ANDREAS SATTLER

Informationelle Privatautonomie

Jus Privatum
264

Mohr Siebeck

JUS PRIVATUM

Beiträge zum Privatrecht

Band 264

Andreas Sattler

Informationelle Privatautonomie

Synchronisierung von Datenschutz- und Vertragsrecht

Mohr Siebeck

Andreas Sattler, geboren 1982; Studium der Rechts- und Wirtschaftswissenschaften in Bayreuth und Nottingham (LL.M.); Promotionsstipendium der DFG und Mitgliedschaft im DFG-Graduiertenkolleg „Geistiges Eigentum und Gemeinfreiheit", Universität Bayreuth; Dissertation (Emanzipation und Expansion des Markenrechts, Mohr Siebeck, 2015); Rechtsanwalt im Bereich IT-Recht bei CMS Hasche Sigle, Stuttgart; Akademischer Rat a.Z. am Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums und Wettbewerbsrecht an der Ludwig-Maximilians-Universität München; Habilitation; Lehrbefähigung für die Fächer Bürgerliches Recht, Immaterialgüterrecht, deutsches und europäisches Wirtschaftsrecht und Datenrecht; Gründung und Co-Leitung des Center for Intellectual Property Law, Information and Technology (CIPLITEC); seit April 2022: Vertretung des Lehrstuhls für Zivil- und Wirtschaftsrecht, Medien- und Informationsrecht an der Albert-Ludwigs-Universität Freiburg.

Gedruckt und als Open Access Dokument zugänglich gemacht mit der freundlichen Unterstützung des *LMU Open Access Fonds*, des *LMU Post Doc Fonds*, der *Johanna und Fritz Buch Gedächtnisstiftung e.V.* und der Studienstiftung *ius vivum e.V.*

ISBN 978-3-16-161905-2 / eISBN 978-3-16-161906-9
DOI 10.1628/978-3-16-161906-9

ISSN 0940-9610 / eISSN 2568-8472 (Jus Privatum)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Gulde Druck aus der Garamond gesetzt, in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Vorwort

Daten werden seit einigen Jahren als „neues Gold" oder „Öl des 21. Jahrhunderts" bezeichnet. Diese Vergleiche hinken. Im Gegensatz zu Gold und Öl sind Daten immaterielle Güter. Infolgedessen ist ihre Nutzung weder ausschließlich noch rival. Ohne rechtliche Zuweisung beruht die Möglichkeit zur Datennutzung lediglich auf einem faktischen Zugang, allgemein zugängliche Daten kann jedermann nutzen (keine Ausschließbarkeit). Die Nutzung durch eine Person hindert nicht die zeitgleiche Nutzung dieser Daten durch weitere Personen (keine Rivalität). Kurzum: Aufgrund ihrer immateriellen Eigenschaften können Daten eine sehr vielseitig nutzbare Ressource sein.

Dies erklärt, warum Daten zunehmend in den Fokus der Gesetzgeber im europäischen Mehrebenensystem geraten und warum die Gesetzgeber nach Wegen suchen, um die Nutzung von Daten zu fördern; stets in der Erwartung, dass dadurch die wirtschaftliche Effizienz, die technische Innovation und damit letztlich der volkwirtschaftliche Wohlstand gesteigert werden. Die Vorschläge für Ansprüche auf Datenzugang und Datenüberlassung (Data Act), aber auch das Konzept einer Datentreuhand (Data Governance Act) sind aktuelle Beispiele dafür, dass der unionale Gesetzgeber nach Mechanismen sucht, um den „Datenschatz" zu heben. Dabei bezieht der Gesetzgeber zunehmend auch personenbezogene Daten ein. Er folgt damit der wirtschaftlichen Realität. Zahlreiche Dienstleistungen der Betreiber von mehrseitigen Plattformen, insbesondere von Suchmaschinen oder Kommunikationsnetzwerken, werden derzeit maßgeblich durch personalisierte Werbung finanziert. Diese basiert auf dem Einsatz von Tracking-Technologien und der Erstellung von Interessenprofilen anhand des Online-Verhaltens der Nutzer/innen. Weil diese omnipräsenten Geschäftsmodelle bei der Verabschiedung der DS-GVO jedoch weitgehend ausgeblendet wurden und zudem auch nicht berücksichtigt wurde, dass zahlreiche prominente Persönlichkeiten die vermögenswerten Bestandteile ihrer Persönlichkeitsrechte kommerziell verwerten, befindet sich die DS-GVO auf einem Kollisionskurs mit dem Schuldrecht und der ökonomischen Realität. Der Konflikt zwischen der staatlichen Pflicht zum Schutz der informationellen Selbstbestimmung einerseits und der gleichzeitigen Achtung der Privatautonomie der Datensubjekte und der datenverarbeitenden Unternehmen andererseits ist mittlerweile offenkundig. Dennoch besteht derzeit kein überzeugender rechtlicher Rahmen, der die grundrechtliche Pflicht zum Schutz der Datensubjekte und die

wirtschaftliche Realität zum Ausgleich bringt. Diese schwierige Aufgabe wird stattdessen an die Rechtsanwender und damit insbesondere an den EuGH überantwortet.

Die vorliegende Arbeit macht einen Vorschlag, wie dieses Spannungsverhältnis aus dem Schutz von Datensubjekten und der Anerkennung von personenbezogenen Daten als Objekt vertraglicher Austauschbeziehungen aufgelöst werden kann. Dabei bewahrt der Vorschlag den tradierten Rahmen des Rechts auf informationelle Selbstbestimmung, erweitert aber den Handlungsspielraum für Datensubjekte und solche datenverarbeitende Unternehmen, die keine dominanten Gatekeeper sind. Infolgedessen ermöglicht das nachfolgend vorgeschlagene Modell einer abgestützten informationellen Privatautonomie die Synchronisierung von Datenschutz- und Vertragsrecht.

Die Arbeit lag der Juristischen Fakultät der Ludwig-Maximilians-Universität München im Wintersemester 2021/22 als Habilitationsschrift vor. Sie hat entscheidend von einer Reihe von Personen profitiert. Mein Dank gilt in erster Hinsicht meinem akademischen Lehrer, Herrn Professor Ansgar Ohly, der sich früh für dieses Thema begeistern konnte und mir für diese Untersuchung ideale Bedingungen und größtmögliche Freiheiten am Lehrstuhl gewährt hat. Herrn Professor Hans Christoph Grigoleit danke ich herzlich für die sehr zügige Erstellung des Zweitgutachtens und wertvolle inhaltliche Hinweise und Anregungen. Herrn Professor Herbert Zech und Herrn Professor Matthias Leistner danke ich für zahlreiche anregende Gespräche und Diskussionen zum Thema. Herrn Professor Franz Hofmann und Herrn Professor Martin Stierle danke ich für die gute und freundschaftliche Zusammenarbeit an der LMU. Der Druck und die Zugänglichmachung als Open-Access-Publikation wurden großzügig durch den LMU Open Access Fonds, den LMU PostDoc Fonds, die Johanna und Fritz Buch Gedächtnis-Stiftung und die Studienstiftung ius vivum gefördert.

Besonders herzlich danke ich meiner Familie. Meine Frau und mein Sohn mussten mit mir durch die düsteren Täler schreiten, die eine Habilitationsschrift regelmäßig mit sich bringt. Ihnen ist diese Arbeit gewidmet.

Stuttgart, im Mai 2022 Andreas Sattler

Inhaltsübersicht

Inhaltsverzeichnis

Einführung

I. Gegenstand und Zielsetzung

Der rechtliche Schutz vor einer Verarbeitung von personenbezogenen Daten (verkürzt: Datenschutzrecht) ist ein sehr konfliktreiches Rechtsgebiet. Untersucht man das Datenschutzrecht aus privatrechtlicher Perspektive, so sind zwei große Konflikte besonders augenfällig.

Erstens befinden sich das Datenschutzrecht und die besonders erfolgreichen Geschäftsmodelle mehrseitiger Plattformen auf einem Kollisionskurs. Die amerikanischen Unternehmen *Google* (*Alphabet*), *Amazon*, *Facebook* (*Meta Platforms*), *Apple* und *Microsoft* (zusammengefasst: GAFAM) und ihre chinesischen Wettbewerber *Baidu*, *Alibaba* und *Tencent* (zusammengefasst: BAT) stehen stellvertretend für Geschäftsmodelle, die in einem großen Ausmaß auf der Verarbeitung von personenbezogenen Daten ihrer Endnutzer (und Dritter) für ein Profiling beruhen. Dieses Profiling, das durch den Einsatz von Techniken der sog. Künstlichen Intelligenz stetig verbessert wird, liefert die Grundlage dafür, Werbekunden gegen Geld eine personalisierte oder zumindest stratifizierte Werbung gegenüber den Endnutzern anbieten zu können.

Die Kollision zwischen dem Datenschutzrecht und den Geschäftsmodellen mehrseitiger Plattformen ist nicht neu. Solange Plattformbetreiber bei Verstößen gegen das Datenschutzrecht jedoch kaum ökonomische Konsequenzen zu befürchten hatten, genügte es aus ihrer Sicht, den Schutz personenbezogener Daten am Horizont zu beobachten. Das Datenschutzrecht zwang die großen Plattformbetreiber zu keinen oder allenfalls sehr geringen Anpassungen ihrer Geschäftsmodelle.

Am 25.05.2018 hat sich dieses Bild verändert. Obwohl das Potenzial für *tatbestandliche* Konflikte seit der Anwendbarkeit der DS-GVO[1] kaum zugenommen hat – die DS-GVO behält wesentliche Regelungsinhalte der Datenschutz-RL von 1995[2] bei – ist für die datenschutzrechtlich Verantwortlichen das Risiko, also die Kombination aus der Entdeckungswahrscheinlichkeit von Rechtsver-

[1] Verordnung (EU) 2016/679 v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, v. 04.05.2016, S. 1 ff.

[2] Richtlinie 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, v. 23.11.1995, S. 31 ff.

stößen und der Höhe des potenziellen Bußgelds, mit der DS-GVO grundlegend gestiegen. Indem das potenzielle Bußgeld proportional mit dem ökonomischen Erfolg des Verantwortlichen steigt, bewahrt das Datenschutzrecht seine Relevanz auch mit zunehmender Größe des datenschutzrechtlich Verantwortlichen.

Unabhängig davon, ob die Auslegung und Anwendung der DS-GVO in der Praxis ein ausreichendes Mindestmaß an Rechtssicherheit bietet,[3] ob die Kriterien und Details für die Bestimmung eines angemessenen und abschreckenden Bußgelds im Einzelfall überzeugen und ob es sinnvoll und ökonomisch tragfähig ist, den gleichen Regelungsansatz auf andere Rechtsverstöße auszudehnen.[4] Es bestehen keine Zweifel: Die potenzielle Höhe eines Bußgelds gemäß Art. 83 DS-GVO hat die alte Erkenntnis bestätigt, dass die Steuerungsfunktion des Rechts maßgeblich von effektiven Mechanismen zu dessen Durchsetzung abhängt.[5] Um Kollisionen mit der DS-GVO und potentiell hohe Bußgeldbescheide zu vermeiden,[6] sind die Plattformbetreiber zunehmend gezwungen, ihre Geschäftsmodelle, jedenfalls aber die rechtliche Beziehung zu ihren Endnutzern anzupassen.

---

[3] Erst im Jahr 2021 erreichten den EuGH erste Auslegungsfragen von fundamentaler Bedeutung: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = NZKart 2021, 306 ff.; *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[4] Vgl. Art. 26 (Geldbußen) des Vorschlags der EU-Kommission für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM(2020) 842 final (englisch: Digital Markets Act oder kurz: DMA-Vorschlag); sowie Art. 42 (Sanktionen) des Vorschlags der EU-Kommission für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG vom 15.12.2020, COM(2020) 825 final (englisch: Digital Service Act oder kurz: DSA-Vorschlag).

[5] Die Frage, wer neben den Datensubjekten und im Auftrag der betroffenen Datensubjekte (Art. 80 Abs. 1 DS-GVO) zusätzlich gemäß Art. 80 Abs. 2 und Art. 84 Abs. 1 DS-GVO zur Durchsetzung von Ansprüchen aus UWG und UKlaG aktivlegitimiert sein sollte, hat der BGH dem EuGH vorgelegt: *BGH*, Beschl. v. 28.05.2020, I ZR 186/17 = GRUR 2020, 896 (Rn. 35 ff.) – *App-Zentrum*; Für eine Begrenzung auf qualifizierte Verbände: *Köhler*, WRP 2018, 1269 (1272); *ders.*, WRP 2019, 1279 (1283); *Ohly*, GRUR 2019, 686 (688 f.); für eine durch die DS-GVO unbeeinflusste Aktivlegitimation von Mitbewerber nach dem UWG: *Uebele*, GRUR 2019, 694 (697 f.).

[6] Die luxemburgische Datenschutzbehörde (CNPD) verhängte gegen die europäische Tochter von *Amazon* mit Sitz in Luxemburg ein (nicht rechtskräftiges) Bußgeld in Höhe von 746 Mio. Euro (https://www.heise.de/news/Datenschutz-Rekordstrafe-von-746-Millionen-Euro-fuer-Amazon-in-Luxemburg-6152051.html, zuletzt abgerufen am 19.05.2022). Die französische Datenschutzbehörde (CNIL) verhängte 2019 – jeweils nur für Frankreich – eine Strafe von 50 Mio. Euro gegen *Google* (https://www.heise.de/news/DSGVO-Verstoesse-Conseil-d-Etat-bestaetigt-50-Millionen-Strafe-gegen-Google-4790235.html, zuletzt abgerufen am 19.05.2022) sowie im Dezember 2020 in Höhe von 100 Mio. Euro gegen *Google* und 35 Mio. Euro gegen *Amazon* (https://www.heise.de/news/Frankreich-Datenschuetzer-verhaengen-Millionen-Bussgelder-gegen-Google-und-Amazon-4985956.html, zuletzt abgerufen am 19.05.2022). Der Hamburgische Datenschutzbeauftragte hat wegen Verstößen gegen die DS-GVO im Beschäftigungsverhältnis für Deutschland ein Bußgeld von knapp 35,3 Mio. Euro gegen *Hennes & Mauritz* (H&M) verhängt (https://www.heise.de/news/DSGVO-Deutsche-Rekordbusse-von-35-3-Millionen-Euro-gegen-H-M-4917437.html, zuletzt abgerufen am 19.05.2022).

Besonders deutlich wird dies an dem Sachverhalt, der einem Vorlagebeschluss des *ÖOGH* zum *EuGH* zugrunde liegt.[7] Darin geht es maßgeblich darum, ob *Facebook* (jetzt: *Meta Platforms*) die personenbezogenen Daten der Endnutzer – soweit es sich dabei nicht um besonders sensible personenbezogene Daten handelt – vertragsakzessorisch und somit auf Grundlage des Nutzungsvertrags i. V. m. Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig verarbeiten kann, oder ob insoweit spezifische Einwilligungen der Endnutzer erforderlich sind. Dem Vorlagebeschluss des *ÖOGH* ging ein Urteil des *OLG Wien* voraus, in dem dieses das Profiling für personalisierte Werbung durch *Facebook* auf Grundlage eines in der österreichischen Rechtsordnung nicht ausdrücklich geregelten, also atypischen Schuldverhältnisses für rechtmäßig erachtet hatte. Nach Ansicht des *OLG Wien* ist diese Datenverarbeitung (auch) zur Finanzierung des Angebots von *Facebook* und damit zur Erfüllung dieses atypischen Nutzungsvertrags i. S. d. Art. 6 Abs. 1 lit. b DS-GVO erforderlich.[8]

Die Antwort des *EuGH* auf die nun erfolgte Vorlage des *ÖOGH* wird grundlegende Auswirkungen auf die Geschäftsmodelle der Betreiber von solchen mehrseitigen Plattformen haben, die Datensubjekten digitale Produkte bereitstellen und dieses Angebot finanzieren, indem sie mit Hilfe von personenbezogenen Daten Profile über ihre Endnutzer erstellen und diese im Verhältnis zu ihren Werbekunden für personalisierte Werbeansprache monetisieren. Abhängig davon, welche datenschutzrechtliche Grundlage der *EuGH* für solche Austauschverhältnisse zwischen Datensubjekten und Verantwortlichen heranzieht, kommt es für die Rechtmäßigkeit dieser Geschäftsmodelle auf die unionsrechtlich vereinheitlichten Anforderung an die datenschutzrechtliche Einwilligung oder auf das lediglich teilweise harmonisierte nationale Vertragsrecht der Mitgliedstaaten an.[9]

Zweitens wird anhand des Vorlagebeschlusses des *ÖOGH* auch deutlich, dass sich das europäische Datenschutzrecht und das nationale Schuldrecht der Mitgliedstaaten auf einem Kollisionskurs befinden. Die europäische DS-GVO ist weder mit dem nationalen Schuldrecht noch den privatrechtlichen Grundprinzipien synchronisiert.

Sprachlich lässt sich diese Dominanz der DS-GVO daran festmachen, dass die schuldrechtlich zutreffende Bezeichnung von personenbezogenen Daten als „Gegenleistung" einem postmodernen Sakrileg gleichgestellt wird.[10] In voraus-

---

[7] *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[8] *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27. Diese Ansicht ist nicht überzeugend, hierzu unten: Kapitel 3 C.II.4./5 und III.3.

[9] Obwohl es wenig überrascht, dass *Meta Platforms* (ehemals: *Facebook*) häufig beklagte Partei ist, birgt dieses Vorlageverfahren die Gefahr, dass der EuGH sich die Folgen seiner Entscheidung für andere, kleinere Verantwortliche zu wenig bewusst macht.

[10] *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14.03.2017, S. 10/Nr. 17; sowie: Rede von *Giovanni Buttarelli* (ehemaliger EU-Datenschutz-Beauftragter), verfügbar unter

eilender *political correctness* meidet der europäische Gesetzgeber deshalb mittlerweile[11] diesen Begriff, ohne dadurch den tatsächlich bestehenden Konflikt zwischen Datenschutz- und Schuldrecht zu lösen.[12] Zwar soll mit dem europäischen Data Act auch die Nutzung von personenbezogenen Daten verbessert werden; wie dieses Ziel sich jedoch mit den Anforderungen der DS-GVO synchronisieren lässt, bleibt einstweilen offen.[13]

Rechtlich bringen Art. 3 Abs. 8 der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL)[14] und § 327q BGB[15] diese Dominanz der DS-GVO zum Ausdruck. Zwar versucht der deutsche Gesetzgeber das nationale Schuldrecht gegenüber der DS-GVO zu immunisieren. Gemäß § 327q Abs. 1 BGB soll die Abgabe einer datenschutzrechtlichen Erklärung des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Weil jedoch per-

---

https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022 („So, even if some people treat personal data as commodity, under EU law it cannot be a commodity. There might well be market for personal data, just like there is, tragically, a market for live human organs.")

[11] Anders noch *EU-Kommission* Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM/2015/0634 final. (Art. 3 Abs. 1 des Vorschlags erstreckte den Anwendungsbereich auf „alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbraucher *als Gegenleistung* einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form *personenbezogener* oder anderer *Daten erbringt*".

[12] Ohne Bezugnahme auf die zu diesem Zeitpunkt bereits verabschiedete, aber noch nicht umsetzungspflichtige Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL) kam das *OLG Wien* zu einer anderen Beurteilung. Danach sei es insbesondere „legitim, dass ein marktwirtschaftlich operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift. […]. Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten geschuldete „personalisierte Erlebnis" in wesentlichem Maße prägt und der Beklagten zugleich die für den Aufrechterhaltung der Plattform und die Erzielung eines Gewinns notwendigen Einkünfte verschafft." *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 28. Zur fehlenden Synchronisierung zwischen DS-GVO und DID-RL, unten Kapitel 3 C.III.2.

[13] *Europäische Kommission*, Inception of Assessment, Ref. Ares(2021)3527151 v. 28.05. 2021, S. 7 (Likely impacts on fundamental rights): „Since personal data […] fall into the scope of some elements of this initiative (e. g. improving usability of data linked to natural persons), the measure will be designed in a way that fully complies with the existing rules on personal data protection and ePrivacy".

[14] ABl. v. 22.05.2019, L 136/1. Art. 3 Abs. 8 DID-RL lautet: „Das Unionsrecht betreffend den Schutz personenbezogener Daten gilt für alle personenbezogenen Daten, die im Zusammenhang mit Verträgen gemäß Absatz 1 verarbeitet werden. Insbesondere lässt diese Richtlinie die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt. Im Fall von Widersprüchen zwischen Bestimmungen dieser Richtlinie und dem Unionsrecht zum Schutz personenbezogener Daten ist letzteres maßgeblich."

[15] Eingeführt durch das Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen v. 25.06. 2021, BGBl. 2021 Teil I Nr. 37, 30.06.2021, 2123 ff.

sonenbezogene Daten tatsächlich und rechtlich zunehmend als Leistungsgegenstand behandelt und vereinbart werden und einige der derzeit ökonomisch besonders erfolgreichen Geschäftsmodelle von *GAFAM* und *BAT* – in unterschiedlichem Ausmaß – auf dem Zugang zu personenbezogenen Daten beruhen, entspricht dieser schlichte Abgrenzungsversuch in § 327q Abs. 1 BGB eher einem Wunschdenken, als dem Anspruch, die tatsächliche Realität rechtlich abzubilden.[16]

Indem § 327q Abs. 3 BGB alle Ersatzansprüche des *Unternehmers* gegen den *Verbraucher* wegen Abgabe einer datenschutzrechtlichen Erklärung ausschließt, die eine Einschränkung der rechtmäßigen Datenverarbeitung bewirkt, hat der deutsche Gesetzgeber zwar zu einem kräftigen Befreiungsschlag ausgeholt, um den gordischen Knoten aus europäischem Datenschutz- und nationalem Schuldrecht zumindest im B2C-Verhältnis zu lösen. Auf den zweiten Blick erinnert dieser Befreiungsversuch des Gesetzgebers jedoch an den verzweifelten Versuch des *Laokoon*, sich aus dem Griff der Schlangen zu befreien. § 327q BGB ist nicht in der Lage, den tatsächlich bestehenden Konflikt zwischen einer jederzeit und grundlos widerruflichen Einwilligung und dem schuldrechtlichen Prinzip des *do ut des* befriedigend aufzulösen.[17] Eine solche Lösung ist aber jedenfalls in Fällen erforderlich, in denen Datensubjekte ihre personenbezogenen Daten bewusst dafür einsetzen, um ihr monetäres Konsumbudget zu schonen (Verbraucher) oder um selbst Gewinne zu erwirtschaften (Unternehmer).

Die Ursache dafür, dass das Datenschutzrecht und das Schuldrecht sich auf Kollisionskurs befinden, ist leicht zu identifizieren. Beginnend mit dem ersten BDSG von 1977[18] beruht das deutsche und im Anschluss hieran das europäische Datenschutzrecht auf einem Verarbeitungsverbot mit Erlaubnisvorbehalt (§ 3 Abs. 1 BDSG von 1977 – jetzt: Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO). Das Schuldrecht hingegen beruht auf einer Erlaubnis mit Verbotsvorbehalt (§§ 311, 241 BGB).[19]

---

[16] Insbesondere dürfte damit auch noch nicht „jedweder Diskussion um eine mögliche Einschränkung des Widerrufsrechts […] ein Riegel vorgeschoben" worden sein. So aber: *Spindler*, MMR 2021, 528 (530). Hierzu unten Kapitel 5 C.III.

[17] Zum hier unterbreiteten Vorschlag eines befristeten Ausschlusses der Widerruflichkeit durch teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO unten Kapitel 5 C.III, sowie zuvor: *Sattler*, JZ 2017, 1036 (1041 f.). Sollte der EuGH der Rechtsauffassung von *Facebook*, des LG Wien und des OLG Wien folgen, würde das Geschäftsmodell von *Facebook* und anderen durch personalisierte Werbung finanzierten Kommunikationsplattformen nicht nur gemäß Art. 6 Abs. 1 lit. b DS-GVO weitgehend den Vorgaben der DS-GVO entgehen, sondern es entstünden auch schwerwiegende Abgrenzungsschwierigkeiten zum Anwendungsbereich der DID-RL bzw. von §§ 327 ff. BGB. Hierzu Kapitel 3 C.III.3.

[18] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung v. 27.01.1977, BGBl. I Nr. 7 S. 201 ff.

[19] Pointiert: *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, S. 153 (159: „Datenverarbeitung durch Private wird umstandslos einem staatlichen Grundrechtseingriff gleichgestellt und einem umfassenden Rechtfertigungsgebot unterworfen […]. Strukturell ist das nichts anderes als eine ins Horizontalverhältnis gekippte, unmittelbare Grundrechtsbindung Privater").

Kurzum: Bislang ist es weder dem europäischen noch dem – insoweit durch Unionsrecht gebundenen deutschen – Gesetzgeber gelungen, das Datenschutzrecht und das Schuldrecht zu synchronisieren. Auch das dem unternehmerisch handelnden Verantwortlichen gemäß § 327q Abs. 2 BGB eingeräumte, komplexe Kündigungsrecht für den Fall, dass ein als Verbraucher handelndes Datensubjekt die Datenverarbeitung für die Zukunft beendet, ist lediglich ein erster – deutscher – Versuch, diese Kollision abzumildern. Ein *Datenschuldrecht*,[20] das auch personenbezogene Daten als Leistungsgegenstand anerkennt und die ökonomische Realität rechtlich abbildet oder sogar gestaltet, lässt sich auf dieser Grundlage jedoch nicht entwickeln.

Es ist eine banale Erkenntnis, dass die Verarbeitung von personenbezogenen Daten ubiquitär ist. Sie ist zentral für Entwicklungen, die derzeit mit den schillernden Chiffren „Big Data"[21] und „künstliche Intelligenz" (KI)[22] umschrieben werden. Beiden Entwicklungen ist gemeinsam, dass sie die Verarbeitung von personenbezogenen Daten nicht voraussetzen, ihre Vorteile aber insbesondere durch eine Verarbeitung von Daten mit Personenbezug entfalten können.

Zwar sind anonymisierte Daten im Kontext von Big Data und KI nicht wertlos, solange ein abstrakter und damit wissenschaftlicher Erkenntnisgewinn angestrebt wird. Allerdings knüpfen auch der wissenschaftliche, jedenfalls aber der ökonomische Wert von Datenanalysen häufig an den Personenbezug als eine wesentliche semantische Ebene von maschinenlesbar codierter Information (kurz: personenbezogenes Datum) an.[23] Deshalb liegt der Fokus der Arbeit nicht auf der – primär technisch spannenden – Frage, wie eine Verarbeitung von personenbezogenen Daten durch Methoden der Anonymisierung effektiv vermieden oder das Risiko der Verarbeitung durch Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) und Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) verringert werden kann. Vielmehr steht die Frage im Zentrum, inwieweit die Auslegung und Anwendung der DS-GVO eine rechtmäßige und rechtssichere Verarbeitung von personenbezogenen Daten im Privatrechtsverhältnis[24] ermöglicht, ohne dabei gegen das gemäß Art. 8 GRCh (Schutz personenbezogener Daten)

---

[20] Begriffsprägend *Schmidt-Kessel*, Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, BMJV, 03.05.2016, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022.

[21] Aus rechtlicher Perspektive: *Leistner/Antoine/Sagstetter*, Big Data, 2021.

[22] Mit technischer Einführung: *Zech*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, Gutachten für den 73. Deutschen Juristentag, 2020.

[23] Zum Informationsbegriff: *Wiebe*, in: Fiedler/Ullrich (Hrsg.), Information als Wirtschaftsgut, 1997, S. 93 (99 ff.); *Zech*, Information als Schutzgegenstand, 2012, S. 14 ff./114. f./441.

[24] Die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen (Art. 88 DS-GVO i. V. m. § 26 BDSG) weist Besonderheiten auf und bleibt unberücksichtigt: Hierzu: m. w. N.: *Neighbour*, in: Sassenberg/Faber (Hrsg.), Industrie 4.0 und IoT, 2020, S. 277 ff.; *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, 2019.

und gemäß Art. 7 GRCh (Privatsphäre) zu gewährleistende Untermaßverbot zu verstoßen.

Notwendig ist eine privatrechtssensible Auslegung deshalb, weil zunehmend deutlich wird, dass der europäische Gesetzgeber bei Verabschiedung der DS-GVO die rechtliche und ökonomische Realität in den Mitgliedstaaten nur unzureichend erfasst hat. Die DS-GVO nimmt zu wenig Rücksicht auf die tatsächliche Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten, die wiederum eine Verarbeitung von personenbezogenen Daten voraussetzt.[25]

Die Notwendigkeit, bei dieser privatrechtssensiblen Auslegung und Anwendung der DS-GVO auf die Unionsgrundrechte zurückzugreifen, ist der Vielzahl der unbestimmten Rechtsbegriffe in der DS-GVO geschuldet. Diese erschweren die gerichtliche und behördliche Rechtsanwendung derzeit fundamental. Infolgedessen ist es auch für die Wissenschaft eine zentrale Herausforderung *de lege lata* und – soweit dies nicht mehr möglich ist – auch *de lege ferenda* Vorschläge für die Ausgestaltung eines Datenschuldrechts zu unterbreiten, das die informationelle Privatautonomie der Datensubjekte stärkt, dabei aber die multipolaren Grundrechtskonstellationen hinreichend berücksichtigt.[26]

Das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände zur Gewährleistung einer abgestützten informationellen Privatautonomie stellt bereits begrifflich die Privatautonomie und insbesondere die Vertragsfreiheit als ihre wichtigste Ausprägung in den Mittelpunkt. Dabei weicht der Begriff der informationellen Privatautonomie von dem bekannten Begriff der informationellen Selbstbestimmung ab. Letztere ist bereits seit dem *Volkszählungsurteil* des *BVerfG*[27] bekannt.

Diese begriffliche Unterscheidung ist jedoch kein bloßes Glasperlenspiel. Im Gegenteil: Die Gewährleistung einer abgestützten informationellen Privatautonomie ist Ausdruck eines Perspektivenwechsels und dient dazu, Grundannahmen des geltenden Datenschutzrechts kritisch zu hinterfragen, soweit personenbezogene Daten als Gegenstand eines vertraglichen Synallagmas vereinbart werden.

Im Zentrum des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände für das Privatrechtsverhältnis steht die datenschutzrechtliche Einwilligung, die ihrerseits in zwei Stufen ausdifferenziert wird. Infolgedessen ist dieses Stufenmodell in der Lage, eine Synthese aus dem datenschutzrechtlichen Verbot und der schuldrechtlichen Erlaubnis herzustellen und dadurch einem künftiges

---

[25] Zuletzt mit dieser Kritik, jedoch aus Perspektive einer Stärkung von Verbraucherrechten: *Wendehorst*, JZ 2021, 974 (984: „die DSGVO [ist] überhaupt nicht auf den Schutz vermögensrechtlicher Verbraucherinteressen […] zugeschnitten").

[26] Mit dieser Forderung an die Privatrechtswissenschaft: *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 372.

[27] BVerfGE 65, 1 (43) = NJW 1984, 419 ff. – *Volkszählung*.

Datenschuldrecht den Boden zu bereiten. Dadurch gewährleistet das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände die unionsgrundrechtlich verankerte abgestützte informationelle Privatautonomie und ermöglicht die Umsetzung von drei wesentlichen Zielen, ohne dabei den Schutz der Datensubjekte wesentlich zu beeinträchtigen:

Erstens wird die bisherige Kommerzialisierung der vermögenswerten Bestandteile von Persönlichkeitsrechten (wieder) ermöglicht, soweit diese auf eine Verarbeitung von personenbezogenen Daten angewiesen ist.

Zweitens werden personenbezogene Daten – wie von der *EU-Kommission* immer wieder und zuletzt im Kontext des Data Act gefordert – für Innovation und Wachstum im Binnenmarkt nutzbar gemacht, ohne dabei über die Präferenzen der Datensubjekte hinwegzugehen.

Drittens hilft dieses Stufenmodell und insbesondere die kartellrechtsakzessorische und damit asymmetrische Auslegung und Anwendung des Einwilligungstatbestands dabei, die durch die DS-GVO entstandenen Marktzutrittsbarrieren für KMU zu senken.

II. Forschungsstand

Spätestens seit Anfang der 1970er Jahre fordert der technische Fortschritt im Bereich der automatischen Datenverarbeitung den Schutz des Individuums vor einer Verarbeitung personenbezogener Daten immer wieder heraus.[28] Nach einer frühen kritischen Auseinandersetzung mit den ersten deutschen Gesetzen zum Schutz von natürlichen Personen vor einer Verarbeitung von personenbezogenen Daten[29] stagnierte das Interesse, das Privatrechtswissenschaftler dem Datenschutzrecht entgegenbrachten.[30] Das Feld wurde weitgehend dem Verwaltungs- und insbesondere dem Verfassungsrecht überlassen.[31]

[28] Hierzu frühzeitig: *Kilian*, Personalinformationssysteme in deutschen Großunternehmen, 1967; *ders*., Juristische Entscheidung und Elektronische Datenverarbeitung, 1974; *Steinmüller/Lutterbeck/Malmann/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826; *Steinmüller*, EDV und Recht: Einführung in die Rechtsinformatik und das Recht der Informationsverarbeitung, Juristische Arbeitsblätter 1970; *ders*. (Hrsg.), Informationsrecht und Informationspolitik, 1976.

[29] Kapitel 1 A.II.

[30] Zu den wenigen Ausnahmen zählen: *Ebnet*, Der Informationsvertrag, 1995; *A. Wagner*, Binäre Information als Gegenstand des Rechtsverkehrs, 1999; *Kilian*, CR 2002, 921 ff.; *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006; *Unseld*, Die Kommerzialisierung personenbezogener Daten, 2010; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012; *Sandfuchs*, Privatheit wider Willen?, 2015. Zudem ist *Spiros Simitis*, der erste Hessische Datenschutzbeauftragte und Herausgeber des langjährigen Standardkommentars zum BDSG, von Hause aus Privatrechtwissenschaftler.

[31] Hierzu: *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, S. 27 ff.

Obwohl einige wissenschaftliche Beiträge einen vermittelnden Ansatz wählen,[32] leidet die rechtswissenschaftliche Auseinandersetzung weiterhin unter einem – auch institutionell durch die zahlreichen Datenschutzbehörden begünstigten – Übergewicht der öffentlich-rechtlichen Perspektive. Dennoch hat die privatrechtlich ausgerichtete Forschung gerade in den letzten Jahren wegweisende Untersuchungen hervorgebracht.

Besonders hervorzuheben sind die Arbeiten von *Benedikt Buchner*,[33] *Louisa Specht-Riemenschneider*,[34] *Carmen Langhanke*,[35] *Philipp Hacker*[36] *und Jan Niklas Bunnenberg*.[37] Die nachfolgende Analyse profitiert von dieser Forschung und baut hierauf teilweise auf. Dennoch unterscheidet sich das hier vorgeschlagene Stufenmodell der Erlaubnistatbestände und die dadurch gewährleistete abgestützte informationelle Privatautonomie in mehreren wesentlichen Punkten vom bisherigen Forschungsstand.

Der Untersuchungsgegenstand der Arbeiten von *Benedikt Buchner*, *Louisa Specht-Riemenschneider* und *Carmen Langhanke* war das alte BDSG, so dass mit der Anwendbarkeit der DS-GVO – trotz deren weitreichender Kontinuität zur Datenschutz-RL von 1995 – eine Neubewertung erforderlich ist. Zudem gehen alle vorgenannten Autorinnen und Autoren – mit Ausnahme von *Benedikt Buchner* – von einer jederzeitigen und grundlosen Widerruflichkeit der datenschutzrechtlichen Einwilligung aus. Infolgedessen dominiert das Datenschutzrecht das Schuldrecht in einer Weise, die – zumindest im B2B-Verhältnis – nach hier vertretener Ansicht nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar ist. *Benedikt Buchner* wiederum spart das Verhältnis zwischen Datenschutzrecht und AGB-Recht weitgehend aus.[38]

Weil alle bisherigen Arbeiten von einer Dominanz des Datenschutzrechts gegenüber dem Schuldrecht ausgehen,[39] bleibt – jedenfalls nach hier vertretener Auffassung – nicht viel vom Grundsatz der Privatautonomie, einschließlich der Möglichkeit zur Selbstbindung, übrig.

---

[32] *Masing*, NJW 2012, 2305 ff.; *Kingreen/Kühling*, JZ 2015, 213 ff.; *von Lewinski*, Die Matrix des Datenschutzrechts, 2014.

[33] Die informationelle Selbstbestimmung im Privatrecht, 2006.

[34] *Specht*, Die Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

[35] Daten als Leistung, 2018.

[36] Datenprivatrecht, 2020.

[37] Privates Datenschutzrecht, 2020.

[38] Das ist im Ergebnis wenig schädlich, weil infolge der seit 2018 vorrangig anzuwenden Grundsätze aus Art. 5 Abs. 1 DS-GVO der AGB-Kontrolle lediglich geringe Bedeutung zukommt. Hierzu: Kapitel 3 C.I.3.; a. A. *Hacker*, Datenprivatrecht, 2020, 417 ff. (430 ff.), sowie *Wendehorst*, JZ 2021, 974 (983 f.).

[39] Für eine stärkere Berücksichtigung schuldrechtlicher Grundsätze: *Metzger*, JIPITEC 2017, 2 (6 f.); *ders*., AcP 216 (2016), 817 (833); *ders*., in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (36 ff.).

Jan Niklas Bunnenberg will der Bindungswirkung einer Erklärung von Datensubjekten nur dann gemäß Art. 6 Abs. 1 lit. b DS-GVO (sog. vertragsakzessorische Datenverarbeitung) einen Vorrang vor dem Widerrufsinteresse des Datensubjekts einräumen, wenn das Interesse des Verantwortlichen infolge einer Abwägung im Einzelfall ausnahmsweise überwiegt.[40] Dieser Ansatz überzeugt systematisch nicht, weil er die beiden Erlaubnistatbestände gemäß Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) und gemäß Art. 6 Abs. 1 lit. f DS-GVO (Datenverarbeitung infolge einer Interessenabwägung) im Ergebnis vermengt und stets auf eine *ex post*-Interessenabwägung im Einzelfall angewiesen ist.[41]

Philipp Hacker ordnet die frei widerrufliche Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) als schuldrechtliche Bedingung für die Leistungserbringung durch den Verantwortlichen ein.[42] Infolgedessen verschmelzen Software und Recht potenziell zu dem von *Lawrence Lessig* konstatierten „Code is Law".[43] Allerdings soll es dem Verantwortlichen im Fall eines allzu „opportunistischen Widerrufs" der Einwilligung durch das Datensubjekt ausnahmsweise möglich sein, die Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO fortzusetzen.[44] Sofern personenbezogene Daten vertraglich als Leistungsgegenstand vereinbart werden, soll deren Verarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig sein, soweit dieses Synallagma einer gerichtlichen Angemessenheitskontrolle standhält.[45]

Obwohl sich die von *Hacker* und in dieser Arbeit bearbeitete Thematik teilweise überschneidet, wird nachfolgend eine andere Lösung vorgeschlagen. Die Skepsis gegenüber einer gerichtlichen Angemessenheitsprüfung des vertraglichen Synallagmas mündet in den nachfolgend herausgearbeiteten Vorschlag einer abgestützten informationellen Privatautonomie, der im Unterschied zu

---

[40] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 264 f.

[41] Das Interesse des Datensubjekts am Widerruf der Einwilligung (Art. 6 Abs. 1 lit. a i. V. m. Art. 7 Abs. 3 S. 1 DS-GVO) wird mit einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) kombiniert und soll anschließend die Fortsetzung der Datenverarbeitung auf Grundlage eines bindenden Vertrags gemäß Art. 6 Abs. 1 lit. b ermöglichen. Hierzu unten Kapitel 3 B.II.

[42] *Hacker*, ZfPW 2019, 148 (172 ff.); *ders.*, Datenprivatrecht, 2020, S. 228 f.; so auch *Rafał Mańko*, Contracts for the supply of digital content and digital services, Bericht des Wissenschaftlichen Dienstes des EU-Parlaments (EPRS) vom 27.11.2017, S. 8 („The report deletes the term *counter-performance*, criticized by the EDPS, and replaces it with the term *condition*"), verfügbar unter http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf, zuletzt abgerufen am 19.05.2022; *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 37; ähnlich: *Riehm*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 194 f. Hierzu: Kapitel 4 A.II.5.

[43] *Lessig*, Code is law, 1999.

[44] *Hacker*, Datenprivatrecht, 2020, S. 278. In diese Richtung auch bereits: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 ff.

[45] *Hacker*, Datenprivatrecht, 2020, S. 445 ff./473 ff. Zu den Bedenken an einer praktischen Umsetzung dieses Ansatzes: Kapitel 3 C.I.2.e. und C.I.3. Zu den Nachteilen für die unionsweit einheitliche Wirkung der DS-GVO: Kapitel 3 C.II.

Stichwortverzeichnis