menschen des 21. Jahrhunderts. Der weltweite Austausch von Informationen dient als Motor für Innovationen, neue Geschäftsmodelle und Wachstum. Durch das Zusammenspiel von globaler Vernetzung und Digitalisierung können Unternehmen Prozesse effizienter gestalten, Innovationszyklen verkürzen und Kernkompetenzen neu verteilen.

Die revolutionären neuen Möglichkeiten, die das Internet hervorgebracht hat, ergeben sich vor allem daraus, dass es offen ist und ohne Rücksicht auf nationale Hoheitsgebiete entwickelt wurde. Die Daten bewegen sich schnell und unvorhersehbar – in der Regel, ohne dass der Benutzer dies weiß oder zugestimmt hat (Daskal 2015: 330). Die ungeheure Menge an Daten und die Fähigkeit, diese auszuwerten, bringt neue Erkenntnismöglichkeiten hervor. Innovationen wie Cloud-Computing ermöglichen einen geräteunabhängigen On-Demand-Zugriff auf Speicher und damit für die Nutzer eine weltweite Verfügbarkeit von Wissen und Information (Fraser 2016).

Welche neuen Möglichkeiten sich durch die globale Vernetzung ergeben, lässt sich am Beispiel Catena-X zeigen. Catena-X ist ein offenes, länderübergreifendes und datengetriebenes Ökosystem für Stakeholder aus der Automobilindustrie. Nicht nur Automobilhersteller und klassische Automobilzulieferer sind Teil des Netzwerks, sondern auch Anbieter aus der gesamten industriellen Wertschöpfungskette, wie SAP und BASF – bis hin zu Recyclingfirmen. (Bitkom Events 2021: Min. 02:20-07:40). Ziel ist der län-

derübergreifende Austausch und die gemeinsame Arbeit an neuen und innovativen Lösungen, z.B. im Bereich der Einsparung von Treibhausgasemissionen. Innerhalb des Netzwerks können die Teilnehmer Informationen, Anwendungen und Infrastrukturen anbieten oder gemeinsam an branchenspezifischen Lösungen arbeiten. So können Zulieferer von anderen Lieferanten Produktionsfähigkeiten (Manufacturing-as-a-Service) einkaufen, um auf diesem Weg zu einer optimierten, flexiblen und vor allem resilienten Lieferkette zu kommen (Fraunhofer-Institut 2022: Min. 01:00-05:00). Das Netzwerk Catena-X zeigt, welche erheblichen Potentiale globale Netzwerke erschließen können.

2 Einschränkung des grenzüberschreitenden Informationsflusses

Der globale Informationsfluss ist jedoch keine Selbstverständlichkeit. In den vergangenen Jahren ist die Zahl der Länder, die den Datenfluss einschränken oder behindern wollen, stetig gewachsen. Viele Entwicklungs- und Industrieländer haben Datenlokalisierungsgesetze erlassen, durch die der Datenfluss eingedämmt wird – darunter Kanada, Vietnam, Iran, China, Brasilien, Indien, Australien, Korea, Nigeria und Russland (Bowman 2015). Datenlokalisierungsgesetze schreiben im Allgemeinen vor, dass bestimmte Daten von Bürgern auf den Servern des jeweiligen Landes gespeichert und verarbeitet werden müssen. Im Einzelnen sind die Vorschriften zur Datenlokalisierung – abhängig von der damit verfolgten Absicht – von Land zu Land unterschiedlich (Yayboke 2021).

2.1 Motive für digitale Schranken

Die Motive für die nationale Regulierung des grenzüberschreitenden Datentransfers sind unterschiedlich. In manchen Ländern steht der Schutz der Rechte von Bürgern im Vordergrund. Dort zielen die Gesetze vor allem darauf ab, die Grundrechte des Einzelnen im Internet angesichts ausländischer Überwachung und weit verbreiteter Verletzungen der Privatsphäre zu schützen (Fraser 2016). Andere Länder sehen in dem freien Informationsfluss vor allem eine Bedrohung für die öffentliche Ordnung oder die nationale Sicherheit. Daher versuchen sie, Kontrolle über die Datenströme zu gewinnen, um das durchzusetzen, was sie als „digitale Souveränität“ verstehen. Ein weiteres Ziel kann der Schutz nationaler oder wirtschaftlicher Souveränität sein. Viele Regierungen sorgen sich auch wegen neuer Konkurrenz durch ausländische Dienstleister, insbesondere in Bereichen, die traditionell von ausländischer Konkurrenz isoliert waren (Ahmed und Chander 2015: 1).

Ein weiteres Motiv: Die Angst vor Cyberattacken. Für Hackerangriffe gibt es weltweit viele Beispiele. Im Jahr 2021 wurde das iranische Transport- und Verkehrsministerium gehackt, was zu einem Ausfall der Webseite

führte. Einen Tag zuvor hatten Hacker das iranische Eisenbahnsystem lahmgelegt, indem sie unter anderem gefälschte Nachrichten über angebliche Zugverspätungen oder -ausfälle auf Anzeigetafeln an Bahnhöfen im ganzen Land veröffentlichten (The New Arab 2021). Seit dem russischen Angriffskrieg auf die Ukraine geht auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) von einer höheren Gefahrenlage für Deutschland aus (BSI 2022).

2.2 Drei Länderbeispiele

Anhand dreier Länder soll beispielhaft erklärt werden, mit welchen Regelungen und Maßnahmen Regierungen den Datentransfer und Informationsfluss einschränken und welche Konsequenzen dies haben kann.

2.2.1 China – „Digitale Souveränität“

Der Begriff „digitale Souveränität“ hat seinen Ursprung in China. Dahinter verbirgt sich der Wunsch, nationale Selbstbestimmung auch in Zeiten globaler digitaler Vernetzung sicherstellen zu können (Pohle und Lang 2019). Ausdruck dieses Bestrebens ist das „Cybersecurity-Gesetz“, das die Volksrepublik China im Jahr 2017 erlassen hat. Ziel des Gesetzes ist es, den Datenschutz, die Datenlokalisierung und die Cybersicherheit im Interesse der nationalen Sicherheit zu verbessern. Das Gesetz richtet sich insbesondere an Netzwerkbetreiber und damit auch an in China tätige internationale Unternehmen. Dies bedeutet: Unternehmen müssen ihre relevanten Daten in China speichern und dürfen diese nur unter besonderen Voraussetzungen exportieren. Zudem ist vorgeschrieben, dass ausländische Unternehmen mit Behörden der öffentlichen Sicherheit zusammenarbeiten und auf Anfrage Informationen herausgeben müssen. Das Gesetz ist außerordentlich weit gefasst und z.B. im Vergleich zur EU- Datenschutzgrundverordnung viel weniger konkret. So bleibt unklar, wie Unternehmen Verbraucherdaten nutzen dürfen. Ein weiteres Gesetz verpflichtet Anbieter von Clouddienstleistungen, eine Telekommunikationslizenz zu erwerben, die ausschließlich an Joint Ventures mit Sitz in China und mit chinesischer Beteiligung erteilt wird.

Das „Cybersecurity-Gesetz“ hat bei ausländischen Technologie-Unternehmen, die in China tätig sind, die Sorge ausgelöst, dass China dem staatlichen Zugriff auf Daten mehr Bedeutung beimisst als dem Schutz der Privatsphäre von Einzelpersonen und Unternehmen (Maranto 2020). Rechtsexperten warnen davor, dass Unternehmen aufgefordert werden können, den chinesischen Behörden Quellcodes oder andere wichtige Informationen bereitzustellen (Wagner 2017). Sie sehen die Gefahr, dass geistiges Eigentum und private Informationen staatlichem Missbrauch ausgesetzt sind (Maranto 2020). Das US-amerikanische Federal Bureau of Investigation (FBI) warnt, dass das Gesetz Unternehmen, die lediglich Daten über Server in China übermitteln, dazu zwingen könnte, sich Datenüberwachung und Spionage zu unterwerfen (Wagner 2017).

Als Reaktion auf diese Gesetzgebung haben viele internationale Firmen den Fokus auf Lokalisierung gelegt und arbeiten in China mit lokalen Anbietern wie Tencent oder Alibaba zusammen. Die Autobauer BMW, Daimler

und Volkswagen haben eigene Datenzentren in China errichtet, um die zunehmend strengeren chinesischen Datenschutzbestimmungen erfüllen zu können (Gusbeth 2022).

2.2.2 Russland – Abschottungspolitik und hohe Geldbußen

Russland ist dem chinesischen Beispiel gefolgt und zielt ebenfalls darauf ab, seine eigene digitale Souveränität zu stärken (Pohle und Lang 2019). Im April 2019 verabschiedete die Duma ein Gesetz zum Betrieb eines russischen Internet-Segments „RuNet“, das von den inländischen Medien den Titel „Sovereign RuNet“ erhalten hat (Stadnik 2019). Nach Einschätzung von Experten setzt die Regierung darauf, sich im Falle eines feindlichen Übergriffs vom globalen Internet abkoppeln zu können (Epifanova 2020; Pohle und Lang 2019).

Bereits im Jahr 2015 hatte die Duma ein Datenlokalisierungsgesetz erlassen. Dies schreibt vor, dass personenbezogene Daten russischer Staatsbürger nur auf Servern gespeichert werden dürfen, die sich innerhalb der Russischen Föderation befinden (Heidemann 2015).

Für Unternehmen ist die Speicherung der Daten auf Servern in Russland nicht nur technisch kompliziert und betriebswirtschaftlich kostspielig (Blinov 2020). Bei Verstößen drohen zudem hohe Geldbußen – bei erstmaligen Zuwiderhandlungen zwischen 16.000 und 96.000 US-Dollar – sowie die Sperrung von Webseiten (Shaftan 2019). Europäischen Unternehmen bereitet auch Kopfschmerzen, dass die Speicherung eines Teils ihrer Benutzerdatenbank außerhalb der EU gegen europäische Datenschutzvorschriften (Artikel 45 DSGVO) verstoßen kann (Blinov 2020).

Die russischen Gesetze haben schon vor dem Krieg in der Ukraine die Beziehung von internationalen Unternehmen zu Kunden in Russland erschwert. Bei Unternehmen, die personenbezogene Daten russischer Bürger verarbeiten, haben die Anforderungen bereits zu erheblichen Kosten geführt (Karpukhin und Sivkova 2017). Aufgrund der spezifischen Lokalisationserfordernisse ist es darüber hinaus unzulässig, Daten-Back-ups in international verteilten Datencentren zu machen. Ausländische Unternehmen stehen daher oft vor dem Dilemma, entweder gegen geltendes Recht zu verstoßen oder erhöhte Betriebsunterbrechungsrisiken in Kauf nehmen zu müssen. Als Konsequenz des Krieges in der Ukraine hat SAP im April 2022 angekündigt, sich aus dem Russlandgeschäft zurückzuziehen und ihre Cloud-Datencenterpräsenz in Russland im vergangenen Jahr beendet.

2.2.3 Saudi-Arabien – Abwehr von Cyberattacken

Die Nationale Cybersicherheitsbehörde (NCA) des Königreichs Saudi-Arabien hat im Jahr 2020 Regelungen für Cloud-Cybersicherheitskontrollen erlassen. Ziel des Gesetzes ist die Abwehr von Cyberangriffen. In der Tat war das Königreich in der Vergangenheit häufig Opfer von Cyberattacken. Im Jahr 2020 verzeichnete Saudi-Arabien Kreisen zufolge über 22,5 Millionen Cyberattacken (Olech 2021).

Nach dem „Cybersicherheitsgesetz“ müssen Unternehmen für die grenzüberschreitende Übermittlung von Daten eine Genehmigung der zuständigen Behörde einholen. Zudem sehen die NCA-Regularien vor, dass aus-

ländische Firmen die Cloudinfrastruktur, in der sie Daten von Behörden und Unternehmen von nationalem Interesse speichern, von den Daten anderer Kunden trennen.

Auch dieses Gesetz stellt eine Herausforderung für Unternehmen dar: Ausländische Clouddienstleister können ihre Dienste nur unter erschwerten Bedingungen anbieten, da sie bei der Bekämpfung von Cyberangriffen mangels Zugriffsrechte von außerhalb des Königreichs auf die lokale Cloudinfrastruktur gegebenenfalls nicht auf ein globales Netzwerk zurückgreifen dürfen.

3 Wirtschaftliche Auswirkungen der „digitalen“ Schranken

Insgesamt ist zu befürchten, dass die Verschärfung der nationalen Grenzen zu einer „Balkanisierung des Internets“, also einer Loslösung einzelner Länder führen wird (Ahmed und Chander 2015). Dadurch könnte das globale Netzwerk in „verschiedene unterschiedliche, idiosynkratische Internets“ (Hill 2012: 10) zerfallen, was zu Verzögerungen, Ineffizienzen und höheren Kosten führt (Fraser 2016).

Sollte sich der Trend zu digitalen Grenzzäunen weiter durchsetzen, könnte dies eine Umgestaltung der gesamten technischen Architektur des Internets und dessen Verwaltungsstrukturen nach sich ziehen (Hill 2014: 4). Globale Dienstleister müssten mit höheren Kosten für die jeweilige Bereitstellung von physischer Infrastruktur rechnen. Aber auch auf der „Produktseite“ gäbe es Konsequenzen, denn aufgrund des hohen administrativen Aufwands und der Kosten wären viele Leistungen für die Unternehmen nicht mehr durchführbar bzw. würden sich nicht mehr lohnen (Fraser 2016).

Viele global agierende Unternehmen finden sich aufgrund der unterschiedlichen lokalen Gesetzesanforderungen zudem in einer „komplexen Reihe verschiedener Rechtssysteme wieder, die widersprüchliche Mandate auferlegen und widersprüchliche Rechte verleihen“ (Meinrath 2013; Fraser 2016). Durch die Verarbeitung und Umsetzung der rechtlichen Erfordernisse steigt nicht nur der unternehmensinterne Verwaltungsaufwand, sondern auch die Kosten. Aufgrund der manchmal unvorhersehbaren Rechtslage kann das Risiko eines Markteintritts für Unternehmen zu hoch sein.

Die regionale Abschottung erweist sich insbesondere für Entwicklungsländer als nachteilig. So zögern internationale Unternehmen, in Ländern zu investieren, denen es an der nötigen Stabilität mangelt (Fraser 2016). Der Verzicht auf die Einrichtung lokaler digitaler Infrastrukturen kann wiederum zu Lücken bei den Internetdiensten in diesen Ländern führen (Lehrer 2014).

Bei alledem ist wichtig zu bedenken, dass das eigentliche Ziel der Datenlokalisation – der „Schutz der Daten“ – durch Abschottung oft gar nicht erreicht wird. Die Absicherung von Datenschutz und Datensicherheit durch technologische Maßnahmen basiert auf technischem Fortschritt und „Best-Practices“. Länder, die sich abschotten, haben erfahrungsgemäß

einen schlechteren Zugang zu technischen Lösungen als global agierende Unternehmen. Außerdem ist zu befürchten, dass lokale Speicheranbieter aufgrund geringerer finanzieller Ressourcen und Fachkenntnisse sowie eines reduzierten Wettbewerbsdrucks nicht die gleiche Strenge an den Tag legen wie international agierende Unternehmen (Arlen und Connor 2015; Fraser 2016). Ähnliches gilt für die Internet-Sicherheit: National abgekapselte Dateninfrastrukturen machen es Dritten zunächst schwerer, Spionage zu betreiben. Andererseits wiegt der Verlust globaler Kompetenzen auch in der Cyberattackenbekämpfung schwer.

4 Fazit

Die Vorteile einer vernetzten, globalen Wirtschaft liegen auf der Hand: Kollaboration über Grenzen hinweg kann Synergien fördern – und in manchen Fällen sogar zur Lösung globaler Herausforderungen beitragen. Dazu braucht es eine gesunde Balance, denn die Länderbeispiele zeigen eindrücklich, wie politisch gefärbte Restriktionen globalisierte Wertschöpfungsketten beeinflussen können. Es wird deutlich, dass nationale, unkoordinierte Bestrebungen nicht die Lösung sind. Vielmehr führen protektionistische Bestrebungen zu Wettbewerbsverzerrungen und sind für Menschen und Unternehmen oft mit wirtschaftlichen und gesellschaftlichen Nachteilen verbunden. Für die von den jeweiligen Ländern angestrebten Ziele wie Wirtschaftswachstum und Datensouveränität erweist sich die Abschottung als kontraproduktiv. Da aber ein Ende der nationalen Bestrebungen nicht absehbar ist, wäre ein möglicher Lösungsansatz, dass man Regulierungen stärker hinsichtlich des jeweiligen Datentyps ausdifferenziert. Beispielsweise ist nachvollziehbar, dass es länderübergreifend für besonders klassifizierte Daten (sensible, geheimschutz-relevante Daten) Restriktionen gibt, die Bestand haben müssen. Soweit solche – vornehmlich hoheitliche – Datentypen nicht betroffen sind, sollten Datenlokalisierungsbestrebungen im Hinblick auf die mit ihnen verbundenen erheblichen Nachteile kritisch hinterfragt werden.

Dass das politische Streben nach der Aufrechterhaltung eines freien Internets weitergeht, zeigte sich auch auf einem Treffen der G7-Handelsminister am 22. Oktober 2021 in London. In einer Erklärung zum digitalen Handel äußerten die Handelsminister ihre Besorgnis über digitalen Protektionismus und Autoritarismus und forderten den freien Datenfluss: Digital- und Telekommunikationsmärkte sollen wettbewerbsfähig, transparent, fair und für internationalen Handel und Investitionen zugänglich sein (GOV.UK 2021). Es ist ein Appell, der hoffentlich gehört wird.

Literaturverzeichnis

Ahmed, U., A. Chander. 2015. Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows. E15Initiative. [online] https://e15initiative.org/publications/information-goes-global-protecting-privacy-security-and-the-new-economy-in-a-world-of-cross-border-data-flows/. [10.11.2022].

Arlen, J., B. O'Connor. 2015. Xenophobia is Hard on Data: Forced Localization, Data Storage, and Business Realities. [online] https://sector.ca/sessions/xenophobia-is-hard-on-data-forced-localization-data-storage-and-business-realities/. [10.11.2022].

Barlow, J. P. 1996. A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. [online] https://www.eff.org/de/cyberspace-independence. [10.11.2022].

Bitcom Events. 2021. Catena-X: Eine Dateninfrastruktur für die automobile Wertschöpfungskette. [video] https://www.youtube.com/watch?v=Df4-qpLfw8E. [10.11.2022].

Blinov, O. 2020. Encrypt your data in order to make GDPR and Russian Data Localization Law compatible. [online] https://iapp.org/news/a/encrypt-your-data-in-order-to-make-gdpr-and-russian-data-localization-law-compatible/. [10.11.2022].

Bowmann, C. 2015. A Primer on Russia's New Data Localization Law. *Proskauer Privacy Law Blog* 27.08.2015. [online] https://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/. [10.11.2022].

Bundesamt für Informationssicherheit. 2022. Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine (archiviert). [online] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html. [10.11.2022].

Chander, A., U. P. Lê. 2015. Data Nationalism. Emory Law Journal 64(3): 677-739.

Daskal, J. 2015. The Un-Territoriality of Data. *The Yale Law Journal* 125(2): 326-398.

Epifanova, A. 2020. Deciphering Russia's "Sovereign Internet Law". Tightening Control and Accelerating the Splinternet. DGAP Analyse No. 2. [online] https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law. [10.11.2022].

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB. 2022. Manufacturing-as-a-Service in Catena-X. [video] https://www.youtube.com/watch?v=CHMBS92BS3s. [10.11.2022].

Fraser, E. 2016. Data Localisation and the Balkanisation of the Internet. *scripted - A Journal of Law, Technology & Society* 13(3).

GOV.UK. 2021. The Digital Trade Principles agreed by the G7 countries at the G7 Trade Track on 22 October 2021. [online] https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles. [10.11.2022].

Gusbeth, S. 2022. China kontrolliert den Export von Daten künftig strenger – die Cyberaufsicht könnte die digitale Entflechtung so beschleunigen. *Handelsblatt* 01.09.2022. [online] https://www.handelsblatt.com/politik/international/regulierung-china-kontrolliert-den-export-von-daten-kuenftig-strenger-die-cyberaufsicht-koennte-die-digitale-entflechtung-so-beschleunigen/28643316.html. [10.11.2022].

Hill, J. 2012. Internet Fragmentation. Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers. Harvard University.

Hill, J. 2014. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders. The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014. [online] http://dx.doi.org/10.2139/ssrn.2430275.

Karpukhin, A., D. Sivkova. 2017. How to comply with the Russian requirements on localisation of personal data. *Financier Worldwide*. ExpertBriefing. [online] https://www.financierworldwide.com/how-to-comply-with-the-russian-requirements-on-localisation-of-personal-data#.Y2AugXbMI2w. [10.11.2022].

Kindle, F. 2020. Unternehmen investieren 6,8 Billionen US-Dollar in Digitalisierung. [online] https://www.netzwoche.ch/news/2020-11-03/bis-2023-unternehmen-investieren-68-billionen-us-dollar-in-digitalisierung. [10.11.2022].

Lehrer, N. 2014. African Datacenters: Challenges in Developing Countries. *tech.co*. [online] https://tech.co/news/african-datacenters-2014-09. [10.11.2022].

Maranto, L. 2020. Who Benefits from China's Cybersecurity Laws? *CSIS New Perspectives on Asia Blog* 25.06.2020. [online] https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws. [10.11.2022].

Meinrath, S. 2013. We Can't let the Internet Become Balkanized. *Slate* 14.10.2013. [online] http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html. [10.11.2022].

Olech, A. 2021. Cybersecurity in Saudi Arabia. Institute of New Europe. [online] https://ine.org.pl/en/cybersecurity-in-saudi-arabia/. [10.11.2022].

Pohle., A., J. Lang. 2019. Digitale Souveränität als Frage der Selbstbestimmung im digitalen Raum. Deutsche Gesellschaft für die Vereinten Nationen e. V. [online] https://dgvn.de/meldung/digitale-souveraenitaet-als-frage-der-selbstbestimmung-im-digitalen-raum. [10.11.2022].

PwC. 2022. CIO, CTO and Technology Leaders. CIOs, CTOs and technology leaders. Latest findings from PwC's Pulse Survey. [online] https://www.pwc.com/us/en/library/pulse-survey/executive-views-2022/technology-leaders.html. [10.11.2022].

Shaftan, V. 2019. Russian Data Localisation law: now with monetary penalties. The Norton Rose Fulbright Data Protection Report. [online] https://www.dataprotectionreport.com/2019/12/russian-data-localization-law-now-with-monetary-penalties/. [10.11.2022].

Stadnik, I. 2019. A closer look at the „sovereign Runet" law. School of Public Policy. [online] https://www.internetgovernance.org/2019/05/16/a-closer-look-at-the-sovereign-runet-law/. [10.11.2022].

Taylor, P. 2022. Amount of data created, consumed, and stored 2010-2020, with forecasts to 2025. [online] https://www.statista.com/statistics/871513/worldwide-data-created/. [28.12.2022.].

The New Arab. 2021. Humorous hackers hit Iran's railroad system in cyberattack. [online] https://english.alaraby.co.uk/news/humorous-hackers-hit-irans-railroad-system-cyberattack. [10.11.2022].

Wagner, J. 2017. Chinas Cybersecurity Law: What You Need to Know. *The Diplomat* 01.06.2017. [online] https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/. [10.11.2022].

Yayboke, E. 2021. The Real National Security Concerns over Data Localization. Center for Strategic and International Studies. [online] https://www.csis.org/analysis/real-national-security-concerns-over-data-localization. [10.11.2022].