Schutz der Privatsphäre in einer vernetzten Welt

Unter besonderer Berücksichtigung des „Rechts auf Vergessenwerden“

Yuko Nishitani[*]

I. Einleitung

In diesem Beitrag geht es um den Schutz der Privatsphäre in einer vernetzten Welt unter besonderer Berücksichtigung des „Rechts auf Vergessenwerden“. Die Entstehung einer vernetzten Welt in der „Society 5.0“ hat heute eine andere Dimension als das traditionelle Internet. Bisher, in der „Society 4.0“, waren Informationen in erster Linie auf bestimmte Webseiten gestellt und dort von Menschen abrufbar. Die Datenübertragung erfolgte durch menschliche Handlung über die elektronische Telekommunikation. Heute werden Massendaten durch unterschiedliche Medien interaktiv oder automatisch weltweit verbreitet. Dazu zählen u. a. die Suchmaschinen wie „Google“ oder

---

* Yuko Nishitani, Professorin der Universität Kyōto, Japan. Dieser Beitrag beruht auf dem Vortrag der Autorin, den sie auf der Tagung „Shaping the Law for a Society 5.0“ am 6. Juli 2018 in Bochum gehalten hat. Der vorliegende Text ist aktualisiert, hat aber weitgehend das Format des Vortragstextes beibehalten, und die Fußnoten sind auf ein Minimum beschränkt. Die Autorin bedankt sich herzlichst bei Frau Karla Rupp-Alene für ihre Korrekturarbeit und Herrn Prof. Dr. Peter Windel, Herrn Prof. Dr. Karl Riesenhuber, Herrn Prof. Dr. Frank Rosenkranz und Herrn Dr. Robert Korves für ihre freundliche Einladung und die Gastfreundschaft in Bochum.

die „Social Networking Services“ (SNS) wie etwa „Facebook“. Mithilfe akkumulierter personenbezogener Daten können die Eigenschaften, Interessen und Meinungen einer Person ohne Mühe analysiert und beeinflusst werden. Dass sogar das Wahlergebnis eines mächtigen Staates auf diese Weise beeinflusst worden sein dürfte, zeigt die Dimension der Problematik.

Vor diesem Hintergrund leuchtet sofort ein, wie wichtig es ist, den Schutz der Privatsphäre und denjenigen personenbezogener Daten in der heutigen vernetzten Welt zu gewährleisten. Denn sind erst einmal Daten ins Netz gestellt, egal ob sie der Wahrheit entsprechen oder nicht, werden sie sofort grenzenlos verbreitet. Es ist erforderlich, Mechanismen zu schaffen, mithilfe derer die Bürger ihre eigenen Informationen kontrollieren können. Diese Problematik wird z. Z. sowohl in Europa als auch in Japan und den USA vielfach diskutiert.

Im Folgenden wird zuerst kurz der allgemeine rechtliche Rahmen zum Datenschutz in der EU, Japan und den USA dargestellt. Die Datenschutz-Grundverordnung der EU (DS-GVO) von 2016[1] spielt eine wichtige Rolle, und zwar nicht nur in Europa, sondern auch in den USA und Japan (II.). Anschließend wird als eine besondere Problematik mit Beispielcharakter, auf das „Recht auf Vergessenwerden“, das „right to be forgotten“, eingegangen. Der EuGH hat 2014 in seiner „Google“-Entscheidung ein „Recht auf Vergessenwerden“ angeregt und damit für große Aufmerksamkeit gesorgt (III.). Es gilt vor allem darüber nachzudenken, ob und inwieweit das „Recht auf Vergessenwerden“ grenzüberschreitend gewährleistet werden kann. Dabei ist auf die konkurrierenden Rechte von Nutzern und Anbietern zu achten. Es besteht ein Spannungsverhältnis zwischen dem Schutz der Privatsphäre einerseits und der Informations- und Meinungsfreiheit andererseits. Ferner entstehen kollisionsrechtliche Fragen, wobei die Qualifikation des „Rechts auf Vergessenwerden“ noch nicht eindeutig beantwortet ist (IV.). Einige zusammenfassende Betrachtungen schließen den Beitrag ab (V.).

II. Rechtlicher Rahmen des Schutzes der Privatsphäre und der personenbezogenen Daten

1. Datenschutz-Grundverordnung in der EU

Die Datenschutz-Grundverordnung der EU von 2016 schafft den wichtigsten rechtlichen Rahmen zum Schutz der Privatsphäre und der personenbe-

1 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, ABl. EU vom 4.5.2016, L 119/1.

zogenen Daten. Sie hat die EG-Richtlinie von 1995[2] überarbeitet und abgelöst. Die Datenschutz-Grundverordnung geht jedoch weit darüber hinaus, indem sie unmittelbar für alle Mitgliedstaaten und Bürger rechtlich verbindlich ist und sehr ausführliche Regelungen enthält. Ziel der Datenschutz-Grundverordnung ist es, den einzelnen Personen das Recht auf Kontrolle über ihre eigenen Informationen zu verleihen und damit die Art und Weise einzuschränken, wie Organisationen personenbezogene Daten nutzen und verbreiten.[3] Daher hat die Verordnung sowohl die Schaffung privatrechtlicher Handlungs- und Entscheidungsnormen als auch die öffentlichrechtliche Regulierung zum Gegenstand. Die Europäische Kommission hat im Januar 2017 ferner einen Vorschlag für eine Verordnung über den Schutz der Privatsphäre und elektronische Kommunikation (ePrivacy) vorgelegt, so dass eine weitere Gesetzgebung zur Regulierung der Cookies und sonstiger Datenspeicherung im Internet zu erwarten ist.[4]

Die Datenschutz-Grundverordnung schafft eine ganze Reihe von Individualrechten. Erstens hat die betroffene Person ein „Auskunftsrecht“ (Art. 15 DS-GVO), das heißt, sie kann sich erkundigen, ob und inwieweit welche ihrer personenbezogenen Daten verarbeitet werden. Zweitens ist ein „Recht auf Berichtigung“ (Art. 16 DS-GVO) gewährleistet, so dass eine unverzügliche Berichtigung unrichtiger personenbezogener Daten verlangt werden kann. Drittens ist, worauf noch näher einzugehen sein wird, ein „Recht auf Löschung“ personenbezogener Daten, nämlich das „Recht auf Vergessenwerden“ (Art. 17 DS-GVO), vorgeschrieben. Darüber hinaus haben die Bürger auch ein „Recht auf Einschränkung der Datenverarbeitung“ (Art. 18 DS-GVO), ein „Recht auf Datenübertragbarkeit“ (Art. 20 DS-GVO) und ein „Widerspruchsrecht“ (Art. 21 DS-GVO). Die betroffene Person hat auch das Recht, nicht einer automatisierten Verarbeitung, u. a. einem Profiling, unterworfen zu werden (Art. 22 DS-GVO).

Diese Palette der Individualrechte beruht auf dem Gedanken, dass der Datenschutz in Europa als Grundrecht gewährleistet ist. Das „Recht auf informationelle Selbstbestimmung“ ist nämlich in der EU-Charta und der

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG vom 23.11.1995, L 281/31.

3 P. CAREY (Hrsg.), Data Protection. A Practical Guide to UK and EU Law (5. Aufl., Oxford 2018) 2.

4 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10. Januar 2017, COM(2017) 10 final.

EMRK (Art. 8 Abs. 1 Charta; Art. 8 Abs. 1 EMRK) ebenso verankert[5] wie im deutschen GG (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). In Europa gilt der Datenschutz als eine Frage der Menschenwürde.[6]

2. USA

Diese Normenverflechtung der Datenschutz-Grundverordnung in der EU ist nicht ohne Einfluss auf die Weltmärkte geblieben, wobei in den USA zum Datenschutz aber nur vereinzelte Bundesgesetze vorhanden sind.[7] Zwischen den USA und der EU ist 2016 ein Abkommen geschlossen worden, um einen gemeinsamen Rahmen zum Datenschutz („Privacy Shield") [8] zu schaffen. Inwieweit sich allerdings die in der Datenschutz-Verordnung verankerten Individualrechte in den USA durchsetzen lassen, bleibt noch abzuwarten, zumal nach dem U.S.-amerikanischen Verständnis der Grundrechte auf die Informations- und Meinungsfreiheit der Betreiber mehr Wert gelegt wird als in Europa. Das diesbezügliche Urteil des U.S. Supreme Court vom 22. Juni 2018 könnte auf diese Abwägung einen gewissen Einfluss haben, indem es zum Schutz der Privatsphäre im digitalen Zeitalter

5 Art. 8 der Charta der Grundrechte der Europäischen Union (ABl. EU 2016 C 202/389) regelt den Schutz personenbezogener Daten wie folgt: „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

6 Der Präsident der Europäischen Kommission, *Jean-Claude Juncker,* äußerte 2016, dass in Europa „der Schutz der Privatsphäre eine Rolle" spiele: „Das ist eine Frage der Menschenwürde", siehe J.-C. JUNCKER, Lage der Union 2016: Hin zu einem besseren Europa – einem Europa, das schützt, stärkt und verteidigt (gehalten in Straßburg am 14.9.2016), abrufbar unter: *http://europa.eu/rapid/press-release_IP-16-3042_de.htm.* Auch zitiert in: H. MIYASHITA, *EU ippan dēta hogo kisoku* [Über den Schutz allgemeiner Daten in der EU] (Tōkyō 2018) 2.

7 Das sind insbesondere der „Children's Online Privacy Protection Act 1998" (15 U.S.C. §§ 6501 ff.), der „Gramm-Leach-Bliley Act 1999" in Bezug auf Kreditinstitute (15 U.S.C. §§ 6801 ff.), der „Fair Credit Reporting Act 2003" zum Schutz der auf Verbraucher bezogenen Daten (15 U.S.C. §§ 1681 ff., erlassen durch den „Fair and Accurate Credit Transactions Act 2003, der allgemeine „Privacy Act 1974" (5 U.S.C. § 552a.) und der „Video Privacy Protection Act 1988" (18 U.S.C. § 2710). Siehe dazu H. MORI (Hrsg.), *Nichi/Bei/Ou kojin jōhō hogo & data protection no kokusai jitsumu* [Internationale Praxis zum Datenschutz in Japan, den USA und der EU] (Shōji Hōmu 2017) 132 ff.

8 Siehe dazu *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.*

von den Bundesstaaten im Allgemeinen die Festschreibung eines Genehmigungserfordernisses verlangte, um von Mobiltelefonunternehmen Daten über die physische Präsenz der Kunden zu erhalten.[9]

3. Japan

a) Anpassung an die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung der EU hat in Japan große Aufmerksamkeit erregt. Es sind bereits zahlreiche Bücher und Sonderausgaben von Zeitschriften spezifisch zu der Verordnung erschienen. Der Grund dafür ist nicht nur, dass die Verordnung für japanische Unternehmen, die ihre Niederlassung in der EU haben oder die zum Zweck ihrer Geschäfte personenbezogene Daten der in der EU befindlichen Personen verarbeiten, unmittelbar relevant ist (Art. 3 Abs. 2 DS-GVO). Die Verordnung ist auch extraterritorial anwendbar. Vor allem sind in der EU gesammelte personenbezogene Daten nur in diejenigen Drittstaaten übertragbar, die ein angemessenes Schutzniveau bieten (Art. 44 DS-GVO). Dazu müssen Drittstaaten entweder von der Europäischen Kommission einen Angemessenheitsbeschluss erhalten (Art. 45 DS-GVO) oder es müssen in Einzelfällen geeignete Garantien bzw. Ausnahmen vorliegen (Art. 46 bzw. 49 DS-GVO). Damit soll im Ausland grundsätzlich das gleiche Schutzniveau wie das der Datenschutz-Grundverordnung erreicht werden, wodurch die EU ihre eigenen Regulierungsinteressen, gegebenenfalls mit Geldbußen, durchzusetzen vermag.[10]

Um die Qualifikation durch den Angemessenheitsbeschluss hat sich die japanische Datenschutzkommission unter der Führung des Kabinetts seit Mitte 2017 bemüht. Aufgrund sorgfältiger Vorbereitungen und Verhandlungen mit den zuständigen Stellen der EU hat die japanische Datenschutzkommission mehrere „Richtlinien zum Schutz personenbezogener Daten“ erlassen,[11] die zusätzlich zu den vorhandenen gesetzlichen Vorschriften (vgl. Art. 6 Datenschutzgesetz)[12] eine Anpassung an die Datenschutz-

9 US Supreme Court, 22.6.2018, *Carpenter v. United States* (abrufbar unter: *https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf*). Der Präsident des Supreme Court, Chief Justice John G. Roberts, hat dazu festgestellt: „We decline to grant the state unrestricted access to a wireless carrier's database of physical location information“; zit. bei A. LIPTAK, In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy, New York Times, 22.6.2018, abrufbar unter: *https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html/*.

10 MORI (Hrsg.) (Fn. 7) 219 ff.

11 Abrufbar auf der Webseite der Datenschutzkommission: *https://www.ppc.go.jp/personalinfo/legal/*.

Grundverordnung der EU ermöglichen sollen.[13] Mit dem Abschluss der Überprüfung des Datenschutzniveaus Japans seitens der EU am 17.7.2018 wurden zugleich zwischen der EU und Japan das „Economic Partnership Agreement" (EPA) sowie das „Strategic Partnership Agreement" (SPA) abgeschlossen. Der Datenschutz wurde also im Rahmen der völkerrechtlichen Handelsabkommen verankert,[14] womit Japan am 23.1.2019 als der 13. Staat auf der Welt einen Angemessenheitsbeschluss der Europäischen Kommission erhalten hat.[15]

b) Rechtslage in Japan

Zur Rechtslage des Datenschutzes in Japan ist zunächst darauf hinzuweisen, dass der Schutz der Privatsphäre und personenbezogener Daten verfassungsrechtlich nicht ausdrücklich vorgeschrieben ist. Er wird aber im Wege der Auslegung aus Art. 13 der japanischen Verfassung abgeleitet, der die Achtung der Würde des Individuums und sein Recht auf Streben nach Glück („pursuit of happiness") als Persönlichkeitsrecht festschreibt.

Auf der einfachgesetzlichen Ebene ist ein dualistischer Schutzmechanismus vorhanden. Einerseits gibt es das Datenschutzgesetz von 2003, das als Grundlagengesetz zum Datenschutz nicht nur die staatlichen und kommunalen Verwaltungskörperschaften, sondern auch die Internet- und Mobiltelefonanbieter als Adressaten erfasst.[16] Andererseits garantiert das Gesetz über die elektronische Kommunikation von 1984[17] die Vertraulichkeit einer solchen Kommunikation. Damit sind die Mobilfunkbetreiber und Internetanbieter zur Geheimhaltung der über sie abgewickelten Kommunikationen verpflichtet, und im Falle einer Verletzung dieser Pflicht unterliegen sie

12 *Kojin jōhō no hogo ni kansuru hōritsu* [Gesetz über den Schutz personenbezogener Daten], Gesetz Nr. 57 vom 30.5.2003, zuletzt geändert durch das Gesetz Nr. 16 vom 31.5.2019.

13 S. FUJIWARA, *Nihon to EU no kojin jōhō hogo hōsei no hikaku* [Vergleichender rechtlicher Rahmen zum Datenschutz in Japan und der EU], Jurisuto 1521 (2018) 19.

14 S. FUJIWARA, *GDPR o meguru hōteki kadai – tokushoku to ryūiten* [Rechtliche Fragen um die DS-GVO: Charakteristika und Anmerkungen], Jurisuto 1534 (2019) 15.

15 Die sonstigen Staaten hatten einen Angemessenheitsbeschluss aufgrund der Datenschutz-Richtlinie 95/46/EG erhalten (es sind bislang Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay sowie die USA). Siehe dazu die Webseite der Europäischen Kommission (abrufbar unter: *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*).

16 Darüber hinaus gibt es eine Auslegungsrichtlinie, die den Gesetzestext an die digitale Kommunikation anpassen soll.

17 *Denki tsūshin jigyō-hō* [Gesetz über die elektronische Kommunikation], Gesetz Nr. 86 vom 25.12.1984, zuletzt geändert durch das Gesetz Nr. 5 vom 17.5.2019.

straf- und verwaltungsrechtlichen Sanktionen. Die beiden Gesetze erzielen die regulatorische Steuerung von Handlungen der Anbieter mittels straf- und verwaltungsrechtlicher Sanktionen, nicht aber schaffen sie Individualrechte. Als privatrechtliche Rechtsbehelfe kommen mithin nur vertragliche oder deliktische Ansprüche in Frage.

Zur Anpassung des Schutzniveaus an die Datenschutz-Grundverordnung der EU ist anzumerken, dass die oben genannten „Richtlinien" auf die Regulierung des Handelns der Anbieter ausgerichtet sind. Es ist allerdings nicht klar, ob damit ein hinreichender Mechanismus zum Datenschutz geschaffen werden kann, zumal die oben genannten, in der EU-Grundverordnung enthaltenen Individualrechte, wie die Auskunfts- und Berichtigungsrechte sowie das „Recht auf Vergessenwerden", in den japanischen Richtlinien nicht vorhanden sind. Damit diese subjektiven Rechte privatrechtlich als individual einklagbare Rechte ausgestaltet werden können, muss sich noch eine entsprechende Rechtsprechung in Japan entwickeln, was dauern kann. Japanische Unternehmen müssen jedoch stets darauf achten, dass die durch die Datenschutz-Grundverordnung verankerten Rechte der EU eingreifen können, wenn und soweit es sich um auf dem europäischen Markt verarbeitete personenbezogene Daten handelt. Dies könnte tatsächlich zu einem Problem werden, zumal bei Verstößen Geldbußen von bis zu 20 Millionen EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des Unternehmens angeordnet werden können.[18]

III. Recht auf Vergessenwerden

1. EU

a) „Google"-Fall

Die Entscheidung des EuGH vom 13.5.2014 im sogenannten „Google"-Fall wird oftmals als das erste Urteil zitiert, das ein „Recht auf Vergessenwerden" anerkannt hat, ohne es jedoch ausdrücklich anzusprechen.[19] In dem Fall ging es um einen Spanier mit Wohnsitz in Spanien, der sich 2010 beschwerte, dass bei der Google-Suchmaschine Links zu einer Tageszeitung von 1998 auftraten, die auf eine Anzeige zur Versteigerung seines Hauses wegen seiner Schulden aufgrund nichtgezahlter Beiträge für die Sozialversicherung hinwiesen. Die Frage war, ob Google Spain und Google Inc. aufgrund der damaligen Datenschutz-Richtlinie von 1995 verpflichtet gewesen waren, diese personenbezogenen Daten zu löschen.

18 Im Falle des Verstoßes gegen die Regelungen der Datenschutz-Grundverordnung ist die Verhängung einer Geldbuße vorgesehen (Art. 83 DS-GVO).

19 EuGH, 13.5.2014, *Google Spain SL & Google Inc. ./. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González*, Rs. C-131/12, ECLI:EU:C:2014:317.

Der EuGH hat diese Frage bejaht. Er legte dar, dass jede betroffene Person das Recht habe, von dem Verantwortlichen die Berichtigung, Löschung oder Sperrung von Daten zu erhalten, wenn ihre Verarbeitung nicht angemessen oder zweckmäßig sei. Es sei dafür nicht erforderlich, dass die Suchergebnisse konkrete Schäden verursachten. Der Grund hierfür ist darin zu sehen, dass der Eingriff in das Grundrecht auf Datenschutz bei der Suchmaschine gravierender ausfällt als bei der einfachen Einstellung von Informationen auf eine Webseite, zumal die Suchmaschine den Zugang zu Informationen in weitestem Umfang ermöglicht. Auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten kann im Laufe der Zeit nicht mehr den ursprünglichen Zwecken entsprechen. Damit haben die Betreiber der Suchmachine eine eigene, von der Informationsquelle unabhängige Verpflichtung, die betreffenden Links zu beseitigen.

b) Art. 17 der Datenschutz-Grundverordnung

Mit der Verabschiedung der Datenschutz-Grundverordnung von 2016 ist das „Recht auf Vergessenwerden" gesetzlich verankert worden. Dieses Recht ist dann zu beachten, wenn die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr notwendig sind, die betroffene Person ihre Einwilligung widerruft oder Widerspruch einlegt, oder wenn die Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 DS-GVO). Andererseits sind einige Rechtfertigungsgründe zum Schutz des Verantwortlichen vorgesehen. Ein Rechtfertigungsgrund liegt beispielsweise dann vor, wenn die Verarbeitung der Daten zur Ausübung der Meinungs- bzw. Informationsfreiheit oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 17 Abs. 2 DS-GVO). Wie die Grenze zwischen den konkurrierenden Interessen zu ziehen ist, bleibt der weiteren Entwicklung der Rechtsprechung und der akademischen Diskussion überlassen.

2. USA

Bezüglich der USA ist anzumerken, dass es gemäß dem „First Amendment" der Bundesverfassung in erster Linie gilt, die Meinungsfreiheit zu gewährleisten. Man steht dort dem „Recht auf Vergessenwerden" skeptisch gegenüber, weil es als eine Art „Zensur" missbraucht werden und die Massenmedien oder die SNS unnötig abschrecken könnte. Vielmehr wird auf das Recht der Bürger, die Wahrheit zu erfahren, oder auf die Informations- und Meinungsfreiheit der Anbieter abgestellt.[20]

20 H. MIYASHITA, *Netto shakai to „wasurerareru kenri" no igi to kadai. Amerika to yōroppa no giron o tegakari ni* [Internet-Gesellschaft und die Bedeutung und die Fragen bezüglich des „Rechts auf Vergessenwerden". Anhand des Diskussions-

3. Japan

In Japan hat der Oberste Gerichtshof (OGH) in seinem Beschluss vom 31.1.2017 zum ersten Mal zu dieser Frage Stellung genommen.[21] Der japanische Kläger war strafrechtlich verurteilt, weil er mit einer Schülerin eine sexuelle Beziehung gegen Bezahlung eingegangen und damit eine Minderjärigenprostitution vorlag. Drei Jahre nach der Verurteilung und Begleichung der Geldstrafe machte er gegen Google Inc. aufgrund der Persönlichkeitsverletzung einen Anspruch auf Beseitigung sowie Unterlassung geltend und verlangte, die Informationen über sein Verbrechen aus der Suchmaschine zu löschen. Der OGH hat die Klage abgewiesen.

Ohne ein einziges Mal den Begriff „Recht auf Vergessenwerden" zu verwenden, hat der OGH diese Frage im Rahmen des Rechts auf den Schutz der Privatsphäre behandelt. Der OGH hat sich auf eine einzelfallbezogene Interessenabwägung gestützt und danach gefragt, ob die Interessen des Individuums an der Löschung der Information diejenigen der Allgemeinheit an deren Veröffentlichung überwogen. Im Ergebnis hat der OGH die Meinungsfreiheit von Google und das allgemeine Interesse der Öffentlichkeit an der Kenntniserlangung der Minderjährigenprostitution, die ein schweres Verbrechen darstellt, respektiert. Zwar hat es der OGH nicht ausgeschlossen, dass im Einzelfall die Interessen einer Privatperson, ihre personenbezogenen Informationen nicht publik machen zu lassen, gegebenenfalls die Interessen der Plattformbetreiber, Informationen anbieten zu können, überwiegen können. Dennoch scheinen die Richter auf die Funktion der Suchmaschine als einer Infrastruktur zur Informationsverbreitung großen Wert zu legen, da diese die Gesellschaft wesentlich beeinflusst und deren Anzeige von Suchergebnissen zugleich als eine auf der Datenverarbeitung beruhenden Meinungsäußerung des Plattformbetreibers schutzwürdig erscheint. Damit stößt die Betreibung einer Suchmaschine nur dann an ihre Grenzen, wenn die individuellen Interessen am Schutz der Privatsphäre *offensichtlich* überwiegen.

Anzumerken ist allerdings, dass heutzutage mächtige Internetanbieter oder Plattformbetreiber, wie „GAFA" (Google, Amazon, Facebook und Apple), eine starke Stellung innehaben und tatsächlich den Markt, und teilweise auch die Politik, beeinflussen können. Ihre Verarbeitung personenbezogener Daten hat daher auf die gesamte Wirtschaft und Gesellschaft eine entscheidende Auswirkung, was den Schutz der Privatsphäre eines

---

stands in den USA und Europa], in: Y. Okuda (Hrsg.), *Netto shakai to wasurerareru kenri. Kojin data sakujo no saibanrei to sono hōri* [Internet-Gesellschaft und das Recht auf Vergessenwerden. Gerichtsentscheidungen zur Löschung personenbezogener Daten und ihre rechtlichen Gründe] (Tōkyō 2015) 3 ff.

21 Oberster Gerichtshof Japans, 31.1.2017, Minshū 71-1, 63.

jeden Individuums aufs Spiel setzen kann. Um „GAFA“ und sonstige Internetanbieter einer verwaltungsrechtlichen Regulierung zu unterwerfen, werden zur Zeit in Japan gesetzliche Maßnahmen zur Stärkung des Kartellrechts erwogen, damit die Wettbewerbsbehörde zur Kontrolle und Beseitigung des Missbrauchs einer „marktbeherrschenden Stellung“ durch einen Internetanbieter eingreifen kann. Ob und wie aber die Individualrechte auf Berichtigung oder Vergessenwerden direkt oder indirekt durchgesetzt werden können, dürfte indes noch abzuwarten sein.

IV. IPR-Fragen zum „Recht auf Vergessenwerden“

Während in Europa das „Recht auf Vergessenwerden“ als Grundrecht konzipiert und in der Datenschutz-Grundverordnung verankert worden ist, hat es sich in den USA oder Japan noch nicht als subjektives Recht durchgesetzt. Damit fallen die Interessenabwägung und die Grenzziehung hinsichtlich der Informationsverbreitung in diesen Ländern unterschiedlich aus.

Dies beeinflusst die kollisionsrechtlichen Fragen, wenn die betroffene Person gegen einen Diensteanbieter ihr „Recht auf Vergessenwerden“ auszuüben sucht. Zuerst muss die internationale Zuständigkeit der Gerichte bejaht werden, die sich in der EU grundsätzlich nach der Brüssel I-Verordnung richtet.[22] Bemerkenswert ist aber, dass Art. 79 Abs. 2 DS-GVO die internationale Zuständigkeit für Klagen gegen einen Verantwortlichen erweitert, indem der Kläger wahlweise an der Niederlassung des Anbieters oder am eigenen Aufenthaltsort eine Klage erheben kann. In einer dem „Google“-Fall des EuGH entsprechenden Fallkonstellation wird damit die Zuständigkeit der spanischen Gerichte problemlos begründet.[23] Als materielles maßgebendes Recht greift in der EU die Datenschutz-Grundverordnung ein, wobei die Frage noch offenbleibt, ob die Rom II-Verordnung[24]

22 Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (Neufassung), ABl. EU vom 20.12.2012, L 351/1; für die Mosaiktheorie, siehe EuGH, 21.12.2016, *Concurrence SARL ./. Samsung Electronics France SAS, Amazon Services Europe Sàrl,* Rs. C-618/15, IPRax 2017, 605; dazu T. Lutzi, Gerichtsstand am Schadensort und Mosaikbetrachtung bei Wettbewerbsverletzungen im Internet, IPRax 2017, 552.

23 Nach den japanischen Zuständigkeitsregelungen würde man auch auf ein vergleichbares Ergebnis kommen, und zwar gemäß Artt. 3-2 ff. Zivilprozessgesetz, insbesondere aufgrund des Erfolgsorts des Delikts (Art. 3-3 Nr. 8) oder der Pluralität der Parteien (Art. 3-6). Siehe dazu DG Tōkyō vom 30.11.2016, Hanrei Taimuzu 1438, 186.

24 Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht („Rom II“), ABl. EU vom 31.7.2007, L 199/40. In Japan ist strittig, ob zur

trotz des Ausschlusses der Verletzung der Privatsphäre und der Persönlichkeitsrechte aus ihrem Anwendungsbereich (Art. 2 Abs. 2 lit. g Rome II) noch eine Rolle spielen kann.

Ob allerdings ein auf dieser Grundlage in einem EU-Mitgliedstaat gefälltes Urteil in den USA oder Japan anerkannt und vollstreckt werden kann, ist eine andere Frage. Angesichts der Tatsache, dass die Individualrechte nach der Datenschutz-Grundverordnung stärker ausgeprägt sind als in den USA oder Japan, könnte die Anerkennung eines in einem EU-Mitgliedstaat ausgesprochenen Urteils möglicherweise am jeweiligen *ordre public* scheitern, zumal in den USA die konkurrierenden Grundrechte der Informations- und Meinungsfreiheit gegenüber den Individualrechten auf Schutz der Privatsphäre überwiegen würden.[25] Dieses Ergebnis ist zum Schutz der Privatsphäre der betroffenen Person nicht ideal, lässt sich aber wohl nicht vermeiden, solange die Schutzniveaus in verschiedenen Staaten unterschiedlich ausfallen.

Eine weltweite Ubiquitätsanordnung zur Löschung personenbezogener Daten gegen alle Suchmaschinen auf der Welt würde derzeit noch zu weit gehen. Es ist exemplarisch, dass das Haager Übereinkommen über die Anerkennung und Vollstreckung ausländischer Urteile von 2019 in Ermangelung einheitlicher Ausgangspunkte zwischen den Staaten den Schutz der Privatsphäre aus seinem Anwendungsbereich ausgeschlossen hat.[26] Die weitere Entwicklung bleibt mithin der Rechtsprechung und der Lehre überlassen.

V. SCHLUSS

Die rechtlichen Fragen in einer vernetzten Welt kennen keine staatlichen Grenzen. Es ist deshalb wichtig, sich stets vor Augen zu halten, dass weit-

---

Bestimmung des anwendbaren Rechts Art. 19 des Rechtsanwendungsgesetzes (*Hō no tekiyō ni kansuru tsūsoku-hō* [Gesetz über die allgemeinen Regeln über die Anwendung von Gesetzen], Gesetz Nr. 78 vom 21.6.2006) anwendbar ist, welcher die Anknüpfung für Verleumdungen regelt, oder ob das allgemeine Deliktstatut nach Art. 17 Rechtsanwendungsgesetz zur Anwendung kommt.

25 In den USA werden auch ausländische Schadensersatzurteile wegen Verleumdung (Persönlichkeitsverletzung) nur dann anerkannt, wenn der gleiche verfassungsrechtliche Standard der Meinungsfreiheit in dem Urteilsstaat gewährleistet ist. Siehe „Speech Act" (28 U.S.C. §§ 4102 ff.); vgl. M. IWAMOTO, *Beikoku ni okeru gaikoku meiyo kison hanketsu shōnin shikkō-hō to sono wagakuni heno eikyō* [Gesetz über Anerkennung und Vollstreckung ausländischer Urteile aufgrund Verleumdung und sein Einfluss auf Japan], Kokusai Shōtorihiki Gakkai Nenpō 21 (2019) 1 ff.

26 Art. 2 Abs. 1 lit. l der „Hague Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters" (noch nicht in Kraft).

reichende rechtsvergleichende Untersuchungen eine wichtige Rolle spielen. Um eine internationale rechtliche Angleichung zu erreichen, könnte man langfristig die Schaffung eines Einheitsrechts oder zumindest bestimmte *Soft Law*-Mechanismen bzw. die Selbstregulierung der betreffenden Industrien anstreben. Vor diesem Hintergrund kann man die Hoffnung nicht genug betonen, dass wir durch eine weitere Zusammenarbeit zwischen Deutschland bzw. Europa, Japan und den USA viel voneinander lernen und uns gegenseitig bereichern werden.

ZUSAMMENFASSUNG

In der heutigen vernetzten Welt spielt es eine wichtige Rolle, wie man die Verarbeitung und Verwendung personenbezogener Daten reguliert und die Privatsphäre des Einzelnen schützt. Mit der Verabschiedung der Datenschutz-Grundverordnung von 2016 hat die EU einen vollständigen rechtlichen Rahmen geschaffen, der sowohl die öffentlich-rechtliche Regulierung zum Datenschutz als auch die privatrechtliche Rechtsdurchsetzung durch die Betroffenen vorsieht und verschiedene Individualrechte begründet. Im Gegensatz dazu ist der Datenschutz in den USA und Japan noch nicht so weit entwickelt, obwohl die EU durch Handelsabkommen mit den beiden Staaten die Angleichung des Datenschutzniveaus anstrebte. Dieser Befund trifft grundsätzlich auch für den Schutz des „Rechts auf Vergessenwerden" zu, wobei dieses Recht in Japan allmählich durch Rechtsprechung im Rahmen des Schutzes der Privatsphäre des Individuums verankert wird. Der unterschiedliche Schutzstandard sowie der divergierende rechtliche Rahmen des Datenschutzes in der EU, den USA und Japan wirken sich auf die kollisionsrechtliche Ebene aus, in der verschiedene Probleme bisher offen geblieben sind. Weitere Entwicklungen in diesen Ländern werden hoffentlich durch vergleichende Forschungen und regen wissenschaftlichen Austausch gefördert.

SUMMARY

In today's closely connected and digitalized world, regulating the processing and use of personal data and protecting the privacy of individuals are crucial topics. By enacting the 2016 General Data Protection Regulation (GDPR), the EU has constituted a comprehensive legal framework that extends to both public regulation and private enforcement of data protection, done by providing for different individual rights. In the USA and Japan, on the other hand, data protection has not yet developed as far as in the EU, despite the EU having sought to require these countries to achieve a comparable level of data protection through trade agreements. These findings principally apply to the "right to be

forgotten", although this right is gradually finding its way into case law in Japan as the right to privacy. The different state of discussion and the varying legal frameworks for data protection in the EU, the USA and Japan have an impact on the conflict of laws, which still leaves a number of questions unanswered. Further developments in these countries will hopefully be enhanced through comparative research and extensive academic exchanges.