BEITRÄGE

Prof. Dr. Dirk Staudenmayer*

Die Anpassung des Privatrechts an die digitale Wirtschaft

Die Digitalisierung ist einer der Trends dieses Jahrhunderts. Sie wird unsere Wirtschaft und Gesellschaft umwälzen, wie man es nur mit der Industriellen Revolution vergleichen kann.[1] Dabei ist die digitale Wirtschaft nicht ein Sektor oder Teil der Gesamtwirtschaft. Vielmehr wird unsere gesamte Wirtschaft über kurz oder lang digital sein. Es scheint einen politischen, wirtschaftlichen und gesellschaftlichen Konsens zu geben, dass die Digitalisierung überwiegend positive Auswirkungen hat oder zumindest unvermeidbar ist. Hieraus folgt, dass dieser Prozess gesteuert werden sollte, um die positiven Effekte für Wirtschaft und Gesellschaft zu erreichen und mögliche negative Auswirkungen zu vermeiden. Das Recht, darunter auch das Privatrecht, ist eines dieser Steuerungsmittel.

Dabei sind grundlegende Werte unserer Gesellschaft, vor allem die Grundrechte zu bewahren, wie z.B. bei der Nutzung von künstlicher Intelligenz. Das Weißbuch der Europäischen Kommission[2] verfolgt das Ziel der Förderung von künstlicher Intelligenz. Dabei schlägt die Kommission einen Rechtsrahmen vor, bei dem der Mensch im Mittelpunkt steht und der deshalb auch die Grundrechte schützt. Es kann aber auch um andere, für Wirtschaft und Bürger wichtige Ziele gehen, für die das Privatrecht die Instrumente zur Verfügung stellt.[3]

I. Anpassung des Privatrechts an die Erfordernisse der Datenwirtschaft

Eine zentrale Komponente der Digitalisierung ist die Entstehung der Datenwirtschaft.[4] Es wurde gesagt, dass im 21. Jahrhundert Daten die Produktionsfaktoren Grundbesitz und Maschinen als wichtigstes Vermögen ablösen werden.[5] Die Europäische Kommission betont dementsprechend auch, dass Daten im Mittelpunkt der Digitalisierung stehen.[6] Das Privatrecht als Teil eines Regelungsrahmens kann diese Entwicklung fördern und gleichzeitig grundlegende Elemente unserer Wirtschafts- und Wettbewerbsordnung bewahren bzw. weiterentwickeln.

Insbesondere die Verbreitung des Internets der Dinge und die Datafizierung von Fertigungs- und Vertriebsprozessen haben zur Entstehung einer Datenwirtschaft mit einer riesigen Masse von Daten geführt, dem sogenannten Phänomen von „Big Data". Dieses wird (im Englischen) häufig durch drei „V"[7] charakterisiert: high volume, high velocity und high variety.

Einige Beispiele mögen die Mengen, von denen hier die Rede ist, verdeutlichen. Bereits im Jahre 2013[8] verarbeitete Google mehr als 24 Petabytes[9] Daten an einem einzigen Tag. Dies entsprach mehrere tausend Male der Menge des gesamten gedruckten Materials in der Bibliothek des amerikanischen Kongresses. Im selben Jahr wurde die Menge von global gespeicherter Information auf 1.200 Exabytes[10] geschätzt. Wenn man diese Daten auf CD-ROM gespeichert hätte, hätte dies fünf Türme geschaffen, die den Mond erreichen. Das Jahr 2013 liegt allerdings, was die Menge von gespeicherten und verarbeiteten Daten angeht, in der digitalen Steinzeit. Der schnelle Anstieg von verarbeiteten und gespeicherten Daten in den letzten Jahren ist noch viel eindrucksvoller. Es gibt Schätzungen, wonach nur in den Jahren 2016 und 2017 90 % aller weltweit vorhandenen Daten geschaffen wurden.[11] Die Europäische Kommission erwähnt Schätzungen, nach denen die Menge der weltweit produzierten Daten von 33 Zettabyte[12] im Jahr 2018 auf voraussichtlich 175 Zettabyte im Jahr 2025 zunehmen wird.[13]

* Der Autor ist Referatsleiter „Vertragsrecht" der Generaldirektion Justiz und Verbraucherschutz und Honorarprofessor der Westfälischen Wilhelms-Universität Münster. Der vorliegende Beitrag gibt seine persönliche Meinung wieder.

1 Vgl. die grundlegende These von Brynjolfsson/McAfee, The Second Machine Age, 2014, S. 6 ff.

2 Weißbuch zur Künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen vom 19. 2. 2020, COM (2020) 65 final, S. 3.

3 So untersuchen das Weißbuch und der es begleitende Bericht der Europäischen Kommission (über die Auswirkungen künstlicher Intelligenz auf Sicherheit und Haftung vom 19.2.2020, COM (2020) 64 final) auch Fragen der privatrechtlichen Haftung für Schäden, die durch künstliche Intelligenz verursacht werden. S. die Beiträge in *Lohsse/Schulze/Staudenmayer* (Hrsg.), Liability for Artificial Intelligence and the Internet of Things – Münster Colloquia on EU Law and the Digital Economy IV, 2019.

4 Sie ist Gegenstand der Mitteilung der Kommission „Eine europäische Datenstrategie" vom 19.2.2020, COM (2020) 66 final.

5 *Harari*, 21 Lektionen für das 21. Jahrhundert, 4. Aufl. 2020, S. 136.

6 *Harari* (Fn. 6), S. 1.

7 Es ist unklar, wer als Erster die häufig benutzte, weil sehr treffende Beschreibung verwendet hat. In der Zwischenzeit kamen noch andere „V" und Merkmale ohne „V" dazu.

8 Die folgenden Beispiele stammen von *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 8 ff.

9 Ein Petabyte entspricht 10^{15} Bytes.

10 Ein Exabyte entspricht 10^{18} Bytes.

11 S. www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2d35a00560ba, abgerufen am 28. 7. 2019.

12 Ein Zettabyte entspricht 10^{21} Bytes.

13 S. Fn. 5, S. 2.

Die zentrale Frage der Datenwirtschaft, auf die das Privatrecht eine Antwort finden sollte, ist, wer Zugang zu diesen Daten hat[14] und zu welchen Bedingungen man sie wirtschaftlich nutzen kann. Dies betrifft sowohl die Verbraucher- als auch die Unternehmensdimension der Datenwirtschaft. Sollen der Verbraucher bzw. das Datensubjekt einen wirtschaftlichen Vorteil davon haben, wenn sie Zugang zu personenbezogenen Daten gewähren? Und wenn ja, welcher sollte dies sein und wie könnte dies rechtlich ausgestaltet werden? Sollte ein Unternehmen Zugang zu von einem anderen Unternehmen gehaltenen Daten haben, um neue, daten-basierte Produkte und Dienstleistungen entwickeln, bzw. anbieten zu können?[15]

1. Wirtschaftlicher Vorteil für den Verbraucher bei Zugang zu personenbezogenen Daten

Hier sind zunächst die Fälle zu betrachten, bei denen es auch für den Verbraucher in steigendem Maß erkennbar ist, dass er für den Zugang zu seinen Daten in der Tat eine Gegenleistung erhält.

a) Erster Schritt: Zugang zu personenbezogenen Daten als Gegenleistung in der Richtlinie zu Verträgen über digitalen Inhalt

aa) Anwendungsbereich

Bei der Vorbereitung des Richtlinienvorschlags zu Verträgen über digitale Inhalte und Dienstleistungen[16] hatte die Kommission auf der Grundlage von Studien und einer EU-weiten Umfrage in ihrer Gesetzesfolgenabschätzung[17] festgestellt, dass ein relativ großer Teil von digitalen Inhalten oder digitalen Dienstleistungen nicht mit Geld bezahlt, sondern dem Verbraucher gegen Zugang zu personenbezogenen Daten zur Verfügung gestellt wird. Dies war besonders in Märkten der Fall, in denen Zugang zu audio-visuellen Inhalten, wie z.B. zu Sportereignissen gewährt wurde oder der Verbraucher digitale Musik hören, e-Bücher lesen oder digitale Spiele benutzen konnte. Gleichzeitig ging dieser Trend Hand in Hand mit einem immer größer werdenden Bewusstsein der Verbraucher, dass ihre Daten Geld wert sind und dass sie in der Tat mit Daten bezahlen, auch wenn sie Online-Angebote „umsonst" nutzen.[18]

Zusätzlich zur Bedeutung von Daten als „Zahlungsmittel" für die betreffenden Märkte ist es auch belangreich, dass der Übergang zwischen Geschäftsmodellen, die auf Geldzahlung basieren, und solchen auf der Grundlage von Daten als „Zahlungsmittel" fließend ist. Beispielsweise bei sogenannten Freemium Modellen erfolgt der Zugang zu einem digitalen Inhalt zunächst gegen Daten, aber ein späterer Zugang oder ein Upgrade muss dann mit Geld bezahlt werden.

Daher unternahm der europäische Gesetzgeber einen wichtigen ersten Schritt auf dem Weg zu einer rechtlichen Anerkennung der Tatsache, dass der Zugang zu personenbezogenen Daten eine wirtschaftliche Leistung darstellt, für die mit Recht auch eine Gegenleistung erwartet werden kann. Am 20.5.2019 wurde die Richtlinie zu Verträgen über digitalen Inhalt und digitale Dienstleistungen (VDRL)[19] verabschiedet. Sie regelt Gewährleistungsrechte für Verbraucher, die nicht vertragsgemäße digitale Inhalte erwerben. Ihr Anwendungsbereich[20] ist auch eröffnet, wenn personenbezogene Daten in einem Vertrag anstelle einer Gegenleistung in Form einer Geldzahlung gegeben werden.[21] Die Einbeziehung von Daten als Gegenleistung in die VDRL erfasst personenbezogene Daten wie z.B. Name, Emailadresse, Alter, Geschlecht o.Ä., wenn man sich auf einer Webseite für eine „kostenlose" Leistung „registriert". Dabei kommt es auf den Zeitpunkt der Datenübermittlung nicht an.[22] Sie kann unmittelbar nach Vertragsschluss erfolgen oder wie bei der kontinuierlichen Bereitstellung von digitalen Dienstleistungen über einen längeren Zeitraum, z.B. bei sozialen Medien, auch zu einem späteren Zeitpunkt.

Die VDRL stellt damit sicher, dass die Äquivalenzbeziehung zwischen Leistung und Gegenleistung, d.h. hier Daten, gewahrt ist, selbst wenn die Leistung fehlerhaft ist. In diesem Fall stellen die Gewährleistungsrechte die Äquivalenz wieder her.

Aufgrund der wirtschaftlichen und rechtspolitischen Auswirkungen war die Einbeziehung von Daten als Gegenleistung ein im Rat und im Europäischen Parlament (EP) sehr kontroverser Punkt. Dabei stellte die Stellungnahme des Europäischen Datenschutzbeauftragen[23] ein Ende des Meinungsbildes dar. Sie betonte nämlich, dass es einen Markt für personenbezogene Daten wie auch einen Markt für lebende menschliche Organe gäbe. Dies würde aber noch lange nicht bedeuten, dass der Gesetzgeber diese Entwicklung auch billigen müsse. Man könne ein Grundrecht nicht monetarisieren und zum Gegenstand einer

14 *Harari* (Fn. 6), S. 141 meint, dass es „die wichtigste politische Frage unserer Zeit" sein könnte, wie man den Besitz von Daten regelt.

15 Mit dieser Frage beschäftigte sich bereits die Mitteilung der Kommission „Aufbau einer Europäischen Datenwirtschaft" vom 10.1.2017, COM (2017) 9 final, S. 9 ff.

16 KOM(2015) 634 endg. vom 9.12.2015. S. hierzu *Staudenmayer* ZEuP 2016, 801 ff.

17 SWD (2015) 274 final, vom 9.12.2015, S. 15. In Deutschland nehmen 76 % der Internetnutzer ausschließlich oder vor allem Online-Angebote wahr, bei denen kein Geld gezahlt wird; vgl. die Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) „Daten – Ware und Währung", 2014, S. 10, abrufbar unter www.divsi.de.

18 Dies betrifft drei Viertel der deutschen Internetbenutzer. Vgl. DIVSI Studie (ebenda), S. 11.

19 Richtlinie 2019/770, ABl. L 136/1 v. 22. 5. 2019. Zur Einführung über die VDRL s. *Staudenmayer* NJW 2019, 2497 ff. Für eine Vertiefung s. die Kommentierung der VDRL in *Schulze/Staudenmayer*, EU Digital Law, 2020.

20 S. Art. 3 Abs. 1 UA 2.

21 Dies wird begrüßt von *Kern* in: *Stabentheiner/Wendehorst/Zöchling-Jud* (Hrsg.), Das neue europäische Gewährleistungsrecht, 2019, S. 39; *Morais Carvalho* EuCML 2019, 197; *Sein/Spindler* ERCL 2019, 263, *Savin* Copenhagen Business School Law Research Paper Series No 19-35, S. 10 ff., abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3474289.

22 Erwägungsgrund 24.

23 Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, Tz. 69, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf.

gewerblichen Transaktion machen,[24] oder wie es noch plakativer in der Diskussion ausgedrückt wurde, man könne „kein Preisschild auf ein Grundrecht kleben". Dementsprechend betrachtete die Stellungnahme Formulierungen wie „mit Daten zahlen" nicht nur als irreführend, sondern als gefährlich, wenn sie in Rechtsform gegossen würden.[25]

Diese Auffassung übersah geflissentlich, dass Grundrechte schon Gegenstand wirtschaftlicher Transaktionen sind; man denke z.B. an das Recht am eigenen Bild.[26] Vor allem aber war allen in der Debatte klar, dass in der wirtschaftlichen Realität die betreffenden Verträge schon massenweise abgeschlossen werden. Eine irgendwie geartete negative Bewertung dieser Verträge durch den Gesetzgeber wurde daher auch in der Diskussion im Rat und EP nicht ernsthaft ins Auge gefasst. Vielmehr galt es sicherzustellen, dass der Verbraucher in den Fällen, in denen mangelhafter digitaler Inhalt oder digitale Dienstleistungen geliefert werden, nicht ohne Rechte ist, sondern Gewährleistungsrechte hat, die denen für Waren vergleichbar sind.[27]

Die jeweilige Mehrheit in Rat und EP folgte deshalb im Ergebnis dem Kommissionsvorschlag und bezog personenbezogene Daten in den Anwendungsbereich der VDRL ein. Hingegen sind Waren, die nicht mit Geld, sondern mit Daten bezahlt werden, in der gleichzeitig verabschiedeten Richtlinie über den Warenkauf[28], die die 1999 verabschiedete Verbrauchsgüterkaufrichtlinie[29] ersetzt, nicht enthalten. Angesichts dessen, dass eine solche Praxis zum Zeitpunkt des Gesetzgebungsverfahrens – im Gegensatz zu digitalem Inhalt – als nicht eben häufig eingestuft wurde, verzichteten sowohl der Kommissionsvorschlag[30] als auch der Gesetzgeber auf deren Einbeziehung.

Allerdings schlug diese schwierige Diskussion zur Einbeziehung von Daten in den Anwendungsbereich der VDRL sich auch anderweitig in deren Text nieder. Im Kommissionsvorschlag[31] war noch davon die Rede, dass „der Verbraucher (...) eine andere Gegenleistung als Geld in Form personenbezogener (...) Daten erbringt." Die VDRL tut hingegen ihr Möglichstes, Formulierungen zu vermeiden, dass Daten „als Gegenleistung" für digitalen Inhalt gegeben werden. Sie verwendet daher die Formulierung, dass „der Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienstleistungen bereitstellt (...) und der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt", ohne die Leistung, d.h. die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen, mit der Bereitstellung personenbezogener Daten ausdrücklich zu verknüpfen. Dabei kann sie natürlich nicht verbergen, dass es sich ebenso wie bei der Zahlung von Geld um eine Gegenleistung handelt, ohne dass sie ausdrücklich so genannt wird.[32] Weiterhin wird (über-)deutlich klargestellt,[33] dass die Datenschutzgrundverordnung[34] (DS-GVO) Anwendung findet.

Überdies überlässt es die VDRL den Mitgliedstaaten zu beurteilen, ob es sich bei der Zurverfügungstellung von personenbezogenen Daten überhaupt um einen gültigen Vertrag handelt.

Schon der Kommissionsvorschlag[35] verfolgte nicht die Absicht, einen rechtlichen Rahmen für das gesamte Internet zu schaffen. Er wollte dies dadurch erreichen, dass der Verbraucher Daten als Gegenleistung im Rahmen eines Vertrages erbringt und nur diejenigen Daten einbezogen sind, die der Verbraucher „aktiv (...) erbringt". Zusätzlich enthielt der Kommissionsvorschlag eine Definition des Vertragsbegriffes[36]. Die Anforderung desVorliegens eines Vertrages war vor allem deswegen vorgesehen, um so den Rechtsbindungswillen der Parteien sicherzustellen[37]. Die Bedingung der „aktiven" Erbringung von Daten hatte dieselbe Zielrichtung. Sie verfolgte den Zweck sicherzustellen, dass der Verbraucher sich bewusst war, dass er eine Gegenleistung erbringt und sollte auch Metadaten und IP-Adresssen ausschließen.[38]

Während des Gesetzgebungsprozesses wurden allerdings dann sowohl Begriff als auch Definition des Vertrages sowie die Bedingung der „aktiven" Erbringung von Daten gestrichen. Nur der erste UAbs. von Art. 3 Abs. 1, der die Lieferung von digitalem Inhalt oder Dienstleistungen gegen Geldzahlung betrifft, bezieht sich jetzt auf einen Vertrag. Der zweite UAbs., der die Lieferung von digitalem

24 Ebenda, Tz. 17.
25 Ebenda, Fn. 27.
26 Auch das Gutachten der Datenethikkommission, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=C73BFB1C152B1C36260B34A8E61AE2F3.2_cid364?__blob=publicationFile&v=6, S. 104, bekräftigt, dass der verfassungsrechtliche Persönlichkeitsschutz es auch umfasst, geschützte Aspekte zu vermarkten und führt weitere Argument an, warum der Vergleich mit Organhandel nicht angebracht ist.
27 S. Erwägungsgrund 24.
28 Richtlinie 2019/771 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, ABl. L 136/28 v. 22. 5. 2019. Als Einführung hierzu s. *Staudenmayer* NJW 2019, 2889 ff. Für eine Darstellung der Gemeinsamkeiten beider Richtlinien s. *Staudenmayer* ZEuP 2019, 663 ff.
29 Richtlinie 1999/44 v. 25. 5. 1999, ABl. EG L 171/12 v. 7. 7. 1999. Siehe zu dieser Richtlinie *Staudenmayer* in: Grundmann/Medicus/Rolland, Europäisches Kaufgewährleistungsrecht, 2000, S. 27 ff.
30 KOM(2015) 635 endg. v. 9.12.2015.
31 Fn. 17, Art. 3 Abs. 1.
32 Ebenso: *Metzger* JZ 2019, 579; *Kern* (Fn. 23), S. 39; *Schulze* ZEuP 2019, 701, *Sein/Spindler* ERCL 2019, 265; *Savin*, Copenhagen Business School Law Research Paper Series No 19-35, S. 12.
33 In Art. 3 Abs. 8 und den ErwGr 24, 37-40.
34 Verordnung (EU) 2016/679 v. 27. 4. 2016, ABl. 2016, L 119, 1.
35 Art. 3 Abs. 1.
36 Als „eine Vereinbarung, die darauf abzielt, Pflichten zu begründen oder andere rechtliche Wirkungen herbeizuführen". S. Art. 2 Nr 7, der die Definition von Art. 2 (a) der Verordnung über ein Gemeinsames Europäisches Kaufrecht (GEK) (Vorschlag der Kommission v. 11. 10. 2011, KOM (2011), 635 endg.) aufgreift; vgl. auch Article 30 GEK. Als Einführung in das GEK s. *Staudenmayer*, Gemeinsames Europäisches Kaufrecht – Textausgabe 2011, S. VII ff., für eine vertiefte Erklärung s. die Kommentierungen zu diesen Artikeln in *Schulze* (Hrsg.), Common European Sales Law (CESL), 2012.
37 Was in allen europäischen Rechtsssystemen eine Bedingung für einen Vertragschluss ist. S. Note IV.12 DCFR, II.-4:101 in *von Bar/Clive* (Hrsg.), Principles, Definitions and Model Rules of European Private Law – Draft Common Frame of Reference (DCFR) Volume 1 (2009) und von einem rechtsgeschichtlichen und rechtsvergleichenden Standpunkt *Christandl* in: Jansen/Zimmermann (Hrsg.), Commentaries of European Contract Laws, Art 2:101 (1), Tz. 9-15.
38 *Staudenmayer* ZEuP 2016, 808.

Inhalt oder Dienstleistungen betrifft, wenn personenbezogene Daten erbracht werden, enthält dagegen nicht den Begriff des „Vertrages". Dies sollte die Schlußfolgerung vermeiden, dass immer, wenn personenbezogene Daten erbracht werden, auch ein Vertrag vorliegt. Art. 3 Abs. 10 und Erwägungsgrund 12 legen schon allgemein fest, dass die Regeln über Vertragsschluss dem nationalen Recht überlassen sind. Im spezifischen Zusammenhang der Erbringung von Daten überlässt es Erwägungsgrund 24 den Mitgliedstaaten, festzustellen, ob die Anforderungen für einen gültigen Vertragsschluss erfüllt sind.[39] Zusätzlich interpretiert Erwägungsgrund 25 den Begriff des Vertrages dahingehend, dass die Erhebung von Metadaten wie Informationen zum Browserverlauf oder zum Gerät des Verbrauchers nicht als Gegenleistung für einen gültigen Vertrag anzusehen ist, außer wenn das nationale Recht dies so vorsieht.[40]

Von der Sache her geht dieses Ergebnis in dieselbe Richtung wie der Kommissionsvorschlag. Die Formulierung, dass der Verbraucher Daten „bereitstellt", impliziert bereits eine „aktive Erbringung". Ein wesentliches Beispiel von (aus Verbrauchersicht) „passiver" Sammlung von Daten, d.h. Metadaten, ist zudem vom Anwendungsbereich grundsätzlich ausgeschlossen. Während das Ergebnis also sinnvoll ist, ist es eine andere Frage, ob es regelungstechnisch gut war, so vorzugehen. Es wäre vermutlich besser gewesen, das Vertragskriterium beizubehalten. Schließlich geht sogar die DS-GVO davon aus, dass die Einwilligung nicht nur eine einseitige Erklärung ist, sondern im Rahmen eines Vertrages gegeben werden kann. In ihrem Erwägungsgrund 42 postuliert sie nämlich, dass die AGB-Richtlinie[41] auf eine vom Verantwortlichen vorformulierte Einwilligung Anwendung findet, was wiederum das Vorliegen eines (Verbraucher-)Vertrages voraussetzt.

Dem stand allerdings eine allgemeinen Tendenz[42] im Rat entgegen, in der VDRL so wenig wie möglich in die Bereiche des allgemeinen Vertragsrechts einzugreifen. Die Verweisungen auf das nationale Recht hinsichtlich des Zustandekommens eines gültigen Vertrages sind jedenfalls Ausdruck dieser Tendenz.

bb) Offene Fragen

Die Folgen dieser Einbeziehung für das allgemeine Vertragsrecht sind deshalb auch weitgehend dem nationalen Recht überlassen. Dieser Ansatz war aus Sicht der Mitgliedstaaten und im Interesse einer zügigen Verabschiedung der VDRL[43] verständlich. Er lässt aber Fragen offen, die die Behandlung von Daten im Vertragsrecht betreffen; einige Beispiele sollen hier erwähnt werden.

So regelt die VDRL z.B. ausdrücklich nicht, was mit einem Vertrag passiert, wenn der Verbraucher die für die Verarbeitung der Daten gegebene Einwilligung widerruft.[44] Hier wird sich bei der Umsetzung die Frage stellen, welche Auswirkungen die DS-GVO auf das Privatrecht der einzelnen Mitgliedstaaten hat. Dies berührt nicht zuletzt die Struktur eines synallagmatischen Vertrages (und die Kriterien der „consideration", bzw. der „causa"/„cause", wo solche Kriterien in den jeweiligen nationalen Rechten benutzt werden[45]). In der Praxis wird häufig die Einwilligung[46] die Rechtsgrundlage für die Datenverarbeitung sein.[47] Wenn aber der Verbraucher jederzeit seine Gegenleistung, d.h. den Zugang zu den personenbezogenen Daten, widerrufen kann, stellt sich die Frage, welche Auswirkungen das auf die noch zu erbringende Leistung haben soll, z.B. ob man als nationaler Umsetzungsgesetzgeber auch dem Unternehmer ein Widerrufsrecht gewähren sollte.[48] Allerdings muss man hier berücksichtigen, dass in der Praxis die Daten, zu denen Zugang gewährt wird, meistens innerhalb kürzester Zeit nach Vertragsschluss monetarisiert werden.[49] Im Übrigen wird man die DS-GVO-Regeln über die Einwilligung berücksichtigen müssen. Nach Art. 7 Abs. 4 DS-GVO mag die Freiwilligkeit der Einwilligung ein Thema sein, wenn die Einwilligung nach Art. 7 Abs. 3 Satz 1 DS-GVO widerrufen wird und in diesem Fall auch die vertraglich geschuldete Leistung nicht mehr erbracht werden müsste.

Ein anderes Beispiel, das im Gesetzgebungsverfahren diskutiert, aber nicht in der Richtlinie geregelt wurde, ist die Frage, was mit Verträgen über digitale Inhalte oder Dienstleistungen passiert, die mit Daten bezahlt werden, aber bei denen ein Verstoß gegen eine Bestimmung der DS-GVO vorliegt. Einerseits könnte hier argumentiert werden, dass solche Verträge wegen der unmittelbaren Anwendbarkeit der DS-GVO rechtswidrig und damit unwirksam seien. Andererseits würde eine Unwirksamkeit zu dem unerwünschten Ergebnis führen, dass der Verbraucher außer seinen Rechten aus der DS-GVO keine Gewährleistungsrechte mehr hätte. Damit wäre zudem der Unternehmer, der die DS-GVO nicht respektiert, in einer besseren Situation als derjenige Unternehmer, der sich rechtstreu verhält.[50] Da die DS-GVO keine Rechtsfol-

39 *Metzger* JZ 2019, 584 sieht dies zu Recht häufig als gegeben an.
40 Zur Behandlung von Metadaten in der VDRL, s. *Staudenmayer*, Art. 3 VDRL, Tz. 38 in *Schulze/Staudenmayer*, EU Digital Law, 2020.
41 Richtlinie 93/13 über mißbräuchliche Klauseln in Verbraucherverträgen, ABl. L 95/29 v. 21. 4. 1993.
42 S. hierzu *Staudenmayer* ZEuP 2019, 676 ff.
43 Zu den verschiedenen Positionen des Rates und des EP im Gesetzgebungsverfahren hinsichtlich der Verabschiedung der VDRL und der Warenkaufrichtlinie sowie der Auswirkungen des Zeitdrucks s. *Staudenmayer* ZEuP 2019, 667.
44 Erwägungsgrund 40.
45 Hinsichtlich der verschiedenen Ansätze in den nationalen Rechten s. notes IV. 13. – 29. DCFR, II.-4:101 in *von Bar/Clive* (Fn. 38) und von einem rechtsgeschichtlichen und rechtsvergleichenden Standpunkt *Christandl* in: Jansen/Zimmermann (Fn. 38), Art 2:101 (1), Tz. 17-20.
46 .Art. 6 Abs. 1 a) DSGVO.
47 S. auch das Beispiel im Erwägungsgrund 24 Satz 9.
48 Z.B. will die Datenethikkommission (Fn. 27), S. 105, es dem Anbieter ermöglichen, seine Leistung mit sofortiger Wirkung einzustellen, wobei er allerdings keinen Zahlungsanspruch wegen erbrachter Leistung haben soll und ein Zurückfallen in ein Bezahlmodell auch ausgeschlossen sein soll.
49 Vgl. die Stellungnahme des Europäischen Datenschutzbeauftragten (Fn. 24), Tz. 69.
50 P. Hacker, „Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive", in: *Lohsse/Schulze/Staudenmayer* (Hrsg.), Data as Counter performance – Contract Law 2.0?, 2020, S. 59 f.

gen für den Vertrag vorsieht, mag ein vermittelnder Ansatz eine Lösung für die Fälle darstellen, bei denen nur ein Element der Durchführung des Vertrages, aber nicht der ganze Vertrag gegen die DS-GVO verstößt. Ein solcher Ansatz könnte Elemente wie den sachlichen und persönlichen Schutzzweck der Bestimmung der DS-GVO, gegen die verstoßen wurde, und die bereits in der DS-GVO vorgesehenen Sanktionen für den Unternehmer in Betracht ziehen. Er könnte z.B. dazu führen, dass der Vertrag oder die entsprechende vertragliche Leistung nur für die Partei, die gegen eine DS-GVO-Bestimmung verstoßen hat, undurchsetzbar wird.[51]

Ein letztes Beispiel, das allerdings nicht im Gesetzgebungsverfahren diskutiert wurde, betrifft die Frage, was passiert, wenn sich der Verbraucher entsprechend Art. 3 Abs. 1 UAbs. 2 VDRL verpflichtet, Daten bereitzustellen, das aber dann nicht tut. Kann eine solche Verpflichtung seitens des Unternehmers durchgesetzt werden?

Diese Beispiele zeigen, dass das Problem nicht ein eventueller Widerspruch zwischen der VDRL und der DS-GVO ist, den der Gesetzgeber in Art. 3 Abs. 8 UAbs. 2 VDRL glaubte, zu Gunsten der DS-GVO entscheiden zu müssen. Ein solcher Widerspruch besteht nicht. Beide Rechtsakte finden parallel, aber aus verschiedenen Blickwinkeln auf dieselbe Situation Anwendung. Die DS-GVO regelt die Rechte des Datensubjekts, während die VDRL vertragsrechtliche Gewährleistungsansprüche festlegt.

Das Problem ist vielmehr die fehlende vertragsrechtliche Unterfütterung der DS-GVO. Die Regelung von Rechten und Pflichten von Privatrechtssubjekten in der Datenwirtschaft kann nicht nur dem Datenschutzrecht überlassen werden, sondern muss vielmehr auch durch das Privatrecht geregelt werden.[52] Ob dies dazu führt, der Debatte über ein Datenschuldrecht einen weiteren Impuls zu geben[53], ist nicht abzusehen. In Anbetracht der Flexibilität des Vertragsrechts ist es wahrscheinlich unnötig, an ein „Vertragsrecht 2.0" zu denken. Einige Anpassungen, z.B. zur vertragsrechtlichen Unterfütterung der DS-GVO, könnten jedoch durchaus erwägenswert sein.

b) Weitere Schritte?

Die VDRL enthält mit der Einbeziehung von Daten, die in einem Vertrag anstelle einer Gegenleistung in Form einer Geldzahlung gegeben werden, eine bahnbrechende Neuerung und eröffnet damit eine neue Dimension der Anpassung des Privatrechts an den Übergang zur digitalen Wirtschaft. Die langfristige Bedeutung der VDRL mag aber noch hierüber hinausgehen. Sie könnte darin liegen, Änderungen anzustoßen, wie personenbezogene Daten im Wirtschaftsverkehr gesehen und als Gegenstand von Transaktionen rechtlich gehandhabt werden. Dies betrifft Verträge, in denen der Verbraucher die Verarbeitung seiner Daten ermöglicht, ohne dass er eine Gegenleistung (außer weiteren Angeboten für Produkte oder Dienstleistungen)[54] erhält. Dementsprechend erkennt auch die Datenstrategie der Kommission an, dass die VDRL jedenfalls einen ersten Schritt getan hat, Einzelpersonen bei der Ausübung ihrer Rechte zu stärken.[55] Dieser erste Schritt wurde in der Richtlinie zur Modernisierung der Verbraucherschutzvorschriften, die auch Daten als Gegenleistung aufnahm, inzwischen auch bestätigt.[56]

Man kann schlichtweg nicht mehr ignorieren, dass Daten – auch personenbezogene Daten – einen wirtschaftlichen Wert haben und Gegenstand von privatrechtlichen Transaktionen sind. Solche Transaktionen werden bereits jetzt massenhaft abgeschlossen. Verhindern kann man sie nicht mehr; es wäre auch fraglich, ob das sinnvoll wäre. Es ist vielmehr zu erwarten, dass sie in der Zukunft noch stärker wachsen. Das Ziel sollte daher sein, einen passenden (auch Privat-)Rechtsrahmen zur Verfügung zu stellen.

Die Datenethikkommission der Bundesregierung geht davon aus, dass Personen, die an der Generierung von Daten beteiligt sind, z.B. als Datensubjekt, Rechte in Bezug auf diese Daten zustehen.[57] Sie sieht hier ein Recht auf digitale Selbstbestimmung begründet, das über das grundgesetzliche und durch die DS-GVO ausgestaltete Recht auf informationelle Sebstbestimmung hinausgeht. Dieses Recht auf digitale Selbstbestimmung würde auch die selbstbestimmte wirtschaftliche Verwertung der eigenen Datenbestände sowie den selbstbestimmten Umgang mit nicht-personenbezogenen Daten, die etwa durch den Wirkbetrieb eigener Geräte generiert werden, umfassen.[58]

Dies könnte im Wesentlichen auf zwei (eventuell kumulativen) Wegen geschehen.[59] Eine Möglichkeit ist, einen Vermittler einzuschalten, der das Datenmanagement oder die treuhänderisch Verwaltung von Daten für den Verbraucher übernimmt,[60] ähnlich wie z.B. Verwertungsgesellschaften Autorenrechte wahrnehmen und den Autoren Tantiemen zukommen lassen. Solche Vermittler könnten gemeinnützig oder mit Gewinnerzielungsabsicht handeln.

Die zweite Möglichkeit könnte darin bestehen, für solche Daten, die in der Blockchain zur Verfügung stehen, auf den Vermittler und die dadurch entstehenden Kosten zu verzichten und sog. Smart Contracts[61] zu verwenden.[62]

---

51 Vgl. die in DCFR *von Bar/Clive* (Fn. 38), II.-7:302 Abs. 3 genannten Elemente sowie die Comments in C.-E.

52 *Ackermann* ZEuP 2018, 767 f.

53 Vgl. die Beiträge in *Lohsse/Schulze/Staudenmayer* (Fn. 51); *Wendland* ZvglRWiss 2019, 191 (196) m.w.N.

54 Allerdings könnte eine Dienstleistung gerade in der Einholung oder dem Vergleich von Angeboten liegen. In der Regel sollte man aber wohl den Erhalt zusätzlicher Werbung nicht als Gegenleistung ansehen.

55 Fn 5, S. 5.

56 Art. 4 Abs. 2 (b) der Richtlinie 2019/2161, ABl. L 328/7 v. 18. 12. 2019.

57 Fn. 27, S. 82.

58 Fn. 27, S. 17, 85.

59 Vgl. die Datenstrategie der Kommission (Fn. 5), S. 12, 23 f. und die Datenethikkommission (Fn. 27), S. 133 ff.

60 Vgl. *Wendehorst*, „Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", in: Lohsse/Schulze/Staudenmayer (Hrsg.), Trading Data in the Digital Economy: Legal Concepts and Tools – Münster Colloquia on EU Law and the Digital Economy III, 2017, S. 349 ff.

Trotz des irreführenden Namens sind Smart Contracts keine Verträge an sich, sondern Computercode, der es ermöglicht, in der Blockchain[63] Verträge zu schließen und selbständig auszuführen.

In der zugrundeliegenden Vereinbarung würde das Datensubjekt seine Einwilligung zur Datenverarbeitung geben und sich verpflichten, sie nur unter bestimmten Bedingungen, z.B. wenn die andere Vertragspartei ihre Verpflichtungen verletzt, zu widerrufen. Zeitraum und Zweck der Datenverarbeitung sowie die dafür gegebene Gegenleistung könnten präzise nach standardisierten Optionen im Voraus festgelegt werden. Smart Contracts funktionieren in Vereinbarungen, bei denen die entsprechenden Verpflichtungen des betreffenden Vertrages vorhersehbar und objektiv nachprüfbar sind und ihre Ausführung damit programmiert werden kann.

Zum vertragsrechtlicher Schutz des einwilligenden Verbrauchers würde die AGB-Richtlinie auf die zugrundeliegende Vereinbarung Anwendung finden. Bereits die DS-GVO geht in ihrem Erwägungsgrund 42 davon aus, dass eine vom Verantwortlichen vorformulierte Einwilligungserklärung der AGB-Richtlinie mit ihrem Transparenzgebot und den Bestimmungen zu mißbräuchlichen Klauseln unterworfen ist.

Diese Möglichkeit hätte erstens den Vorteil sicherzustellen, dass Verbraucher als Datensubjekte dergestalt Kontrolle über ihre Daten hätten, dass sie einen wirtschaftlichen Nutzen aus der Datenverarbeitung durch andere Parteien ziehen können. Hierbei handelt es sich um ein Ziel, das eine Mehrheit deutscher Verbraucher wohl unterstützen würde.[64] Der zweite Vorteil dieser Lösung wäre es, die Anwendung und Durchsetzung der DS-GVO effektiver zu gestalten. Sie würde über das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO[65] hinausgehen und dessen Grenzen in der praktischen Anwendung[66] vermeiden. Vor allem aber könnte sie angesichts des „erheblichen Vollzugsdefizits im Bereich des Datenhandels“[67] der DS-GVO hilfreich sein. Wenn personenbezogene Daten unter Verstoß gegen die DS-GVO weitergegeben und verarbeitet werden, so bleiben diese Verstöße ungeahndet, solange das Datensubjekt oder die zuständige Behörde nichts davon erfahren. Letztere Kenntnis dürfte in der Praxis aber nur dann gegeben sein, wenn sich der Verantwortliche nicht nur illegal, sondern auch noch ungeschickt verhält, z.B. wenn das Datensubjekt personalisierte Werbung von einer Partei erhält, bei der es sicher ist, dass es die entsprechende Einwilligung nicht gegeben hat. Damit wären Smart Contracts nicht nur eine Möglichkeit, dem Verbraucher einen wirtschaftlichen Vorteil für die Verarbeitung seiner Daten zu sichern, sondern auch ein Mittel, seine Rechte nach der DS-GVO effektiver durchzusetzen.

Beide genannten Wege – die treuhänderische über einen Dritten und die eigenständige Verwaltung von eigenen Daten über Smart Contracts – könnte eine Rolle bei der Entwicklung und Einrichtung „persönlicher Datenräume“[68] spielen.

2. Stärkung der Stellung der Datenhabenichtse gegenüber den Datenbesitzern?

Daten sind das Blut in den Adern der Datenwirtschaft.[69] Immer mehr gegenwärtige, aber noch viel mehr zukünftige, innovative Geschäftsmodelle benötigen Daten. Damit schafft die Datenwirtschaft verschiedene Arten von neuen Abhängigkeiten, die mit der Kontrolle über/dem Zugang zu Daten zusammenhängen.

Eine solche Abhängigkeit kann zunächst mit dem Zugang zur Cloud als der Infrastruktur der Datenwirtschaft zu tun haben. Ein solcher Zugang ist nötig, um digitale Geschäftsmodelle zu betreiben, vor allem, wenn sie auf künstlicher Intelligenz aufbauen. Unter welchen Bedingungen ein Unternehmen Zugang zu den in der Cloud gelagerten Daten hat, kann für sein digitales Geschäftsmodell bedeutsam sein.[70] Abhängigkeiten können auch in der Beziehung zu Plattformen als einer immer wichtigeren und deshalb marktmächtigen Vertriebsform bestehen. Plattformen bringen zwar Angebot und Nachfrage zusammen, werfen aber u.a. die Frage auf, ob und unter welchen Bedingungen Unternehmen, die über sie Produkte und Dienstleistungen vertreiben, Zugang zu den Vertriebsdaten haben.[71] Dieser Beitrag beschäftigt sich mit der Frage, ob und unter welchen Bedingungen Unternehmen, die für die Entwicklung, bzw. das Betreiben ihres Geschäftsmodells Daten benötigen, die einem anderen

61 Zur Einführung vgl.: *De Filippi/Wright*, Blockchain and the Law: The Rule of Code, 2018, S. 72 ff.; *Guggenberger*, „The Potential of Blockchain Technology for the Conclusion of Contracts“, in: Schulze/Staudenmayer/Lohsse (eds.), Contracts for the Supply of Digital Content: Regulatory Gaps and Challenges, Münster Colloquia on EU Law and the Digital Economy II, 2017, S. 85 f., 94 ff.

62 Vgl. auch die Datenstrategie der Kommission (Fn. 5), S. 13.

63 Für einen Überblick über rechtliche Fragen der Blockchain Technologie vgl. *De Filippi/Wright* (Fn. 62). Hinsichtlich der Blockchain Geschäftsmodelle vgl. *Tapscott/Tapscott*, Blockchain Revolution – How The Technology Behind Bitcoin Is Changing Money, Business And The World, 2016, S. 178 ff. Zu mehr grundsätzlichen Fragen hinsichtlich code is law (vgl. *Lessig*, Code, 2nd edition 2006, S. 5) und law is code, die in diesem Beitrag nicht diskutiert werden können, vgl. *De Filippi/Hassan*, Blockchain technology as a regulatory technology: From code is law to law is code, First Monday, 5 December 2016, abrufbar unter https://firstmonday.org/ojs/index.php/fm/article/view/7113.

64 S. DIVSI Studie (Fn. 18), S. 12, 15.

65 *Drexl* jipitec 2017, 286, betont zu Recht, dass Art. 20 DS-GVO eher ein Verbraucherschutz- als ein Datenschutzrecht ist.

66 Vgl. die Datenstrategie der Kommission (Fn. 5), S. 12.

67 Datenethikkommission (Fn. 27), S. 82.

68 Vgl. die Datenstrategie der Kommission (Fn. 5), S. 23 f.

69 So die Datenstrategie der Kommission (Fn. 5), S. 3.

70 Für eine Einleitung in die vertragsrechtliche Problematik s. *Staudenmayer*, „Towards a European Private Law of the Digital Economy? – Trends“, in: Janssen/Schulte-Nölke (Hrsg.), Researches in European Private Law and Beyond – Contributions in Honour of Reiner Schulze's Seventieth Birthday, 2020, S. 81 ff. S. auch die Datenstrategie der Kommission (Fn. 5), S. 10 f., 22, die die Abhängigkeit der digitalen Wirtschaft von Cloud-Infrastrukturen erwähnt sowie auf vertragsrechtliche Probleme hinweist.

71 Für eine Einleitung in die Problematik s. *Staudenmayer* (Fn. 71), S. 78 ff.S. auch die Datenstrategie der Kommission (Fn. 5), S. 9 f.

Unternehmen zur Verfügung stehen, dazu Zugang haben sollten.[72]

a) Zugang zu Daten als Problem

Die Frage des Zugangs zu Daten ist vor allem auch wegen der wachsenden Bedeutung des Internets der Dinge (Internet of Things – IoT) relevant. Die Zahl von IoT-Anwendungen entwickelte sich von 3.81 Milliarden (2.28 im Verbraucherbereich) im Jahre 2014 zu 11.2 Milliarden im Jahre 2018 (7.04 im Verbraucherbereich); für 2019 lautete die Schätzung 20.41 Milliarden (12.86 im Verbraucherbereich).[73] Geschäftsmodelle, die auf dem IoT beruhen, wie z.B. „vorausschauende Instandhaltung"[74] oder „präzise Landwirtschaft"[75] sind nur aufgrund von Zugang zu Daten möglich.

Daten als Ressource haben u.a. zwei hier relevante Eigenschaften. Im Unterschied zu anderen Ressourcen führt der Gebrauch von Daten nicht dazu, dass für andere Nutzer weniger Daten zur Verfügung stehen oder diese abgenutzt sind und deswegen weniger gut benutzt werden können (sog. Nicht-Rivalität). Daten könnten deswegen ohne weiteres geteilt werden.[76] So teilen z.B. Unternehmen Daten, weil sie ein strategisches Interesse haben, Standards für zukünftige Geschäftsmodelle zu beeinflussen oder weil sie dazu anregen wollen, ihre eigenen Dienstleistungen mit anderen Produkten oder Dienstleistungen zu integrieren.

Während die Nicht-Rivalität eigentlich das Teilen von Daten befördern sollte, sind Daten auch eine Ressource, zu der man den Zugang leicht ausschließen kann. In der Praxis bleiben die gesammelten Daten meist innerhalb des Unternehmen, dem sie zur Verfügung stehen. Eine Analyse von vorhandenen Daten wird, wenn überhaupt, meist vom Unternehmen selbst vorgenommen oder an Subunternehmer innerhalb enger vertraglicher Grenzen hinsichtlich z.B. Zweck und Zeitdauer der Nutzung weitergegeben. Benutzt werden die Daten oft zur Effizienzverbesserung interner Prozesse. Wenn sie für die Entwicklung neuer Dienstleistungen benutzt werden, sind diese meist eng mit den traditionellen, nicht datenverwertenden Produkten oder Dienstleistungen verbunden.[77] Wenn Unternehmen nicht ein Eigeninteresse haben, Daten zu teilen, ist es gut möglich, dass Daten nicht oder nur zu einem Preis verkauft werden, der es sehr oder sogar prohibitiv teuer macht, ein auf Daten basierendes Geschäftsmodell zu entwickeln oder zu betreiben.

Das Interesse an Datenzugang kann mit einem Beispiel zur „vorausschauenden Instandhaltung" erklärt werden. Autofahrer könnten bald durch mit dem IoT verbundene Sensoren in ihren Reifen informiert werden, dass das Profil ihrer Hinterreifen weniger als 1,6 mm[78] beträgt und dass diese Reifen ersetzt werden sollten. Zusammen mit dieser Nachricht könnte der Bildschirm in ihrem Auto sie auch informieren, dass die Kosten für zwei Neureifen beim nächstgelegenen Vertragshändler des Autoherstellers 298,99 EUR betragen würden und ihnen die Möglichkeit geben, direkt einen Termin beim Vertragshändler zu vereinbaren. Zusätzlich könnte der Bildschirm dem Autofahrer auch vorschlagen, nicht nur die Hinterreifen, sondern alle vier Reifen zu ersetzen, was beim Vertragshändler für einen Sonderpreis von 398,99 EUR möglich wäre. Falls nicht nur der Autohersteller, sondern auch unabhängige Reparaturbetriebe Zugang zu den Daten hätten, könnten auch sie dem Verbraucher eventuell günstigere Angebote unterbreiten. Zudem könnten nicht nur unabhängige Reparaturbetriebe an den Daten interessiert sein, sondern auch der Reifenproduzent, um sein Produkt zu verbessern, und Kfz-Versicherer, um dem Autofahrer eine auf sein Fahrverhalten zugeschnittene Versicherungspolice anzubieten.

Ähnliche Beispiele könnten auch aus dem Bereich der nicht-personenbezogenen Daten erwähnt werden. So würde sich bei Flugzeugtriebwerken, Fahrzeugen von Speditions- oder Nahverkehrsunternehmen, oder Maschinen jeglicher Art die Frage stellen, ob der Produzent des gesamten Produktes oder eines mit Daten sammelnden Sensoren ausgestatteten Teiles, der Betreiber und unabhängige Reparaturbetriebe Zugang zu den für „vorausschauende Instandhaltung" nötigen Daten haben. Wer sollte also z.B. bei Flugzeugen, deren Triebwerke Daten sammeln, Zugang für die zur Reparatur oder zur „vorausschauenden Instandhaltung" der Triebwerke nötigen Daten haben: der Treibwerkshersteller, der Flugzeughersteller, das Luftfahrtunternehmen oder ein unabhängiger Reparaturbetrieb? Wenn z.B. nur der Flugzeughersteller Datenzugang und damit allein die Möglichkeit hat, solche Dienstleistungen anzubieten, sollte dann auch das Luftfahrtunternehmen Zugang zu den Daten verlangen können, um einen billigeren unabhängigen Reparaturbetrieb beauftragen oder die entsprechenden Dienstleistungen in Eigenregie übernehmen zu können?

In der Mitteilung zur Datenwirtschaft[79] hatte die Kommission bereits 2017 das Problem beschrieben, einige Ziele und Löungen skizziert und eine Konsultation gestartet. Im Lichte der vielfachen Betonung der Vertragsfreiheit in dieser Konsultation[80] hatte die Kommission einen vorsichtigen Ansatz gewählt und freiwilliges Teilen von

72 S. zu dieser Thematik schon die Beiträge in *Lohsse/Schulze/Staudenmayer* (Fn. 61).

73 S. https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/.

74 Vorausschauende Instandhaltung („predictive maintenance") informiert den Betrieber von Geräten von vorneherein, wann welche Instandhaltungsmaßnahme nötig werden wird. Im Gegensatz zu routinemäßig durchgeführter Instandhaltung in regelmäßigen Abständen, ist vorausschauende Instandhaltung billiger und effizienter, hängt aber von Daten ab, die durch mit dem IoT verbundene Sensoren gesammelt werden.

75 „Präzise Landwirtschaft" („precision farming") würde es z.B. einer landwirtschaftlichen Maschine erlauben, spezifische Pflanzen genau zu dem Zeitpunkt zu bewässern, wenn der Zustand des Bodens und der Pflanze es erfordert. Sie benutzt mit dem IoT verbundene Sensoren oder Dronen, die die hierfür nötigen Daten sammeln.

76 Vgl. die Arten von Datenteilung in Commission Staff Working Document v. 10. 1. 2017, SWD (2017) 2 final, S. 14 f.

77 Ebenda, S. 15.

78 § 36 Abs. 3 S. 3 StVZO.

79 Fn. 16, S. 10 ff.

Daten fördern wollen. [81] Der von ihr vorgelegte Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors litt allerdings daran, dass er an Dateninhaber gerichtet war, die willens waren, Daten unter fairen Bedingungen zu teilen. Er schuf keinen Anreiz für Dateninhaber, die gar nicht oder nur unter erschwerenden Bedingungen Daten teilen wollen.

In ihrer neuen Datenstrategie[82] gibt die Kommission noch immer grundsätzlich ihrem Ansatz eines freiwilligen Teilens von Daten durch Verträge den Vorzug. Ein besonderer Akzent wird auf Nutzungsrechte an gemeinsam erzeugten Daten, vor allem im industriellen IoT-Umfeld gelegt. Sie erwägt aber auch, wenn besondere Umstände dies erfordern, die Gewährung des Zugangs zu Daten verbindlich vorzuschreiben. Dies solle unter fairen, zumutbaren, angemessenen und nichtdiskriminierenden Bedingungen geschehen. Ein Recht auf Datenzugang solle stets sektorspezifisch sein und nur dann gewährt werden, wenn in diesem Sektor ein Marktversagen festgestellt wird bzw. vorherzusehen ist und durch das Wettbewerbsrecht allein nicht behoben werden kann. Der Umfang eines Datenzugangsrecht solle den berechtigten Interessen des Dateninhabers Rechnung tragen und mit dem Rechtsrahmen im Einklang stehen. Dabei wird auf Anwendungen dieses Grundsatzes im Gemeinschaftsrecht verwiesen.[83] Dieser Ansatz geht zurück auf die Mitteilung zur Datenwirtschaft von 2017, in der bereits ein Zugangsrecht zu Daten auf der Grundlage von FRAND (Fair, Reasonable And Non-Discriminatory) Bedingungen erwogen wurde.[84]

b) Freiwilliges Teilen von Daten

Zu Recht gibt die Kommission dem freiwilligen Teilen von Daten durch Verträge den Vorzug. Wenn nämlich der Markt funktioniert, ist kein Eingreifen des Gesetzgebers nötig. Wenn aber ein Unternehmen die Daten für die Entwicklung bzw. den Betrieb seines Geschäftsmodells der digitalen Wirtschaft benötigt, kann eine Abhängigkeitssituation entstehen, die vom Dateninhaber bei der Vertragsgestaltung ausgenutzt werden könnte. Daher stellt sich die Frage nach der Missbrauchskontrolle von AGB,[85] die zwar den Vertragsparteien einen breiten Spielraum bei der Vertragsgestaltung einräumen, aber auch dem unfairen Ausnutzen neuer Abhängigkeiten in der digitalen Wirtschaft[86] Grenzen setzen könnte.

Für Mitgliedstaaten wie Deutschland oder die nordische Staaten ist dies kein Problem, da sie über eine AGB – Kontrolle in Unternehmensverträgen verfügen. In der Mehrheit der Mitgliedstaaten gibt es solche Bestimmungen allerdings nicht. Im EU-Recht gibt es nur vereinzelte Beispiele für eine AGB – Kontrolle. Als wichtigstes Beispiel wäre die AGB-Richtlinie zu erwähnen, die auf Verbraucherverträge Anwendung findet und mit einer Generalklausel sowie einer Liste von Beispielen arbeitet.[87] Die anderen Rechtsakte haben einen engeren Anwendungsbereich oder betreffen nur spezifische Verträge, da sich der Gemeinschaftsgesetzgeber bei Unternehmensverträgen nur vorsichtig an eine AGB-Kontrolle herantastet. Die Zahlungsverzugsrichtlinie benutzt für Zahlungsklauseln eine Generalklausel und eine „schwarze", d.h. per se unzulässige, Klausel sowie eine „graue" Klausel, bei der die Unzulässigkeit nur vermutet wird.[88] Die Richtlinie zu unlauteren Handelspraktiken beim Verkauf von Agrarerzeugnissen und Lebensmitteln enthält eine Liste von schwarzen Klauseln (die teilweise dadurch zulässig werden können, wenn sie klar und eindeutig vereinbart wurden).[89] Das Gemeinsame Europäische Kaufrecht (GEK) übernahm für Verbraucherverträge im Wesentlichen die Regelung der AGB – Richtlinie, fügte aber eine schwarze und graue Liste hinzu.[90] Für vertragliche Klauseln in Handelsverträgen enthielt es eine zwingend ausgestaltete Generalklausel, die sich in ihrem Maßstab an die Zahlungsverzugsrichtlinie anlehnt.[91]

Eine Inhaltskontrolle von Vertragsklauseln im Zusammenhang mit dem Teilen von Daten könnte, den Beispielen der Zahlungsverzugsrichtlinie und des GEK folgend, eine Generalklausel verwenden. Wie bei den o.a. Präzedenzfällen sollte eine solche Generalklausel ein niedrigeres Schutzniveau als in Verbraucherverträgen mit ihrem strukturellen Ungleichgewicht[92] vorsehen, da es sich hier um Unternehmensverträge handelt, bei denen höhere Sorgfaltsanforderungen gelten. Die Generalklausel könnte als Standard den in der Zahlungsverzugsrichtlinie und dem GEK benutzten Test der gegen den Grundsatz von Treu und Glauben und den redlichen Geschäftsverkehr verstoßenden groben Abweichung von einer guten Handelspraxis aufnehmen.

Dieser allgemeine Test könnte zweifach konkretisiert werden. Einerseits sollten bei einem solchen Eingriff in die Vertragsfreiheit die legitimen Interessen beider Vertragsparteien berücksichtigt werden. Dies bedeutet, dass den Gerichten Grundsätze für die Auslegung einer solchen Generalklausel an die Hand gegeben werden sollten, wie dies auch in der Zahlungsverzugsrichtlinie und im GEK

80 Zusammenfassender Bericht der Konsultation zur Initiative Aufbau einer europäischen Datenwirtschaft, S. 6 ff., abrufbar unter https://ec.europa.eu/information_society/newsroom/image/document/2017-36/synopsis_report_de_A1B68505-9B90-1599-014B9412B-FF80BC0_46649.pdf.
81 Mitteilung v. 25. 4. 2018, COM (2018) 232 final, S. 10 und Guidance on sharing private sector data in the European data economy, SWD (2018) 125 final S. 5-8.
82 Fn. 5, S. 7 ff.
83 Ebenda, S. 15 f.
84 Fn. 16, S. 15 und SWD (Fn. 77), S. 36 ff.
85 Eine solche wurde von der Kommission bereits in der Mitteilung zur Datenwirtschaft (Fn. 16), S. 14, in Erwägung gezogen.
86 Eine Inhaltskontrolle für das freiwillige Teilen von Daten könnte auch für das Teilen von Daten in Plattformverträgen (Fn. 72) oder für Verträge über den Zugang zur Cloud (Fn. 71) nutzbar gemacht werden.
87 Art. 3 und Anhang.
88 Art. 7 der Richtlinie 2011/7, ABl. L 48/1 v. 23. 2. 2011.
89 Art. 3 der Richtlinie 2019/633, ABl. L 111/59 v. 25. 4. 2019.
90 Kapitel 8, Abschnitte 1 und 2 (Fn. 37), insbes. Art. 83-85.
91 Kapitel 8, Abschnitte 1 und 3 (Fn. 37), insbes. Art. 86 und 81. S. auch Art. 70.
92 Vgl. *Staudenmayer*, „Die Richtlinien des Verbraucherprivatrechts – Bausteine für ein europäisches Privatrecht", in: Schulze/Schulte-Nölke (Hrsg.), Europäische Rechtsangleichung und nationale Privatrechte, 1999, S. 67 f.

geschehen ist. Diese könnten die Interessen der Vertragsparteien aufgreifen, wie sie schon von der Kommission beschrieben wurden.[93] Die betreffenden Verträge sollten den Zugang zu Daten verbessern, ihr Teilen erleichtern und Lock-in Effekte vermeiden. Gleichzeitig sollten sie Investitionen schützen und eine angemessene Rendite für den Dateninhaber gewährleisten.

Man könnte, wie bei der AGB-Kontrolle für Verbraucherverträge im GEK, eine solche Generalklausel auch durch eine schwarze und/oder graue Liste konkretisieren. Der praktische Effekt von solchen Listen ist zwar beschränkt, da die Vertragspraxis solche Klauseln leicht vermeiden kann. Ihr eigentlicher Wert besteht aber darin, den Gerichten Beispiele für die Auslegung der Generalklausel zur Verfügung zu stellen.

c) Recht auf Zugang zu Daten?

Wenn man ein Recht auf Zugang zu Daten erwägt, stellt sich zunächst die Frage, ob überhaupt und wenn ja, in welchen Situationen, ein solches Recht gewährt werden sollte. Weiterhin wären Bedingungen für einen solchen Zugang festzulegen, die die legitimen Interessen der beteiligten Parteien wahren.

aa) Erwägungen zur Begründung und zum Anwendungsbereich eines Datenzugangsrechts

Für ein mögliches Datenzugangsrecht ist zunächst die Nicht-Rivalität von Daten als Wirtschaftsressource bedeutsam. Sie kann dazu führen, dass ihre Nutzung dem Dateninhaber jedenfalls keine Nachteile[94] und dem Unternehmen, dass ein Datenzugangsrecht ausübt, wirtschaftliche Vorteile verschafft. Wünschenswert wäre es, dass der Dateninhaber auch darüberhinausgehende Vorteile, z.B. in Form einer finanziellen Gegenleistung oder einer wirtschaftlichen Beteiligung an der Nutzung der Daten, hat.

Ein anderes, relevantes Element eines möglichen Datenzugangsrecht sollte wohl auch sein, dass der betreffenden Datensatz für die Entwicklung oder das Weiterführen des betreffenden digitalen Geschäftsmodells unerläßlich ist. Dies würde bedeuten, dass das Geschäftsmodell nicht mit ähnlichen Daten entwickelt, bzw. betrieben werden und das Unternehmen die Daten nicht zu zumutbaren Bedingungen aus einer anderen Quelle erhalten könnte.

Es kann auch erheblich sein, ob das Unternehmen, das Zugang zu Daten haben möchte, selbst innerhalb der betreffenden Wertschöpfungskette an der gemeinsamen Erzeugung der Daten beteiligt war. In diesen Fällen kann ein berechtigtes Interesse leichter bejaht werden, da die Nutzung der Daten als ein Ausgleich für die Beteiligung an der Erzeugung verstanden werden kann.

Wie bereits erwähnt, ist kein Eingreifen des Gesetzgebers nötig, wenn der Markt dazu führt, dass Daten geteilt werden. Dies bedeutet, dass, wie von der Kommission erwähnt, ein Datenzugangsrecht nur in den Sektoren Anwendung finden sollte, in denen der Markt von alleine nicht zu diesem Ergebnis führt. Ein Recht auf Datenzugang sollte damit wohl nicht horizontal, sondern nur sektorspezifisch begründet werden, um Besonderheiten der jeweiligen Märkte berücksichtigen zu können. Ein Beispiel hierfür könnte der mit dem o.a. Beispiel bereits erläuterte Reparatur und Kundendienstleistungsmarkt für Fahrzeuge sein. Die Kommission hat in ihrer neuen Datenstrategie angekündigt, die sektorielle Gesetzgebug u.a. in diesem Licht zu überprüfen.[95]

Eng mit der Frage des Marktversagens verwoben ist der auch von der Kommission angesprochene Punkt, inwieweit in solchen Fällen ein Eingreifen des Wettbewerbsrechts in der Lage ist, einen funktionierenden Markt wiederherzustellen. Ohne dies vertieft erörtern zu können,[96] ist es doch offensichtlich, dass das Wettbewerbsrecht hier zwei Schwächen hat. Zunächst sind die Schwelle und Bedingungen für ein Eingreifen des Wettbewerbsrechts, insbesondere das Vorliegen einer marktbeherrschenden Stellung iSd. Art. 102 AEUV, hoch. Zudem kann es Jahre dauern, um eine wettbewerbsrechtliche Entscheidung zu treffen und rechtskräftig werden zu lassen. In diesem Zeitraum sind die sich sehr schnell entwickelnden Märkte der digitalen Wirtschaft so umgestaltet, dass der Effekt einer wettbewerbsrechtlichen Entscheidung weitgehend ins Leere gehen kann. Es ist daher wohl nötig, Wettbewerbsrecht und -politik an die technologischen Entwicklungen sowie die Märkte und Teilnehmer der digitalen Wirtschaft anzupassen.[97] Solche Anpassungen können aber wohl nur Teil eines rechtlichen Rahmens sein, der auch andere Maßnahmen enthalten sollte.[98]

Eine ebenfalls sektorsezifisch zu regelnde Frage beträfe die Herkunftsmärkte der Unternehmen, die Datenzugang haben wollen. Einerseits ginge es wohl zu weit, von einem Unternehmen, das Daten gesammelt hat, zu verlangen, diese mit einem Konkurrenten im selben Markt zu teilen. Andererseits wäre es unproblematisch, einem Unternehmen Zugang zu gewähren, das in einem Markt tätig ist und die Daten zu einem Zweck nutzen will, die in keiner Beziehung zum Markt des Dateninhabers stehen. Die Grauzone wären die vor-, bzw. nachgelagerten und benachbarten Märkte, d.h. wenn es um Daten geht, die es einem anderen Unternehmen erlauben könnten, zum Markt des Dateninhabers Zugang zu erhalten und damit dessen Konkurrent zu werden. Zusätzliche Kriterien, wie z.B. der Zweck und die Dauer der Nutzung der Daten, zu denen Zugang gewährt wird, könnten hier eine hilfreiche, einschränkende Wirkung haben.

93 S. die Mitteilung zur Datenwirtschaft (Fn. 16), S. 12 f.
94 Vgl. Datenethikkommission (Fn. 27), S. 82.
95 Fn. 5, S. 25 f., 32.
96 Vgl. *Crémer/De Montjoye/Schweitzer*, Competition Law in the Digital Era, 2019.
97 S. die von der Kommission in der Datenstrategie (Fn. 5), S. 16, angekündigten Maßnahmen.
98 Auch *Crémer/De Montjoye/Schweitzer* (Fn. 97), S. 52 f., 99 f., 107, 126 erachten in bestimmten Situationen ein regulatorisches Eingreifen für notwendig.

Schließlich muss das Teilen von Daten mit dem allgemeinen Rechtsrahmen in Übereinstimmung stehen. Dies bedeutet, dass keine Pflicht bestehen kann, urheberrechtlich geschützte Daten oder solche, die Geschäftsgeheimnisse[99] darstellen, teilen zu müssen. Weiterhin müsste das Teilen von personenbezogenen Daten mit der DS-GVO im Einklang stehen.

bb) Mögliche Bedingungen für ein Datenzugangsrecht

Für die Ausgestaltung von Bedingungen eines Datenzugangsrechts wäre einerseits eine mögliche Abhängigkeitssituation des Unternehmens, das Zugang zu den Daten benötigt, um sein Geschäftsmodell zu entwickeln, bzw. zu betreiben, zu berücksichtigen. Andererseits sollte ein Unternehmen, das investiert hat, um Daten zu sammeln, eine angemessene Rendite erhalten.[100]

Die aus dem Wettbewerbsrecht[101] stammenden und von der Kommission erwähnten[102] FRAND-Prinzipien wurden vom Gesetzgeber in einer Reihe von Gemeinschaftsrechtsakten benutzt.[103] Ihre (neben allen Unterschieden) hier relevante Gemeinsamkeit ist, dass der Gesetzgeber in bestimmten Sektoren ein rechtspolitisches Bedürfnis auf Datenzugang erkannt und mit ähnlichen Grundsätzen geregelt hat. Dieses rechtspolitische Ziel könnte hier in der gerade für Start-ups und KMU besonders wichtigen Innovationsförderung gesehen werden, die auf der Grundlage von mehr zugänglichen Daten zu neuen Produkte und Dienstleistungen führt und damit positive Auswirkungen auf Wertschöpfung und Wirtschaftswachstum hat.[104] Diese Prinzipien könnten deshalb auch für ein Recht auf Datenzugang nutzbar gemacht werden.[105] Die FRAND-Prinzipien oder die von der Kommission in der Datenstrategie zusätzlich genannten Grundsätze der Zumutbarkeit und Transparenz[106] stellen dabei (nur) eine Zielsetzung dar. Grundsätzlich sollte man es den Parteien überlassen, die Art und Höhe der Gegenleistung und die nähere Ausgestaltung des Datenzugangs zu verhandeln.[107]

Bei dem Resultat dieser Verhandlung könnte das Fairnessgebot sich in Form der bereits beim freiwilligen Datenteilen erwähnten Inhaltskontrolle niederschlagen, um zu verhindern, dass aufgrund der Abhängigkeitssituation unfaire Vertragsklauseln benutzt werden, die z.B. dazu führen könnten, dass die Nutzung der Daten zu stark beschränkt wird. Das Nichtdiskriminierungserfordernis würde ganz klassisch bedeuten, dass Unternehmen, die aus vergleichbaren Herkunftsmärkte stammen und zu vergleichbaren Zwecken Datenzugang benötigen, nicht ohne triftigen Grund unterschiedlich behandelt werden sollten.

Das Transparenzgebot könnte es erlauben, zu beurteilen, ob das Angebot des Dateninhabers den Grundsätzen des Datenzugangsrechts entspricht, insbesondere die Kosten des Dateninhabers deckt und eine angemessene Rendite wiederspiegelt. Dies dürfte allerdings nicht soweit gehen, dass vertrauliche Geschäftsinformationen preiszugeben wären.

Die Schlüsselfrage ist allerdings, wie denn die Gegenleistung für die Gewährung des Datenzugangsrechts zu bestimmen ist. Hierfür wären die Grundsätze der Angemessenheit (Reasonable) und der Zumutbarkeit relevant.

Wenn die Parteien sich nicht auf die Höhe der Gegenleistung einigen können, könnte es sinnvoll sein, eine Bestimmung des Preises durch einen neutralen Dritten vorzusehen.[108] Diese Möglichkeit wird im internationalen Handelsverkehr durchaus praktiziert.[109] Dem Dritten könnten dispositive Grundsätze als Hilfestellung zur Festsetzung der Gegenleistung an die Hand gegeben werden. Hierzu gibt es Vorbilder im europäischen und internationalen Vertragsrecht. So sieht die Handelsvertreterrichtlinie bei einer fehlenden Vereinbarung über die Vergütung vor, dass der Handelsvertreter Anspruch auf eine ortsübliche, und in Ermangelung einer solchen auf eine angemessene Vergütung hat, wobei alle Einzelfallumstände zu berücksichtigen sind.[110] Dieses Beispiel ist deswegen interessant, weil die Richtlinie auch dem Schutz der Handelsvertreter dient,[111] die typischerweise in einem gewissen Abhängigkeitsverhältnis zum Unternehmer stehen. Ähnliche Hilfestellungen sind in den UNIDROIT Principles of International Commercial Contracts[112], den Principles on European Contract Law[113], dem DCFR[114] und dem GEK[115] für die Fälle vorgesehen, dass die dritte Person den Preis

99 Art. 2 Nr. 1 der Richtlinie 2016/943 über den Schutz vertraulicher Geschäftsinformationen, ABl. L157/1 v. 15. 6. 2016.
100 Dies wurde schon in der Mitteilung zur Datenwirtschaft (Fn. 16), S. 12 f., betont.
101 Eine Einführung in die Standard Essential Patents Doktrin bietet Competition policy brief, Issue 8, June 2014, abrufbar unter https://ec.europa.eu/competition/publications/cpb/2014/008_en.pdf. Vgl. auch *Heim/Nikolic*, A FRAND Regime for Dominant Digital Platforms, jipitec 2019, 41 ff. m.w.N. zu neueren Entscheidungen.
102 S. Fn. 83 und 85.
103 Die wichtigsten Beispiele sind die Verordnung 1907/2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), ABl. L 136/3 v. 29. 5. 2007, Art. 27 und 30, Erwägungsgründe 50 f., die Verordnung 2018/858 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern, ABl. L 151/1 v. 14. 6. 2018, Art. 61-63, Erwägungsgrund 50 und die Elektrizitätsrichtlinie 2019/944, ABl. L 158/125 v. 14. 6. 2019, Art. 3 Abs. 4, 17 Abs. 3 (c), 23, 34. S. auch die Richtlinie 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors
ABl. L 172/56, v. 26.6.2019, Art. 3, 6, 11, die Zahlungsdiensterichtlinie 2015/2366, ABl. L 337/35, v. 23. 12. 2015, Art. 66 f. und die Horizont 2020 Verordnung 1290/2013, ABl. L 347/81, v. 20. 12. 2013, Art. 48.
104 Vgl. die Datenstrategie der Kommission (Fn. 5), S. 1, 3 und 5 f.
105 S. auch *Drexl* jipitec 2017, 290 f., der die REACH Verordnung als Vorbild nimmt; *Crémer/De Montjoye/Schweitzer* (Fn. 98), S. 97, 109 und *Heim/Nikolic* jipitec 2019, 55 (allerdings für Plattformen).
106 Fn. 5, S. 16. Das Transparenzerfordernis ist in der englischen Fassung, aber nicht in der deutschen Fassung enthalten.
107 *Drexl* jipitec 2017, 285, schlägt vor, hierzu einen Verhandlungsrahmen einzurichten, der dem Huawei-Urteil des EuGH (v. 16.7.2015 – C-170/13, Tz. 60 f.) entspricht.
108 Darüberhinausgehend schlägt *Drexl* jipitec 2017, 290, ein Schiedsverfahren vor, wenn keine Einigung erreicht werden kann.
109 S. Comment A. DCFR, II.-9:106 (Fn. 38).
110 Art. 6 Abs. 1 der Richtlinie 86/653, ABl. L 382/18 v. 31. 12. 1986.
111 Vgl. die Rspr. des EuGH (Urt. v. 30. 4. 1998 – C-215/97 – Bellone, Tz. 13; Urt. v. 9. 11. 2000 – C-381/98 – Ingmar, Tz. 20).
112 Art. 5.1.7 (3).
113 Art. 6:106.
114 II.–9:106 (Fn. 38).
115 Art. 75 (Fn. 37).

nicht festsetzen kann oder will, bzw. einen grob unangemessenen Preis festsetzt. Auch das UN-Kaufrecht enthält einen ähnlichen Maßstab.[116]

III. Ausblick

Bei der Vorlage ihres kürzlich vorgelegten massiven Wiederaufbauprogramms angesichts der Corona-Krise hat die Kommission den Akzent ganz deutlich auf die doppelte grüne und digitale Wende und bei letzterer als eines der auschlaggebenden Element auf den Ausbau der Datenwirtschaft gelegt. Zugang zu Daten spielt herbei eine wichtige Rolle.[117]

Es bleibt abzuwarten, inwieweit „persönliche Datenräume", die Smart Contracts nutzen, und ein sektorielles, auf FRAND-Bedingungen beruhendes Datenzugangsrecht bei der weiteren Entwicklung der Datenwirtschaft eine Rolle spielen. Klar ist jedenfalls, dass die Fragen des Zugangs zu und der Nutzung von Daten das Privatrecht in Europa noch sehr stark beschäftigen werden.

Summary

In order to reap the economic and societal advantages of digitisation, it will be necessary to establish a suitable legal framework. Private law will need to adapt to the needs of the data economy. In particular, it should provide an answer to the central question of the data economy: Who has access to data and how can data be used commercially? In the realm of B2C, this raises the issue whether the consumer should have an economic benefit in the event of access to his or her personal data. The Directive on contracts for the supply of digital content takes a groundbreaking first step towards regulating personal data as subject of commercial transactions. 'Smart contracts' could go a step further. Equally important is the B2B dimension. Should a business whose business model depends on data have an access right to data held by another business? If so, what should be the conditions for such a right?

Prof. Dr. Dirk Staudenmayer

116 Art. 55.
117 Mitteilung der Kommission „Die Stunde Europas – Schäden beheben und Perspektiven für die nächste Generation eröffnen" vom 27. 5. 2020, COM (2020) 456 final, S. 1 f., 11 ff.

Prof. Dr. Burghard Piltz*

Incoterms® 2020

Nach mehrjährigen Vorarbeiten, internationalen Konferenzen in Peking und London und Auswertung von mehr als 3.000 Kommentaren aus der Handelspraxis[1] hat die International Chamber of Commerce (ICC), Paris, im Herbst 2019 unter der Bezeichnung Incoterms® 2020[2] eine aktualisierte Fassung der von ihr erstmals im Jahre 1936[3] herausgegebenen Regeln zur Auslegung international gebräuchlicher Handelsklauseln vorgelegt. Die Bedeutung der Incoterms für die Handelspraxis ist enorm. Nach Erkenntnissen der ICC kommen die Klauseln der Incoterms® in 90 % aller internationalen Kaufverträge zum Einsatz, werden täglich mehr als 200.000 Mal zu Rate gezogen und haben sich als internationaler Standard durchgesetzt.[4] Die neuen Incoterms® 2020 gelten seit dem 1. Januar 2020.[5]

I. Fortentwicklung des Regelwerks

Die neuen Incoterms® 2020 bedeuten keine Revolution, sondern eher eine Evolution im Sinne einer Fortentwicklung der bisherigen Regeln. Die Incoterms® 2020 passen die bisherige Fassung der Incoterms an die aktuellen Entwicklungen und Bedürfnisse der Geschäftspraxis an, strukturieren neu, ergänzen und straffen bisherige Aussagen und formulieren viele ihrer Regeln jetzt klarer als zuvor. Ein wesentliches Anliegen der Überarbeitung war,

* Der Autor hat als Mitglied der von der ICC/Paris international aufgestellten, neunköpfigen Drafting Group in den vergangenen vier Jahren an der Erarbeitung der neuen Incoterms® 2020 unmittelbar mitgewirkt und ist als Rechtsanwalt im Hamburger Büro der Kanzlei Ahlers & Vogel PartG mbB tätig.

1 Näher dazu *Radtke* ICC Germany-Magazin 8/2019, 38 ff.
2 Incoterms® 2020 by the International Chamber of Commerce (ICC), als ICC-Publikation 723 ED zu beziehen bei ICC Deutschland e. V., Wilhelmstraße 43 G, 10117 Berlin.
3 Zur Entwicklungsgeschichte der Incoterms siehe *Ramberg* in: Andersen/Schroeter (Hrsg.), Sharing International Commercial Law across National Boundaries, Festschrift for Albert H. Kritzer, 2008, S. 394 ff.
4 Incoterms® 2020 video, abrufbar unter *https://www.incoterms2020.de/* (letzter Abruf am 20.03.2020).
5 Näher dazu *Graf von Bernstorff*, Incoterms® 2020, 2020; *Oertel* RIW 2019, 701 ff.; *Piltz* IHR 2019, 177 ff.; *Noels* Tijdschrift voor Internationale Handel en Transportrecht 2019, 501 ff.; *Niggebrugge/Alink* Nederlands Tijdschrift voor Handelsrecht 2019, 286 ff.; *van Hall* EJCCL 2019, 45 ff.