

Die neue Ära des Datenhandels: Daten als Währung und Gegenleistung

Dagmar Gesmann-Nuissl und Stefanie Meyer

Zusammenfassung

Mit der Umsetzung der Digitale Inhalte-Richtlinie und der Warenkauf-Richtlinie in das deutsche BGB (§§ 327 ff. BGB) ist eine bereits seit längerem ausgeübte Praxis gesetzlich präzisiert worden: Das Bezahlen mit Daten. Das neu geschaffene Datenschuldrecht bewegt sich auf der Schnittstelle zwischen Vertragsrecht und Datenschutzrecht. Dabei entsteht ein Spannungsverhältnis zwischen der Etablierung einer erfolgreichen Datenwirtschaft auf Basis privatautonomer vertragsrechtlicher Beziehungen einerseits und der Sicherstellung der digitalen Datensouveränität der Verbraucher andererseits. Bezogen auf Verträge über digitale Produkte stellen sich vor allem vertragsrechtliche Fragen, etwa zum Zustandekommen und der Ausgestaltung der Vertragsverhältnisse. Dem gegenüber stehen datenschutzrechtliche Fragestellungen, die von den schuldrechtlichen Voraussetzungen unberührt bleiben (§ 327q BGB). Dort stehen die Informiertheit und die Freiwilligkeit der Einwilligung in die Datenverarbeitung sowie die Wahrung datenschutzrechtlicher Grundsätze, wie das Kopplungsverbot, im Vordergrund (Art. 7 DSGVO). Eine erfolgreiche Datenökonomie muss dieses Spannungsverhältnis auflösen, wobei die subjektive (souveräne) Willensbildung der Verbraucher, die sowohl im Rechtsbindungswillen als auch in der wirksamen datenschutzrechtlichen Einwilligung zum Ausdruck kommt, oberste Priorität genießt. Um beides gleichermaßen zu sichern, wird ein übersichtliches und leicht zugängliches Portal zum Schutz der Datensouveränität in der Datenwirtschaft vorgeschlagen. Es zeigt dem Verbraucher auf einen Blick den Wert seiner Daten in Bezahlvorgängen, was seine Willensbildung unterstützt sowie seiner Entscheidungsfreiheit dient und zugleich seine Datensouveränität wahrt. Dieser Beitrag befasst sich mit den rechtlichen Grundlagen, die bei der Entwicklung eines solchen Portals zu berücksichtigen sind.

„Not everything that can be counted counts and
not everything that counts can be counted.“¹

1. Einleitung

Im Jahre 2011 wurde ein bemerkenswerter Eintrag in das Guinness-Buch der Rekorde vorgenommen: Das US-amerikanische Unternehmen *See Virtual Worlds* hat den virtuellen Planeten „Calypso“ für einen Preis von 6 Millionen US-Dollar gekauft.² Aber auch spezifische Items in ausgewählten Computerspielen erzielen – gemessen an der Virtualität der Produkte – hohe Preise: Zuletzt wurde z. B. das Schwert „Schallende Wut“ innerhalb des Computerspiels *Diablo 3* für 40 Milliarden „Gold“ verkauft, was einem Wert von 14.000 US-Dollar entspricht.³

Rechtsgeschäfte mit virtuellen Gegenständen sind nicht neu. Wurden sie bislang dem Rechtskauf (§ 453 BGB) oder atypischen Verträgen (§§ 311, 241 ff. BGB) zugeordnet, sind durch die Digitale Inhalte-Richtlinie (DIRL – Richtlinie (EU) 2019/770), die Warenkaufrichtlinie (WKRL – Richtlinie (EU) 2019/771) und deren Umsetzung in das nationale Recht in den §§ 327 ff. BGB spezielle Regelungen hinzugetreten, die bestimmte Aspekte zu digitalen Produkten verbraucherschützend „vor die Klammer ziehen“. Bezogen auf sog. digitale Inhalte bestimmt der Wortlaut des § 327 Abs. 1, Abs. 3 BGB nun ausdrücklich, dass solche virtuellen Gegenstände wahlweise gegen Entgelt, gegen Bezahlung von Wertedarstellungen (wie das „Gold“ in *Diablo 3*) oder aber gegen das Bereitstellen von Daten erworben werden können. Letzteres wirft Fragen auf, namentlich, wie genau aufkommende Konflikte zwischen dem Privat- und Datenschutzrecht behandelt werden müssen, damit schuld- und datenschutzrechtliche Rechte und Pflichten in gleichem Maße beachtet und in Einklang gebracht werden können.

Der folgende Beitrag nimmt sich dieser Problematik an. Dabei werden zunächst die rechtlichen Grundlagen betrachtet, die bei der Entwicklung

-
- 1 Cameron, *Informal Sociology, a Casual Introduction to Sociological Thinking*, 1963: Random House; zuweilen wird dieses Zitat aber auch Albert Einstein (1955), Hilliard Jason, Stephen Ross, Lord Platt oder George Pickering zugerechnet.
 - 2 <https://www.guinnessworldrecords.com/world-records/92207-most-valuable-virtual-object> (abgerufen am 18.04.2024), wobei in der dortigen Beschreibung als Käufer das Tochterunternehmen von *See Virtual Worlds* (*See Digital Studios*) genannt wird; der Rekord als solches wird dem Mutterkonzern zugeschrieben.
 - 3 <https://www.esports.com/de/items-waffen-und-skins-5-spiele-mit-extrem-teuren-inhalten-215415> (abgerufen am 30.01.2024).

eines nutzerorientierten Werkzeugs berücksichtigt werden müssen, das der informierten ökonomischen Nutzung personenbezogener Daten bei der Bereitstellung digitaler Produkte dient. Ferner wird eine erste, initiale Idee zur praktischen Lösung vorgestellt.

2. Ökonomische Relevanz von Daten und deren rechtliche Grundlagen

Das wohl renommierteste Beispiel der Ökonomisierung von personenbezogenen Daten ist das Setzen sog. Cookie-Banner. Durch den Einsatz von Cookies auf Webseiten und der damit einhergehenden Verarbeitung personenbezogener Daten wird es dem Anbieter möglich, das Nutzerverhalten zu ermitteln und Werbung sowie zukünftige Angebote gezielter zu platzieren. Mit anderen Worten wird mit Cookies Geld verdient, da sich so die gewonnenen Nutzerdaten monetarisieren lassen. Letzteres geht allerdings nicht grenzenlos, sondern erfordert (sofern die Cookies nicht zwingend erforderlich sind, vgl. § 25 Abs. 2 Nr. 2 TTDSG) zumindest eine wirksame und informierte Einwilligung in die Datenverarbeitung seitens des Nutzers bzw. ein berechtigtes Interesse an der Weiterverarbeitung, die über ein voreingestelltes Ankreuzkästchen auf der Webseite des Anbieters hinausreichen muss.⁴

Personenbezogene Daten können allerdings noch in anderer Hinsicht Bestandteil von Leistungen oder Leistungsversprechen sein. Gerade im Umfeld digitaler Angebote werden viele Inhalte als „kostenlos“ beworben, was aber lediglich bedeutet, dass für die Inhalte kein Entgelt zu entrichten ist, aber dennoch personenbezogene Daten – etwa in einem Registrierungsprozess oder während des sich daran anschließenden Nutzerverhaltens (z. B. Häufigkeit von Einkäufen, Art und Weise derselben) – erhoben werden.⁵

Die Wertschöpfung auf der Basis der erlangten Daten ist demnach vielfältig. Sie reicht von der Wertschöpfung durch das Kalibrieren bestimmter Vorhersagemodelle, über die Wertschöpfung durch Vorhersagen selbst, bis hin zu datenfinanzierten Geschäftsmodellen bzw. monetären Grundmodellen, die um eine Datenflusskomponente ergänzt werden.⁶ Dabei sind

4 EuGH, Urt. v. 01.10.2019, Az. C-673/17, NJW 2019, 3433; vgl. Besprechung u.a. von *Gesmann-Nuissl*, InTeR 2019, 190 (190 ff.).

5 *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (84).

6 *Hacker*, ZfPW 2019, 148 (153-157).

die Verwertungsmethoden recht unterschiedlich. Zum Teil werden die erhobenen Daten weiterverkauft. Zunehmend interessanter gestaltet sich für die Verwerter allerdings die gezielte Ansprache von Nutzern in der personalisierten Werbung oder das Generieren eines Nutzerprofils.⁷ Selbst eine Datenerhebung zu Marktforschungszwecken kann einen geldwerten Vorteil bringen, da sich selbst aus einem depersonalisierten Datensatz noch Gewinne erzielen lassen.⁸

In der Vergangenheit zeigte sich, dass trotz der bekannten Monetarisierungsmöglichkeit von Daten viele Nutzer dann doch recht freizügig bei der Herausgabe ihrer personenbezogenen Daten sind und damit prinzipiell eine „kostenfreie Leistung“ erbringen. Gleichzeitig steigt ihr Wunsch nach dem umfassenden Schutz ihrer Persönlichkeitsrechte. Dieser Widerspruch zwischen der Freigiebigkeit des Einzelnen in Bezug auf seine personenbezogene Daten und dem Bedürfnis nach hinreichendem Grundrechtsschutz wird als *Privacy Paradox* bezeichnet.⁹

Der Schutzbedürftigkeit der Verbraucher nimmt sich nun die EU an, welche die DIRL und die WKRL mit dem Ziel in Kraft setzte, das Vertrauen der Verbraucher in Bezug auf den Erwerb digitaler Produkte und Waren mit digitalen Elementen von europäischen Unternehmen zu stärken und einen digitalen europäischen Binnenmarkt zu fördern.¹⁰ Der Unionsgesetzgeber strebt gem. Art. 4 DIRL und Art. 4 WKRL eine Vollharmonisierung in allen Mitgliedstaaten an, sodass die Mitgliedstaaten entsprechende Vorschriften einführen und dabei die in den Richtlinien festgelegten Mindest- und Maximalstandards beachten müssen. Der nationale Gesetzgeber hat in Umsetzung der Richtlinien mit den §§ 327 ff. BGB spezielle Regelungen für Verbraucherverträge geschaffen, wobei die Grundsätze zum Schutze der Verbraucher gem. § 312 Abs. 1a BGB nach § 327 Abs. 3 BGB anzuwenden sind, wenn Verbraucher einem Unternehmer personenbezogene Daten bereitstellen oder sich hierzu verpflichten. Zu einer solchen Transaktion bedarf es einer informierten selbstbestimmten Entscheidung – sowohl bezogen auf den privatautonomen Vertragsschluss, als auch hinsichtlich der datenschutzrechtlich relevanten Herausgabe von Daten. Der Brücken-

7 Langhanke/Schmidt-Kessel, EuCML 2015, 218 (219); vgl. dazu auch Gesmann-Nuissl/Meyer, in: International Conference on Human-Agent Interaction (HAI '23), 2023.

8 Schmidt-Kessel/Grimm, ZfPW 2017, 84 (88).

9 Norberg u.a., JCA 2007, 100 (100 ff.).

10 Blassl, WM 2023, 1907 (1908); Bittner, VuR 2022, 9 (9); Meller-Hannich, DAR 2021, 493 (494); Stierle, IPRB 2021, 66 (66); Riehm/Abold, CR 2021, 530 (530 f.).

schlag zwischen Privatautonomie und Datenschutz (wie ihn auch Art. 1 Abs. 3 DSGVO vorsieht) wurde durch die DIRL sowie die Regelungen der §§ 327 ff. BGB geschaffen¹¹ und zeigt sich überdies in § 327q BGB, wonach die Ausübung datenschutzrechtlicher Betroffenenrechte und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Darauf wird an späterer Stelle noch einzugehen sein (siehe Kap. 4.2).

3. Anwendungsbereich des Datenschuldrechts

Die §§ 327 ff. BGB beziehen sich auf Verbraucherverträge über digitale Produkte.¹² Damit gelten die Regelungen nicht für jedwede Vertragsabschlüsse und nicht für alle am Rechtsverkehr Beteiligten, sondern nur für Verträge, die sich im digitalen Raum abspielen und schützenswerte Personengruppen (Verbraucher) betreffen.

Für die Definition von Verbraucherverträgen ist § 310 Abs. 3 BGB maßgeblich – es muss sich um einen Vertrag zwischen einem Unternehmer i. S. d. § 14 BGB und einem Verbraucher i. S. d. § 13 BGB handeln. Die §§ 327 ff. BGB umfassen damit alle Verbraucherverträge zur Bereitstellung digitaler Produkte, insbesondere Austauschverträge wie Kauf- oder Werkverträge oder Dauerschuldverhältnisse wie Miet-, Leasing- oder Dienstverträge.¹³ Ein spezielles „Digitalvertragsrecht“ mit einer B2C-Geltung wurde nicht geschaffen.¹⁴

Während die DIRL bereits in ihrem Titel die „Bereitstellung digitaler Inhalte und digitaler Dienstleistungen“ getrennt aufführt, spricht § 327 Abs. 1 BGB zusammenfassend von digitalen Produkten. Allerdings gliedert sich auch dieser Begriff in die von der DIRL eingeführten Begrifflichkeiten „digitale Inhalte“ und „digitale Dienstleistungen“ auf, wie § 327 Abs. 2 BGB verdeutlicht. Es soll sichergestellt werden, dass die Definitionen technologieoffen bleiben und auch künftige Entwicklungen einbeziehen können.¹⁵ Die Begründung zum Gesetzesentwurf verdeutlicht, dass nicht der Inhalt

11 Schmitz/Buschew, MMR 2022, 171 (171).

12 Für einen Überblick, auch hinsichtlich der weitergehenden (Aktualisierungs-) Pflichten siehe: *Gesmann-Niessl u.a.*, in: BSI- Tagungsband zum 18. Deutschen IT-Sicherheitskongress, 2022, 35 (35 ff.)

13 Riehm/Abold, CR 2021, 530 (531).; Kirchhefer-Lauber, JuS 2021, 1125 (1126 u. 1129).

14 Blassl, WM 2023, 1907 (1908).

15 BT-Drs. 19/27653, S. 38.

maßgeblich ist, sondern „die Art und Weise, wie die Daten reproduzierbar beziehungsweise wiedergabefähig festgehalten werden, nämlich in digitaler Form“.¹⁶ Digitale Inhalte sind gem. § 327 Abs. 2 S. 1 BGB bzw. Art. 2 Nr. 1 DIRM Daten, die in digitaler Form erstellt oder bereitgestellt werden. Darunter fallen etwa Computerprogramme, Anwendungen, Video-, Audio- und Musikdateien, digitale Spiele, elektronische Bücher und andere elektronische Publikationen.¹⁷ Digitale Dienstleistungen nach § 327 Abs. 2 S. 2 BGB bzw. Art. 2 Nr. 2 DIRM sind Dienstleistungen, die dem Verbraucher die Erstellung, die Verarbeitung oder die Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen (Nr. 1) oder die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen (Nr. 2).¹⁸ Dies umfasst Angebote wie Software-as-a-Service, Datei-Hosting, Cloud-Computing, gemeinsame Spiele, cloudbasierte Textverarbeitung, soziale Netzwerke, Portale oder Plattformen.¹⁹ Daneben treten gem. § 327 Abs. 4 BGB digitale Produkte, die aufgrund eines Kundenwunsches speziell angefertigt wurden, wie etwa maßgeschneiderte Software oder 3D-gedruckte Waren. Ebenso gilt der Großteil der Vorschriften der §§ 327 ff. BGB (d. h. alle mit Ausnahme der §§ 327b und 327c BGB) für Verbraucherverträge über die Bereitstellung von körperlichen Datenträgern, die ausschließlich als Träger digitaler Inhalte dienen (§ 327 Abs. 5 BGB). Dies können DVDs, CDs, USB-Sticks oder Speicherkarten sein.

Zeitgleich mit der DIRM wurde die WKRL verabschiedet. Auch diese bezieht sich ausschließlich auf Verbraucherverträge (Art. 3 WKRL), die – ebenso wie die DIRM – auf körperliche Gegenstände („Waren“, vgl. auch Art. 3 DIRM) anzuwenden ist. Beide Richtlinien sind eng miteinander verwoben, dennoch muss der Anwendungsbereich im Einzelfall abgegrenzt werden. Im Unterschied zur DIRM gilt die WKRL insbesondere nicht nur für digitale Produkte. Mit der Einführung des § 327a BGB hat der Gesetzgeber versucht, die Abgrenzung der Anwendungsbereiche zu verdeutlichen, indem er sog. „Paketverträge“ eingeführt hat. Dies sind Verträge, die neben der Bereitstellung digitaler Produkte die Bereitstellung anderer Sachen oder

16 BT-Drs. 19/27653, S. 38.

17 ErwGr. 19 der DIRM sowie BT-Drs. 19/27653, S. 39.

18 Zur Abgrenzung von „digitalen Inhalten“ und „digitalen Dienstleistungen“ im Einzelnen: *Riehm*, RDi 2022, 209 (2011).

19 ErwGr. 19 der DIRM sowie BT-Drs. 19/27653, S. 39.

die Bereitstellung anderer Dienstleistungen zum Gegenstand haben, § 327a Abs.1 S.1 BGB. Damit geht er über den Wortlaut der Richtlinie hinaus, da nicht mehr nur „Waren“, sondern „Sachen“ i. S. d. § 90 BGB umfasst sind. § 327a BGB umfasst konsequenterweise auch Verbindungen von digitalen Produkten und unbeweglichen Sachen.²⁰ Ein klassisches Beispiel, für das die §§ 327 ff. BGB im Rahmen eines Paketvertrages auf den Vertragsteil des digitalen Produktes Anwendung finden, ist der Kauf eines Fernsehers mit Streaming-Abonnement. Hingegen finden die Vorschriften der WKRL infolge deren nationaler Umsetzung im Sachmangel-Gewährleistungsrecht Anwendung, wenn die Waren, die digitale Produkte enthalten, so von den digitalen Produkten abhängig sind, dass die Funktion ohne sie nicht erfüllt werden kann (z. B. das Betriebssystem eines Staubsaugerroboters). IoT-Produkte sind damit einheitlich dem Anwendungsbereich der WKRL unterstellt; Gewährleistungsansprüche richten sich damit nach den aus § 437 BGB folgenden Rechten.²¹

Die Unterscheidung ist deshalb maßgeblich, da im Rahmen des Anwendungsbereichs der §§ 327 ff. BGB für die vertragliche Leistung ein „Preis“ gezahlt werden muss, der in dieser Konstellation eben auch im Bezahlen mit digitalen Wertedarstellungen (§ 327 Abs.1 S.2 BGB, wie z. B. einer In-Game-Währung eines Computerspiels als digitales Produkt) oder im Bereitstellen von personenbezogenen Daten liegen kann (§ 327 Abs.3 BGB). Da der Konflikt zwischen datenschutzrechtlichen Schutzbestimmungen und der Privatautonomie demnach nur im Anwendungsbereich der DRL und folglich der §§ 327 ff. BGB auftreten kann, werden sich die folgenden Ausführungen allein auf die Auswirkungen der DRL beziehen.

4. Vertragsrechtliche Aspekte des Datenschuldrechts

Zwar ist der Anwendungsbereich der §§ 327 ff. BGB eröffnet, sobald ein Verbrauchervertrag über digitale Produkte vorliegt. Allerdings finden sich keine speziellen Regelungen über den Vertragsabschluss in den entsprechenden Paragraphen, sodass die allgemeinen Regeln der §§ 145 ff. BGB einschlägig sind.

20 BT-Drs. 19/27653, S. 46.

21 Spindler, MMR 2021, 451 (452).

4.1 Vertragsschluss

Das Vorliegen eines Vertrages nach nationalem Recht ist Dreh- und Angelpunkt, wie auch ErwGr. 25 der DURL klarstellt: „Diese Richtlinie sollte auch nicht in Fällen gelten, in denen der Unternehmer nur Metadaten wie Informationen zum Gerät des Verbrauchers oder zum Browserverlauf erhebt, es sei denn, der betreffende Sachverhalt gilt als Vertrag nach nationalem Recht.“ Ein Vertrag ist ein zweiseitiges Rechtsgeschäft, konkret die von mindestens zwei Vertragspartnern erklärte Einigung über die Begründung oder Änderung eines Schuldverhältnisses, § 311 BGB. Dies kann einseitig verpflichtend sein (wie im Falle eines Schenkungsversprechens gem. § 518 BGB, oder einer Bürgschaft gem. § 765 BGB) oder zweiseitig verpflichtend (synallagmatisch wie ein Kaufvertrag gem. § 433 BGB oder ein Mietvertrag gem. § 535 BGB). Digitale Produkte und die durch diverse Technologien erwachsenden Möglichkeiten eines digitalen Vertragsschlusses lassen die Äußerungen der korrespondierenden Willenserklärungen und damit den Vertragsschluss auf vielfältige Art und Weise zu. Der deutsche Gesetzgeber scheint in Anbetracht der Gesetzesbegründung sehr schnell bei der Annahme eines Vertrages im digitalen Kontext: „Für die Annahme eines Vertragsschlusses könnte beispielsweise sprechen, dass der Unternehmer den Dienst oder die Leistung erbringt, weil er den Verbraucher motivieren will, auf seiner Seite weitere Webseitenaufrufe zu tätigen oder Dienste oder Leistungen in Anspruch zu nehmen, weil er Einnahmen für auf seiner Seite dargestellte Werbung erzielen will, deren Höhe in aller Regel von den Zugriffszahlen abhängt, oder weil er mit dem Einsatz von Tracking-Technologien und der nachfolgenden Anzeige personalisierter Werbung wirtschaftliche Vorteile anstrebt.“²² Bei Cookies oder Tracking-Tools wäre dann immer schon von einem Vertragsschluss auszugehen.²³ Ob in diesem Falle aber tatsächlich ein Rechtsbindungswille beider Parteien anzunehmen ist, scheint mehr als fraglich.²⁴ Einmal mehr ist es daher ratsam, den Gedanken hinter der Rechtsprechung zur Cookie-Banner-Problematik²⁵ (Gestaltung des Einwilligungsprozesses) heranzuziehen und diesen vom Datenschutz- ins Schuldrecht zu übertragen. Alleine aus der vorgefundenen Situation (aktiviertes

22 BT-Drs. 19/27653, S. 40.

23 Spindler, MMR 2021, 451 (453).

24 Schmitz/Buschew, MMR 2022, 171 (174).

25 EuGH, Urt. v. 01.10.2019, Az. C-673/17, NJW 2019, 3433; vgl. Besprechung u.a. von Gesmann-Nuissl, InTeR 2019, 190 (190 ff.).

Häkchen bzw. Webseitenaufruf) lässt sich noch keine rechtlich bindende Erklärung ableiten, die datenschutz- oder schuldrechtliche Folgen verursachen kann. Ein Rechtsbindungswille kann doch nur dann angenommen werden, wenn er zuvor auch gebildet wurde. Andererseits kann erst die Annahme eines Vertragsschlusses den Verbraucher unter den Schutzschirm der §§ 327 ff. BGB stellen, sodass schon in dessen Interesse die Hürden nicht allzu hoch angesetzt werden dürfen, was wohl auch die schnelle Annahme eines Vertrages im digitalen Kontext nach der Gesetzesbegründung erklärt. Am Rechtsbindungswillen des Unternehmers bestehen hingegen keine Zweifel. Gerade wenn auf Seiten des Unternehmers Daten verarbeitet werden, weil deren werbliche Nutzung für ihn Einkünfte verspricht, kann stets auf einen Rechtsbindungswillen des Unternehmers geschlossen werden.²⁶

Die Feststellung des Rechtsbindungswillens auf Seiten des Verbrauchers als zentrale Voraussetzung für einen Vertragsschluss einschließlich der datenschuldrechtlichen Folgen ist daher ein Aspekt, der einer weiteren Untersuchung bedarf (vgl. Kap. 6.).

4.2 Vertragliche Pflichten

Ist die Hürde des Vertragsschlusses genommen, sind die jeweiligen Rechte und Pflichten zu betrachten. Auf Seiten des Unternehmers steht die Pflicht, das digitale Produkt (sprich: digitale Inhalte oder digitale Dienstleistungen) bereitzustellen. Dies kann wahlweise in Form einer einmaligen Bereitstellung (vergleichbar eines Kaufes) oder einer dauerhaften Bereitstellung (vergleichbar einer Miete) von digitalen Inhalten und Dienstleistungen erfolgen.²⁷ Bezogen auf die eingangs genannten Beispiele sind die Zugänge zu Servern von Computerspielen als dauerhafte Bereitstellung, das Verschaffen eines digitalen Schwertes als einmalige Bereitstellung zu verstehen. Demgegenüber steht – als Gegenleistung – die Pflicht zur Zahlung eines Preises in Form von Geld, digitaler Wertedarstellungen oder personenbezogener Daten.

Eine Schwierigkeit bei der Annahme eines Vertragsschlusses ebenso wie bei der Bestimmung der korrespondierenden Pflichten ist, dass damit zwar die Hauptleistungspflichten feststehen und somit theoretisch ein zweisei-

²⁶ Kramme, RDⁱ 2021, 20 (22).

²⁷ Riehm/Abold, CR 2021, 530 (531).

tig verpflichtendes (synallagmatisches) Schuldverhältnis vorliegen sollte. Denn schließlich ist die Situation des Zahlens mit Daten doch mit der des Zahlens eines Geldbetrages im Rahmen eines klassischen Kaufvertrags gem. § 433 BGB vergleichbar und es scheint unlogisch, die Situation des Zahlens mittels Daten (also Daten für das digitale Schwert) nun anders zu bewerten. Gleichwohl wurde eine solche synallagmatische Einordnung durch den Gesetzgeber gerade nicht getroffen²⁸, weil er in der Bereitstellung von Daten gerade keine „Gegenleistung“ festmachen wollte.²⁹ Dies wird zum einen damit begründet, dass der Begriff und Deutungsumfang der „Gegenleistung“ bei Daten unklar sei.³⁰ Grob umrissen kann man den Begriff der Gegenleistung folgendermaßen definieren: Ein „transaktionspezifisches, typischerweise [...] vermögensmehrendes Äquivalent zur Leistung, welches [...] ein Austauschverhältnis prägt und [...] nicht vom Gegenleistungsbegriff ausgeschlossen wurde.“³¹ Im Kontext des Bezahlers mit personenbezogenen Daten sei – so der Europäische Datenschutzbeauftragte – der Begriff „Gegenleistung“ irreführend, da ein Verbraucher stets wisse, dass er mit Geld bezahle – nicht aber, wenn er mit Daten bezahle.³² Aus diesem Grund lasse sich die Parallele nur eingeschränkt ziehen und eine synallagmatische Gegenleistung sei ausgeschlossen. Da die Verknüpfung zur Leistung des Unternehmers aber nicht zwingend synallagmatisch, sondern auch konditional oder kausal sein könne³³, würden sich andere Möglichkeiten eröffnen. Nach Ansicht des Gesetzgebers und des Europäischen Datenschutzbeauftragten soll es im Falle der Bereitstellung von Daten also genügen, dass eine schuldrechtlich kausale Verknüpfung vorliegt – ein Synallagma ist nicht erforderlich.³⁴

Tatsächlich stellt sich die Situation aber so dar, dass die reine Bereitstellung (d. h. das Zurverfügungstellen) von personenbezogenen Daten für die Geschäftszwecke des Unternehmers kaum ausreichend sein wird, weil die Daten allein so nicht ökonomisch eingesetzt werden können. „Daten“ im Sinne des § 327 Abs. 3 BGB orientieren sich am Begriff der personenbe-

28 Schmitz/Buschuew, MMR 2022, 171 (174).

29 BT-Drs. 19/27653, S. 35; EDPS, Stellungnahme 4/2017, S. 11 ff.

30 EDPS, Stellungnahme 4/2017, S. 11 f.

31 Hacker, ZfPW 2019, 148 (158 ff.); zu den Situationen des Ausschlusses vom Gegenleistungsbegriff siehe ders. S. 169 ff.

32 EDPS, Stellungnahme 4/2017, S. 12.

33 Hacker, ZfPW 2019, 148 (150).

34 Grüneberg/Grüneberg, BGB, § 312 Rn. 3b; anders Hacker, der eine konditionale Verknüpfung annimmt: ZfPW 2019, 148 (196 f.).

zogenen Daten aus Art. 4 Nr. 1 DSGVO.³⁵ In den hier angesprochenen Fallkonstellationen (wie der Kauf eines virtuellen Items) werden dabei hauptsächlich Name, E-Mail-Adresse, Geburtsdatum, Standort und IP-Adressen übermittelt.³⁶ Allein das Zurverfügungstellen dieser Daten kann aber nicht ausreichend sein, um das Vertragsverhältnis auszufüllen, da deren Verarbeitung ohne vorherige Einwilligung unzulässig wäre. Im Mittelpunkt der vertraglichen Pflicht steht damit einmal mehr die Einwilligung in datenschutzrechtlicher Hinsicht als Voraussetzung für das Bereitstellen der Daten als solches.³⁷ Bewertet man die dargestellte vertragliche Konstellation, so lässt sich feststellen, dass die reine Bereitstellung der Daten eigentlich nur nachgeordneten Charakter besitzen kann; die datenschutzrechtliche Einwilligung ist jedenfalls wesentlicher Teil der Gegenleistung.

Weil eine datenschutzrechtliche Betrachtungsweise zu einem mit der schuldrechtlichen Betrachtung in Konflikt stehenden Ergebnis kommt, kommt § 327q BGB zum Tragen. Danach bleibt die Möglichkeit der Ausübung der Datenschutzrechte des Verbrauchers uneingeschränkt erhalten, indem klargestellt wird, dass die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lässt, § 327q Abs. 1 BGB.³⁸ Abs. 2 der Vorschrift bestimmt, dass dem Unternehmer im Falle eines Widerrufs der datenschutzrechtlichen Einwilligung des Verbrauchers (Art. 7 Abs. 3 DSGVO) ein außerordentliches Kündigungsrecht bei Dauerschuldverhältnissen zusteht. Schließlich bestimmt § 327q Abs. 3 BGB, dass der Unternehmer aus der Geltendmachung der datenschutzrechtlichen Ansprüche keine vertraglichen oder gesetzlichen Ersatzansprüche ableiten darf.³⁹ Nur wenn der Verbraucher keine Nachteile aus einem Widerruf erleidet, kann eine Einwilligung im Sinne des Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO freiwillig sein (vgl. ErwGr. 42 DSGVO). In der Praxis mag § 327q BGB das Verhältnis zwischen Datenschuld- und Datenschutzrecht gut klären – gerade in Situationen, in denen sich beide Konstellationen jedoch diffus und widersprechend gegenüberstehen (vgl. Kap. 5) muss dieses Problem jedoch durch eine weniger harte Trennung aufgelöst werden (vgl. Kap. 6.).

35 BT-Drs. 19/27653, S. 40.

36 Schmidt-Kessel/Grimm, ZfPW 2017, 84 (87).

37 Schmidt-Kessel/Grimm, ZfPW 2017, 84 (90).

38 Blassl, WM 2023, 1941 (1942); Bittner, VuR 2022, 9 (12); Stierle, IPRB 2021, 66 (68).

39 Blassl, WM 2023, 1941 (1942); Bittner, VuR 2022, 9 (12).

4.3 Gewährleistungspflichten

Davon losgelöst stehen den Verbrauchern, die einen solchen Vertrag über digitale Produkte schließen, die in den §§ 327 ff. BGB genannten Gewährleistungsrechte zu. Dabei bestehen die bekannten Rechte wie die Nacherfüllung, Kündigung, Minderung oder Schadensersatz – allerdings in angepasster Form. Es kommt den betroffenen Verbrauchern insbesondere eine Beweislastumkehr in § 327k BGB zugute. § 327d BGB (i.V.m. §§ 327e bis 327g BGB) erweitert zudem den Produktmangelbegriff; das digitale Produkt muss kumulativ den subjektiven und objektiven Anforderungen und den Anforderungen an die Integration entsprechen, § 327d Abs. 1 S. 1 BGB. Schließlich gelten gem. § 327f BGB besondere Aktualisierungspflichten – ein Unterlassen stellt einen Produktmangel dar. Für einen detaillierten Überblick über die einzelnen Regelungen, die im Verhältnis von Schuld- und Datenschutzrecht nur eine untergeordnete Rolle spielen, sei auf die einschlägige Literatur verwiesen.⁴⁰

Im Verhältnis von Datenschutz- und Schuldrecht wird die Regelung des § 327o Abs. 2 S. 1 BGB zur Vertragsbeendigung bedeutsam (wobei sich die Beendigungsgründe als solche aus §§ 327c, 327m und 327r BGB ergeben). Im Fall der Vertragsbeendigung hat der Unternehmer dem Verbraucher die Zahlungen zu erstatten, die der Verbraucher zur Erfüllung des Vertrags geleistet hat. Dies ist eine Umsetzung der Art. 15 u. 16 DRL. § 327p Abs. 2 BGB ergänzt, dass nicht personenbezogene Daten, die der Verbraucher bereitgestellt hat, nicht weiter genutzt werden dürfen, wenn keine Ausnahmen aus § 327p Abs. 2 S. 2 Nrn. 1-4 BGB vorliegen. Für personenbezogene Daten gelten die Regeln der DSGVO und die damit einhergehenden Löschpflichten aus Art. 17 DSGVO.⁴¹ Es stellt sich die Frage, wie die Rückgewährverpflichtung aus § 327o Abs. 2 S. 1 BGB hinsichtlich personenbezogener Daten umzusetzen ist – eine Problematik, die auch der Europäische Datenschutzbeauftragte erkannt hat, als er verneinte, dass Bereitstellung von Daten und Bereitstellung eines digitalen Produktes im synallagmatischen

40 *Blassl*, WM 2023, 1907 (1907 ff.); *Blassl*, WM 2023, 1941 (1941 ff.); *Bittner*, VuR 2022, 9 (9 ff.); *Paal/Wais*, DStR 2022, 1164 (1164 ff.); *Mayer/Möllnitz*, RDt 2021, 333 (333 ff.); *Stierle*, IPRB 2021, 66 (66 ff.); *Riehm/Abold*, CR 2021, 530 (530 ff.); *Güster/Booke*, MMR 2022, 92 (92 ff.); *Schreier/Michels*, RDt 2022, 381 (381 ff.); *Felsch u.a.*, MMR 2022, 18 (18 ff.); *Gesmann-Nuissl u.a.*, in: BSI- Tagungsband zum 18. Deutschen IT-Sicherheitskongress, 2022, 35 (35 ff.); *Spindler*, MMR 2021, 451 (451 ff.).

41 *Spindler*, MMR 2021, 528 (529).

Gegenseitigkeitsverhältnis stehen dürfen.⁴² Wie damit allerdings auch praxisgerecht verfahren werden kann, wird zu klären sein (vgl. Kap. 6.).⁴³

5. Datenschutzrechtliche Anforderungen des Datenschuldrechts

Mit der Klarstellung in § 327q BGB sind und bleiben die datenschutzrechtlichen Erklärungen möglich, wirksam und lassen den Vertragsschluss unberührt. Datenschutz- und schuldrechtliche Rechte und Pflichten bestehen damit nebeneinander. Das funktioniert geräuschlos jedoch nur, wenn die beiden Rechtsgebiete nicht ineinandergreifen – was sie aber aufgrund der auch für den Vertragsschluss notwendigen Einwilligung in die Datenverarbeitung machen. Ohne eine wirksame Einwilligung ist die geschuldete „Bereitstellung“ von Daten – wie bereits angedeutet (vgl. Kap. 4.2) weitestgehend nutzlos für den Unternehmer.

Auf den ersten Blick scheinen das BGB (bzw. die DURL) und das Datenschutzrecht unterschiedliche Zielsetzungen zu haben: Das BGB ist bezogen auf die Privatautonomie der Bürger zueinander und das Datenschutzrecht ist auf den Persönlichkeitsschutz bezogen, d. h. auf individuelle Statusbeziehungen.⁴⁴ Dies gilt jedoch nicht absolut, da die Regelungsgehalte naturgemäß ineinandergreifen müssen. Beispielsweise wird der Einzelne in der Ausübung seiner Privatautonomie dergestalt eingeschränkt, als dass gewisse Vorschriften (u.a. insbesondere auch die §§ 327 ff. BGB) zum individuellen Schutz Grenzen setzen. Ebenso ist das Datenschutzrecht (und das damit verbundene Recht auf informationelle Selbstbestimmung, vgl. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 7 und 8 GRCh, respektive Art. 1 Abs. 2 DSGVO) nicht schrankenlos gewährleistet. Im Rahmen der Prüfung der Verhältnismäßigkeit muss gegen andere Grundrechte abgewogen werden, wie beispielsweise in Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO.

5.1 Rechtmäßige Datenverarbeitung – insbesondere Einwilligung

Da die gesamte DSGVO Anwendung findet, ist im Grundsatz die Einwilligung in die Datenverarbeitung nicht die einzige Möglichkeit, zulässiger-

⁴² EDPS, Stellungnahme 4/2017, S. 12.

⁴³ Vgl. dazu: Metzger in: Münchner Kommentar zum BGB, § 327o Rn. 9.

⁴⁴ Schmidt-Kessel/Grimm, ZfPW 2017, 84 (85).

weise die Daten für die gewünschten ökonomischen Zwecke zu nutzen. Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO stellt eine Rechtsgrundlage für die Verarbeitung von Daten dar, wenn dies für die Erfüllung eines Vertrages mit der betroffenen Person oder aber zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Allerdings muss hierfür ein Vertrag (vgl. Kap. 4.1) vorliegen oder eine Maßnahme für vorvertragliche Regelungen; insbesondere muss die Verarbeitung aber dem Zweck dienen, den Vertrag zu erfüllen. Dies ist insbesondere der Fall bei der Preisgabe der E-Mail-Adresse, um die digitalen Inhalte zu erhalten⁴⁵ – im Falle von Computerspielen auch durch die Verknüpfung mit den Account-Daten zur Freischaltung der erworbenen Features. Zu einem anderen Zweck dürften die so bekannt gewordenen Daten aber nicht verarbeitet werden. Entscheidender Punkt im Anwendungsfall des Bezahlens mit Daten im Sinne der §§ 327 ff. BGB ist aber, dass die Daten nicht zur Vertragserfüllung verarbeitet werden, sondern diese im Rahmen der datenökonomischen Einsatzmöglichkeiten zu bspw. Marketingzwecken verwendet werden. Dies ist nach allgemeiner Meinung auch nicht durch den Rechtfertigungsgrund des Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO gedeckt.⁴⁶ Da zudem auch Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO im Rahmen des dort vorausgesetzten „berechtigten Interesses des Verantwortlichen“ bislang lediglich Betrugsprävention, Direktwerbung sowie Maßnahmen zur Verbesserung von IT-Systemen inkludiert,⁴⁷ und damit alle darüberhinausgehenden Aktivitäten ausnimmt, bleibt die vorherige Einwilligung im Sinne des Art. 6 Abs. 1 lit. a) DSGVO die zumeist einzige Möglichkeit, den datenschutzrechtlichen Anforderungen gerecht zu werden.⁴⁸

Eine wirksame Einwilligung bedarf einiger Voraussetzungen, vgl. Art. 6 Abs. 1 UAbs. 1 lit. a), Art. 7 und Art. 4 Nr. 11 DSGVO. Die Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO ist freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abzugeben; es muss eindeutig sein, dass die betroffene Person (der Verbraucher) mit der Datenverarbeitung zum angegebenen Zweck einverstanden ist. Da dies der Verantwortliche (hier der datenverarbeitende Unternehmer) gem. Art. 7 Abs. 1 DSGVO

45 Schmitz/Buschew, MMR 2022, 171 (172).

46 Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, Art. 6 Rn. 33; Sattler, JZ 2017, 1036 (1040).

47 BeckOK DatenschutzR/Albers/Veit, 47. Ed. 1.2.2024, DS-GVO Art. 6 Rn. 68.

48 Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, Art. 6 Rn. 33: „Die Verarbeitung von Daten als Entgelt kann vielmehr nur auf die Einwilligung der betroffenen Person gestützt werden“.

nachzuweisen hat, wird dies in der Regel auf elektronischem Wege geschehen.

Informiertheit nach Art. 4 Nr. 11 DSGVO bedeutet, dass die Einwilligung nur für den konkreten Fall und in Kenntnis der Sachlage abgegeben sein darf, vgl. ErwGr. 32 S. 1 DSGVO. Erforderlich ist eine Information durch den Unternehmer vor Abgabe der Einwilligung, die andernfalls nicht informiert sein kann. ErwGr. 42 S. 4 DSGVO sieht vor, dass mindestens über die Identität des Verantwortlichen und über die Zwecke der Verarbeitung informiert werden soll. Das EDPB hält es, angelehnt an Art. 13 Abs. 2 lit. c) DSGVO, für erforderlich, dass zumindest die Identität des Verantwortlichen, die Verarbeitungszwecke und die Art der Daten benannt werden, ein Hinweis auf das Widerrufsrecht und ggf. ein Hinweis auf automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO erfolgt und auf mögliche Verarbeitungsrisiken bei Drittstaatentransfers (vgl. Art. 49 Abs. 1 lit. a) DSGVO) hingewiesen wird.⁴⁹ Sofern sich eine Einwilligung auf mehrere Verarbeitende erstrecken soll – und das ist im Falle der Datenwirtschaft ein durchaus denkbare Szenario – muss sich dies aus den Informationen ergeben. Fraglich ist, ob die Datenverarbeitung gerechtfertigt ist, wenn zwar eine Einwilligung in Datenflüsse zwischen verbundenen Unternehmen erteilt wurde, aber einzelne Konzernunternehmen erst nach der Einwilligung hinzukommen.⁵⁰ Allerdings wird es hier auf die Einwilligungserklärung und deren Wortlaut im Einzelfall ankommen.⁵¹

Im Falle des Bereitstellens von Daten als Preis für die Leistung eines digitalen Produkts ist insbesondere auch die Maßgabe des Art. 7 Abs. 2 DSGVO zu beachten. Erfolgt nämlich „die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung [...] so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist“. Schriftform in diesem Zusammenhang bedeutet nicht etwa ein Schriftstück mit entsprechender Unterschrift wie § 126 BGB dies versteht, sondern erfasst grundsätzlich jede eindeutige schriftliche oder elektronische Willensbekundung (vergleichbar zu § 126b BGB).⁵² Im Falle der Bereitstellung von Daten erfolgt die Einwilligungserklärung in die Datenverarbeitung zumeist elektronisch – und vor allen Dingen im Zuge eines Vertragsschlusses, z. B. nach § 433 BGB. Zu be-

49 EDPB, Leitlinien 5/2020, Rn. 64.

50 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 38.

51 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 38.

52 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 41; Klement, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, Art.. 7 Rn. 76.

achten ist also, dass die Einwilligung zur Datenverarbeitung vom Angebot bzw. der Annahme zum Vertragsabschluss (§§ 145 ff. BGB) klar unterschieden werden kann, da sie andernfalls nicht verbindlich sind (Art. 7 Abs. 2 S. 2 DSGVO).

Dreh- und Angelpunkt der Einwilligung – insbesondere im Falle des Datenschuldrechts – ist die Freiwilligkeit der Einwilligung, vgl. Art. 4 Nr. 11, Art 7 Abs. 4 und ErwGr. 32, 42 und 43 DSGVO. Eine Einwilligung ist nur dann als freiwillig zu betrachten, wenn sie ohne jeden Druck oder Zwang abgegeben werden kann.⁵³ ErwGr. 42 fordert eine echte und freie Wahl, sodass die betroffene Person in der Lage sein muss, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Gerade im Rahmen des „Bezahlens“ mit Daten werden Anreize wie die vermeintliche Kostenfreiheit geschaffen, aber auch sonstige verhaltensökonomische Methoden eingesetzt, um die Verbraucher gezielt zu steuern. Hierfür gibt es zulässige Methoden⁵⁴; Grenzen bestehen jedoch da, wo Verbraucher gezielt getäuscht und manipuliert werden, wie in den Fällen der *Dark Pattern*.⁵⁵ ErwGr. 43 DSGVO greift schließlich das Ungleichgewicht zwischen den beteiligten Personen auf, das bei der Beurteilung der Freiwilligkeit eine große Rolle spielt. Beispielhaft werden hier Behörden als Verantwortliche genannt – es ist jedoch nicht ausgeschlossen, dass ein vergleichbares Ungleichgewicht auch anzunehmen ist, wenn es sich um das Verhältnis Unternehmer und Verbraucher handelt. Eine solche Machtasymmetrie wird von einigen Kritikern der DIRM und deren Umsetzung angenommen, weil keine andere Möglichkeit bestehe, als die Privatheit preiszugeben.⁵⁶ Dies lässt sich umso mehr diskutieren, wenn es sich um minderjährige oder ältere Verbraucher handelt (vulnerable Gruppen). Eine Besonderheit gilt für die Einwilligung Minderjähriger in Bezug auf Dienste der Informationsgesellschaft gem. Art. 8 DSGVO.

5.2 Datenschutzrechtliche Grundsätze - insbesondere Kopplungsverbot

Ein die Freiwilligkeit der Einwilligung beeinflussender Grundsatz der DSGVO ist das in Art. 7 Abs. 4 DSGVO normierte Kopplungsverbot. Es

53 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 19.

54 Wie beispielsweise das Nudging, vgl. Kollmar/Schirmbacher, WRP 2020, 1015 (1017).

55 Martini u.a., ZfDR 2021, 47 (49 ff.); Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 19.

56 Schmitz/Buschew, MMR 2022, 171 (173).

handelt sich um ein allgemeines, nicht etwa um ein absolutes Kopplungsverbot.⁵⁷ Dies wird aus der Formulierung „in größtmöglichem Umfang“ deutlich.⁵⁸ Das Kopplungsverbot findet wohl hauptsächlich Anwendung auf Kopplungen von Vertragsschluss und Einwilligung⁵⁹ – wie in den nun durch §§ 327 ff. BGB erlaubten Fällen des Bezahlens mit Daten. Allein schon deswegen muss dieser bestehende Konflikt aufgelöst werden (vgl. Kap. 6.).

Von Art. 7 Abs. 4 DSGVO werden zunächst – das liegt aufgrund der Einordnung nahe – nur zulässige Verarbeitungen umfasst.⁶⁰ Es genügt nicht, dass nur der Verbraucher subjektiv das Gefühl hat, dass er eine echte Wahl hat, sondern diese Wahl muss objektiv bestimmbar sein. Insbesondere in Konstellationen, in denen es im Einzelfall angebracht ist, für verschiedene Verarbeitungssituationen eine gesonderte Einwilligung einzuholen, dies aber nicht geschieht, oder in Fällen, in denen die Vertragserfüllung von der Einwilligung abhängig ist, diese aber objektiv nicht für die Erfüllung des Vertrages erforderlich ist, ist eine objektive Wahlfreiheit ausgeschlossen und damit eine Kopplung zu bejahen.⁶¹ Oftmals trifft aber genau dies – um die Cookie-Problematik aufzugreifen – auf die Cookie-Banner zu. Dort werden Nutzer häufig die Einwilligung in die Verwendung von Tracking-Cookies abgeben, obwohl diese für die Erbringung der Dienstleistung (Anzeige der Webseite) nicht nötig wäre.⁶²

Teilweise wird das (allgemeine) Kopplungsverbot als ein erheblicher Eingriff in die Privatautonomie betrachtet. Insbesondere in Bezug auf das Datenschuldrecht kommt gerade die Diskrepanz zwischen zum Privatautonomie und Datenschutz zum Tragen, weswegen es essentiell ist, dass das Kopplungsverbot eben nicht absolut, sondern nur in einem verhältnismäßig angemessenen Umfang angewendet wird.⁶³ Unverhältnismäßigkeit wäre allenfalls dann zu bejahen, wenn der Unternehmer eine herausgehobene (Monopol-)Stellung besäße und die Verbraucher auf die Leistungen ange-

57 EDPB, Leitlinien 05/2020, Rn. 34 u. 35; a.A.: *Dammann*, ZD 2016, 307 (311).

58 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 23.

59 ÖOGH, Urt. v. 31.8.2018, Az. 6 Ob 140/18h, BeckRS 2018, 30960 Rn. 35.

60 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 25.

61 EDPS, Stellungnahme 4/2017, S. 21.

62 EDPS, Stellungnahme 4/2017, S. 13.

63 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 27.

wiesen wären.⁶⁴ Vorliegend kommt zudem die Maßgabe des ErwGr. 42 DSGVO zum Tragen, nach dem eine Person keine „Nachteile“ erleiden darf, wenn die Einwilligung versagt wird. Handelt es sich bei den Nachteilen lediglich um Preisnachlässe, soll das nicht das Kopplungsverbot zur Anwendung bringen.⁶⁵ Auch das Ablehnen eines Vertrages kann kein Nachteil im Sinne des ErwGr. 42 DSGVO sein, da gerade dies Basis jedweder privatautonomen Handlung (z.B. eines Vertrages) ist. Zudem ist bei der Auslegung des Kopplungsverbotes in Bezug zum Datenschuldrecht die Intention des Richtlinien- und des Gesetzgebers zu berücksichtigen, die die Verknüpfung ja gerade gewollt haben.⁶⁶ Zusätzlich greift das Argument, dass seitens des Verbrauchers zumeist die Wahl des Preises (Entgelt, digitale Wertedarstellungen oder personenbezogene Daten) verbleibt – allein im Falle der alleinig möglichen Datenzahlung kommt das Argument erneut im Zuge der Freiwilligkeit zum Tragen, muss jedoch auch hier im Kontext der gesetzgeberisch gewollten privatautonomen Entscheidung betrachtet werden.

Unter Kap. 5.1 wurde bereits angesprochen, dass die Daten zu keinem anderen Zweck verwendet werden dürfen als zu dem, in den eingewilligt wurde. Dies folgt aus Art. 5 Abs. 1 lit. b) DSGVO. Diese Zweckbindung gilt vom Zeitpunkt der Erhebung bis zur Zweckerfüllung an.⁶⁷ Eine Zweckänderung ist grundsätzlich unzulässig. Ausnahmen hierzu finden sich in Art. 6 Abs. 4 DSGVO; dann aber ist der Betroffene hierüber zu informieren, Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO.

5.3 Widerruf der Einwilligung und Löschpflichten

Ist der Zweck erreicht, sind die personenbezogenen Daten zu löschen, vgl. Art. 17 Abs. 1 lit. a) DSGVO. Das Gleiche gilt auch für diejenigen Fälle, in denen der Verbraucher gem. Art. 7 Abs. 3 DSGVO seine Einwilligung widerruft. Dazu hat er – worüber er entsprechend informiert werden muss (Kap. 5.2) – das jederzeitige Recht. Dies lässt, wie § 327q BGB regelt, die Wirksamkeit des Vertrags unberührt (Kap. 4.3). Damit bleibt die Datenver-

64 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 27; unter Verweis u.a. auf: Buchner, DuD 2016, 155 (158); Gierschmann, ZD 2016, 51 (54); a.A.: EDPB, Leitlinien 05/2020, Rn. 38; BeckOK DatenschutzR/Stemmer, DS-GVO, Art. 7, Rn. 45.

65 EDPB, Leitlinien 05/2020, Rn. 50.

66 Gola/Heckmann/Schulz, DS-GVO, Art. 7, Rn. 30.

67 Gola/Heckmann/Pötters, DS-GVO, Art. 5, Rn. 18.

arbeitung bis zum Ausspruch des Widerrufs wirksam, es handelt sich um eine ex nunc-Wirkung. Allerdings hat der Unternehmer gem. § 327q Abs. 2 BGB in diesen Fällen das Recht, den Vertrag zu kündigen.

Wird der Widerruf nach Art. 7 Abs. 3 DSGVO ordnungsgemäß ausgeübt, sind die Daten zu löschen, wenn es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt (Art. 17 Abs. 1 lit. b) DSGVO). Insbesondere im Rahmen des ökonomischen Datenverkehrs, der durch das Datenschuldrecht etabliert wird, ist die Sicherstellung der Löschung ein großes praktisches Problem.

6. Konfliktpotenziale und -lösungen

Im Zuge der Untersuchung zu den rechtlichen Grundlagen des Datenschuldrechts wurden einige problematische Punkte aufgezeigt, die es in der Praxis – insbesondere auch im Vorgriff zur Einrichtung eines Datenwirtschaftsportals (vgl. Kap. 6.3) – zu lösen gilt; das Spektrum reicht von rein vertragsrechtlichen (wie den Rechtsbindungswillen und das Verhältnis von Leistung und Gegenleistung) über rein datenschutzrechtliche (Informiertheit und Freiwilligkeit der Einwilligung) bis hin zu verbindenden, „datenschuld-schutzrechtlichen“ Fragestellungen (wie die Frage nach dem Kopplungsverbot und der Rückabwicklung des Vertrages).

6.1 Rechtliche Konfliktlösung

Rein rechtlich sind diese Problempunkte nur durch verbraucherfreundliche Auslegung und Anwendung der Normen zu lösen. Es sind jedoch die Wertungen, die der Gesetzgeber generell zur Anwendung bringen möchte, mitzudenken. Hinsichtlich der vertragsrechtlichen Problempunkte des Rechtsbindungswillens und des Vertragsschlusses gilt Folgendes: Im Falle eines Vertragsschlusses, bei dem ein Verbraucher aktiv die Wahl zwischen der Bezahlung eines Preises, Bezahlung mit digitalen Wertedarstellungen oder Bezahlung mit personenbezogenen Daten hat und sich für Letzteres entscheidet, ist die Annahme eines Rechtsbindungswillens unproblematisch. Fraglich ist vielmehr, ob – ähnlich wie bei der Cookie-Problematik – allein die vorgefundene Situation für die Annahme eines Vertrages ausreichen kann, da hier die Willensbildung mehr als problematisch ist. Allerdings ist

die Intention des Gesetzgebers wertend heranzuziehen: Der Verbraucher soll durch die §§ 327 ff. BGB besonders geschützt werden. Die weitgehende Ablehnung eines Rechtsbindungswillens würde ihm diese Schutzvorschriften vorenthalten und er wäre schutzloser gestellt.⁶⁸ Gerade wenn der Unternehmer ein Interesse an der ökonomischen Weiterverarbeitung der Daten hat und eine „Leistung“ erhält, sollte der Verbraucher nicht schutzlos bleiben und ein Vertrag angenommen werden. Dies gilt umso mehr, als gerade in solchen digitalen (Kauf-)Situationen vulnerable Gruppen, wie Minderjährige oder Ältere, dazu neigen, besonders naiv zu agieren und daher besonderen Schutz bedürfen (insbesondere auch, weil Minderjährige von Gesetzes wegen gesteigert geschützt sind).⁶⁹

Auch die Fragestellung nach dem Synallagma sollte der gesetzgeberischen Intention gerecht werden. Gegenleistungen müssen nicht notwendigerweise synallagmatisch verknüpft werden, sondern es ist ebenso eine kausale oder konditionale Verknüpfung denkbar.⁷⁰ Auch, wenn die Kaufsituation und die Zahlung eines Entgeltes intuitiv an ein Synallagma denken lässt, bleibt der Verbraucher bei einer kausalen oder konditionalen Verknüpfung nicht schutzlos (vgl. §§ 812 ff. BGB). Diese Problematik wurde im Vorfeld hinreichend diskutiert und der Wortlaut des Gesetzes entsprechend zurückhaltend formuliert.⁷¹

Bezüglich des datenschutzrechtlichen Grundsatzes des Kopplungsverbot aus Art. 7 Abs. 4 DSGVO ist der gesetzgeberische Wille in die Beurteilung einzubeziehen. Lehnt man mit der wohl herrschenden Meinung ein absolutes Kopplungsverbot ab⁷², bedeutet die Annahme eines allgemeinen Kopplungsverbot, dass die Möglichkeit der Verbindung von vertraglichen Pflichten und „geschuldeter“ bzw. vielmehr kausal verknüpfter Datenbereitstellung möglich ist – insbesondere eben auch, weil der Gesetzgeber diese Möglichkeit wollte. Dies wird insbesondere dann kein Problem darstellen, wenn der Verbraucher die Wahl zwischen Entgelt, digitalen Wertedarstellungen und personenbezogenen Daten hat. Es verbleibt jedoch die gleiche Problematik wie beim Vertragsschluss – wie ist im Falle von Datenerhebungen zu verfahren, die nicht wirklich nötig sind und hinsichtlich derer die Wahlfreiheit in gewisser Hinsicht wegfällt. Dies wird aber nicht auf rein

68 Kramme, RDt 2021, 20 (22).

69 Vgl. zur Gesamtproblematik im Kontext: Gesmann-Nuissl/Meyer, Robotics 2022, 11, 125.

70 Hacker, ZfPW 2019, 148 (150).

71 EDPS, Stellungnahme 4/2017, S. 12.

72 EDPB, Leitlinien 05/2020, Rn. 34 u. 35.

rechtlicher Ebene zu lösen sein. Hier bedarf es eines praktischen Umsetzungsansatzes, der die Informiertheit des Verbrauchers im Sinne des Art. 4 Nr. 11 und Art. 7 DSGVO in den Blick nimmt und über die Grundlagen und Rechtsfolgen in verständlicher Weise aufklärt (vgl. Kap. 6.2). Gerade die Informiertheit und Freiwilligkeit der Einwilligung muss sich im digitalen Umfeld stimmig an die technische Umgebung anpassen und nachvollziehbar bleiben.

In der Kombination Schuld- und Datenschutzrecht hat auch die Rückabwicklung des Vertrages seinen Raum. Für nicht personenbezogene Daten findet § 327o Abs. 2 S. 1 BGB Anwendung – „Zahlungen“ sind zu erstatten. In Bezug auf personenbezogene Daten verweist Art. 16 Abs. 2 DRL auf die DSGVO; einen entsprechenden Hinweis gibt es im BGB nicht, ist jedoch aufgrund der Regelung des § 327q BGB naheliegend. Die personenbezogenen Daten des Verbrauchers sind damit infolge eines Widerrufs der Einwilligung nach Art. 7 Abs. 3 DSGVO gem. Art. 17 Abs. 1 lit. b) DSGVO zu löschen. Darauf besteht bereits ein datenschutzrechtlicher Anspruch – ein Argument dafür, dass es schuldrechtlicher Löschungsansprüche als Folge eines Synallagmas im BGB nicht mehr bedarf. Für die Rückabwicklung innerhalb dieses Vertragsverhältnisses und für den Löschanspruch bestehen also keine anderen Anforderungen als bei jedem anderen Widerruf der Einwilligung.

6.2 Praktische Konfliktlösung

Die hinreichende Aufklärung hinsichtlich der Voraussetzungen und Folgen eines Vertragsschlusses, damit (1) ein Rechtsbindungswille gebildet werden kann und (2) die Einwilligung freiwillig und informiert erfolgen kann, bedarf eines praktischen, verbraucherfreundlichen und verständlichen Ansatzes. Die Reaktion auf die Cookie-Rechtsprechung des EuGHs⁷³ sowie auf die Umsetzung des Art. 5 Abs. 3 ePrivacyRL in § 25 TTDSGG hinsichtlich des vorangekreuzten Zustimmungskästchens war, dass nunmehr große (oftmals rechtswidrig gestaltete) Cookie-Banner auf der Webseite erscheinen und das Einwilligungskästchen zentral präsentiert wird, was dazu führt, dass Verbraucher den Banner wegklicken wollen und in die Erhebung von Tracking-Cookies einwilligen, ohne die Folgen zu reflektieren. Die-

73 EuGH, Urt. v. 01.10.2019, Az. C-673/17, NJW 2019, 3433.

se oder vergleichbare Cookie-Banner sind im Hinblick auf § 25 TTDSG rechtswidrig, da insoweit alternative, gleichartig präsentierte Formen der Zustimmung bzw. Ablehnung angeboten werden müssen.⁷⁴ Im Hinblick auf die Datenökonomie und dem Bezahlen mit Daten sind die Folgen aber noch weitreichender als beim bloßen Einsatz von Tracking-Cookies, da diese Daten, regelmäßig verbunden mit den personenbezogenen Daten usw., verwendet werden, um umfassende Profile zu bilden und Nutzer gezielt zu manipulieren.⁷⁵ Eine mit Cookie-Bannern vergleichbare – sich in der Praxis als nicht effektiv erweisende – Aufklärung sollte hier nun nicht angestrebt werden, weil dies dem Interesse des Verbraucherschutzes zuwiderläuft. Insbesondere, wenn es um die ökonomische Verwertung und Verarbeitung personenbezogener Daten geht, sollte auf eine konkrete und gezielte Aufklärung besonders Wert gelegt werden, damit die (auch wenig reflektierenden) Verbraucher genügend Informationen erhalten, um eine individuelle Abwägung treffen zu können.

Der praktische Ansatz sollte dabei die Idee des Bezahlens mit Daten und die damit einhergehenden Willenserklärungen besser aufzeigen. Die Tatsache, dass den Daten stärker denn je ein Wert zugeschrieben wird, muss bereits in der Information berücksichtigt werden und eine zentrale Rolle einnehmen.

6.3 Konkrete Ausgestaltung des Lösungsansatzes

Es bedarf eines intuitiv nutzbaren Werkzeugs, welches es den Nutzern ermöglicht, informiert und selbstbestimmt mit ihren personenbezogenen Daten im dynamischen und virulenten Marktumfeld zu agieren. Dieses Werkzeug benötigt zum einen ein Datenwertmanagement als wesentlichen Baustein. Es muss zum einen herausgefunden werden, welchen subjektiven Wert Daten für den Nutzer haben (können), um zum anderen einen objektiven Wert für die Daten bestimmen zu können. In Ansehung einer möglichst hohen Nutzerfreundlichkeit muss dieses Werkzeug in seiner Ausgestaltung und Anwendbarkeit einfach und leicht zugänglich sein. Es muss sichtbar werden, dass es die Interessenkonflikte von Verbrauchern und Unternehmen aufgreift und löst. Ziel sollte ein intuitives Portal zum Schutz der Datensouveränität in der Datenwirtschaft sein, das zu einer

74 Assion/Schneider, TTDSG, § 25 Rn. 30 f.

75 Langhanke/Schmidt-Kessel, EuCML 2015, 218 (219).

zentrale Anlaufstelle für Verbraucher wie auch Unternehmen wird, um personenbezogene Daten objektiv und fair zu bewerten bzw. bewerten zu können.

Die Einrichtung eines solchen Portals bedarf zunächst einiger Voruntersuchungen. Insbesondere müssen rechtskonforme Metriken entwickelt werden, die es ermöglichen, den Datenwert zu bestimmen. Da dieser Datenwert je nach Blickwinkel (ob aus Unternehmer- oder Nutzersicht) unterschiedlich ausfallen kann, ist vorab eine Untersuchung auf Basis eines quantitativen Marktforschungsansatzes angezeigt.⁷⁶ Bezogen auf konkrete Kaufentscheidungen könnte den Probanden (in der Rolle von Verbrauchern) hier aufgezeigt werden, ob sie den genannten Kaufpreis für ein digitales Produkt zahlen wollen oder personenbezogene Daten dafür preisgeben wollen. Indem die Preishöhe stetig angepasst wird, lässt sich hier die Schwelle Preis-personenbezogenes Datum bestimmen und in der Folge ein auf den Probanden bezogener subjektiver Wert des Datums. Nachdem den Probanden daraufhin unternehmerische Verarbeitungsmöglichkeiten aufgezeigt werden und sie über die Reichweite der Datenverarbeitung informiert werden (und damit dem Wert aus unternehmerischer Sicht), könnte der gleiche Test erneut stattfinden und so ein objektivierter Daten-Wert gebildet werden. Dies gibt zur Vorbereitung der Darstellung des Werkzeugs wertvolle Aufschlüsse hinsichtlich folgender Fragen: Welche Datenfreigaben sind dem Konsumenten mehr wert als andere? Gibt es unterschiedliche Präferenzen bezogen auf die Personengruppen? Gibt es Datenfreigaben, die nach erfolgter Aufklärung tabu sind? Daraus wiederum folgen wertvolle Hinweise (auch aus unternehmerischer Sicht) hinsichtlich der Frage, welche Wahlmöglichkeiten effektiv angeboten werden können oder nicht.

Die konkrete Umsetzung und Sichtbarmachung des Datenwertes kann beispielsweise in Form eines digitalen Daten-Zwillings geschehen, der auf einen Blick zeigt, welche Daten welchen Wert haben und wie sich dieser verändern könnte bzw. wird, wenn diese Daten in die Wirtschaft zur ökonomischen Verwertung gegeben werden. Letzteres lässt sich ohne weiteres auf einem Portal realisieren, auf das Unternehmer und Verbraucher gleichermaßen zugreifen können. Ein solches Portal ist auch hinreichend lebendig, so dass sich einerseits Preisschwankungen zu den Datenwerten abbilden lassen und andererseits der Tatsache Rechnung getragen werden

76 Beschrieben u.a. bei: Johnson, R. M., & Orme, B. K. (2007). *A new approach to adaptive CBC*. Sawtooth Software Inc. Sawtooth Software Research Papers Series.

kann, dass Daten – anders als Entgelt – mehrfach als Preis eingesetzt werden können, was ebenfalls deren Wert verändern würde.

Die vorgestellte Lösung (das „Datenwirtschaftsportal“) muss zwingend als unabhängige und objektive Instanz funktionieren, wenn sie als wichtiges Element die Aufklärung während der vertragsrechtlichen Willensbildung unterstützen, und zur datenschutzrechtlichen Folgeabschätzung hinsichtlich der Konsequenzen der Einwilligung beitragen soll. Sie muss Vertrauen generieren. Die Dynamik, die in einer solchen Portallösung angelegt ist, kann fortlaufend weitere Entwicklungen aufnehmen und hierdurch das Konzept der datenschutz- und datenschuldrechtlichen Symbiose weiter ausgestalten. Das Nutzerverhalten wird dabei fortlaufend evaluiert werden müssen, um auf Basis neuer Erkenntnisse und Entwicklungen das Portal fortlaufend anzupassen. Ferner bleibt die Darstellung des Datenwertes hinreichend flexibel, der sich aufgrund der Häufigkeit des Datenbereitstellens, der Nutzerpräferenzen und aufgrund des Einsatzgebietes beim Bezahlen mit Daten verändern wird. Daten erhalten einen „Marktpreis“, ähnlich wie Aktien oder Emissionswerte. Ferner können neu aufkommende, digitale Ökosysteme über das Portal stetig berücksichtigt und eingebunden werden. Hinzu kommt, dass die Erfahrung der Nutzer im Umgang mit ihren personenbezogenen Daten nicht nur in das Design des Portals einfließen, sondern durch das Nutzen des Portals wachsen wird. Selbst wenig reflektierende Gruppen, wie z. B. Minderjährige oder ältere Nutzer können (und werden) ein Gefühl für den Wert ihrer personenbezogenen Daten entwickeln. Eine stetige Evaluation stellt schließlich sicher, dass das Portal synergetisch mit Nutzern und Unternehmen (d. h. den Akteuren am Markt) zusammenspielt. Es soll kein regulierender Markt geschaffen werden (welcher weitere Fragen mit sich bringt), sondern es soll ausschließlich die Selbstbestimmung der Verbraucher gesteigert werden, sodass deren Teilhabe an datenbasierten, digitalen Geschäftsmodellen möglich wird und sich über die erlangten Erkenntnisse die Datenwirtschaft insgesamt weiter entwickeln lässt.

7. Ergebnis

Die vorangegangene Untersuchung hat gezeigt, wie das neue Datenschuldrecht auf Grundlage der DURL in das deutsche Zivilrecht implementiert wurde. Es wurde festgestellt, dass die im Vorfeld und auch nach Inkrafttreten der DURL und der §§ 327 ff. BGB geäußerten rechtlichen Bedenken

lösbar sind und dass ein Ausgleich von datenschuld- und datenschutzrechtlichen Vorgaben möglich ist. Die objektiv bestehenden Konflikte sind allesamt versöhnbar und können im Interesse des Verbraucherschutzes einer lebensnahen Lösung zugeführt werden.

Die noch verbleibenden Probleme zeigen sich auf subjektiver Seite, zum einen bei der Bildung des eindeutigen vertraglichen Rechtsbindungswillens und zum anderen bezogen auf die Informiertheit und Freiwilligkeit der Einwilligung bezüglich der Herausgabe von Daten in datenschutzrechtlicher Hinsicht. Um dennoch Privatautonomie und informelle Selbstbestimmung zur Entfaltung zu bringen, haben wir ein „Datenwirtschaftsportal“ vorgeschlagen, welches dazu beitragen kann, die erkannten Defizite zu überwinden. Zum einen macht es den Preis für Daten und damit die Gegenleistung auch in Verträgen nach §§ 327 ff. BGB hinreichend transparent und nachvollziehbar. Zum anderen verhilft es den Verbrauchern zu bewussten, informierten und freiwilligen Entscheidungen im Sinne der DSGVO.

In der neu aufkommenden Datenwirtschaft kann sich die Plattform zu einem unverzichtbaren Werkzeug entwickeln, wenn alle Akteure im Markt, die Verbraucher und Unternehmen, dort synergetisch zusammenwirken. Dies würde zugleich die allgemeine Akzeptanz bezüglich der Datenwirtschaft sowohl auf Verbraucher- als auch auf Unternehmensseite befördern. Wenn es zudem gelingt, die Entwicklung eines solchen Portals nicht nur anzustoßen, sondern dynamisch weiterzuentwickeln, kann dieses jedenfalls den Zweispalt zwischen Datensouveränität der Verbraucher und monetären Interessen der Datenwirtschaft auflösen und auch als Beispiel für weitere Anwendungen dienen, wenn das Konstrukt des Bezahls mit Daten nicht nur im digitalen Umfeld etabliert wird, sondern auch nicht-digitale Produkte einen alternativen Preis bekommen.

Literatur

- Assion, Simon (Hrsg.) (2022): TTDSG. Baden-Baden: Nomos.
- Bittner, Lydia (2022): Verträge über digitale Produkte – der Beginn des digitalen Zeitalters im BGB. *Verbraucher und Recht (VuR)*, 1/22, S. 9-15.
- Blassl, Johannes (2023): Neues digitales Vertragsrecht – Teil I. *Zeitschrift für Wirtschafts- und Bankrecht, Wertpapiermitteilungen (WM)*, 41/23, S. 1907-1912.
- Blassl, Johannes (2023): Neues digitales Vertragsrecht – Teil II. *Zeitschrift für Wirtschafts- und Bankrecht, Wertpapiermitteilungen (WM)*, 42/23, S. 1941-1946.
- Buchner, Benedikt (2016): Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. *Datenschutz und Datensicherheit (DuD)*, 40(3), S. 155-161. <https://doi.org/10.1007/s11623-016-0567-0>

- Bundesregierung (2021). Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. BT-Drs. 19/27653. Berlin: Deutscher Bundestag.
- Cameron, William Bruce (1963): *Informal Sociology, A Casual Introduction to Sociological Thinking*. New York: Random House.
- Dammann, Ulrich (2016): Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwarteter Fortschritt, Schwächen und überraschende Innovationen. *Zeitschrift für Datenschutz (ZD)*, 7/16, S. 307-314.
- Do, Thomas (2021): Items, Waffen und Skins – 5 Spiele mit extrem teuren Inhalten. Esports.com vom 30.05.2021. <https://www.esports.com/de/items-waffen-und-skins-5-spiele-mit-extrem-teuren-inhalten-215415> (abgerufen am 30.01.2024).
- European Data Protection Board (EDPB) (04.05.2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (abgerufen am 07.02.2024).
- European Data Protection Supervisor (EDPS) (14.03.2017): Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte. https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_de.pdf (abgerufen am 05.02.2024).
- Felsch, Johannes Claudio, Kremer, Julian und Wagener, Jonas (2022). Handhabung der neuen Aktualisierungspflicht bei digitalen Produkten. Anwendungsbereich, Inhalt und Dauer anhand zweier konkreter Beispiele. *Multimedia und Recht (MMR)*, 1/22, S. 18-23.
- Gesmann-Nuissl, Dagmar (2019): Rechtsprechungsreport. *Zeitschrift zum Innovations- und Technikrecht (InTeR)*, 4/19, S. 190-195.
- Gesmann-Nuissl, Dagmar, Kunitz, Stephan und Rätze, Michael (2022): Chefsache Aktualisierung – mehr Sicherheit durch Updatepflicht. In: *Cyber-Sicherheit ist Cheffinnen- und Chefsache, Tagungsband zum 18. Deutschen IT-Sicherheitskongress, 2022*. Bonn: SecuMedia, 2022, S. 35 – 50.
- Gesmann-Nuissl, Dagmar and Meyer, Stefanie (2023): From Self to Avatar as Likeness: Legal Barriers and Opportunities. In: *International Conference on Human-Agent Interaction (HAI '23), December 04-07, 2023, Gothenburg, Sweden*. ACM, New York, NY, USA. <https://doi.org/10.1145/3623809.3623935>
- Gesmann-Nuissl, Dagmar and Meyer, Stefanie (2022): Siri 2.0 - Conversational Commerce of Social Bots and the New Law of Obligations of Data: Explorations for the Benefit of Consumer Protection. *Robotics*, 11(6), S. 125. <https://doi.org/10.3390/robotics11060125>
- Gierschmann, Sibylle (2016): Was „bringt“ deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt. *Zeitschrift für Datenschutz (ZD)*, 2/16, S. 51-55.
- Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *Kommentar Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. 3. Aufl. München: C.H.Beck.
- Grüneberg, Christian (Hrsg.) (2023): *Kommentar Bürgerliches Gesetzbuch*. 82. Aufl. München: C.H.Beck.

- Guinnessworldrecords: Most Valuable Virtual Object. <https://www.guinnessworldrecords.com/world-records/92207-most-valuable-virtual-object> (abgerufen am 18.04.2024).
- Güster, Florian und Brooke, Christina (2022): Umsetzung der Warenkaufrichtlinie. Rechtssichere Implementierung von negativer Beschaffenheitsvereinbarung und Verjährungsverkürzung bei Gebrauchtwagen im Internet. *Multimedia und Recht (MMR)*, 2/22, S. 92-97.
- Hacker, Philipp (2019): Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht. *Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW)*, 2/19, S. 148-197.
- Johnson, Richard M. und Orme, Bryan K. (2007). A New Approach to Adaptive CBC. Sawtooth Software Research Paper Series. <https://sawtoothsoftware.com/resources/technical-papers/a-new-approach-to-adaptive-cbc>.
- Kirchhefer-Lauber, Anna (2021): Verbraucherverträge über digitale Produkte. Die deutsche Umsetzung der Digitale-Inhalte-Richtlinie im BGB. *Juristische Schulung (JuS)*, 12/21, S. 1125-1129.
- Kollmar, Frederika und Schirmbacher, Martin (2020): Kommentar zum Urt. d. BGH v. 28.05.2020, Az. I ZR 7/16. *Wettbewerb in Recht und Praxis (WRP)*, 8/20, S. 1015-1017.
- Kramme, Malte (2021): Vertragsrecht für digitale Produkte. Die Umsetzung der Digitale-Inhalte-Richtlinie im Schuldrecht AT. *Recht Digital (RDl)*, 1/21, S. 20-29.
- Langhanke, Carmen und Schmidt-Kessel, Martin (2015): Consumer Data as Consideration. *Journal of European Consumer and Market Law (EuCML)*, 6/2015, S. 218-223.
- Martini, Mario, Drews, Christian, Seeliger, Paul und Weinzierl, Quirin (2021): Dark Patterns. Phänomenologie und Antworten der Rechtsordnung. *Zeitschrift für Digitalisierung und Recht (ZfDR)*, 1/21, S. 47-74.
- Mayer, Maximilian und Möllnitz, Christina (2021): Gewährleistung für „smarte“ Produkte nach Umsetzung der Digitale Inhalte- und Warenkauf-Richtlinie. *Recht Digital (RDl)*, 7/21, S. 333-340.
- Meller-Hannich, Caroline (2021): Die Warenkaufrichtlinie und ihre Umsetzung. *Deutsches Autorecht (DAR)*, 9/21, S. 493-497.
- Norberg, Patricia A., Horne, Daniel R. und Horne, David A. (2007): The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs (JCA)*, 41(1), S. 100-126.
- Paal, Boris P. und Wais, Niklas (2022): Ein Update für das BGB: Die Umsetzungen der Warenkauf- und Digitale-Inhalte-Richtlinie im Überblick. *Deutsches Steuerrecht (DStR)*, 23/22, S. 1164-1168.
- Riehm, Thomas (2022): Verträge über digitale Dienstleistungen. *Recht Digital (RDl)*, 5/22, S. 209-216.
- Riehm, Thomas und Abold, Metawi Adrian (2021): Rechtsbehelfe von Verbrauchern bei Verträgen über digitale Produkte. Einführung in das neue Gewährleistungsrecht für die Digitalisierung. *Computer und Recht (CR)*, 8/21, S. 530-540.
- Säcker, Jürgen, Rixecker, Roland, Oetker, Hartmut und Limperg, Bettina (Hrsg.) (2022): Münchner Kommentar zum BGB, Band 3. 9. Auflage. München: C.H.Beck.
- Sattler, Andreas (2017): Personenbezogene Daten als Leistungsgegenstand. *JuristenZeitung (JZ)* 72/21, S. 1036-1046.

- Schmidt-Kessel, Martin und Grimm, Anna (2017): Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten. *Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW)*, 1/17, S. 84-108.
- Schmitz, Barbara und Buschuew, Ellen (2022): (Be-)Zahlen mit Daten. Im Spannungsverhältnis zwischen Verbot mit Erlaubnisvorbehalt und Privatautonomie. *Multimedia und Recht (MMR)*, 3/22, S. 171-176.
- Schreier, Hans-Georg und Michels, André (2022): Negative Beschaffenheitsvereinbarung im digitalen Vertragsrecht und bei Waren mit digitalen Elementen. Zum praktischen Umgang mit Mängellisten. *Recht Digital (RDi)*, 9/22, S. 381-390.
- Simitis, Spiros, Hornung, Gerrit und Spiecker gen. Döhmman, Indra (Hrsg.) (2019): *Datenschutzrecht*. 1. Auflage. Baden-Baden: Nomos.
- Spindler, Gerald (2021): Umsetzung der Richtlinie über digitale Inhalte in das BGB. Schwerpunkt 1: Anwendungsbereich und Mangelbegriff. *Multimedia und Recht (MMR)*, 6/21, S. 451-457.
- Spindler, Gerald (2021): Ausgewählte Rechtsfragen der Umsetzung der digitalen Inhalte-Richtlinie in das BGB. Schwerpunkt 2: Rechtsbehelfe, Beweislastregelungen und Regress zwischen Unternehmern. *Multimedia und Recht (MMR)*, 7/21, S. 528-533.
- Stierle, Martin (2021): Der Regierungsentwurf zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. *IP-Rechtsberater (IPRB)*, 3/21, S. 66-71.
- Wolff, Heinrich Amadeus, Brink, Stefan und v. Ungern-Sternberg, Antje (Hrsg.) (2023): *BeckOK Datenschutzrecht*. 46. Aufl. (Stand 01.11.2023). München: C.H.Beck.