„Data Free Flow with Trust“ - Auf der Suche nach dem Vertrauen

Marie-Louise Gächter

Zusammenfassung

Am Weltwirtschaftsforum 2019 in Davos kündigte der damalige japanische Premierminister Shinzō Abe an, eine internationale Ordnung für freien und auf gegenseitigem Vertrauen basierenden Datenfluss (*Data Free Flow with Trust*) schaffen zu wollen. Das ehrgeizige Projekt möchte mit dem Schlüsselbegriff „Vertrauen“ eine Grundlage schaffen, welche die Interoperabilität zwischen den vielfältigen und verschiedenartigen Datenschutzsystemen weltweit gewährleisten soll. Die Suche nach dieser Vertrauensbasis gestaltet sich aber schwieriger als erwartet, denn die Haltung der Staaten bzw. Regierungen gegenüber dem Schutz personenbezogener Daten ist von sehr unterschiedlichen Wertevorstellungen und Traditionen geprägt. Zudem wird die Interoperabilität im Sinne einer gleichberechtigten Kooperation dadurch erschwert, dass insbesondere die europäische Datenschutz-Grundverordnung Anspruch auf Geltung auch außerhalb der Grenzen des Europäischen Wirtschaftsraums (EWR) erhebt und mit ihren strengen Regelungen wenig Spielraum lässt für andere Systeme, was den Datentransfer aus dem EWR in einen Drittstaat betrifft.

Der Beitrag beleuchtet die Chancen und Hindernisse für einen *Data Free Flow with Trust* und kommt zum kritischen Schluss, dass derzeit vor allem noch die Hindernisse überwiegen und eine auf Vertrauen basierende Interoperabilität aktuell wenig Chancen hat, Realität zu werden.

1. Einleitung

Das Weltwirtschaftsforum in Davos war 2019 Schauplatz einer ambitionierten Ankündigung des japanischen Premierministers Shinzō Abe, wonach es an der Zeit sei, eine internationale Ordnung für freien und vertrauens-

würdigen Datenfluss (*Data Free Flow with Trust*) zu schaffen.[1] Die Ankündigung erfolgte zeitgleich mit der Annahme des Angemessenheitsbeschlusses für Japan unter Art. 45 der Datenschutz-Grundverordnung (DSGVO) durch die Europäische Kommission.

In diesem Vorhaben wird Vertrauen prominent als Schlüsselbegriff in den Mittelpunkt gestellt. Die beteiligten Staaten bzw. Regierungen wollen damit auf der Grundlage des Vertrauens nach langer Suche endlich einen Rahmen für einen globalen Datenfluss schaffen. Der Begriff Vertrauen bleibt aber unklar, und es stellt sich die Frage, ob er nicht eher politischer Rhetorik denn einer veritablen gemeinsamen und tragfähigen Basis entspricht.

Dieser Beitrag macht sich auf die Suche nach dem Vertrauen und geht der Frage nach, ob Vertrauen tatsächlich das entscheidende Element sein kann, das einen globalen Datenfluss legitimieren kann. Dies vor allem deshalb, weil die aktuellen Entwicklungen in der Frage des internationalen Datentransfers zwischen der EU und den USA nicht nur vertrauensfördernd sind. Insbesondere ist zu klären, wer wem vertrauen soll und auf welcher Grundlage dieses Vertrauen basieren kann.

Ähnliche Ungewissheit besteht im Hinblick auf den Begriff der (personenbezogenen) Daten. Der Begriff personenbezogen wird unterschiedlich ausgelegt, und selbst wenn sich der Data Free Flow with Trust aus Sicht der Initiatoren grundsätzlich nur auf nicht personenbezogene Daten beziehen soll, so stellen die unterschiedlichen Verständnisse dazu das Vorhaben auf eine weitere schwierige Probe. Was für die eine Seite personenbezogen ist, fällt für die andere Seite nicht darunter und das anzuwendende Regelwerk ändert sich je nach Perspektive. Erschwerend kommt hinzu, dass personenbezogene Daten in Europa zu einem Schlüsselbegriff für Selbstbestimmung und Privatsphäre geworden sind, sehr weit ausgelegt werden und auch grundrechtlich geschützt sind. Außerhalb Europas ist dies aber noch lange nicht zum Standard geworden, und es zeichnet sich hier auch aktuell kein Paradigmenwechsel ab.

1 *Abe*, Toward a New Era of "Hope-Driven Economy": The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting, 2019.

2. Der bisherige Weg zu einem Data Free Flow with Trust

Nach der Ankündigung in Davos 2019 wurde die Idee des Data Free Flow with Trust am G20 Gipfel im Sommer 2019 im japanischen Osaka im Rahmen des Themenschwerpunkts „Innovation" vertieft behandelt. Premierminister Abe unterstrich erneut die immense Bedeutung eines globalen Datenflusses für die zunehmende Digitalisierung, für die er internationale Regelungen insbesondere im Zusammenhang mit E-Commerce im Rahmen der WTO als wesentlich erachtete. Diese Bekenntnisse fanden ihren Niederschlag in den beiden Deklarationen des Gipfels, der „G20 Osaka Leaders' Declaration"[2] sowie der „Osaka Declaration on Digital Economy"[3].

Die G20 Osaka Leaders' Declaration sieht den globalen Datenfluss als große Chance für eine Steigerung der Produktivität und Innovation sowie die nachhaltige Entwicklung, anerkennt aber gleichzeitig, dass damit etliche Herausforderungen verbunden sind, darunter vor allem das Recht auf Privatsphäre und der Schutz personenbezogener Daten. Durch die Bewältigung dieser Herausforderungen soll der freie Datenfluss erleichtert und das Vertrauen der Konsumenten und der Wirtschaft gestärkt werden.[4] Privatsphäre, Datenschutz, geistiges Eigentum und Sicherheit sollen zudem mittels normativer Regelungen gewährleistet werden. Der explizite Hinweis auf den Datenschutz macht deutlich, dass personenbezogene Daten sehr wohl eine Rolle in dem Projekt spielen. Datenschutz wird in dem Dokument nicht nur als Herausforderung, sondern sogar als Grundlage des Vertrauens qualifiziert, wodurch der Ansatz weitgehend dem europäischen Kurs zu folgen scheint. Es ist aber freilich unklar, ob dies auch tatsächlich dem Bestreben der Initiatoren entspricht.

Als weitere, essentielle Voraussetzung wird zudem auf die Notwendigkeit der Interoperabilität der unterschiedlichen rechtlichen Rahmenbedingungen hingewiesen. Damit lässt sich als erster Anhaltspunkt für die Suche nach dem Vertrauen festhalten, dass gesetzlich normierter Datenschutz eine Grundlage für das Vertrauen der Konsumenten und der Wirtschaft bieten kann. Die Brücke zwischen den unterschiedlichen Ausprägungen der ge-

2 https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

3 https://www.wto.org/english/news_e/news19_e/osaka_declration_on_digital_economy_e.pdf

4 Der Originaltext in Rz. 11 der G20 Osaka Leaders' Declaration lautet: "By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust."

setzlichen Normierungen soll mittels Interoperabilität hergestellt werden und eine zusätzliche Vertrauensbasis bieten.

Das zweite Dokument, die Osaka Declaration on Digital Economy, wurde von 78 Staaten unterzeichnet und fokussiert gänzlich auf das große Potenzial des Datenflusses. Das Verständnis für die Rolle des Vertrauens vertieft sie nicht weiter. In der Erklärung wird vielmehr der Grundstein gelegt für den sogenannten „Osaka Track", der den Weg ebnen soll für Verhandlungen im Rahmen der WTO über globale Regelungen zum E-Commerce. Indien, Indonesien, Ägypten und Südafrika haben auf eine Unterzeichnung der Erklärung verzichtet.[5] Insbesondere Indien begründete dies damit, dass Daten als eine neue Form des Wohlstands als nationales Gut zu betrachten seien. Folglich sollten bei der Frage eines Data Free Flow with Trust auch die Interessen von Entwicklungsländern berücksichtigt werden, denn Daten dürften nicht nur dem Wirtschaftswachstum dienen, sondern auch der Entwicklung.[6] Verhandlungen zur Frage eines globalen Datenflusses müssten daher auf globaler Ebene stattfinden und sollten nicht in die Hände einer ausgewählten wirtschaftsorientierten Staatengruppe gelegt werden.

Im Januar 2023 folgten weitere Präzisierungen im Briefing Paper des Weltwirtschaftsforums zum Thema „Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows" (World Economic Forum 2023). In diesem Papier wird wiederholt festgehalten, dass die unterschiedlichen nationalen Regelungen zur Wirtschaftsentwicklung, zum Schutz von personenbezogenen Daten sowie zu Grundrechten und nationalen Sicherheitsbedenken zu einer geopolitischen Fragmentierung führen und den Data Free Flow vor große Herausforderungen stellen. Als zusätzliche Hürde werden die zunehmenden gesetzlichen Verpflichtungen zur lokalen Datenspeicherung in vielen Ländern identifiziert. Der Lösungsvorschlag, wie mit diesen vielfältigen nationalen Regelungen umzugehen ist, und vor allem, wie ihrem bedeutenden Einfluss auf den internationalen Datenfluss begegnet werden kann, wird auch hier in der Herstellung von Interoperabilität gesehen. Dabei wird erneut das Vertrauen ins Spiel gebracht, das Bestandteil dieser Interoperabilität sein soll.

Interoperabilität wird allgemein definiert als die „Fähigkeit unterschiedlicher Systeme, möglichst nahtlos zusammenzuarbeiten".[7] Um die Leistungsfähigkeit der Interoperabilität beurteilen zu können, braucht es aber zuerst

5 *Greenleaf*, Privacy Laws & Business International Report 2019, 18 (19).
6 Ibid.
7 Definition gemäß Duden online.

eine Auseinandersetzung mit den Systemen, für welche eine Zusammenarbeit gewährleistet werden soll. Je weiter deren zugrundeliegende Konzepte voneinander entfernt sind, desto schwieriger wird ihre nahtlose Zusammenarbeit und umso weniger Platz bleibt für das Vertrauen. Eines dieser grundlegenden Konzepte ist der Begriff der Daten und dabei vor allem die Unterscheidung und Definition von personenbezogenen und nicht-personenbezogenen Daten. Diese Grundsatzfrage wird in den unterschiedlichen Rechtskreisen sehr individuell beantwortet und hängt ab von den zugrundeliegenden Werten und Traditionen.

3. Der Begriff der Daten

In Davos betonte Premierminister Abe, dass seine Initiative des Data Free Flow with Trust selbstverständlich nur nicht-personenbezogene Daten umfassen sollte, während personenbezogene Daten, Daten in Bezug auf Geistiges Eigentum und nationale Geheimdienstinformationen eines besonderen Schutzes bedürften. Entgegen dieser scheinbar klaren Abgrenzung lassen die auf Abes Ankündigung folgenden Debatten und Dokumente keine eindeutige Schlussfolgerung zu, welche Arten von Daten tatsächlich von dem Projekt erfasst sein sollen. Die zahlreichen Hinweise auf Datenschutzbestimmungen, Privatsphäre und Grundrechte lassen eher vermuten, dass sich die Initiatoren sehr wohl bewusst sind, dass das Projekt nicht isoliert von den Fragen rund um personenbezogene Daten realisiert werden kann. Die große Frage betrifft vor allem die Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten bzw. die Definition dieser beiden Begriffe in den unterschiedlichen Rechtsordnungen. Das Briefing Paper des Weltwirtschaftsforums (World Economic Forum 2023) nennt die Unsicherheiten in Bezug auf die Definition des Begriffs „personenbezogene Daten" erstmals unmissverständlich als Hürde für den Data Free Flow with Trust, geht allerdings in Folge nicht näher darauf ein. Ohne dass es explizit in den Diskussionen zum Ausdruck gebracht wird, dürfte damit wohl vor allem die Diskrepanz zwischen der Europäischen Union (EU) bzw. dem Europäischen Wirtschaftsraum (EWR) und den USA, aber auch zahlreichen anderen Staaten außerhalb des EWR, gemeint sein.

Aber selbst wenn es gelingen sollte, sich auf einheitliche Definitionen zu einigen, wäre eine Trennung von personenbezogenen und nicht-personenbezogenen Daten für den Data Free Flow with Trust sowohl für den

privaten wie auch öffentlichen Sektor mit hohen bis sehr hohen Kosten verbunden und wohl kaum durchgängig zu erreichen.[8] Der Schutz der personenbezogenen Daten wird demnach immer ein wesentliches Element im Projekt bleiben.

3.1 Daten und Datenschutz in Europa

Im EWR wird nur die Kategorie der personenbezogenen Daten vom Datenschutzrecht, sprich der DSGVO erfasst.[9] Für nicht-personenbezogene Daten gilt eine eigene Verordnung.[10] Zur Gewährleistung eines besseren Verständnisses des nicht immer einfachen Verhältnisses zwischen den beiden Rechtstexten und Datenkategorien hat die Europäische Kommission Leitlinien erlassen.[11] Einer der Grundsätze lautet, dass in dem Falle, dass sich eine Trennung der Kategorien nicht herstellen lässt, die Bestimmungen für die personenbezogenen Daten auf das gesamte Datenkonglomerat Anwendung finden. Zusätzlich regeln weitere europäische Rechtstexte die Verarbeitung von (nicht-)personenbezogenen Daten im EWR bzw. der EU.[12]

8 *Casalini/López*, Trade Policy Paper 2019, 34.

9 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) (ABl. L 119 vom 4.5.2016, S. 1).

10 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (ABl. L 303 vom 28.11.2018, S. 59).

11 Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union vom 29. Mai 2019, COM(2019) 250 final.

12 So etwa die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39); Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89); Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Zur Beurteilung der Frage, welche Daten als personenbezogen gelten, hat zudem der Gerichtshof der Europäischen Union (EuGH) eine reichhaltige Rechtsprechung zur Verfügung gestellt, deren Tendenz klar dahin geht, im Zweifel Daten der Kategorie der personenbezogenen Daten zuzuordnen.[13] Getragen wird diese weite Auslegung vom europäischen Grundverständnis, dass Datenschutz ein eigenständiges Grundrecht ist.[14] In Nicht-EU-Staaten, die dem Europarat angehören, gilt, dass der Schutz personenbezogener Daten zumindest vom Recht auf Privatsphäre in Art. 8 der Europäischen Menschenrechtskonvention (EMRK) mitumfasst ist,[15] sofern die nationalen Verfassungen nicht ebenfalls ein explizites Grundrecht auf Datenschutz vorsehen.[16] Der Ehrgeiz der EU geht aber darüber noch hinaus, indem dieses sehr weitreichende Grundrechtsverständnis über die Grenzen der territorialen Jurisdiktion ausgeweitet wird und Anspruch erhebt auf eine extraterritoriale Anwendung, wenn bestimmte Anknüpfungspunkte zum EWR vorhanden sind. Diese folgen einerseits aus Art. 3 Abs. 2 DSGVO und andererseits aus Kapitel V DSGVO betreffend internationalen Daten-

13 Vgl. EuGH, *Patrick Breyer gegen Bundesrepublik Deutschland*, Urteil vom 19. Oktober 2016, C-582/14, ECLI:EU:C:2016:779; EuGH, *YS gegen Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel gegen M und S.*, Urteil vom 17. Juli 2014, C-141/12 und C-372/12, ECLI:EU:C:2014:2081. Vgl. näher dazu: *Zuiderveen Borgesius*, Eur. Data Prot. L. Rev. 2017; *Tracol*, Computer Law & Security Review 2015; *Lynskey*, Modern Law Review 2018; *Purtova*, Law, Innovation and Technology 2018; *Finck/Pallas*, International Data Privacy Law 2020.

14 Art. 8 der Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391) sieht den „Schutz personenbezogener Daten" als eigenständiges Grundrecht vor.

15 Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet das Recht auf Achtung des Privat- und Familienlebens, das gemäss ständiger Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte auch das Recht auf Schutz personenbezogener Daten umfasst. Vgl. beispielsweise EGMR, *Drelon gegen Frankreich*, Urteil vom 8. September 2022, Nr. 3153/16 und 27758/18 oder EGMR, *Big Brother Watch and Others gegen das Vereinigte Königreich*, Urteil der Grossen Kammer vom 25. Mai 2021, Nr. 58170/13, 62322/14 and 24969/15.

16 So bestimmt etwa Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft, dass jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat. Wenngleich Art. 13 selbst den Titel „Schutz der Privatsphäre" trägt, wird der Schutz vor Missbrauch der Daten nicht in den Schutz der Privatsphäre integriert, sondern als eigenes Schutzobjekt in Abs. 2 explizit erwähnt. Art. 35 der albanischen Verfassung sieht wiederum einen klaren Schutz personenbezogener Daten vor und hebt sogar explizit einige der Rechte der betroffenen Personen auf Verfassungsstufe. Ähnlich weitreichend regelt auch Art. 34 der armenischen Verfassung den Schutz personenbezogener Daten.

transfer. Im Zusammenhang mit Letzterem hatte der EuGH in seinem Schrems-II Urteil im Juli 2020 festgestellt, dass die Datenübermittlung in die USA in zwei Punkten aus europäischer Sicht nicht rechtskonform ist.[17] Dies ist zum einen der fehlende Rechtsschutz für die betroffenen Personen und zum anderen der Zugriff US-amerikanischer Behörden auf Daten aus dem EWR, welcher die (am europäischen Grundrechtsstandard gemessenen) Kriterien der Erforderlichkeit und Verhältnismäßigkeit nicht einhält.[18]

3.2 Daten und Datenschutz in den USA

Außerhalb Europas wird der Begriff „personenbezogene Daten" vor allem im Konsumentenrecht angesiedelt und nicht als Element verstanden, das grundrechtlichen Schutz genießt. Zugegeben, auch in Europa treten die beiden Rechtsbereiche in eine zunehmend enger werdende Beziehung,[19] wenngleich nur einem Bereich Grundrechtscharakter zugestanden wird, während der andere unter dem Titel Verbraucherschutz als Ziel in Art. 169 des Vertrags über die Arbeitsweise der Europäischen Union aufgelistet ist.

In den USA, wo Datenschutz nicht auf gesamtstaatlicher Ebene, sondern bislang nur in einzelnen Bundesstaaten gesetzlich geregelt ist, werden personenbezogene Daten und Konsumentenrecht als Einheit betrachtet.[20] Dies ist vor allem daran ersichtlich, dass es der Federal Trade Commission obliegt, Grundsätze für die faire Nutzung von personenbezogenen Daten auf Basis des Konsumentenrechts zu entwickeln.[21] Die mannigfachen gesetzlichen Regelungen in den USA bringen es zudem mit sich, dass einzelne Fragen unterschiedliche Lösungen erfahren, unter anderem die Definition des Begriffs „personenbezogene Daten".[22] Der Unterschied zeigt sich bei der Frage, ob sich personenbezogene Daten auf eine identifizierte oder direkt identifizierbare Person beziehen müssen, oder ob es sich auch um Daten handeln kann, die erst in Verbindung mit zusätzlichen Informationen, die

17 EuGH, *Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems,* Urteil vom 16. Juli 2020, C-311/18, ECLI:EU:C:2020:559.

18 Für eine detaillierte Analyse dieser Entscheidung vgl. etwa: *Sury,* Informatik Spektrum 2020, 354; *Heper*, Jahrbuch für Vergleichende Staats-und Rechtswissenschaften 2022, 125.

19 *Helberger* u.a., Common Market Law Review 2017, 1427.

20 *Solove/Hartzog*, Columbia Law Review 2014, 584; *Schwartz/Solove*, California Law Review 2014, 877.

21 *Rustad/Koenig*, Florida Law Review 2019, 365 (381).

22 *Schwartz/Solove*, California Law Review 2014, 877 (888f.).

eventuell nur bei einer dritten Stelle verfügbar sind, die Identifizierung einer natürlichen Person ermöglichen. Von wenigen Ausnahmen abgesehen ist der erste Ansatz in den USA vorherrschend.[23] Daraus ergeben sich Diskrepanzen zwischen der DSGVO und amerikanischem Recht vor allem bei den Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die ein Gerät oder Software-Anwendungen und Tools oder Protokolle liefern, oder sonstigen Kennungen wie Funkfrequenzkennzeichnungen. Diese können gemäß Erwägungsgrund 30 der DSGVO „Spuren" hinterlassen, die letztlich in Kombination mit anderen Kennungen und Informationen dazu dienen können, Personen zu identifizieren. Der California Consumer Privacy Act (CCPA) sowie der California Privacy Rights Act (CPRA), als erstes umfassendes US-Gesetz in Bezug auf die Verarbeitung personenbezogener Daten, erkennen zwar Online-Kennungen ebenso wie Informationen, welche durch die Interaktion mit dem Internet oder einem anderen elektronischen Netzwerk generiert werden, als personenbezogene Daten an, wenn diese Information „identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[24] Weder diese Legaldefinition noch die Rechtsprechung in den USA beantworten aber die Frage, ob damit eine Online-Kennung, vor allem die IP-Adresse, eindeutig als personenbezogenes Datum eingestuft wird oder nicht.[25] Anders der EuGH, der hier eine klare Meinung vertritt und IP-Adressen einschließlich dynamischer IP-Adressen als personenbezogene Daten qualifiziert.[26]

Die Debatten rund um Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die Geräte oder Software-Anwendungen und -Tools oder Protokolle liefern und die Frage von deren Personenbezug haben einen erheblichen Einfluss auf den internationalen Datentransfer. Nachdem diese Daten aus EWR-Sicht der DSGVO unterfallen, wird aktuell – nach dem Wegfall des Angemessenheitsbeschlusses für die USA – der Nutzung unterschiedlicher Tools wie Google Analytics[27] etc. im EWR die unkomplizier-

23 Zu den Ausnahmen zählt Children's Online Privacy Protection Rule (COPPA), 78 Fed. Reg. 3972 (Jan. 17, 2013). Eventuell lässt sich der hier gewählte strengere Schutz damit begründen, dass es in dem Gesetz explizit um den Schutz von Kindern geht.

24 Cal. Civ. Code § 1798.140 (v).

25 *Zetoony*, Loyola University Chicago Journal of Regulatory Compliance 2022, 1 (4).

26 EuGH, *Patrick Breyer gegen Bundesrepublik Deutschland*, Urteil vom 19. Oktober 2016, C-582/14, ECLI:EU:C:2016:779.

27 Das Beispiel von Google Analytics erlangte deshalb besondere Bedeutung, als die Organisation NOYB nach dem EuGH-Urteil Schrems II eine Reihe von Beschwerden

teste Rechtsgrundlage entzogen. Die Hürden, einen alternativen Weg für Datenübermittlungen in die USA zu finden, sind in der Praxis so groß, dass der transatlantische Datentransfer einen bedeutenden Rückgang erfahren müsste, würden alle EWR Datenexporteure der strengen Auslegung des EuGH Folge zu leisten versuchen.

Aber nicht nur bei der Frage, was unter personenbezogenen Daten zu verstehen ist, gibt es Unterschiede. Ebenso finden sich unterschiedliche Sichtweisen in Bezug auf die zu schützenden Individuen und die verantwortlichen Stellen. Unter der DSGVO sind dies sämtliche natürliche Personen im EWR, während die einschlägigen US-Gesetze die Betonung auf Konsumenten legen. Auch wenn der Begriff Konsument im jeweiligen Gesetzestext dann konkret mit „Bürger" eines bestimmten Staates definiert wird und damit zumindest im Wortlaut dem EWR-System angeglichen wird, hat der Grundgedanke des „Konsumentenschutzes" weitere Auswirkungen, nämlich auf die verantwortlichen Stellen. Nachdem Datenschutz gemäß diesem Verständnis nur Konsumenten als Schutzobjekte hat, werden die verantwortlichen Stellen auf Unternehmen eingeschränkt. Vor allem Behörden werden nicht verpflichtet. Im Gegenteil, ihnen kommen sogar weitreichende Befugnisse zu, auf Daten von in- und ausländischen Bürgern zuzugreifen. Aber auch bei den Unternehmen gelten die Datenschutzbestimmungen nicht umfassend, denn auch hier bestehen ergänzende Kriterien, etwa die Bedingung im CCPA/CRPA, dass es sich um Unternehmen handeln muss, die einen bestimmten Mindestumsatz erreichen und die jährlich Daten von mindestens 100'000 Konsumenten oder Haushalten kaufen, erhalten, verkaufen oder teilen, oder einen bestimmten Prozentsatz des Umsatzes mit dem Verkauf oder Teilen von Daten generieren.[28] Im Vergleich zu diesem stark sektoral ausgeprägten Datenschutzsystem der USA konnten sich bislang die Befürworter eines gesamtstaatlichen Datenschutzgesetzes (noch) nicht durchsetzen.

3.3 Daten und Datenschutz im asiatisch-pazifischen Raum

Die USA ist keine Ausnahme, was die fehlende Verbindung von Datenschutz zu den Grundrechten betrifft. Auch wenn es Ausnahmen wie etwa

gemäss Art. 77 DSGVO einreichte, die fast gleichlautend entschieden wurden und die Rechtsgrundlage für die Nutzung dieses Tools in Frage stellten.

28 Ähnlich auch der Virginia Consumer Data Protection Act (VCDPA), der etwas niedrigere Hürden ansetzt und das Mindestmaß mit 25'000 Konsumenten bestimmt.

Japan gibt, werden in zahlreichen Staaten im asiatisch-pazifischen Raum Daten häufig als „Beiwerk" von gehandelten Waren oder Dienstleistungen betrachtet. Ähnlich wie in den US-Gesetzen werden auch hier Definitionen von personenbezogenen Daten sehr offen formuliert. So folgt etwa aus dem südkoreanischen Gesetz, dass personenbezogene Daten nicht notwendigerweise Online-Kennungen, Geräte- oder verhaltensbezogene Informationen, Informationen zum Surfverhalten sowie User-Interaktionen (advertising information, inference information, Internet browsing and search records, and information about Internet websites/ application programs/advertisements and user interactions) umfassen.[29] Ebenso zeigt sich hier die Tendenz, Pseudonymisierung in die Nähe der Anonymisierung zu bringen und somit zumindest teilweise aus dem Bereich der personenbezogenen Daten auszuklammern.[30] Ähnliche Tendenzen sind auch in der 2020 erfolgten Reform des japanischen Datenschutzgesetzes sichtbar. Die neue Kategorie von „in pseudonymisierter Form verarbeiteten Daten" bleibt zwar weiterhin Teil der personenbezogenen Daten, wird aber von einzelnen Betroffenenrechten ausgenommen.[31] Etliche Gesetze erlauben den Unternehmen, diese Daten etwa für interne Zwecke, wie Unternehmensanalysen oder die Entwicklung von Berechnungsmodellen zu verwenden. Auch sind pseudonymisierte Daten nicht verpflichtend zu löschen, selbst wenn die personenbezogenen Daten für den ursprünglich erhobenen Zweck nicht mehr erforderlich sind. Für zukünftige statistische Analysen dürfen sie weiterhin gespeichert bleiben. Die Begriffe Unternehmensanalysen, Statistiken oder Berechnungsmodelle sind vage gehalten und gewinnorientierte Zwecke scheinen dabei nicht überall ausgeschlossen.

Andererseits haben sich Indien, China, Malaysia, Vietnam und zahlreiche weitere Staaten für verstärkte Verpflichtungen zur lokalen Datenspeicherung ausgesprochen, die vor allem den E-Commerce bzw. Finanzbereich betreffen und etwa Zahlungsdienstleister verpflichten, die Daten von Kunden aus den jeweiligen Staaten national zu speichern.[32] Dies stößt wiederum vor allem bei den USA auf großes Unverständnis.

29 *Park* u.a., Asian Journal of Innovation and Policy 2020, 339 (353).

30 Ibid., 339 (342); vgl. auch die diesbezüglichen Bestimmungen im Angemessenheitsbeschluss für Südkorea, Rz. 82.

31 *Joo/Kwon*, Government Information Quarterly 2023, 1 (5f.); vgl. auch den Angemessenheitsbeschluss für Japan, Rz. 30-32.

32 Vgl. etwa Reserve Bank of India, Statement on Developmental and Regulatory Policies vom 5. April 2018, wo unter Pkt. 4 folgende Anweisung erfolgt: „It is observed that at present only certain payment system operators and their outsourcing

In Bezug auf das Grundverständnis des Schutzes personenbezogener Daten lautet das Argument häufig, dass „asiatische Werte" nicht vereinbar seien mit dem westlichen Grundrechtsverständnis, das bisweilen aus asiatischer Sicht sogar als eine moderne Erweiterung des Imperialismus betrachtet wird.[33] Aus Grundrechtsdokumenten, politischen Debatten und auch der Literatur lässt sich ableiten, dass das Individuum gegenüber dem Kollektiv in Asien oft eine nachrangige Bedeutung einnimmt. Damit wird auch erklärt, warum in der politischen Agenda vieler asiatischer Staaten wirtschaftliche Entwicklung und politische Stabilität (in welcher Form diese auch immer gewährleistet wird) höher gewertet werden als zivile und politische Rechte einschließlich des Rechts auf Privatsphäre und des Schutzes personenbezogener Daten.[34]

Auch wenn diese Aussagen einen Hang zum Klischee haben und der Vereinfachung dienen, sind sie in Bezug auf die Wertung des Schutzes personenbezogener Daten nicht ganz von der Hand zu weisen und erklären viele staatliche Entscheidungen, aber auch die Haltung vieler Menschen in Staaten wie beispielsweise Indien in Bezug auf die Verarbeitung ihrer personenbezogenen Daten.[35] Sie lassen deshalb auch Rückschlüsse auf das unterschiedliche Verständnis des im Rahmen des Data Free Flow with Trust aufgeworfene Konzept des Vertrauens zu. Europa hat nach dem zweiten Weltkrieg unmissverständlich den Weg eingeschlagen, dass Grundrechte und entsprechende Mechanismen zu ihrer Durchsetzung die Grundlage eines friedlichen Zusammenlebens sind. Entsprechend vertrauen die Menschen darauf, dass durch diese Mechanismen, die auf staatlicher wie internationaler bzw. regionaler Ebene angesiedelt sind, eine Kontrolle gegenüber

partners store the payment system data either partly or completely in the country. In order to have unfettered access to all payment data for supervisory purposes, it has been decided that all payment system operators will ensure that data related to payment systems operated by them are stored only inside the country within a period of 6 months". URL: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR264270719E5CB28249D7BCE07C5B3196C904.PDF. Vgl. allgemein zur zunehmenden Tendenz der Datenlokalisierung: *Basu*, The retreat of the data localization brigade: India, Indonesia and Vietnam.

33 Vgl. *Freeman*, The Pacific Review 1996, 352 (364); *Rustad/Koenig*, Florida Law Review 2019, 365 (387).

34 Vgl. unter anderem *Ghai*, Hong Kong Law Journal 1993; *Chan*, in: Tuck-Hong (Hrsg.), Human Rights and International Relations in the Asia Pacific Region, 2017, 25 (35).

35 *Chatterjee*, International Journal of Law and Management 2019, (170) 177.

dem Staat und zunehmend auch gegenüber nicht-staatlichen Akteuren entstanden ist.

Asiatische Wertvorstellungen sind hingegen stark vom Kommunitarismus geprägt, dem der westliche Individualismus gegenübersteht. Die individuelle Freiheit, Privatsphäre und (informationelle) Selbstbestimmung, die Grundlage des europäischen Datenschutzes ist, trifft bei vielen Regierungen im asiatischen Raum oft auf Unverständnis.[36] Und selbst wenn diese oder ähnliche Konzepte vorhanden sind, wie etwa in Japan, ist ihr Verständnis nicht unbedingt identisch mit demjenigen in Europa.[37]

3.4 Sonderfall China hinsichtlich Daten und Datenschutz

In der staatlichen *State Informatization Development Strategy 2006–2020* betont China die immense Bedeutung von Daten, insbesondere deren Rolle als zentraler Produktionsfaktor und Garant für den Wohlstand der Gesellschaft. Die nationale Big Data-Strategie steht darin ebenso wie die staatlich organisierten Big Data-Zentren im Mittelpunkt. Die Grund- und Freiheitsrechte der Bürgerinnen und Bürger sollen demgegenüber einen „realistischen" Schutz erhalten und der Schutz personenbezogener Daten gestärkt werden. Eine gesetzliche Regelung zum Datenschutz findet sich entsprechend in dem am 1. November 2021 in Kraft getretenen *Personal Information Protection Law* (PIPL). Die darin enthaltene Definition personenbezogener Daten basiert auf der Vorlage der DSGVO und umfasst „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen lassen und in elektronischem oder anderem Format gespeichert werden".[38] Einer der Hauptunterschiede zur DSGVO liegt jedoch in den strengen Vorschriften zur verpflichtenden Datenspeicherung in China. Genaue Kriterien oder Vorgaben dafür finden sich im Gesetz allerdings nicht. Beachtlich sind auch die Einschränkungen und Hürden für den Datentransfer außerhalb Chinas. Trotz der stellenweisen Orientierung am Text der DSGVO wurde der entsprechende Regelungsgehalt der DSGVO nicht übernommen. Insgesamt ist festzustellen, dass China mit dem neuen Datenschutzgesetz trotz formeller und teilweise inhaltlicher Anlehnung an das DSGVO-Modell keineswegs einem Grundrecht zur Durch-

36 *de Vries/Meijknecht*, International Journal on Minority and Group Rights 2010, 75 (86).
37 *Beer*, Asian Survey, 437 (439f.).
38 *Wang Han/Munir*, European Data Protection Law Review 2018, 535; *Geller*, GRUR International 2020, 1191 (1193).

setzung verhelfen will, sondern auf soziale Kontrolle, gesamtgesellschaftliche Interessen und natürlich die nationale Sicherheit als zu erreichende Ziele setzt.[39]

Dies bringt ein chinesischer Autor folgendermaßen zum Ausdruck: „Asian values [put] emphasis on a quest for consensual solutions, communitarianism rather than individualism, social order and harmony, respect for elders, discipline, a paternalistic state, and the primary role of government in economic development."[40]

3.5 Zwischenfazit

Die Beispiele der unterschiedlichen staatlichen und regionalen Lösungsansätze für den Umgang mit personenbezogenen Daten könnten noch beliebig fortgesetzt werden, was aber den Umfang dieses Beitrags sprengen würde. Die genannten Beispiele reichen aus, um auf ein grundlegendes Problem hinzuweisen. Der Umgang mit Daten ist weit mehr als eine Frage der Gesetzgebung, es geht um wesentlich tiefer liegende gesellschaftliche Konzepte und Werte, auf denen die jeweiligen rechtlichen Lösungsansätze beruhen. Im Grunde geht es um die Frage, ob personenbezogene Daten als Werte und Interessen zu qualifizieren sind, welche durch die Grund- und Menschenrechte geschützt werden sollen, oder ob sie im Dienst der Gemeinschaft, der Wirtschaft und/oder der nationalen Sicherheit stehen. Und damit geht es letztlich auch um die Frage, worauf Menschen wirklich vertrauen, wenn es um die Verarbeitung bzw. Übermittlung ihrer Daten geht.

In Europa steht das Menschenrecht auf Privatsphäre bzw. des Schutzes personenbezogener Daten im Mittelpunkt der Frage der Verarbeitung von Daten. Damit einhergehend ist die weite Auslegung des Begriffs „personenbezogene Daten" und die vor allem vom EuGH festgelegte, niedrige Schwelle für die Identifizierbarkeit von Personen. Hinzu kommt, dass sowohl der EuGH[41] als auch der Europäische Gerichtshof für Menschenrechte (EGMR)[42] dem Zugang zu einer gerichtlichen Überprüfung der Rechtmäßigkeit einer Datenverarbeitung einen immens hohen Stellenwert

39 *Geller*, GRUR International 2020, 1191 (1192).

40 Zitiert in *Tomuschat*, Human Rights. Between Idealism and Realism 2003, 70.

41 EuGH, *Schrems II*, Rz. 95.

42 EGMR, *Roman Zakharov gegen Russland,* Urteil der Grossen Kammer vom 4. Dezember 2015, Nr. 47143/06, Rz. 234: "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the

einräumen. Ebenso zeigen die beiden Gerichtshöfe auf, dass sie für einen Zugriff staatlicher Stellen auf personenbezogene Daten strenge Maßstäbe ansetzen und dabei vor allem die Erforderlichkeit und Verhältnismäßigkeit genau überprüfen und auch von Drittstaaten einfordern, soweit Daten aus dem EWR betroffen sind.

Ein zweiter Ansatz in Bezug auf den Schutz personenbezogener Daten, der vor allem in den USA dominiert, ist die starke Verknüpfung der Verarbeitung von Daten mit der Wirtschaft und den Unternehmen. Vereinfacht dargestellt, sind Daten bei diesem Ansatz Teil des Trade-offs einer Konsumentenbeziehung und Konsumenten sollen selbst entscheiden, welchen Wert sie ihren personenbezogenen Daten dabei zumessen. Daten nehmen damit die Rolle eines Wirtschaftsgutes ein, das ebenso wie Produkte und Dienstleistungen Teil des freien Marktes ist. Auf der anderen Seite stehen US-Behörden weitreichende Möglichkeiten für einen Zugriff auf personenbezogene Daten für Zwecke der nationalen Sicherheit zur Verfügung.

In Asien hingegen lässt sich ein anderer Ansatz finden. In der politischen Agenda der meisten asiatischen Regierungen werden die wirtschaftliche Entwicklung, das Interesse der Gemeinschaft und die politische Stabilität sowie die nationale Sicherheit höher gewertet als zivile und politische Rechte des Individuums. Neben der politischen Agenda spielt hier auch die Wertvorstellung der Gesellschaft, in der die Gemeinschaft einen hohen Stellenwert einnimmt, eine Rolle und lässt somit das Recht des Individuums auf Privatsphäre in den Hintergrund treten. Nicht eindeutig geklärt ist damit aber die Frage, ob die Menschen bezüglich ihrer personenbezogenen Daten entgegen der hohen Wertschätzung der Gemeinschaft doch einen erweiterten Schutz als wünschenswert erachten.

Eine zusätzliche Komponente wurde von Indien ins Spiel gebracht, das dem Osaka Track unter anderem mit der Begründung ferngeblieben ist, dass Daten als eine neue Form des Wohlstands und entsprechend als nationales Gut zu betrachten seien. Folglich sollten bei der Frage eines Free Flow of Data auch die bislang vernachlässigten Interessen von Entwicklungsländern berücksichtigt werden.[43]

---

measures taken without his or her knowledge and thus able to challenge their legality retrospectively … or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications".

43 *Greenleaf*, Privacy Laws & Business International Report 2019.

Schließlich sind auch noch jene Staaten in die Debatte miteinzubeziehen, denen Datenschutzbestimmungen ganz oder fast gänzlich unbekannt sind, wie etwa Indonesien, Pakistan oder viele Staaten im mittleren Osten und in Ozeanien. Auch wenn internationale Datentransfers aus Sicht dieser Staaten unproblematisch sind, findet nur sehr wenig Datenimport in diese Länder statt.

Die aufgezeigten Ansätze sind in den meisten Fällen nicht ausschließlich aufzufinden, sondern oft in Kombination vorhanden. Viele staatliche Lösungsansätze befinden sich auch irgendwo dazwischen, so kann der australische Ansatz beispielsweise zwischen Europa und den USA angesiedelt werden.

4. Interoperabilität der Systeme

Das Ziel der Interoperabilität ist es, zu gewährleisten, dass unterschiedliche Systeme nahtlos zusammenarbeiten und, im Falle des Data Free Flow with Trust, Mechanismen geschaffen werden, die es erlauben, dass „systems, regulatory frameworks, technologies or standards interact, communicate and function with those of other operators or countries".[44] Der Osaka Track will diese Interoperabilität vor allem im Bereich des E-Commerce sicherstellen.

Zu den größten Hürden, die der Interoperabilitäts-Mechanismus neben der Frage seiner generellen Anwendbarkeit abhängig von der Definition der personenbezogenen Daten überbrücken muss, gehören die in den nationalen bzw. regionalen Datenschutzgesetzen vorzufindenden Bestimmungen für den Datentransfer außerhalb der eigenen Jurisdiktion sowie Verpflichtungen zur lokalen Datenspeicherung. Für ersteres stellt zweifelsfrei die DSGVO die beträchtlichste Herausforderung dar, denn mit ihrem Kapitel V zur Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen hat sie ein eigenes, sehr straffes Regime geschaffen, mit dem sie das Schutzniveau der Daten auch in Drittstaaten angemessen aufrechterhalten will. Mit dieser spezifischen Regelung macht Europa klar, dass der internationale Transfer von Daten als autonomes Prozedere zu werten ist, das zwar einen praktischen Bezug haben kann zum Austausch von Wirtschaftsgütern, aber nicht dessen Regelungen folgt. Obwohl Kapitel V DSGVO prima facie keine extraterritoriale Anwendung der DSGVO zum Ziel hat, sondern nur Datenexporteuren im EWR Aufla-

44 *Casalini/López*, Trade Policy Paper 2019, 6.

gen für ihren Datentransfer in einen Drittstaat auferlegt, hat das System eine weitreichende Wirkung auf Drittstaaten und deren Rechtsordnungen, wie die aktuellen Diskussionen rund um die Ausgestaltung des EU-US Data Privacy Framework als Nachfolger des EU-US Privacy-Shields zeigen. Gemäß EuGH sind nämlich an einen Datentransfer unter anderem die Bedingungen geknüpft, dass einerseits betroffenen Bürgern in den jeweiligen Drittstaaten die Möglichkeit einer gerichtlichen Überprüfung der Datenverarbeitung zur Verfügung steht und andererseits der Zugriff staatlicher Behörden auf diese Daten nur in verhältnismäßigem und erforderlichem Ausmaß erfolgt – gemessen aus europäischer Sicht selbstverständlich am europäischen Grundrechtsstandard.

Angesichts dieses engen Korsetts stellt sich die Frage, ob die DSGVO überhaupt Platz lässt für eine Interoperabilität im Sinne einer *Kooperation* mit anderen Rechtssystemen oder ob sie vielmehr den (nicht verhandelbaren) Maßstab vorgibt, der erreicht werden muss, wenn Datenexporteure in EWR-Staaten in einen Free Flow of Data involviert sind. Bereits heute sieht sich der europäische Maßstab bisweilen der Kritik eines neuen „Imperialismus" ausgesetzt.[45] Diese Kritik wendet sich insbesondere gegen den Trend, dass zahleiche Staaten außerhalb des EWR-Raums die DSGVO als Modell für ihre nationalen Datenschutzgesetze verwenden, ohne dass dies immer ihren Rechtstraditionen entspricht.

Zwischenzeitlich wurde 14 Staaten von der Europäischen Kommission mit einem Angemessenheitsbeschluss attestiert, dass sie über ein dem EWR-Standard angemessenes Datenschutzniveau verfügen. Art. 45 sowie Erwägungsgrund 104 der DSGVO geben die Kriterien für den Angemessenheitsbeschluss vor und machen kein Geheimnis aus ihrer Orientierung am europäischen bzw. internationalen Menschenrechtsstandard. Ebenfalls zu berücksichtigen sind Vorschriften über die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit sowie die öffentliche Ordnung und das Strafrecht. Diese Bereiche sind gemäß Art. 2 Abs. 2 DSGVO nicht einmal vom Anwendungsbereich der DSGVO umfasst, finden aber trotzdem Beachtung, wenn es um die Frage der Angemessenheit von Drittstaaten geht. Zudem ist nicht zu vergessen, dass auch die Richtlinie (EU) 2016/680 für den Datenschutz bei Polizei und Justiz die Möglichkeit eines

45 *Fabbrini/Celeste*, German Law Journal 2020, 55 (56). In dieselbe Richtung geht die Aussage: „Be ready for the Brussels Effect — It's coming to Data and AI" - vgl. dazu *Rzeszucinski*, Forbes v. 26. Mai 2022.

Angemessenheitsbeschlusses enthält. 2021 erhielt Großbritannien als erster Drittstaat einen solchen Angemessenheitsbeschluss.

Das Beispiel der aktuellen Verhandlungen zum EU-US Data Privacy Framework wirft die Frage auf, ob der mit dem Angemessenheitsbeschluss zu regelnde Datenfluss zwischen den beiden Jurisdiktionen tatsächlich als „nahtlose" Kooperation zweier Systeme gedacht ist, oder die Vorgaben EU-seitig gemacht werden. Grundbedingung für den Datentransfer ist gemäß Entwurf des Angemessenheitsbeschlusses die Gewährleistung von „privacy rights and their effective implementation, supervision and enforcement"[46] sowie von „rules intended to limit interferences with the fundamental rights of the persons whose data is transferred from the Union, which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and provides effective legal protection against interferences of that kind".[47] Auch die Frage der Definition personenbezogener Daten (einschließlich besonderer Kategorien) wird im Sinne Europas gelöst, indem die Definition der DSGVO übernommen wird und auch pseudonymisierte Daten für Forschungszwecke mitumfasst sind, selbst wenn der Schlüssel in Europa verbleibt.[48] Ebenso ist die Zweckbestimmung des Art. 5 Abs. 1 Bst. b DSGVO Teil der Bedingungen[49] und konterkariert somit die allgemein zu beobachtende Tendenz, über die Pseudonymisierung einzelne Datenschutzbestimmungen wie die Zweckbestimmung und vor allem die Betroffenenrechte einzuschränken.

Europa macht damit zweifelsfrei die strengsten Vorgaben, aber auch andere Jurisdiktionen, wie Australien, sehen Bedingungen für den Datentransfer in Drittstaaten vor. China hingegen versucht, mit Verpflichtungen zur Speicherung im Inland, wofür als Gründe die Cyberspace Sovereignty und Netzwerksicherheit angegeben werden, Datentransfers in Drittstaaten stark zu reduzieren.[50] Selbst in Fällen, wo ein internationaler Datentransfer gesetzlich nicht ausgeschlossen ist, ist ein solcher Transfer von zahlreichen, meist schwierig zu erfüllenden Voraussetzungen abhängig, für die zudem wenig Rechtssicherheit besteht.

46 Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Dezember 2022, Rz. 4.
47 Ibid., Rz. 4.
48 Ibid., Rz. 11.
49 Ibid., Rz. 14.
50 *Geller*, GRUR International 2020, 1191 (1200); *Feng*, Asia Pacific Law Review 2019, 62 (72).

Die aktuelle Situation zeigt, dass es zumindest in naher Zukunft wohl kaum möglich sein wird, im Dialog systemübergreifende Gemeinsamkeiten zu identifizieren, die schließlich als tragfähige Basis bzw. Interoperabilitäts-Mechanismus für ein globales digitales Ökosystem zum Einsatz kommen können. Neben dem Dialog fehlt es aktuell auch an einer internationalen Institution, die für die Etablierung der Interoperabilität verantwortlich zeichnen könnte. Die Bemühungen auf Ebene der WTO und der OECD gehen kaum über Leitlinien oder Briefing Papers hinaus. Praktische Schritte setzt, wie ausgeführt, lediglich die EU, allerdings nicht im Dialog und nicht immer mit einer Suche nach Gemeinsamkeiten und nahtloser Zusammenarbeit, sondern mit klaren Bedingungen, unter denen ein internationaler Datentransfer aus ihrer Sicht, und gemessen am europäischen Grundrechtsstandard, rechtmäßig erfolgt. Immerhin erlauben so aktuell 30 EWR-Staaten und 14 Drittstaaten mit Angemessenheitsbeschluss einen Data Free Flow with Trust in einem Datenraum, der ein Viertel der Staaten weltweit umfasst. Prozentual betrachtet sind dies ca. 820 Millionen Menschen, allerdings nur gut 10% der Weltbevölkerung. Darüber hinaus wird es aber schwierig, vor allem auch mit Blick auf die zunehmenden gesetzlichen Verpflichtungen zur lokalen Datenspeicherung.

5. Fazit zur Suche nach dem Vertrauen

Diese Entwicklungen lassen darauf schließen, dass Interoperabilität vor schwierigen Herausforderungen steht. Somit fällt sie auch als Grundlage für das Vertrauen in ungehinderte internationale Datentransfers weg. Dies ist bedauerlich, denn die Grundidee ist nicht zu unterschätzen, kann Vertrauen im weitesten Sinn doch einen wesentlichen Beitrag zum Gelingen internationaler Kooperation leisten.[51] Zurzeit allerdings scheint es eher so zu sein, dass zwar die meisten Regierungen mit dem Element Vertrauen argumentieren und den Menschen die jeweiligen nationalen oder regionalen Lösungsansätze als Vertrauensbasis anbieten, was in vielen Fällen auch recht gut gelingt. So vertrauen Menschen in Europa auf den Grundrechtsschutz. In den USA vertrauen sie auf den freien Markt, auf dem sie ihre Daten als handelbares Gut in eine Kundenbeziehung einbringen. Im asiatisch-pazifischen Raum vertrauen sie darauf, dass ihre Daten einem höheren Gut, vor allem der Gemeinschaft, dem Wirtschaftswachstum und

51 *Brugger* u.a., Zeitschrift für Internationale Beziehungen 2013.

der nationalen Sicherheit dienen. In China speziell werden Daten vertrauensvoll dem Staat überlassen, der für gesellschaftliches Wohlergehen und soziale und nationale Sicherheit und Kontrolle sorgen soll. In Entwicklungsländern schließlich wird darauf vertraut, dass Daten der Entwicklung dienen. Nicht vergessen werden darf bei dieser Kategorisierung, dass die einzelnen Systeme natürlich unterschiedliche Ausprägungen erfahren und Elemente kombinieren können. Auch ist das Vertrauen der Bevölkerung nicht immer vollumfänglich zu gewinnen, und es gibt sowohl in Europa Stimmen, die bereit sind, ihre Daten als Wirtschaftsgut einzubringen wie es in Asien und den USA diejenigen gibt, die dem Weg, den die Regierungen beschreiten, kritisch gegenüberstehen.

Für einen Data Free Flow (with Trust) scheint Vertrauen allerdings derzeitig nicht wirklich eine tragfähige Basis zu sein. Der europäische Ansatz in dieser Frage ist eindeutig und in einer Anpassung des nationalen Rechtsrahmens der Drittstaaten an die europäische Lösung zu finden. Vertrauen muss damit allerdings nicht notwendigerweise verbunden sein, kann es aber natürlich werden, wenn die Drittstaaten mit der Anpassung an die DSGVO auch das Vertrauen in den Grundrechtsschutz übernehmen. Dies scheint im Moment allerdings eher unrealistisch und somit wird der Data Free Flow wohl noch eine längere Zeit eine Gemengelage unterschiedlicher Lösungsansätze bleiben. Abzuwarten bleibt außerdem, welche Rolle künftig die Konvention 108+ des Europarates in dieser Frage spielen wird. Auch sie hat ihre Wurzeln in der europäischen Grundrechtstradition, ist aber explizit auch offen für Drittstaaten außerhalb Europas und bietet Hoffnung für eine neue grenzüberschreitende Vertrauensbasis.

Literatur

Abe, Shinzō (2020): Toward a New Era of "Hope-Driven Economy": the Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting. URL: https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (besucht am 16. 02. 2023).

Basu, Arindrajit (2020): The retreat of the data localization brigade: India, Indonesia and Vietnam. *The Diplomat* vom 10. Jan. 2020. URL: https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/ (besucht am 19. 02. 2023).

Beer, Lawrence W. (1981) Group Rights and Individual Rights in Japan. *Asian Survey* 21(4), S. 437–53.

Brugger, Philipp; Hasenclever, Andreas; Kasten, Lukas (2013): Vertrauen Lohnt Sich: Über Gegenstand und Potential eines vernachlässigten Konzepts in den internationalen Beziehungen. *Zeitschrift für Internationale Beziehungen*, 20(2), S. 65-104.

Casalini, Francesca und López, González Javier (2019): Trade and Cross-Border Data Flows. *OECD Trade Policy Papers*, No. 220, Paris: OECD Publishing.

Chan, Joseph (1995): The Asian Challenge to Universal Human Rights: A Philosophical Appraisal. In: Tuck-Hong Tang, James (Hrsg.): *Human Rights and International Relations in the Asia Pacific Region*. London: Pinter, S. 25-38.

Chatterjee, Sheshadri (2019): Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. *International Journal of Law and Management*, 61(1), S. 170-190.

de Vries, Byung Sook und Meijknecht, Anna (2010): Is There a Place for Minorities' and Indigenous Peoples' Rights within ASEAN?: Asian Values, ASEAN Values and the Protection of Southeast Asian Minorities and Indigenous Peoples. *International Journal on Minority and Group Rights*, 17(1), S. 75-110.

Fabbrini, Federico und Celeste, Edoardo (2020): The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 21(S1), S. 55-65.

Feng, Yang (2019): The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, 27(1), S. 62-82.

Finck, Michèle und Pallas, Frank (2020): They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), S. 11-36.

Freeman, Michael (1996): Human rights, democracy and 'Asian values'. *The Pacific Review*, 9(3), S. 352-366.

Geller, Anja (2020): How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective. *GRUR International*, 69(12), S. 1191-1203.

Ghai, Yash (1993), Asian Perspectives on Human Rights. *Hong Kong Law Journal*, 23(3), S. 342-357.

Greenleaf, Graham (2019): G20 Makes Declaration of 'Data Free Flow With Trust': Support and Dissent. *Privacy Laws & Business International Report*, 160, S. 18-19.

Helberger, Natali; Zuiderveen Borgesius, Frederik; Reyna, Agustin (2017): The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law. *Common Market Law Review*, 54(5), S. 1427-1465.

Heper, Joshua (2022): Schrems als Handlungsauftrag: die Zukunft internationaler Datentransfers aus europäischer Perspektive. *Jahrbuch für Vergleichende Staats-und Rechtswissenschaften*, S. 125-154.

Joo, Moon-Ho und Kwon, Hun-Yeong (2023): Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, S. 1-12.

Lynskey, Orla (2018): Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. *Modern Law Review*, 78(3), S. 522-534.

Park, Sung-Uk; Park, Moon-Soo; Park, Soo-Hyun; Yun, Young-Mi (2020): Keywords Analysis on the Personal Information Protection Act: Focusing on South Korea, the European Union and the United States. *Asian Journal of Innovation and Policy*, 9(3), S. 339-359.

Purtova, Nadezhda (2018): The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), S. 40-81.

Rustad, Michael L. und Koenig, Thomas H. (2019): Towards a Global Data Privacy Standard. *Florida Law Review* 71(2), S. 365-454.

Rzeszucinski, Pawel (26. Mai 2022): Be Ready For The Brussels Effect — It's Coming To Data And AI, Forbes. URL: https://www.forbes.com/sites/forbestechcouncil/2022/05/26/be-ready-for-the-brussels-effect---its-coming-to-data-and-ai/?sh=3d23f7bf3036 (besucht am 16. 02. 2023).

Schwartz, Paul M. und Solove, Daniel J. (2014): Reconciling Personal Information in the United States and European Union. *California Law Review,* 102(4), S. 877-916.

Solove, Daniel J. und Hartzog, Woodrow (2014): The FTC and the new common law of privacy. *Columbia Law Review*, 114(3), S. 584-676.

Sury, Ursula (2020): Die Auswirkungen des EuGH-Urteils C-311/18 „Schrems-II" auf den Datenaustausch mit den USA. *Informatik Spektrum*, 43, S. 354-355.

Tomuschat, Chrisitan (2003): Human Rights. Between Idealism and Realism. Oxford: Oxford University Press.

Tracol, Xavier (2015): Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it. *Computer Law & Security Review*, 31(1), S. 112-119.

Wang Han, Sarah und Bakar Munir, Abu (2018): Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? *European Data Protection Law Review,* 4, S. 535-541.

World Economic Forum (WEF) (2023): Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows, Briefing Paper. URL: https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf (besucht am 17. 02. 2023).

Zetoony, David (2022): Navigating the Chaos of the CCPA: The Most Frequently Asked Questions When Implementing Privacy Programs. *Loyola University Chicago Journal of Regulatory Compliance (JRC)*, 8, S. 1-17.

Zuiderveen Borgesius, Frederik (2017): The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. *European Data Protection Law Review (Eur. Data Prot. L. Rev.)*, 3(1), S. 130-137.