ZfDR

Zeitschrift für Digitalisierung und Recht

1/2021

INHALT:

C.H.BECK

R550202101

Impressum

Herausgeber: Prof. Dr. Susanne Beck, Lehrstuhl für Strafrecht, Strafprozessrecht, Strafrechtsvergleichung und Rechtsphilosophie, Universität Hannover; Prof. Dr. Elisa Hoven, Lehrstuhl für Deutsches und Ausländisches Strafrecht, Strafprozessrecht, Wirtschafts- und Medienstrafrecht, Universität Leipzig; Ministerialrat Dr. Armin Jungbluth, Referatsleiter Rechtsfragen digitale Dienste, Medienwirtschaft, Bundesministerium für Wirtschaft und Energie, Berlin; Prof. Dr. Torsten Körber, LL.M. (Berkeley), Lehrstuhl für Bürgerliches Recht, Kartell- und Regulierungsrecht, Recht der digitalen Wirtschaft, Universität zu Köln; Prof. Dr. Jürgen Kühling, LL.M. (Brüssel), Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht, Universität Regensburg, Vorsitzender der Monopolkommission; Prof. Dr. Mario Martini, Lehrstuhl für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht, Leiter des Programmbereichs Transformation des Staates in Zeiten der Digitalisierung, Deutsche Universität für Verwaltungswissenschaften Speyer; Prof. Dr. Boris Paal, M.Jur. (Oxford), Direktor des Instituts für Medien- und Informationsrecht, Universität Freiburg/Brsg.; Prof. Dr. Dr. Frauke Rostalski, Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung, Universität zu Köln; Prof. Dr. Louisa Specht-Riemenschneider, Lehrstuhl für Bürgerliches Recht, Informations- und Datenrecht, Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht, Universität Bonn.

Schriftleitung: Prof. Dr. Boris Paal, M.Jur. (Oxford), Direktor des Instituts für Medien- und Informationsrecht, Universität Freiburg/Brsg. (verantwortlich für den Textteil)

E-Mail: zfdr@beck.de. Für weitere Informationen: http://www.zfdr.beck.de, ISSN 2703-0776

Verlag: C.H.BECK oHG, Wilhelmstr. 9, D-80801 München, Postanschrift: Postfach 400340, 80703 München, Tel.: 089/38189-0, Telefax: 089/38189398, Postbank München Nr. 6229-802, BLZ 70010080. Der Verlag ist oHG. Gesellschafter sind Dr. Hans Dieter Beck und Dr. h.c. Wolfgang Beck, beide Verleger in München.

Verlagsredaktion: RA Dr. Klaus Winkler, E-Mail. Klaus.Winkler@beck.de, Telefon: (089) 38189-353, Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München

Erscheinungsweise: Vier Hefte jährlich.

Bezugspreise: Die aktuellen Bezugspreise finden Sie im beck-shop. Bestellungen über jede Buchhandlung und beim Verlag.

KundenServiceCenter: Tel.: 089/38189-750, Fax 089/38189-358, E-Mail: abo.service@beck.de; Abbestellungen müssen 6 Wochen vor Jahrgangssende erfolgen.

Adressenänderungen: Bei Adressenänderungen muss neben dem Titel der Zeitschrift die neue und alte Adresse angegeben werden.

Inhaltsverzeichnis

Autorenverzeichnis

Prof. Dr. Boris Paal, M.Jur. (Oxford)
Institut für Medien- und Informationsrecht,
Abt. I (Privatrecht)
Albert-Ludwigs-Universität Freiburg
Rempartstraße 4
79098 Freiburg
boris.paal@jura.uni-freiburg.de

Ass. iur. Christian Drews
Deutsches Forschungsinstitut
für öffentliche Verwaltung (FÖV)
Freiherr-vom-Stein-Str. 2
67346 Speyer
drews@foev-speyer.de

Prof. Dr. Jürgen Kühling, LL.M.
Vorsitzender der Monopolkommission
Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht
Universität Regensburg
Universitätsstraße 31
93053 Regensburg
juergen.kuehling@jura.uni-regensburg.de

Paul Seeliger, M.Jur. (Münster)
Deutsches Forschungsinstitut
für öffentliche Verwaltung (FÖV)
Freiherr-vom-Stein-Str. 2
67346 Speyer
seeliger@foev-speyer.de

Prof. Dr. Dr. Frauke Rostalski
Institut für Strafrecht und Strafprozessrecht
Universität zu Köln
Albertus-Magnus-Platz
50923 Köln
ls-rostalski@uni-koeln.de

Ass. iur. Quirin Weinzierl, LL.M. (Yale)
Deutsches Forschungsinstitut
für öffentliche Verwaltung (FÖV)
Freiherr-vom-Stein-Str. 2
67346 Speyer
weinzierl@foev-speyer.de

Malte Völkening
Institut für Strafrecht und Strafprozessrecht
Universität zu Köln
Albertus-Magnus-Platz
50923 Köln
malte.voelkening@uni-koeln.de

Dr. Alexander Bijok
Triftstraße 52
13353 Berlin
alexanderbijok@gmx.de

Prof. Dr. Mario Martini
Deutsche Universität für
Verwaltungswissenschaften Speyer
Freiherr-vom-Stein-Str. 2
67346 Speyer
martini@uni-speyer.de

Editorial

Prof. Dr. Boris Paal, M.Jur. (Oxford)[*]

Liebe Leserinnen und Leser!

Mit dem Verlag und der gesamten Herausgeberschaft freue ich mich sehr, Ihnen das erste Heft unserer neuen Zeitschrift für Digitalisierung und Recht (ZfDR) vorlegen zu dürfen. Die Verantwortlichen eröffnen mit der ZfDR ein sowohl intra- als auch interdisziplinäres Forum für die Befassung mit Rechtsfragen, die durch die Entwicklungen, Prozesse und Folgen der Digitalisierung induziert werden. Das als klassische, vierteljährlich erscheinende Archivzeitschrift ausgestaltete Periodikum versteht sich als Leitmedium für den akademischen Diskurs, in dem über Entwicklungen, Perspektiven und Standpunkte informiert und diskutiert werden wird. In diesem Sinne will die ZfDR eine Plattform bereitstellen, um die grundlagenbezogene Auseinandersetzung mit der Digitalisierung als einem der prägenden Phänomene im und für das 21. Jahrhundert zu bereichern und voranzutreiben.

Die Zeitschrift verfolgt einen fachsäulenübergreifenden intra- und interdisziplinären Ansatz, der Grundsatzfragen im Schnittfeld von Recht und Digitalisierung adressiert; zugleich bietet das Format auch hinreichend Raum für Gedankenexperimente und die Behandlung von Praxisfolgen. Mit dieser umfassenden Ausrichtung wird sowohl eine Abgrenzung zu bestehenden Publikationen als auch ein Alleinstellungsmerkmal des Angebots begründet, das eine Lücke auf dem Markt schließt und auf die wachsende Nachfrage zu digitalisierungsbezogenen Themen reagiert. Thematisch angesprochen sind vor allem Grundlagenfächer (wie etwa Rechtsethik, Rechtsphilosophie, Rechtsgeschichte und Rechtsvergleichung), Zivilrecht, Strafrecht, Öffentliches Recht, Völkerrecht, Wirtschaftsrecht, IT-Recht sowie Wettbewerbs- und Regulierungsrecht. Hierbei sollen stets die wirtschaftlichen, kulturellen, technischen und gesellschaftlichen Entwicklungsdynamiken, so insbesondere auch die Hausforderungen an das Recht durch digitale Innovationen adäquat Berücksichtigung finden. Stellvertretend für diesen Zugriff steht die Befassung mit dem Antidiskriminierungsrecht, Datenrecht, Immaterialgüterrecht und Sicherheitsrecht ebenso wie die Auseinandersetzung mit den Themenfeldern Künstliche Intelligenz, Autonome Systeme, Blockchain- und Legal Tech-Anwendungen sowie der Plattform-Ökonomie und Intermediären. Insgesamt will die ZfDR der Natur des Themenfelds „Digitalisierung und Recht" als Querschnittsmaterie sowohl in einzelnen Beiträgen als auch in der Gesamtkonzeption der einzelnen Hefte umfassend Rechnung tragen. Das Heft 1, das Sie in den Händen halten, spiegelt diesen breiten, fachsäulenübergreifenden thematischen Anspruch wider: Es erwarten Sie Beiträge zur datenschutzrechtlichen Rahmung von Datentreuhändern (*J. Kühling*), zu Big Data im Strafrecht (*F. Rostalski/M. Völkening*), zu Dark Patterns (*M. Martini/C. Drews/P. Seeliger/Q. Weinzierl*) und zur Kommerzialisierung von personenbezogenen Daten (*A. Bijok*).

---

[*] Der Autor ist Inhaber des Lehrstuhls für Zivil- und Wirtschaftsrecht, Medien- und Informationsrecht sowie Direktor des Instituts für Medien- und Informationsrecht (Abt. I: Privatrecht) an der Albert-Ludwigs-Universität Freiburg.

Ihrer grundlagenbezogenen Ausrichtung entsprechend ermöglicht die ZfDR die Publikation auch und gerade von längeren Beiträgen bis zu einem Umfang von 25 Seiten/80.000 Zeichen. Daneben finden sich in der neuen Zeitschrift über die klassischen Formate (so neben Aufsätzen auch Entscheidungsbesprechungen und Rezensionen) hinaus alternative und innovative Rubriken, wie etwa die „Miniatur". Eine solche Miniatur gibt in der Form eines Kurztextes wertvolle Denkanstöße für neue(re) Fragestellungen im Zeitalter der Digitalisierung und regt zum weiteren Austausch an. Zudem werden in der ZfDR regelmäßig Neuerscheinungen empfohlen, die sich mit der digitalen Transformation insbesondere auch aus philosophischer Sicht oder der Perspektive der Informatik befassen. Schließlich präsentiert die neue Zeitschrift Hinweise auf Termine, Veranstaltungen und moderne Formate der Wissenschaftskommunikation, wie etwa interessante Meinungsblogs oder Apps.

Bitte fühlen Sie, liebe Leserinnen und Leser, sich herzlich aufgefordert, Manuskriptangebote und interessante Mitteilungen an die Schriftleitung heranzutragen sowie mit uns in einen Dialog einzutreten. Wir freuen uns auf einen regen Austausch mit allen, die sich der wachsenden Schar der an dem Themenfeld „Digitalisierung und Recht" Interessierten zugehörig fühlen.

Abschließend wünsche ich Ihnen im Namen aller Herausgeberinnen und Herausgeber eine ebenso spannende wie anregende Lektüre, hoffe darauf, Sie künftig zum festen Leserinnen- und Leserkreis rechnen zu dürfen und bin gespannt auf Ihre Rückmeldungen!

Herzlich
Ihr

Boris Paal
Schriftleiter

Der datenschutzrechtliche Rahmen für Datentreuhänder

Chance für mehr Kommerzialisierungsfairness und Datensouveränität?

Prof. Dr. Jürgen Kühling, LL.M.[*]

In der Realwelt sind zunehmend Datentreuhänder zu beobachten, die als Intermediäre zwischen den Datenver-arbeitern einerseits und den betroffenen Personen andererseits vermitteln. Ihnen wird zu Recht ein Potenzial zugesprochen, dass die betroffenen Personen mit ihrer Hilfe ihre informationelle Selbstbestimmung einschließlich kommerzieller Verwertungsinteressen des Persönlichkeitsrechts gegenüber den Verantwortlichen besser wahrnehmen und auf diese Weise sowohl die Datensouveränität als auch die Kommerzialisierungsfairness steigern können. Im Folgenden wird geprüft, ob das Datenschutzrecht – vor allem der Datenschutzgrundver-ordnung – einen angemessenen Rahmen für jene neuen Akteure bereitstellt oder ob insoweit Anpassungen erforderlich sind, wie sie zuletzt auch von der Kommission in einer „Daten-Governance-Verordnung" vorgeschlagen wurden.

Inhaltsübersicht

[*] Der Autor ist Inhaber eines Lehrstuhls für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht an der Universität Regensburg. Der Beitrag geht in weiten Teilen zurück auf die vom Autor angefertigten rechtlichen Ausführungen in einer für das Bundesministerium für Arbeit und Soziales erstellten interdisziplinären Studie „Datenschutzrechtliche Dimensionen – Datentreuhänder", im WWW abrufbar unter http://ftp.iza.org/report_pdfs/iza_report_104.pdf (zul. aufgerufen am 1.12.2020). Der Autor dankt Dr. Florian Sackmann und Prof. Hilmar Schneider für die zahlreichen Anregungen in diesem Projekt.

I. Einführung

1. Breite der Diskussion

Fragen einer gerechten Datenordnung gehören zu den spannendsten und komplexesten Rechtsfragen der Gegenwart. Dabei geht es sowohl um personenbezogene als auch um nicht personenbezogene Daten. Verschiedene Diskussionen zur Anwendung und Modifikation des geltenden Rechts überlappen sich hier gegenwärtig, so dass es zunehmend schwer fällt, den Überblick zu behalten. Ausgangspunkt ist oftmals ein Unbehagen gegenüber der Entwicklung, dass sich in Deutschland und Europa immer größere Datenbestände in den Händen weniger, oftmals US-amerikanischer Anbieter befinden – von Facebook über Google bis Amazon. Im Kartellrecht werden daher gegenwärtig im Rahmen der 10. GWB-Novelle neue Regeln geschaffen, die unter engen Voraussetzungen einen Zugang zu jenen Datenschätzen marktbeherrschender Unternehmen im Falle eines missbräuchlichen Ausnutzens ihrer Stellung eröffnen.[1] Zugleich

[1] Siehe insbesondere den Vorschlag zur Präzisierung der Essential-Facilities-Missbrauchsvorschrift in § 19 Abs. 2 Nr. 4 GWB und die neuen Regelbeispiele im neuen § 19a GWB, Referentenentwurf des Bundesministeriums für Wirtschaft und Energie, Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen und für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz); siehe dazu die Informationen im WWW abrufbar unter der URL https://bmwi.de/Redaktion/DE/Arti-

soll insgesamt das Kartellrecht geschärft werden, um die Macht der großen Plattformunternehmen einzuhegen. Parallel dazu wurde Anfang Dezember von der Kommission der Entwurf eines „Digital Markets Act" vorlegt, der auf supranationaler Ebene sogar noch schärfere kartellrechtliche und regulatorische Regeln schaffen soll.[2] Parallel dazu gibt es auf nationaler und supranationaler Ebene bereits sektorspezifische Regeln, die darauf abzielen, insbesondere im Verkehrssektor den Zugang zu Daten zu verbessern.[3] In Deutschland wurde zuletzt eine Reformdebatte angestoßen, um den Datenzugang im Bereich der Personenbeförderung zu erleichtern.[4] Hinzu kommen verschiedene Diskussionen (etwa zu einer Neuregelung des Dateneigentums[5]), die bislang noch nicht zu legislativen Konsequenzen geführt haben.

Erste Regelungsansätze lassen sich dagegen in Bezug auf das vorliegende Verständnis der Datentreuhänder erkennen. Für den sehr engen Regelungskontext der „Personal Information Management Services" (PIMS) bei Telekommunikations-diensten wurde im Vorschlag für ein deutsches Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) im vorliegenden Referentenentwurf eine erste Regelung in einem Paragrafen (§ 3) aufgenommen.[6] Danach soll den Endnutzern eine bessere Kontrolle ihrer personenbezogenen Daten ermöglicht werden. Der Betroffene kann seine Daten mittels PIMS verwalten und für mehrere Fälle einheitlich, entweder nach Kategorien oder nach Transaktionen, in die Weitergabe und Verarbeitung seiner Daten einwilligen. Dies soll einen einfacheren und rechtssicheren Datenhandel ermöglichen.[7] In der Norm wird klargestellt, dass Endnutzer ihre Rechte über anerkannte PIMS ausüben können. Dies umfasst insbesondere die Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten oder das Speichern von Informationen auf Endeinrichtungen sowie Zugriff auf dort gespeicherte Informationen. Es finden sich auch Regelungen zur Freiwilligkeit und der erforderlichen Aufklärung des Endnutzers. Die Anerkennung des Dienstes erfolgt zur Wahrung einheitlicher Maßstäbe über den BfDI. Ein Dienst kann anerkannt werden, wenn der Betreiber ein taugliches Sicherheitskonzept vorlegt, durch das er die Voraussetzungen zum Datenschutz und zur Datensicherheit erfüllen kann, wenn er kein wirtschaftliches Eigeninteresse an den verwalteten Daten hat und außerdem unabhängig von Unternehmen ist, die ein solches Interesse haben könnten.

Ende November hat die Europäische Kommission den breiter angelegten Vorschlag einer Daten-Governance-Verordnung vorgelegt. Diese verfolgt nicht nur die ambitionierten Ziele, die Bereitstellung von Daten im öffentlichen Sektor voranzutreiben, die gemeinsame Nutzung von Daten durch Unternehmen gegen Entgelt zu erleichtern und eine Datennutzung aus altruistischen Gründen zu eröffnen, sondern sieht erstmals spezifische Bestimmungen zur Regelung der „Mittler für die gemeinsame Nutzung perso-

---

kel/Service/Gesetzesvorhaben/gwb-digitalisierungsgesetz.html (zul. aufgerufen am 1.12.2020); siehe zu § 19a GWB auch exemplarisch *Kühling*, Unter verschärfter Beobachtung, NZKartR 2020, S. 630 f.

[2] Siehe dazu die Informationen im WWW abrufbar unter der URL https://ec.europa.eu/digital-single-market/en/digital-services-act-package (zul. aufgerufen am 16.12.2020).

[3] Siehe etwa ABl. 2010 L 207, 1.

[4] Vgl. dazu den Vorschlag eines neuen § 3a im Personenbeförderungsgesetz Referentenentwurf der Bundesregierung eines Gesetzes zur Modernisierung des Personenbeförderungsrechts, Stand 3.11.2020, im WWW abrufbar unter der URL https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/entwurf-gesetz-personenbefoerderungsrecht.pdf?__blob=publicationFile (zul. aufgerufen am 1.12.2020).

[5] Siehe dazu kritisch *Kühling/Sackmann*, Irrweg „Dateneigentum". Neue Großkonzepte als Hemmnis für die Nutzung und Kommerzialisierung von Daten, ZD 2020, 24 ff.

[6] Abrufbar im WWW unter der URL https://cdn.netzpolitik.org/wp-upload/2020/08/20200731_RefE_TTDSG-clean.pdf (Abruf: 1.12.2020).

[7] Siehe dazu allgemein *Peitz*/*Schweizer*, Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018, S. 275 (278).

nenbezogener Daten“ im Sinne der DS-GVO vor.[8] Diese auch als „Datentreuhänder“ bezeichneten Akteure können ebenfalls einen entscheidenden Beitrag zu einer fairen Datenordnung für personenbezogene Daten leisten, da sie als Mittler zwischen den betroffenen Personen und den Verarbeitern Erstere bei der Ausübung ihrer Rechte unterstützen können. Datentreuhänder können nicht nur die Datensouveräntität[9] der betroffenen Personen im Umgang mit ihren Daten stärken, sondern zugleich deren damit verbundenen kommerziellen Verwertungsinteressen besser schützen. In diesem Sinne können sie einen Beitrag zur „Kommerzialisierungsfairness“ in der Datenordnung leisten, die eine notwendige Voraussetzung der Zulässigkeit von Datenverarbeitungsprozessen darstellt – sei es auf der Basis einer Einwilligung (s. dazu Art. 7 DS-GVO) bzw. allgemein nach Art. 8 Abs. 2 GrCH bzw. Art. 5 Abs. 1 lit. a DS-GVO („fairly“ bzw. „fairness“[10] – in der englischsprachigen Fassung; „Treu und Glauben“ in der deutschsprachigen Fassung).

Datentreuhänder könnten zugleich als zusätzliche Marktakteure die Macht der „Internetgiganten“ relativieren. Ob sich der „Hoffnungsträger“ der Datentreuhänder durchsetzen wird, ist nicht nur eine Frage der Datenökonomie als ein ebenfalls spannendes Forschungsfeld in den Wirtschaftswissenschaften, sondern auch eine Frage des richtigen normativen Rahmens.

Hintergrund der rechtlichen Herausforderungen ist dabei eine doppelte Schwierigkeit: Zum einen kursieren gegenwärtig nicht nur teils sehr unterschiedliche Vorstellungen, was unter dem Begriff des „Datentreuhänders“ zu verstehen ist, sondern es ist darüber hinaus allenfalls im Ansatz zu erahnen, welche Datentreuhänder-Modelle sich überhaupt in der Realwelt etablieren werden. Zum anderen ist das Datenschutzrecht auch nach dem Inkrafttreten der Datenschutz-Grundverordnung im Mai 2018 immer noch mit erheblichen Unsicherheiten befrachtet. Ein unsicherer „Lebenssachverhalt“ trifft also auf ein Rechtsgebiet, das keine große Rechtssicherheit ausstrahlt. Das macht die aufgeworfenen Fragen aber umso spannender. Dabei fehlt es bislang an vertieften rechtswissenschaftlichen Untersuchungen zu Datentreuhändern im geltenden Recht, die über grobe Problem- und Lösungshinweise hinausgehen. Letztere sind bislang auch eher von Institutionen entwickelt worden.[11] Die Diskussion um den Einsatz von Datentreuhändern ist dabei allerdings keineswegs auf die Europäische Union beschränkt, sondern wird etwa auch in den USA geführt. Das verwundert wenig, sind doch die US-amerikanischen Grundlagen des Schutzes der Privatheit mit dem „Right of Privacy“[12] und dem „Right of Publicity“[13] als dessen Gegenstück von Grund auf sehr viel enger mit dem Gedanken der Kommerzialisierung verbunden,[14] als dies bei der unionsrechtlichen und spezifischer der deutschen persönlichkeitsrechtlichen Dogmatik als Basis des Datenschutzes der Fall ist. So werden Datentreuhänder („Trustee“) etwa in den

[8] Vorschlag für eine Verordnung des EP und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) COM(2020) 767 final vom 25.11.2020, im WWW abrufbar unter der URL https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0767&from=EN (zul. aufgerufen am 1.12.2020).

[9] Dazu am Beispiel der Verarbeitung von Gesundheitsdaten *Kühling*, Gesundheitsdatenschutzrecht im Zeitalter von „Big Data“ – Zeit für eine Neukonzeption nach den Vorschlägen des Ethikrates zur Sicherung einer „Datensouveränität“?, DuD 2020, 182 ff.

[10] Aber auch in einer Vielzahl weiterer Stellen der DS-GVO wird in der englischen Sprachfassung auf den Begriff „fair“ verwiesen (siehe nur Art. 6 Abs. 2 und 3, 13 Abs. 1, 14 Abs. 2, 40 Abs. 2 lit. a und zahlreiche Erwägungsgründe, namentlich 39, 42, 45, 60, 71); siehe dazu auch *Kalimo/Majcher*, The concept of fairness: linking EU competition and data protection law in the digital marketplace, E. L. Rev. 2017, 210.

[11] Siehe dazu insbesondere die in der Fn. 22 zitierten Studien und Stellungnahmen.

[12] *Warren/Brandeis,* The Right to Privacy, Harv. L. Rev. 1890, 200 f.

[13] *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953).

[14] *Peukert,* Persönlichkeitsbezogene Immaterialgüterrechte?, ZUM 2000, 718.

Kontext der Bedeutung der Vertrauensgewährleistung („trust“) in einer Welt des „Überwachungskapitalismus“ („surveillance capitalism“[15]) gerückt.[16] Sehr grundlegend haben etwa *Kang/Shilton/Estrin/Burke/Hansen* als Ergebnis eines interdisziplinären Projekts ein Plädoyer für Datentreuhänder entwickelt, die als „Privacy Data Guardian“ die Daten Privater („Privacy Data Vaults“) verwalten und eine stärker selbstbestimmte Datenverarbeitung ermöglichen sollen.[17]

2. Unterschiedliche Verwendung des Begriffs des Datentreuhänders und heterogene Business-Modelle in der Realwelt

In der Realwelt lassen sich bereits verschiedene Business-Modelle und demzufolge teils gänzlich unterschiedliche Konzepte von Datentreuhändern beobachten. Der verbindende Kern dieser sehr heterogenen Anwendungsfälle ist die Einschaltung eines Dritten.

Bis vor Kurzem etwa vermarktete Microsoft ein Cloud-Angebot für datenschutzbewusste deutsche Unternehmen als Datentreuhänder-Modell. Allerdings ging es nur darum, dass die gespeicherten Daten in Rechenzentren der Deutschen Telekom und damit auf europäischem Territorium verarbeitet werden und Mitarbeiter von Microsoft hierauf nur im Ausnahmefall Zugriff erhalten. Gleichwohl hat dieses Angebot in der juristischen Fachliteratur und auch in der Datenschutzpraxis Aufmerksamkeit erlangt, ging es doch um die spannende Frage, inwiefern dadurch die Daten vor extraterritorialen Zugriffen US-amerikanischer Ermittlungsbehörden geschützt werden können.[18] Dies entspricht jedoch nicht dem vorliegenden Verständnis von „Datentreuhändern“.

Das gilt auch für die im Zuge der Gestaltung des autonomen Fahrens teilweise anzutreffende Verwendung des Begriffs des „Datentreuhänders“ für Anwendungsfälle, in denen die Kfz-Daten bei einer neutralen Stelle gespeichert werden, um bei einem Unfall einen privilegierten Zugang einer der Parteien (Fahrzeugführer/Hersteller) zu vermeiden.[19]

Ausgangspunkt ist also in diesen Konstellationen stets, dass ein Datentreuhänder als dritte Person zwischen verschiedene Akteure geschaltet wird. Dies gilt auch für Angebote, die in der Praxis anzutreffen sind, um das Datenschutzmanagement als Mittler für die Betroffenen zu verbessern, und die im Fokus des vorliegenden Beitrags stehen. Ein zentraler Aspekt ist dabei oftmals eine Unterstützung bei der Abgabe von Einwilligungserklärungen im Sinne des Betroffenen. Jene Angebote sind in Deutschland teils

---

[15] Der Begriff wurde geprägt von *Zuboff*, The Age of Surveillance Capitalism. The Figth for a Human Future at the New Frontier of Power, 2019 (deutsche Ausgabe: Das Zeitalter des Überwachungskapitalismus, 2019); siehe auch als Kurzfassung *dies*., Surveillance Capitalism – Überwachungskapitalismus, APuZ 2019, 4.

[16] Zu letzterem etwa *Richards/Hartzog*, Taking Trust Seriously in Privacy Law, 19 Stan. Tech. L. Rev. 2016, 431; siehe ähnlich auch *Waldman*, Privacy as Trust: Sharing Personal Information in a Networked World, 69 U Miami L Rev 2016, 559.

[17] Siehe ferner *Peppet*, Privacy & the Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries, Iowa Law Review Bulletin 97 2012/2013, 77 und *Regan*, Reviving the Public Trustee Concept and Applying It to Information Privacy Policy, Maryland Law Review 76 2017, 1025

[18] Dazu ausführlich auch unter Analyse der umstrittenen rechtlichen Bewertung in der US-amerikanischen Gerichtspraxis *Schwartz/Peifer*, Datentreuhändermodelle – Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte?, CR 2017, 165 ff.; vgl. ferner *Rath/Kuß/Maiworm*, Die neue Microsoft Cloud in Deutschland mit Datentreuhand als Schutzschild gegen NSA & Co.? Eine erste Analyse des von Microsoft vorgestellten Datentreuhänder-Modells, CR 2015, 98 ff.

[19] Siehe dazu die Analyse bei *Brockmeyer*, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge? Erwägungen zur ausstehenden Regulierung des Speicherorts für die Daten nach § 63a Abs. 1 StVG, ZD 2018, 258 ff.

aus Forschungsprojekten heraus entstanden.[20] Dem vorliegenden Verständnis eines Datentreuhänders nahe kommen etwa Angebote wie „MyData.org“. Kerngedanke der Dienste jener Non-Profit-Organisation ist es, Betroffene transparent darüber zu informieren, wer was wann über sie weiß, ihnen zu helfen, festzulegen, wer die Daten nutzen darf, und diese Entscheidungen im Laufe der Zeit einfach anpassen zu können.[21] Dabei sollen auch Schnittstellen mit Daten verarbeitenden Unternehmen und anderen Akteuren hergestellt werden, so dass eine Kollaboration zwischen dem Intermediär auf beiden Seiten – Verantwortliche und Betroffene – erfolgen soll, im beiderseitigen Interesse aber primär zur Verwirklichung der informationellen Selbstbestimmung der Betroffenen. Teilweise fokussieren sich einzelne Anbieter auch auf spezifische Teilelemente, indem sie etwa Daten ankaufen, anonymisieren und weiterverkaufen. So wirbt der Anbieter „Datacoup“ damit, dass die Internet-Giganten persönliche Daten wie ein öffentliches Gemeingut zu ihren Gunsten ausgebeutet haben, ohne die Betroffenen an den dabei entstehenden Gewinnen angemessen zu beteiligen. Deshalb will „Datacoup“ die Betroffenen als Intermediär bei der Monetarisierung unterstützen.[22] Etwas abweichend davon, aber von der Zielrichtung durchaus vergleichbar, fokussiert das Diensteangebot von „Weople“ vor allem darauf, in großem Umfang das Recht auf Datenportabilität aus Art. 20 DS-GVO für die Betroffenen geltend zu machen, um diese Daten anschließend anonymisiert und unter Beteiligung der Betroffenen am Gewinn zu kommerzialisieren.[23]

3. Begriffselemente eines „Datentreuhänders“ im vorliegenden Kontext und Modelle

In der vorliegenden Betrachtung geht es von diesen zuletzt genannten, exemplarischen ersten „Business“-Modellen für Datentreuhänder ausgehend spezifisch um Intermediäre zwischen den beiden Hauptakteuren des Datenschutzrechts, nämlich den Datenverarbeitern einerseits und den betroffenen Personen andererseits. Nach dem hier zugrunde liegenden Verständnis wird der Datentreuhänder als Vertrauensperson von der betroffenen Person eingesetzt, um die informationelle Selbstbestimmung einschließlich kommerzieller Verwertungsinteressen des Persönlichkeitsrechts gegenüber den Verantwortlichen besser wahrzunehmen.[24] Dies ist etwa denkbar, um Daten an einen Mittelsmann zu übergeben, der sie pseudonymisiert und anschließend dem Verantwortlichen zur Verfügung stellt. Damit kann beispielsweise gewährleistet werden, dass, wenn keine Re-Pseudonymisierung möglich ist, die Daten für den Verantwortli-

[20] Siehe insoweit die Darstellung bei *Horn/Riechert/Müller* in Stiftung Datenschutz (Hrsg.), Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, 12 ff., abrufbar im WWW unter der URL https://stiftungdatenschutz.org/fileadmin/ Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Studie_Neue_Wege_zur_Einwilligung_final.pdf (zul. aufgerufen am 1.12.2020), unter Hinweis insbesondere auf digi.me, LETsmart (Legalisation, Exchange, Transparency), Constent Management for Federated Data Sources (CoMaFeDS), MesInfos, Mydata, MyPermissions, Accesss my Info, Citizenme, Datacoup, personiq, PGuard, Humada, Consberry.

[21] Siehe nähere Informationen im WWW abrufbar unter der URL https://mydata.org/mydata-101/ (zul. aufgerufen am 1.12.2020).

[22] Siehe nähere Informationen im WWW abrufbar unter der URL https://datacoup.com/#first-stop (zul. aufgerufen am 1.12.2020).

[23] Siehe nähere Informationen im WWW abrufbar unter der URL https://weople.space/en/ (zul. aufgerufen am 1.12.2020).

[24] Siehe dazu etwa *Verbraucherzentrale Bundesverband*, Positionspapier vom 19.2.2020, im WWW abrufbar unter der URL https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zul. aufgerufen am 1.12.2020).

chen gar keine personenbezogenen Daten darstellen. Dieser kann mit den – für ihn nicht personenbezogenen – Daten ohne die Restriktionen des Datenschutzrechts agieren. Darüber hinaus kann der Datentreuhänder umfassender in die Datenschutzpräferenzen des Betroffenen eingeweiht werden, um anschließend als Agent für diesen eingesetzt zu werden. So kann der Betroffene die informationelle Selbstbestimmung mit Blick auf die Vielzahl von Datenverarbeitungsprozessen bei der Nutzung diverser Angebote im Internet besser wahrnehmen und von einer Vielzahl von datenschutzrechtlich relevanten Aktionen – insbesondere von Einwilligungserklärungen, aber auch der Nutzung von Betroffenenrechten – entlastet werden. Das ist gerade auch mit Blick auf die immer schnelleren, umfangreicheren und häufigeren Datenverarbeitungsprozesse („Big Data") und erst recht beim Einsatz von Künstlicher Intelligenz von Relevanz. Zugleich soll es dabei insbesondere um die kollektive Durchsetzung des Datenschutzrechts durch Datentreuhänder gehen.

Damit besteht eine weitreichende Überlappung mit dem verbreiteten Verständnis der sogenannten „Personal Information Management Systems (PIMS)". Im Ausgangspunkt geht es bei entsprechenden Diensteanbietern vor allem um ein besseres Management der Einwilligung – gerade in ihrer dynamischen Perspektive – und der Datenschutzpräferenzen. Darüber hinaus können diese jedoch gleichermaßen auf weitere Datenschutzrechte wie die Betroffenenrechte erweitert werden.[25]

Diese Mittlerfunktion entspricht auch dem Verständnis der Kommission von „Mittlern für die gemeinsame Nutzung personenbezogener Daten" im Kommissions-Vorschlag für eine Daten-Governance-Verordnung, wie dessen Art. 9 (insbesondere Abs. 1 lit. b) deutlich macht, auch wenn sich keine entsprechende Definition im Katalog der Begriffsbestimmungen (Art. 2) des Entwurfs findet.

4. Gliederung des Beitrags

Entscheidend ist daher im Kern, inwiefern das geltende Datenschutzrecht eine entsprechende Ausübung wesentlicher Gestaltungsrechte (Einwilligung, Betroffenenrechte etc.) durch einen Datentreuhänder überhaupt zulässt (dazu II.). Für die Verwirklichung von Datentreuhänder-Modellen relevant ist auch, welche Anforderungen an die Datensicherheit greifen und ob diese der Verwirklichung des Ansatzes prinzipiell im Wege stehen (dazu III.). Dasselbe gilt für die Frage nach deren Verantwortung und Haftung (dazu IV.). Auf der Basis dieser Untersuchung zentraler Steuerungsvorgaben des geltenden Rechts kann sodann die Frage beantwortet werden, inwiefern etwaige Defizite einer normativen Anpassung bedürfen, um die Durchsetzung von Datentreuhänder-Modellen zu erleichtern und wenn ja, ob dies im EU-Recht oder im deutschen Recht zu erfolgen hat (dazu VI.).

[25] Siehe dazu insbesondere *Verbraucherzentrale Bundesverband*, Positionspapier vom 19.2.2020, S. 7 f., a.a.O.; siehe ferner *Europäische Kommission*, An emerging offer of „personal information management services", 2016, im WWW abrufbar unter der URL https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 (zul. aufgerufen am 1.12.2020) und *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, 2019, S. 133 f., https://bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf (zul. aufgerufen am 1.12.2020); *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016, s. 6, https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (zul. aufgerufen am 1.12.2020).

II. Datenschutzrechtliche Anforderungen an die Übertragung wesentlicher Gestaltungsrechte an Datentreuhänder

Mit Blick auf die Frage, inwiefern das geltende Datenschutzrecht eine entsprechende Ausübung wesentlicher Gestaltungsrechte durch einen Datentreuhänder zulässt, geht es in materiell-rechtlicher Hinsicht v.a. um die Einwilligung nach Art. 7 DS-GVO (dazu 1.). In prozeduraler Perspektive steht die Ausübung der Betroffenenrechte im Vordergrund (dazu 2.).

1. Vermittlung der datenschutzrechtlichen Einwilligung über Datentreuhänder

Für die Bewertung einer Übertragung datenschutzrechtlicher Gestaltungsrechte an Datentreuhänder ist zu differenzieren. Stellt ein Datentreuhänder etwa nur ein Tool zur Verfügung, um dem Nutzer einen besseren Überblick über die bei unterschiedlichen Verantwortlichen verarbeiteten Daten zu bieten, so ist dies unproblematisch. Letztlich agiert der Datentreuhänder in diesem Fall lediglich als „Bote" des Nutzers, übermittelt also eine fremde Einwilligungserklärung. Komplexer werden die Fragen, wenn dem Datentreuhänder ein eigener Entscheidungsspielraum zusteht, er also eine eigene Einwilligung im fremden Namen abgibt und somit als „Stellvertreter" des Nutzers auftritt oder aber die datenschutzrechtlichen Gestaltungsrechte an sich selbst abtreten lässt und dann im eigenen Namen agiert. Letztlich sind die denkbaren Konstellationen und Geschäftsmodelle noch zu unabsehbar, als dass eine Einordnung in die entsprechenden Kategorien möglich oder sinnvoll wäre. Für die rechtliche Bewertung ist insoweit auch nur von Bedeutung, welche Anforderungen an die Übertragung von Rechten an einen Datentreuhänder zu stellen sind, dem selbst ein gewisser Entscheidungsspielraum zusteht. Diese Frage wird im Folgenden analysiert.

a) Prinzipielle Vertretungsmöglichkeit; allgemeine Anforderung für Datentreuhänder

In Bezug auf die Einwilligung ergeben sich aus allgemeinen Grundsätzen dabei nähere Überlegungen zur Person des Einwilligenden, die so nicht ausdrücklich in der DS-GVO geklärt wurden. So umfasst das Recht auf informationelle Selbstbestimmung grundsätzlich auch die Befugnis des Einzelnen, zu entscheiden, ob er dieses Recht höchstpersönlich oder unter Einschaltung eines Vertreters ausüben möchte. Jedoch gelten für die Erteilung einer entsprechenden Vollmacht – soweit übertragbar – die gleichen Voraussetzungen wie sie auch für die Einwilligung selbst gelten. Daher muss auch die Vollmacht insbesondere zweckbestimmt erteilt werden (dazu näher c)). Eine Generalvollmacht zur umfassenden und unbegrenzten Wahrnehmung des Rechts auf informationelle Selbstbestimmung wäre wegen ihrer fehlenden Unbestimmtheit unwirksam. Ferner muss die Vollmacht ebenso wie die Einwilligung in informierter Weise erteilt werden (dazu näher b)) – jedenfalls insoweit, als die betroffene Person selbst eine Vorstellung von den grundsätzlichen Rahmenbedingungen haben muss, unter denen der Vertreter eine Einwilligung mit Wirkung für und gegen sie erteilt. Darüber hinaus gilt für die Vollmacht, ebenso wie für die Einwilligung selbst, der Grundsatz der jederzeitigen freien Widerrufbarkeit (dazu näher d)). Schließlich sind die Besonderheiten beim Einsatz im Rahmen der Verwaltung von Daten von Kindern zu beachten (dazu e)).

Im Übrigen müssen die weiteren Wirksamkeitsvoraussetzungen des Art. 7 Abs. 4 i.V.m. Art. 4 Nr. 11 DS-GVO erfüllt sein. Die Freiwilligkeit der Einwilligung weist dabei für sich betrachtet keine zusätzlichen Herausforderungen auf, da – gerade im Fall der Entwicklung verschiedener Treuhänder-Modelle[26] – die Betroffenen eine Auswahl bekommen und im Übrigen jederzeit auf das Einschalten eines Treuhänders verzichten können. Auch die Transparenz muss im Rahmen der Ausgestaltung der Einwilligungserklärung gewährleistet sein, sodass – trotz fehlenden Schriftformerfordernisses – angesichts der Komplexität nur eine schriftliche Einwilligung in Betracht kommt. Diese muss schon wegen des Nachweisbarkeitserfordernisses (Art. 7 Abs. 1 DS-GVO) angemessen dokumentiert werden, was jedoch ohnehin schon aus Transparenzgesichtspunkten von den Datentreuhändern gewährleistet sein sollte.

b) Herausforderung 1: Informiertheit der Einwilligung

Größere Schwierigkeiten mit Blick auf Datentreuhänder-Modelle wirft das im Unionsrecht in Art. 4 Nr. 11 DS-GVO ebenfalls geforderte Maß an hinreichender Informiertheit des Einwilligenden auf. Dies ist schon für einzelne Anbieter mit komplexen Datenschutzerklärungen und schwer verständlichen Datenverarbeitungsprozessen oftmals problematisch. Wenn nun der Datentreuhänder darüber hinaus in Bezug auf eine Vielzahl derartiger Akteure das Einwilligungsmanagement übernehmen soll, potenziert sich grundsätzlich das Ausmaß an Informationen. Wie hier der Spagat zwischen einer möglichst umfassenden Information des Betroffenen auf der einen und der Vermeidung der Überforderung auf der anderen Seite bewerkstelligt werden kann, lässt sich nicht abstrakt-generell beantworten. Vielmehr wird es hier an den Datentreuhändern liegen, entsprechende Informationsmechanismen zu entwickeln, die eine Komplexitätsreduktion vorsehen, aber gleichwohl das Ziel der Informiertheit erreichen. Gerade darum geht es ja im Kern bei Datentreuhänder-Modellen. So sollen die Betroffenen einerseits entlastet werden. Andererseits kann nur eine betroffene Person, die alle entscheidungsrelevanten Informationen kennt, Risiken und Vorteile der Einwilligung abschätzen und eine darauf basierende Entscheidung treffen. Ihre Einwilligung kann sich auch nur auf die Umstände beziehen, die ihr bekannt sind. In eine unbestimmte Datenverwendung kann sie daher nicht wirksam einwilligen. Die Datentreuhänder trifft daher wie jeden Verantwortlichen eine umfassende Informationspflicht, insbesondere hinsichtlich der Arten von verarbeiteten Daten, des Verarbeitungszwecks, der Identität des Verantwortlichen und dessen Erreichbarkeit und an welche Empfänger ggf. Daten übermittelt werden, die er *vor* Einholung der Einwilligung erfüllen muss (vgl. im Einzelnen Art. 12 und 13 DS-GVO).[27] Mit Blick auf das Ziel eines möglichst dynamischen Einsatzes von Datentreuhändern müssen diese grundsätzlich auch sinnvolle Aktualisierungsmechanismen entwickeln.

c) Herausforderung 2: (Zweck-)Bestimmtheit der Einwilligung

Gerade wenn die eingesetzten Technologien dynamische Einwilligungen ermöglichen sollen, wird die ohnehin schon komplexe Frage der Bestimmtheit der Einwilligung gegenüber dem Datentreuhänder besonders virulent. Letztlich geht es dabei auch

[26] Sollte es zu einem monopolistischen Anbieter kommen, wären allerdings besondere Anforderungen mit Blick auf das Koppelungsverbot nach Art. 7 Abs. 4 DS-GVO zu beachten; dazu und zum Folgenden *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 499 ff. (im Erscheinen).

[27] Vgl. *Buchner/Kühling* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 7 DS-GVO Rn. 59 f.

um die Möglichkeit etwaiger Zweckänderungen. Insoweit ist in der DS-GVO jedenfalls eine gewisse Flexibilisierung angelegt.

Das Erfordernis der Bestimmtheit der Einwilligungserklärung (Art. 5 Abs. 1 lit. b und Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO), das sich unmittelbar aus dem Zweckbindungsgrundsatz ableitet,[28] steht dabei in engem Zusammenhang mit der Informiertheit. Die betroffene Person kann nur dann die Vorteile und Risiken der Einwilligung einschätzen, wenn sie zum einen in der Lage ist, den Inhalt der Einwilligung zu verstehen und wenn zum anderen die Einwilligungserklärung hinreichend konkret abgefasst ist. Blankoeinwilligungen und pauschal gehaltene Einwilligungserklärungen sind unwirksam.[29]

Dies ist bei einem Datentreuhänder, der über eine Einwilligung eine Vielzahl von Datenverarbeitungsprozessen einer Vielzahl anderer Verantwortlicher legitimieren soll, eine große Herausforderung. Auch insoweit müssen die Treuhänder komplexitätsreduzierende und dynamische Erläuterungsmechanismen entwickeln.

Denn um dem Gebot der Bestimmtheit zu genügen, sind nicht nur die Daten oder die Art der Daten zu benennen, sondern grundsätzlich auch die einzelnen konkreten Phasen der Datenverarbeitung. Das erforderliche Maß an Bestimmtheit lässt sich allerdings nur in der Zusammenschau mit der konkreten Verarbeitungssituation ausmachen. Bei einer Vielzahl von – unter Umständen auch noch komplexen – Verarbeitungsphasen kann nicht die Benennung eines jeden einzelnen Verarbeitungsschrittes gefordert werden. Es reicht dann aus, wenn die relevanten, für die Beurteilung der Tragweite der Erklärung wesentlichen Phasen der Verarbeitung beschrieben sind. Ein gewisser Grad an Unvollständigkeit muss dann schon aus Gründen der Klarheit und der Verständlichkeit hingenommen werden. Umgekehrt sind an das Maß an Bestimmtheit umso höhere Anforderungen zu stellen, je mehr der Persönlichkeitsschutz der betroffenen Person berührt wird.[30] Dies kann gerade bei Datentreuhändern, die zur besseren Verwirklichung des Selbstbestimmungsrechts der betroffenen Personen eingesetzt und gegebenenfalls durch sinnvolle Kontrollmechanismen (etwa eine Governance-Struktur, die das auch absichert) kontrolliert werden, gewisse Vereinfachungen ermöglichen, während gegenüber Verantwortlichen, die in egoistischem Interesse handeln, eher keine Erleichterungen denkbar sind. In diese Richtung zielt von der Logik her auch die Differenzierung zwischen altruistischen und sonstigen Datenmittlern in der von der Europäischen Kommission vorgeschlagenen Daten-Governance-Verordnung (dazu oben I.1. und unten V.4.b)). Hier werden sich die Details erst in Reaktion auf entsprechende Treuhänder-Modelle in der Realität und deren Bewertung durch Datenschutzaufsichtsbehörden entwickeln können. Diese Entwicklung könnte durch klarstellende Hinweise in entsprechenden aufsichtsbehördlichen Dokumenten unterstützt werden (etwa des Europäischen Datenschutzausschusses zur Einwilligung; dazu unten V.5.).

Sofern Datentreuhänder auch Gesundheitsdaten oder andere besondere Kategorien personenbezogener Daten verwalten, muss sich die Einwilligung gemäß Art. 9 Abs. 2 lit. a DS-GVO zudem ausdrücklich auf diese Daten beziehen.

---

[28] *Buchner/Kühling* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 7 DS-GVO Rn. 61.

[29] So zum BDSG a.F. BGH, Urt. v. 19.9.1985 – III ZR 213/83 = BGHZ 95, 362 (367 f.); Urt. v. 10.7.1991 – VIII ZR 296/90 = BGHZ 115, 123 (127); Urt. v. 11.12.1991 – VIII ZR 4/91 = BGHZ 116, 268 (273).

[30] Zum BDSG a.F. *Holznagel/Sonntag* in Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.8 Rn. 49.

d) Herausforderung 3: jederzeitige Widerrufbarkeit

Ganz allgemein stellt das Erfordernis der jederzeitigen Widerrufbarkeit von Einwilligungserklärungen bei bereits begonnener Datenverarbeitung ein Problem dar; bei Datentreuhändern verschärft sich dieses. Die unter dem BDSG a.F. vertretene Auffassung, dass die betroffene Person nur widerrufen konnte, wenn ihr das Festhalten an der Einwilligung objektiv nicht länger zuzumuten war, etwa weil der Verantwortliche die vom Einwilligungsinhalt gezogenen Verarbeitungsgrenzen überschritt oder erforderliche Maßnahmen zur Datensicherheit nicht durchführte oder angesichts sensibler Daten ein Entscheidungswandel den überwiegenden berechtigten Interessen der betroffenen Person entsprach,[31] stößt sich an der Vorgabe der jederzeitigen Widerrufbarkeit in Art. 7 Abs. 3 S. 1 DS-GVO. Andererseits findet sich der Grundsatz von Treu und Glauben auch in der DS-GVO wieder (Art. 5 Abs. 1 lit. a DS-GVO). Ob sich Einschränkungen vor dem Hintergrund dieser scharfen Formulierung weiterhin aufrechterhalten lassen, ist gleichwohl zweifelhaft. Überzeugend erscheint es aber durchaus, jedenfalls in umfassenden Vertragsverhältnissen gewisse Einschränkungen im Interesse der Praktikabilität zuzulassen.[32] Diese dürften dann erst recht für Datentreuhänder gelten. Auch insoweit wären allerdings klärende Hinweise von den Aufsichtsbehörden für Datentreuhänder hilfreich.

e) Besonderheiten beim Einsatz im Rahmen der Verwaltung von Daten von Kindern

Gerade bei den vielfältigen Angeboten im Internet stellt sich schließlich die Frage, ob Datentreuhänder auch im Rahmen der Vertretung bei der Erteilung der Einwilligung von Kindern eingesetzt werden können. Hier sieht die DS-GVO in Art. 8 ausdrücklich Fälle vor, in denen es um die personenbezogenen Daten von Kindern geht, denen direkt sog. Dienste der Informationsgesellschaft angeboten werden.[33] Die Einwilligung muss hier nach Art. 8 Abs. 1 DS-GVO durch den Träger der elterlichen Verantwortung erteilt werden. Alternativ ist auch eine persönliche Einwilligung durch das Kind möglich, dann jedoch mit Zustimmung des Trägers elterlicher Verantwortung. Selbst einwilligungsfähig sind Kinder nach Art. 8 Abs. 1 DS-GVO erst ab Vollendung des 16. Lebensjahres. Diese Vorgaben gelten im Fall des Einsatzes eines Datentreuhänders gleichermaßen. Auch hier könnten Datentreuhänder sogar ein besonderes Potenzial entfalten, da sie die Träger der elterlichen Verantwortung von teils – zeitlich und/oder fachlich – überfordernden Legitimationsentscheidungen entlasten und viel besser eine strukturierende Legitimation generieren können.

2. Ausübung der Betroffenenrechte durch Datentreuhänder

Der Einsatz von Datentreuhändern erscheint sodann für die Ausübung sämtlicher Betroffenenrechte attraktiv. Als erstes sind hier das Recht auf Löschung (Art. 17 DS-GVO) und der Auskunftsanspruch (Art. 15 DS-GVO) zu nennen. So kann gerade durch die technische Versiertheit eines eingeschalteten Intermediärs eine intervallartige Kontrolle im Rahmen der Ausübung eines Auskunftsanspruchs erfolgen, welche Daten

[31] Vgl. zur Rechtslage unter dem BDSG a.F. *Simitis* in Simitis (Hrsg.), Kommentar zum BDSG, 8. Aufl. 2014, § 4a Rn. 99 f.; dem auch unter der DS-GVO folgend *Schaffland/Holthaus* in Schaffland/Wiltfang (Hrsg.), DS-GVO/BDSG, EL 10/17 Stand: Dezember 2017, Art. 7 DS-GVO Rn. 55.

[32] Vgl. dazu *Buchner/Kühling* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 7 DS-GVO Rn. 38 ff.

[33] *Buchner/Kühling* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 8 DS-GVO Rn. 20 f.

über die betroffene Person verarbeitet werden. Je stärker eine Automatisierung derartiger Kontrollanfragen erfolgt, desto eher kann sodann auch ein Abgleich unter Rechtsmäßigkeitsgesichtspunkten erfolgen (beispielsweise: Wurde die Einwilligung der Datenverarbeitung nicht bereits widerrufen?). Dieser kann in der Folge kombiniert werden mit einem etwaigen Löschungsanspruch im Fall der rechtswidrigen Datenverarbeitung und insbesondere Datenspeicherung. Sollten fehlerhafte Daten identifiziert werden, könnte (automatisiert) das Recht auf Berichtigung (Art. 16 DS-GVO) bzw. im Streitfall eine Einschränkung der Verarbeitung (Art. 18 DS-GVO) bzw. das Widerspruchsrecht nach Art. 21 DS-GVO geltend gemacht werden. Die Darstellung bereits angebotener Dienste lässt zudem erkennen, dass – gerade unter kommerziellen Gesichtspunkten – die Geltendmachung des Rechts auf Datenübertragbarkeit nach Art. 20 DS-GVO als Ansatzpunkt für die Kommerzialisierung des informationellen Selbstbestimmungsrechts sinnvoll sein kann.

Es zeigt sich also, dass für alle Betroffenenrechte ein relevantes Potenzial für den Einsatz von Datentreuhändern besteht. Rechtlich erhebliche Probleme bei der Geltendmachung dieser Betroffenenrechte durch Datentreuhänder sind nicht ersichtlich. Denn im Ansatzpunkt gilt hier dasselbe wie in Bezug auf die Einwilligung. So gebietet es die informationelle Selbstbestimmung nachgerade, dass diese Rechte grundsätzlich auch über einen Vertreter geltend gemacht werden können. Allerdings fehlt hier eine entsprechende Diskussion in der Literatur wie bei der Einwilligung. Ergänzend sei darauf hingewiesen, dass für die Betroffenenrechte in Art. 23 DS-GVO eine (begrenzte) Öffnungsklausel für mitgliedstaatliche Regelungen greift. Vorliegend relevante Spezifika, die im nationalen Datenschutzrecht zu abweichenden Besonderheiten führen, sind jedoch nicht ersichtlich.

3. Geltendmachung von Schadensersatzansprüchen durch den Datentreuhänder

Der Datentreuhänder kann unter den Voraussetzungen des Art. 80 Abs. 1 DS-GVO auch einen etwaigen Schadensersatz in der Folge von Datenschutzverstößen des Verantwortlichen für seine Nutzer mit geltend machen. Dafür müsste der Datentreuhänder allerdings „eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist“, sein. Dies hängt vom konkreten Geschäftsmodell des Datentreuhänders ab. Diese Regelung schließt wirksam aus, dass Datentreuhänder missbräuchlich und im Eigeninteresse zur Gewinnerzielung Schadensersatzansprüche durchsetzen.

III. Anforderungen an die Datensicherheit; Datenschutz-Folgenabschätzung

1. Anforderungen an die Datensicherheit

Datentreuhänder-Modelle werden nur dann gesellschaftliche Akzeptanz finden, wenn von ihnen echte Verbesserungen für die Privatsphäre der Nutzer ausgehen. Das Vertrauen der Nutzer in die Integrität der beauftragten Datentreuhänder ist daher das entscheidende Gut. In den letzten Jahren hat sich gezeigt, dass gerade große Datenskandale in Folge von Datensicherheitsproblemen in hohem Maße geeignet sind, Ver-

trauen zu erschüttern. Daher muss gerade bei Datentreuhändern ein besonderes Augenmerk auf die Datensicherheit gelegt werden.

Die zentrale Norm für die Sicherheit der Datenverarbeitung ist Art. 32 DS-GVO. Datentreuhänder können eine Vielzahl von Daten verwalten und verfügen darüber hinaus teilweise über weitere Zugangsmöglichkeiten bei anderen Verantwortlichen. Daher besteht für die Privatsphäre der betroffenen Personen ein erhebliches Risiko, wenn auf Datenbestände des Datentreuhänders unberechtigt Zugriff erlangt wird. Spiegelbildlich sind entsprechend des risikobasierten Ansatzes in Art. 32 DS-GVO für Datentreuhänder die Anforderungen an die IT-Sicherheit besonders hoch. Dabei muss der Datentreuhänder diesen strengen Anforderungen nicht nur genügen, sondern dies auch nachweisen können, Art. 5 Abs. 2 DS-GVO („Rechenschaftspflicht"). In der Praxis kann dieser Nachweis vor allem im Wege einer Zertifizierung (Art. 32 Abs. 3 DS-GVO) durch eine nach Art. 43 Abs. 1 S. 1 DS-GVO i.V.m. § 39 BDSG akkreditierte Zertifizierungsstelle gelingen. Dabei sollte sich die Zertifizierung auch auf die besondere Verantwortung eines Datentreuhänders beziehen. Mit der zunehmenden Etablierung von Datentreuhänder-Modellen dürften sich also eigens auf diese abgestimmte Zertifizierungsprogramme herausbilden. Diese können etwa durch klar erkennbare Siegel bei den Nutzern zusätzliches Vertrauen schaffen. Das wird auch im Daten-Governance-Verordnung-E der Kommission deutlich, die daher zu Recht auf die Einführung einer verpflichtenden Zertifizierung verzichtet.[34]

2. Notwendigkeit bzw. Zweckmäßigkeit einer Datenschutz-Folgenabschätzung

Ergänzend ist darauf hinzuweisen, dass für Datentreuhänder die Durchführung einer Datenschutz-Folgenabschätzung indiziert sein kann. So schreibt die DS-GVO in Art. 35 für bestimmte Verarbeitungsvorgänge verpflichtend vor, dass der Verantwortliche eine Datenschutz-Folgenabschätzung vornimmt. Deren Ziel ist es, dass sich der Verantwortliche in besonders sensiblen Bereichen durch ein strukturiertes Verfahren über die möglichen Folgen der Datenverarbeitungsvorgänge bewusst wird.[35] Die Datenschutz-Folgenabschätzung ist eine vom Verantwortlichen vorzunehmende, strukturierte und dokumentierte Risikoanalyse und -bewertung. Sie hat nach Art. 35 Abs. 7 DS-GVO mindestens eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen, zu enthalten. Ferner müssen dabei eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen erfolgen und die zur Bewältigung dieser Risiken vorgesehenen Abhilfemaßnahmen dargelegt und bewertet werden. Der Gesetzestext nennt in Art. 35 Abs. 3 DS-GVO drei (nicht abschließende) Beispiele, in denen eine Datenschutz-Folgenabschätzung durchzuführen ist.[36] Diese Fälle greifen nicht zwingend für jede denkbare Konstellation der Datentreuhänder. Umfasst das Angebot jedoch beispielsweise in relevantem Umfang Gesundheitsdaten, so ist die Durchführung einer

[34] Siehe S. 6 der Begründung des Erwägungsgrunds 22 Daten-Governance-Verordnung-E.

[35] Vgl. *Jandt* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 35 DS-GVO Rn. 1; siehe hierzu und zum Folgenden auch *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 731 ff. (im Erscheinen).

[36] Vgl. dazu im Einzelnen instruktiv und mit Beispielen *Art. 29-Datenschutzgruppe*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4.4.2017.

Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 DS-GVO zwingend. Vor diesem Hintergrund wäre es denkbar, dass die Aufsichtsbehörden im Rahmen der Erstellung der Liste für Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist, klarstellen, in welchem Umfang dazu auch Datentreuhänder gehören. Schon jetzt kann durch die Art der vom Datentreuhänder verarbeiteten Daten einer der gelisteten Verarbeitungsvorgänge erfasst sein. Sofern beispielsweise der Datentreuhänder in relevantem Umfang Daten verarbeitet und dabei eine „(z)entrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind", vornimmt, wäre er schon deshalb Adressat einer verpflichtenden Datenschutz-Folgenabschätzung.[37]

IV. Verantwortung und Haftung von Datentreuhändern

Im Übrigen sind Haftungsfragen von großer Relevanz, da die jüngst im Rahmen der Datenschutzgrundverordnung und der Begleitgesetzgebung im BDSG vorgenommene massive Verschärfung der Haftung von Datenverarbeitern die Frage aufwirft, ob dadurch die Realisierbarkeit von Datentreuhänder-Modellen gefährdet wird (dazu 2.). Insoweit ist aber zunächst die Frage zu klären, ob die Datentreuhänder lediglich als Intermediär für die durch sie vorgenommene Datenverarbeitung im datenschutzrechtlichen Sinne verantwortlich sind und entsprechend haften oder ob sie einer gemeinsamen Verantwortung mit den eigentlichen Datenverarbeitern unterliegen (dazu 1.).

1. Qualifikation der Rolle des Datentreuhänders als gemeinsame Verantwortlichkeit, als getrennte Verantwortlichkeit bzw. als Auftragsverarbeitung

Das Risiko einer gemeinsamen Verantwortlichkeit ist bislang – soweit ersichtlich – noch gar nicht im Rahmen der Diskussion von Datentreuhändern vertieft worden (dazu sogleich b)). Hintergrund ist insoweit die ausufernde Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit (dazu a)). Sie zwingt dazu, zu prüfen, welche Verantwortung den Datentreuhänder trifft, wenn dieser Daten an Verantwortliche übermittelt und jene Verantwortliche anschließend gegen Datenschutzbestimmungen in einer Art und Weise verstoßen, die vom Datentreuhänder hätte erkannt werden können. Insoweit könnte eine gesamtschuldnerische Haftung (Art. 26 Abs. 3 DS-GVO) des Datentreuhänders mit dem bzw. den Verantwortlichen die Attraktivität dieses Modells und damit ihre Etablierung am Markt deutlich erschweren.

a) Weites Verständnis der gemeinsamen Verantwortlichkeit in der Rechtsprechung des EuGH

Die jüngere Rechtsprechungslinie des EuGH[38] ist dabei so zu verstehen, dass gemeinsam in die Datenverarbeitung eingeschaltete Entitäten im Zweifel auch als gemeinsam Verantwortliche anzusehen sind. Entscheidend ist eine hinreichende, gege-

[37] Siehe dazu Position 15 auf der Liste des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, abrufbar im WWW unter der URL https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorgängen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf (zul. aufgerufen am 1.12.2020).

[38] EuGH, Urt. v. 5.6.2018 – C-210/16, Rn. 31 ff. – *Facebook-Fanpages*; Urt. v. 10.7.2018 – C-25/17, Rn. 65 ff. – *Zeugen Jehovas*; Urt. v. 29.7.2019 – C-40/17, Rn. 75 ff. – *Fashion ID*.

benenfalls auch nur teils überlappende und teils komplementäre Mitwirkung hinsichtlich der für die Datenverarbeitung erforderlichen Mittel. Dasselbe gilt für die Verfolgung eines gemeinsamen Zweckes. Auch hier genügen eine Teilüberlappung und ein gemeinsames kommerzielles Ziel, auch wenn dazu unterschiedliche Interessen an der Datenverarbeitung bestehen. Das gilt insbesondere, wenn im Außenverhältnis eine Arbeitsteiligkeit bei der Datenverarbeitung erfolgt und ein Akteur in die Datenerhebung eingebunden ist und diese überhaupt erst ermöglicht, auch wenn die andere Entität für die technische Abwicklung der Datenverarbeitung gleichermaßen benötigt wird, etwa weil sie entsprechende technische Tools dafür liefert. Im Zweifel kann im Übrigen eine Ausdifferenzierung der gemeinsamen und alleinigen Verantwortung hinsichtlich der verschiedenen Datenverarbeitungsschritte erfolgen. Auch die Aufgaben- und Rollenverteilung bei den gemeinsamen Verarbeitungsschritten kann ausdifferenziert werden. Die gemeinsame Verantwortlichkeit ersetzt damit substantiell Fallkonstellationen, die nach der bisherigen Auslegung im deutschen Recht als Auftragsverarbeitung qualifiziert worden sind.[39] Schon bei einer geringeren Zweck- und Mittelgemeinsamkeit ist nunmehr stattdessen von einer gemeinsamen Verantwortung auszugehen. Die Konsequenzen dieser erst nach Inkrafttreten der DS-GVO eingeleiteten Klarstellung des Konzepts der gemeinsamen Verantwortung, wie es an sich schon vorher unter der DSRL 95/46/EG und damit für das BDSG a.F. und die LDSGe a.F. bereits galt, zeichnen sich erst nach und nach in der deutschen Anwendungspraxis von DS-GVO und BDSG n.F. bzw. LDSGe n.F. ab.

Die Frage nach den jeweiligen Rollen kann vor diesem Hintergrund für die Teilfragen der Bestimmung der Zwecke und der „wesentlichen" Mittel anhand folgender Leitfragen, die teilweise bereits in der Literatur zusammengestellt werden, weiter ausdifferenziert werden.[40] So ist für die Frage, wer über die Zwecke bestimmt, etwa relevant, wer die Verarbeitung initiiert, von ihren Zwecken primär profitiert, ihre Ausgestaltung steuert, die Kundenansprache vornimmt etc. Hinsichtlich der „wesentlichen" Mittel kommt es vor allem auf die Bereitstellung der entsprechenden Datenverarbeitungssysteme und vor allem der Software einschließlich deren Ausgestaltung und des Zugangs sowie des Zugriffs an.[41]

Im Übrigen greift eine bloße Auftragsverarbeitung, wenn der Auftragnehmer die Verarbeitung nur im Rahmen der Weisungen des Auftraggebers vornehmen darf (Art. 29 DS-GVO). Der Verantwortliche bleibt also „Herr der Daten". Dem Auftragsverarbeiter kommt keine Eigenverantwortlichkeit und keine Entscheidungsbefugnis zu, die seine Tätigkeit über die reine Hilfsfunktion im Rahmen fremder Zwecke hinausheben würde. Er fungiert im Verhältnis zum Verantwortlichen gleichsam als „Datensklave" oder als „Marionette".[42] Dies kommt auch in der Definition des Auftragsverarbeiters in Art. 4 Nr. 8 DS-GVO zum Ausdruck, wonach Auftragsverarbeiter jede natürliche und juristische Person, Behörde, Einrichtung oder andere Stelle ist, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Bestimmt ein Auftragsverarbeiter allerdings unter Verstoß gegen die DS-GVO die Zwecke und Mittel der Verarbeitung selbst, gilt er insoweit als Verantwortlicher, Art. 28 Abs. 10 DS-GVO. In diesem Umfang ist der Auftragsverarbeiter folglich wiederum selbst „Verantwortlicher".

---

[39] So zutreffend *Kremer*, Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung, CR 2019, 225 ff.

[40] Siehe ähnlich *Gierschmann*, Gemeinsame Verantwortlichkeit in der Praxis, ZD 2020, 69 (72).

[41] Ähnlich wiederum *Gierschmann*, Gemeinsame Verantwortlichkeit in der Praxis, ZD 2020, 69 (72).

[42] Vgl. *Ernst*, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 4 Rn. 56; vgl. näher zum Begriff des Auftragsverarbeiters auch *Art.-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 16.2.2010.

b) Konsequenzen für Datentreuhänder-Modelle

Vorliegend wird für die Datentreuhänder eine bloße Auftragsverarbeitung ausscheiden, da diese ja gerade das überlegene Wissen über die Mittel der Datenverarbeitung haben, denn die Betroffenen erhoffen sich genau diese Erleichterung durch den Rückgriff auf jenen Intermediär.

Es besteht jedoch das Risiko, dass die Datentreuhänder, gerade im Fall eines kommerziellen Interesses an der Maximierung von Datenverarbeitungen durch andere Verantwortliche, auch wenn dies den Interessen der Betroffenen entspricht, im Rahmen eines kollaborativen Zusammenwirkens mit diesen anderen Verantwortlichen in die Rolle einer gemeinsamen Verantwortlichkeit hineinwachsen. Allerdings bestehen genügend Gestaltungsmöglichkeiten für den Datentreuhänder, sich gleichsam „im Lager" der betroffenen Person anzusiedeln und an dessen Verarbeitungswünschen orientiert nur als Mittler Daten der betroffenen Personen an andere Verantwortliche nach den Wünschen der betroffenen Personen zu übermitteln.[43] Dann bestimmen im Wesentlichen diese anderen Verantwortlichen über die Zwecke der Datenverarbeitung und der Intermediär sorgt nur dafür, dass eine Datenverarbeitung ausschließlich nach den Wünschen der betroffenen Personen erfolgt – oder eben gar nicht. Dasselbe gilt für die Wahrnehmung der Betroffenenrechte. Handelt der Datentreuhänder auch im Interesse anderer Verantwortlicher und stellt sich damit – zumindest auch – in deren Lager, so wird in vielen Fällen eine gemeinsame Verantwortlichkeit anzunehmen sein. Diese Differenzierung – gleichsam im Sinne einer „Lagertheorie" – kann für Datentreuhänder eine vergleichsweise rechtssichere Orientierung bieten, ob mit den anderen Verantwortlichen eine gemeinsame Verantwortlichkeit besteht oder nicht.

Damit sorgt das strenge Haftungsregime der gemeinsamen Verantwortlichkeit zugleich für eine Disziplinierung der Datentreuhänder als Agenten der Interessenwahrnehmung der sie einschaltenden betroffenen Personen. Verfolgen sie diese nicht konsequent, sondern orientieren sich an den Verarbeitungsinteressen der anderen Verantwortlichen, werden sie folgerichtig zu gemeinsamen Verantwortlichen. Dies führt – wie unter 2. noch darzulegen sein wird – in der Konsequenz zu erheblichen Haftungsrisiken. Das durch die gemeinsame Verantwortlichkeit hervorgerufene strenge Haftungsregime schafft daher Anreize, die Interessenkollisionen ausschließen. Um es noch einmal anders zu formulieren: Die verschiedenen bereits in der Praxis anzutreffenden Datentreuhänder-Modelle (dazu oben I.2.) stehen in unterschiedlichem Umfang in der Gefahr, einer gemeinsamen Verantwortlichkeit mit den dritten Datenverarbeitern zu geraten. Agieren sie eher als „Makler" zwischen den anderen Datenverarbeitern und den Betroffenen und versuchen, etwa durch die Optimierung der Schnittstellen mit den anderen Datenverarbeitern eine deren Bedürfnissen entsprechende, möglichst umfassende und reibungslose Datenübermittlungen zu gewährleisten, spricht dies eher für die Annahme einer gemeinsamen Verantwortlichkeit mit diesen. Das kann dann auch für den Fall gelten, dass sie diese Optimierung durchaus im Sinne der Betroffenen vornehmen, um deren kommerziellen Interessen gerecht zu werden. Denn gleichwohl entscheiden sie maßgeblich über die Zwecke und Ausgestaltung der Datenverarbeitung mit und fungieren auch als Interface für die anderen Verantwortlichen, um die Daten der Betroffenen zu erlangen und aufzubereiten. Je stärker sich der Treuhänder dagegen im Lager der Betroffenen positioniert und die Zusammenarbeit mit den anderen Verantwortlichen funktional scharf auf das zur Wahrnehmung der Interessen der Betroffenen nötige beschränkt, desto eher scheidet eine Zuweisung einer gemeinsamen Verant-

[43] In diese Richtung auch Erwägungsgründe 22 und 26 sowie Art. 11 Nr. 10 Daten-Governance-Verordnung-E.

wortlichkeit mit den anderen Verarbeitern aus. Im Einzelfall ist insoweit eine Grauzone markiert und erst die weitere Entwicklung der verschiedenen Geschäftsmodelle wird zur Ausdifferenzierung der hier in der Grundstruktur aufgezeigten rechtlichen Bewertung führen.

2. Haftungsrisiken für Datentreuhänder

Wesentliches Ziel der DS-GVO ist es, eine tatsächliche Beachtung ihrer materiellrechtlichen Vorgaben sicherzustellen. Sie versucht dies durch sehr scharfe Sanktionsmechanismen zu erreichen. Diese betreffen gerade auch Datentreuhänder, die große und teils sehr sensible Datenbestände verwalten. Rechtswidrige Handlungen können daher für Datentreuhänder schwerwiegende Konsequenzen nach sich ziehen.

a) Bußgeldrisiken

Ein wesentliches Element der Datenschutzreform 2018 war die drastische Erhöhung des Bußgeldrahmens für Datenschutzverstöße.[44] Bußgelder können gegenüber Verantwortlichen und Auftragsverarbeitern verhängt werden. Hintergrund war die unter der DSRL herrschende sehr uneinheitliche und auch zurückhaltende Bußgeldpraxis der Aufsichtsbehörden.[45] Die in Art. 83 Abs. 5 DS-GVO normierte maximale Bußgeldhöhe liegt bei 20 Mio. Euro. Wenn der Verantwortliche ein Unternehmen ist – wie wohl im Regelfall – steigt die Obergrenze auf 4 % des Jahresumsatzes, wenn dieser Betrag höher als 20 Mio. Euro ist. Selbst für Verstöße, die die DS-GVO als weniger gravierend einstuft (z.B. reine Organisationsmängel)[46], droht Art. 83 Abs. 4 DS-GVO noch eine maximale Geldbuße von 10 Mio. Euro oder 2 % des Jahresumsatzes an. Es ist dabei auf den jeweiligen Konzern-[47] (!) Welt- (!) Jahresumsatz des vorangegangenen Geschäftsjahres abzustellen, also auf die Einnahmen, die der Konzern des jeweiligen Verantwortlichen im Jahr vor der Verhängung des Bußgeldes weltweit erzielt. Damit wird erkennbar auf die (häufig US-amerikanischen) Internetriesen mit hohen Milliardenumsätzen weltweit abgezielt. Aber auch für Datentreuhänder mit im Zweifel geringeren Umsätzen sind die Bußgelder durchaus empfindlich. Allein das macht die Vorschrift zu einer der wirkungsvollsten der DS-GVO überhaupt.

Erste Anwendungsfälle belegen, dass die Aufsichtsbehörden durchaus auch bereit sind, die neuen Bußgeldrahmen zu nutzen. Zeigten die deutschen Aufsichtsbehörden anfangs noch eher Zurückhaltung, gingen die Aufsichtsbehörden in den anderen Mitgliedstaaten schneller voran.[48] Nachdem die deutschen Aufsichtsbehörden ihre Bußgeldpraxis auch nach Inkrafttreten der DS-GVO noch stark an der früheren Handha-

---

[44] Dieser und die folgenden Absätze sind stark orientiert an *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2020, Rn. 760 ff. (im Erscheinen).

[45] *Bergt* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 83 DS-GVO Rn. 1.

[46] *Neun/Lubitzsch*, EU-Datenschutzgrundverordnung – Behördenvollzug und Sanktionen, BB 2017, 1538 (1542).

[47] Erwägungsgrund 150 der DS-GVO; vgl. *Bergt* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 83 DS-GVO Rn. 28; im Einzelnen ist dies umstritten, da der Wortlaut nur von Unternehmen spricht und erst in der Zusammenschau mit den Erwägungsgründen klar wird, dass der Begriff nicht i.S.d. Art. 4 Nr. 18 DS-GVO, sondern i.S.d. Art. 101 f. AEUV verstanden werden muss; kritisch insoweit *Piltz*, Die Datenschutz-Grundverordnung, K&R 2017, 85 (92); a.A. auch mit durchaus beachtlichem Hinweis auf das Bestimmtheitsgebot *Neun/Lubitzsch*, EU-Datenschutzgrundverordnung – Behördenvollzug und Sanktionen, BB 2017, 1538 (1543).

[48] Zu anschaulichen Beispielen siehe die Hinweise im WWW abrufbar unter der URL https://www.enforce ment tracker.com/ (zul. aufgerufen am 1.12.2020).

bung orientierten und die Höhe nur moderat anpassten,[49] änderten sie ihr Vorgehen relativ schnell und auch in Deutschland kam es zu hohen Bußgeldern in zweistelliger Millionenhöhe, zuletzt sogar auch für vergleichsweise weniger bedeutende Verstöße.[50] Nachdem sich die Aufsichtsbehörden auf Bundes- und Landesebene auf ein einheitliches Bußgeldkonzept[51] geeinigt haben, das sich primär am erzielten Jahresumsatz orientiert, dürften drakonisch anmutende Bußgeldhöhen auch künftig eher die Regel als die Ausnahme sein. Bei den Zumessungskriterien kommt es neben Art, Schwere und Dauer des Verstoßes auch auf die Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens an. Da Datentreuhänder eine Vielzahl auch sensibler Daten verarbeiten, sind die Bußgeldrisiken für Datentreuhänder sehr erheblich, auch wenn diese nicht in jedem Fall große Umsätze erzielen werden.

b) Zivilrechtliche Haftungsrisiken

Neben den Risiken durch Bußgelder tritt das oft weniger beachtete zivilrechtliche Haftungsregime.[52] Denn der datenschutzrechtlich Verantwortliche und der Auftragsverarbeiter, darunter auch Datentreuhänder, sind auch „verantwortlich" im zivilrechtlichen Sinne.[53] Werden Rechte der betroffenen Person verletzt und entsteht ihr hierdurch ein Schaden, so steht ihr ein Ausgleich zu. Eine Besonderheit bei der datenschutzrechtlichen Haftung gegenüber der betroffenen Person ist der im Regelfall fehlende kausale materielle Schaden durch den Datenschutzrechtsverstoß. Unter der DS-GVO wird diesem Umstand dahingehend Rechnung getragen, dass auch ein immaterieller Schaden für ersatzfähig erklärt wird, Art. 82 Abs. 1 DS-GVO. Diese Vorschrift entspricht daher einer gesetzlichen Normierung gemäß § 253 Abs. 1 BGB im nationalen Recht und steht damit nicht im Widerspruch zur allgemeinen Schadenersatzrechtsdogmatik. Ein immaterieller Schaden ist in verschiedenen Konstellationen denkbar. Er dürfte aber jedenfalls dann ausgeschlossen sein, wenn lediglich gegen reine Ordnungsvorschriften verstoßen wird (wie etwa die Pflicht zur Führung eines Verarbeitungsverzeichnisses oder bloße Formalia in Datenschutzklauseln). Aufgrund der Möglichkeit, Ausgleich auch für immaterielle Schäden verlangen zu können, werden sich Verantwortliche und Auftragsverarbeiter künftig vermehrt Ansprüchen Geschädigter ausgesetzt sehen. Die Risiken, die sich daraus ergeben, können je nach Fallkonstellation unter Umständen sogar diejenigen aus der öffentlich-rechtlichen Bußgeldhaftung übersteigen.

Wie bei großen Compliance-Fällen in anderen Bereichen, z.B. dem sog. LKW-Kartell oder der Diesel-Abgas-Thematik bei den großen Fahrzeugherstellern, könnten zu-

[49] Siehe etwa im WWW abrufbar unter der URL https://www.heise.de/newsticker/meldung/Passwoerter-im-Klartext-20-000-Euro-Bussgeld-nach-DSGVO-gegen-Knuddels-de-4229798.html (zul. aufgerufen am 1.12.2020).

[50] Siehe hierzu das Bußgeld in Höhe von fast 10 Millionen Euro für einen eher überschaubaren Datenschutzverstoß im Callcenter von 1&1, das vom LG Bonn, Urt. v. 11.11.2020 Az. 29 OWi 1/20 LG, allerdings deutlich reduziert wurde. In einem Fall schwerwiegender Verstöße durch H&M wurde zuletzt in Deutschland eine Rekordbuße in Höhe von mehr als 35 Millionen Euro erhoben, siehe wiederum die Hinweise im WWW abrufbar unter der URL https://www.enforcementtracker.com/ (zul. aufgerufen am 1.12.2020).

[51] Abrufbar im WWW unter der URL https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf (zul. aufgerufen am 1.12.2020).

[52] Dieser und die folgenden Absätze sind stark orientiert an *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2020, Rn. 765 f. (im Erscheinen).

[53] Hierzu und zum gesamten Abschnitt vertiefend auch *Sackmann*, Die Beschränkung datenschutzrechtlicher Schadensersatzhaftung in Allgemeinen Geschäftsbedingungen, ZIP 2017, 2450; allgemein zum Schadensersatz nach der DS-GVO *Wybitul/Haß/Albrecht*, Abwehr von Schadensersatzansprüchen nach der Datenschutzgrundverordnung, NJW 2018, 113.

künftig auch im Datenschutzrecht die im Vergleich zu möglichen öffentlich-rechtlichen Sanktionen größeren Risiken in einer massenhaften Geltendmachung von Schadensersatzansprüchen liegen. Für Datentreuhänder mit einer Vielzahl von Endkunden könnte ein Verstoß gegen Datenschutznormen dann künftig einen ernstzunehmenden Großschaden bedeuten. Gerade bei solchen Datentreuhändern, die mit umfangreichen Datenbeständen einer Vielzahl von Personen arbeiten, ist das ein realistisches Szenario. Dies gilt insbesondere vor dem Hintergrund, dass sich Unternehmen gegen Klagen von betroffenen Personen aufgrund einer Beweislastumkehr nur schwer verteidigen können, denn Verantwortliche haben die Einhaltung der Datenschutzvorschriften darzulegen und gegebenenfalls zu beweisen.[54] Dies gilt insbesondere in Kombination mit dem zivilprozessualen Instrument der Musterfeststellungsklage.[55] Ob es in der Praxis tatsächlich zu „Klagewellen" kommen wird, lässt sich derzeit noch nicht zuverlässig abschätzen. Jedenfalls die Möglichkeit der Geltendmachung von Ausgleichen für immaterielle Schäden sollte aber gerade für datenverarbeitungsgeprägte Unternehmen wie Datentreuhänder ein Ansporn sein, den Datenschutz ernst zu nehmen.

Ein weiterer wesentlicher Aspekt bei der Beurteilung der Haftungsrisiken für Datentreuhänder ist die relativ strenge Außenhaftung gegenüber den betroffenen Personen. So ergibt sich direkt aus Art. 82 Abs. 4 DS-GVO, dass mehrere an einem Datenverarbeitungsvorgang beteiligte Verantwortliche als Gesamtschuldner auf Schadensersatz haften. Trifft einen der beteiligten Verantwortlichen ein höherer Verschuldensgrad, so findet ein Innenausgleich nach Art. 82 Abs. 5 DS-GVO statt. Dabei ist der Begriff der Beteiligung an der Datenverarbeitung weit zu verstehen.[56] Damit soll nach dem Wortlaut des Gesetzes ein wirksamer Schadensersatz für die betroffene Person sichergestellt werden, Art. 82 Abs. 4 a.E. DS-GVO. Bei Einschaltung eines Datentreuhänders ist einerseits dieser an der Datenverarbeitung beteiligt und andererseits auch der Verantwortliche. Das gilt nach dem Wortlaut der Norm grundsätzlich auch unabhängig von der Frage, ob bei dem konkreten Geschäftsmodell eine gemeinsame Verantwortlichkeit mit dem Datentreuhänder anzunehmen ist. Allerdings sprechen die besseren Gründe dafür, dass die Vorschrift des Art. 82 Abs. 4 DS-GVO aus teleologischen Gesichtspunkten eine Einschränkung erfährt, wenn der Datentreuhänder keine eigenen Interessen an der Datenverarbeitung hat, also rein „im Lager" der betroffenen Person steht. Es gibt dann kein sachlich zu rechtfertigendes Argument, den Datentreuhänder mithaften zu lassen. Letztlich würde er sonst unkalkulierbaren und vor allem nicht sachgerechten Risiken ausgesetzt: Obwohl er als „Agent" der betroffenen Person agiert, müsste er ansonsten für das Fehlverhalten der „Gegenseite" einstehen. Das kann ersichtlich vom Verordnungsgeber nicht gewollt sein. Bei einem sachgerechten Verständnis bietet damit das gegenwärtige Rechtssystem auch ein sinnvolles Anreizregime, um Interessenkollisionen beim Datentreuhänder zu vermeiden.

V. Mögliche Anpassungsbedürfnisse des geltenden Rechts

Während die bisherigen Ausführungen das geltende Recht und damit die gegenwärtigen „Spielregeln" für den Einsatz und gegebenenfalls die Abwehr von Datentreuhän-

[54] Vgl. dazu im Einzelnen *Wybitul*, DS-GVO veröffentlicht – Was sind die neuen Anforderungen an die Unternehmen, ZD 2016, 253 (254); siehe auch *Kühling*, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, 1985.

[55] Dazu auch *Kühling/Sackmann*, Die Musterfeststellungsklage nach Datenschutzverstößen – ein unkalkulierbares Risiko für Unternehmen?, DuD 2019, 347.

[56] *Bergt* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Auflage 2020, Art. 82 DS-GVO Rn. 22.

dern skizziert und analysiert haben, stellt sich nunmehr in einem weiteren Schritt die Frage, inwiefern vor diesem Hintergrund Vorschläge indiziert sind, den Rechtsrahmen in einzelnen oder mehreren Punkten de lege ferenda zu modifizieren, da er sich als defizitär für den sinnvollen Einsatz von Datentreuhändern erwiesen hat und diesen behindert.

1. Belastbarkeit und Funktionsfähigkeit des rechtlichen Rahmens; Vorschläge sektorspezifischer Regelungen

Insoweit hat sich zwar gezeigt, dass angesichts der Vielfalt der bereits jetzt erkennbaren Dienste und der Komplexität der aufgeworfenen Rechtsfragen die im Datenschutzrecht gerade bei innovativen Angeboten übliche Rechtsunsicherheit zu konstatieren ist. Das gilt exemplarisch für die dargestellte Grauzone bei der Rollenzuweisung der Datentreuhänder als allein Verantwortliche für die von ihnen durchgeführte Datenverarbeitung oder als gemeinsam Verantwortliche in Kollaboration mit den anderen Datenverarbeitern (dazu IV.1.). Genau diese Restunsicherheiten ergeben sich jedoch aus der Vielfalt der Angebote und der notwendig abstrakt zu fassenden Regeln in der DS-GVO. Ähnliches gilt für die weiteren aufgezeigten rechtlichen Herausforderungen von der Ausübung der Gestaltungsrechte bis hin zu den Haftungsfragen. Im Übrigen hat sich gezeigt, dass der Rechtsrahmen und im exemplarischen Fall der Frage der gemeinsamen Verantwortlichkeit auch die Rechtsprechung des EuGH hinreichend klare Hinweise geben, unter welchen Voraussetzungen eher eine gemeinsame Verantwortlichkeit anzunehmen ist. Es konnte sogar gezeigt werden, dass die Unsicherheiten in der Grauzone eher den positiven Anreiz setzen sollten, im Zweifel eine starke Ausrichtung des Treuhänder-Modells an den Interessen der Betroffenen und nicht denjenigen anderer Verantwortlicher auszurichten. Dasselbe wurde für die Anreizwirkungen des Haftungsregimes gezeigt (dazu IV.2.b)).

Zudem ist darauf hinzuweisen, dass sich die verschiedenen Angebote und Geschäftsmodelle von Datentreuhändern gerade erst im Markt entwickeln, so dass eine Regelung zum gegenwärtigen Zeitpunkt zwangsläufig ein noch unklares Phänomen normieren müsste. Gleichwohl ist die Schaffung eines rechtlichen Rahmens etwa von der Verbraucherzentrale Bundesverband für die PIMS als zentrales Modell der Datentreuhänder vorgeschlagen worden.[57] Darin sollen etwa Haftungsfragen, Qualitätsanforderungen, Regeln zu den Treuepflichten, zu verbotenen Koppelungen bis hin zu Bestimmungen zur Insolvenz oder Auflösung von Datentreuhändern geklärt werden. Ferner soll normativ verhindert werden, dass sich auf diesem Markt Monopolstellungen ergeben sowie positiv gewährleistet werden, dass PIMS „unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse“ an der Datenverarbeitung handeln. Die vorliegende nähere Untersuchung hat jedoch ergeben, dass das geltende Recht insoweit genügend Spielräume bietet, dafür zu sorgen, dass entsprechende Angebote im Markt vorhanden sind.

2. Zweck- nicht phänomenbezogene Ausrichtung des Rechtsrahmens

Im Übrigen ist ganz allgemein Vorliegendes zu beachten: Die Rechtsordnung ist nicht phänomenbezogen, sondern zweckbezogen strukturiert.[58] Das bedeutet, dass die Rechtsbeziehungen zwischen Rechtssubjekten im Mittelpunkt stehen und nicht um ein-

[57] *Verbraucherzentrale Bundesverband*, Positionspapier vom 19.2.2020, S. 3, abrufbar im WWW unter der URL https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zul. aufgerufen am 1.12.2020).

[58] Dieser Absatz ist stark orientiert an *Kühling/Sackmann*, Rechte an Daten, S. 9, abrufbar im WWW unter der URL https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_ kuehling-sackmann-rechte-an-daten.pdf (zul. aufgerufen am 1.12.2020).

zelne Lebenssituationen herum ausgestaltet werden und jedes denkbare Verhalten in Bezug auf diese in einem Regelungskontext zusammengefasst ist. Insofern entspricht es der Struktur der Rechtsordnung, dass es konsolidierte phänomenbezogene Regelungen für das Phänomen „Datentreuhänder" ebenso wenig gibt wie beispielsweise ein eigenes Regelungswerk, das alle Vorgänge im Gesundheitssektor erfasst. Vielmehr unterliegt auch dieser Lebensbereich unterschiedlichen Normen aus verschiedenen Rechtsgebieten. Die Rechtsordnung ist vielmehr so strukturiert, dass durch Rechtsnormen menschliche Verhaltensweisen adressiert werden, die im Grundsatz erlaubt (Art. 2 Abs. 1 GG) und ausnahmsweise untersagt werden. Ein überzeugendes Regulierungsregime im Hinblick auf einzelne Phänomene kann daher kaum in einzelnen phänomenbezogenen Gesetzen gesucht werden, die dann ihrerseits alle denkbaren Konstellationen abdecken. Gerade in Sektoren mit hoher Änderungsgeschwindigkeit der realen Bedingungen sind legislative Handlungsformen oftmals zu träge, um auf sich ändernde Umstände zu reagieren.[59] Allgemeine Rechtsbegriffe und eine gute Begleitung im exekutiven Vollzug sind insoweit besser geeignet. Es entstünde zudem fast unweigerlich eine Parallelstruktur zu bestehenden Normsystemen mit erheblichen Friktionsflächen zu anderen Regelungsgebieten. Die Folge wäre eine höhere Regelungskomplexität und damit einhergehend eine geringere Rechtssicherheit. Denn auch die gegenwärtigen rechtlichen Vorgaben für die Datenverarbeitung erfolgen sektoral und schutzzweckorientiert. Sie passen sich damit in den verhaltensbezogenen Regelungsansatz der Rechtsordnung ein. Lösungen, die sich in dieses gewachsene Regelungsregime einfügen, versprechen den größeren Nutzen durch hohe Rechtssicherheit und große Akzeptanz. Die Zweckmäßigkeit eines Regelungsbedarfs ist deshalb nicht nur nicht erkennbar, eine Regulierung in einem Spezialgesetz jedenfalls im Sinne einer überlappenden Regelung mit der DS-GVO wäre sogar kontraproduktiv, denn sie würde die Komplexität im Regelungsgefüge weiter steigern.

3. Regelungen nur auf unionaler Ebene (sinnvoll) möglich

Darüber hinaus würde eine derart weit gefasste Regelung eine Fülle rechtlicher Schwierigkeiten mit sich bringen. So wäre zunächst für jede einzelne Regelung zu klären, inwiefern diese auf nationaler Ebene überhaupt zulässig ist, oder ob insoweit eine Änderung bzw. Konkretisierung der DS-GVO erforderlich ist. Sodann wäre zu prüfen, auf welcher Verbandsebene (EU oder Mitgliedstaat) entsprechende Vorgaben in der Sache rechtlich zulässig sind und ob sie etwa gegen Grundrechte verstoßen. Die erste Frage hängt stark davon ab, inwieweit die DS-GVO korrelierende Öffnungsklauseln für mitgliedstaatliche Konkretisierungsmaßnahmen vorsieht.[60] Dies wäre für die vorgeschlagenen Regelungsinhalte im unterschiedlichen Umfang der Fall. Beispielsweise enthält Art. 7 Abs. 4 DS-GVO bereits ein Koppelungsverbot. Eine korrelierende Öffnungsklausel besteht nicht. Insoweit wäre eine normative Konkretisierung also nur auf unionaler Ebene möglich.

Jedenfalls gilt, dass angesichts des notwendig umfassenden Ansatzes der Datentreuhänder, möglichst weitgehend zahlreiche Datenverarbeitungsvorgänge im In- und Aus-

[59] Dazu *Sackmann*, Datenschutz bei der Digitalisierung der Mobilität, 2020, 195.

[60] Dazu grundlegend *Kühling/Martini et. al.*, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, abrufbar im WWW unter der URL http://www.uni-regensburg.de/rechtswissenschaft/oeffentliches-recht/kuehling//medien/k__hling_martini_et_al.-die_dsgvo_und_das_nationale_recht_-_.pdf (zul. aufgerufen am 1.12.2020) und *Kühling/Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 484 ff.

land zu erfassen, eine nationale Regelung, auch sofern entsprechende Kompetenzen partiell bestehen, wenig zielführend wäre.

4. Gegenwärtig Regelungsbedürfnis fraglich

Unabhängig von der Realisierungswahrscheinlichkeit einer sektorspezifischen Ergänzung der DS-GVO ist eine auf Datentreuhänder bezogene Spezialregelung jedenfalls mit einem überlappenden Inhalt zur DS-GVO auch gar nicht wünschenswert, wie eine allgemeine Betrachtung genauso zeigt (dazu a)) wie ein spezifischer Blick auf die konkreten Vorschläge der Kommission zu einer Daten-Governance-Verordnung (dazu b)).

a) Allgemein Skepsis gegenüber einer sektorspezifischen Parallelregelung zur DS-GVO

Das lässt sich exemplarisch am Beispiel des Koppelungsverbots aufzeigen. Dieses wirft als allgemeine horizontale Regelung in einer Fülle von Rechtskonstellationen nach wie vor erhebliche Schwierigkeiten auf, insbesondere was die Anwendung auf die anderen Verantwortlichen selbst – wie etwa soziale Netzwerke wie Facebook – anbelangt.[61] Dass nun gerade die gleichsam „abgeleitete" Frage, wie unzulässige Koppelungen der Datentreuhänder normativ unterbunden werden können, zuvor geklärt werden sollte, erscheint wenig zielführend. Es würde insoweit der zweite Schritt vor dem ersten gemacht.

Dies ist nur ein Beispiel für die fehlende Zweckmäßigkeit normativer Anpassungen zum gegenwärtigen Zeitpunkt. Denn insgesamt ist darauf hinzuweisen, dass jegliche normative Umhegung die ohnehin schon hohe (durch das normative Nebeneinander von DS-GVO und nationalem Datenschutzrecht verschärfte) datenschutzrechtliche Komplexität weiter steigern würde. Das gilt erst recht für einen Ausbau der normativen Vorsteuerung auf nationaler Ebene. Sollte sich im weiteren Verlauf eine Regulierung einzelner Fragen als erforderlich erweisen, so sollte dies in jedem Fall auf unionaler Ebene erfolgen.

Der Ansatz der DS-GVO ist es aber zu Recht, gerade für den Bereich der Datenverarbeitung durch Unternehmen einen abstrakt-generellen Rahmen zu schaffen – ohne bereichsspezifische Regelungen für einzelne Business-Modelle auf unionaler und erst recht nicht auf nationaler Ebene.[62] Dementsprechend sind auch sektorspezifische Datenschutzregelungen für andere Bereiche der Datenverarbeitung nicht indiziert, wie etwa im Bereich der Mobilität (Stichwort „autonomes Fahren").[63] Dieser allgemeine Rahmen soll vielmehr von den Vollzugsbehörden im Rahmen der Anwendung konkretisiert werden – unter der Kontrolle der Rechtsprechung.

b) Skepsis gegenüber den materiell-rechtlichen Vorschlägen der Europäischen Kommission in einer Daten-Governance-Verordnung

Vor diesem Hintergrund ist der Vorschlag der Kommission für eine Daten-Governance-Verordnung, der auch Datentreuhänder regeln soll, um das Vertrauen in sie zu unterstützen, jedenfalls hinsichtlich der zusätzlichen materiell-rechtlichen Regeln skeptisch zu betrachten. So soll die neue Verordnung spezifische Verhaltensregeln

[61] *Buchner/Kühling* in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 7 DS-GVO Rn. 61.

[62] Siehe dazu *Kühling*, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, 1985 ff.

[63] Siehe dazu grundlegend *Sackmann*, Datenschutz bei der Digitalisierung der Mobilität, 2020.

schaffen. Nur privilegierte datenaltruistische Organisationen als Datenmittler, die vor allem die nicht-kommerzielle Verarbeitung von Daten erleichtern sollen, sind von diesen Vorgaben ausgenommen (Art. 14 Daten-Governance-Verordnung-E). Alle Datenmittler soll darüber hinaus eine Notifizierungspflicht treffen (siehe für die nichtaltruistischen Akteure Art. 10 Abs. 1 Daten-Governance-Verordnung-E), die eine Überwachung der Einhaltung der Sonderregeln (Art. 13 Daten-Governance-Verordnung-E) durch kompetente und unabhängige Behörden auf mitgliedstaatlicher Ebene (Art. 12 Daten-Governance-Verordnung-E) ermöglichen soll. Während die Meldung zur Erlangung eines Marktüberblicks und zur Abwehr etwaiger Missbrauchsrisiken noch sinnvoll erscheint, zeigen die zusätzlichen materiell-rechtlichen Regeln, die subsidiär gegenüber der DS-GVO gelten sollen, jedenfalls für den Umgang mit personenbezogenen Daten genau die aufgezeigten Schwierigkeiten im Zusammenspiel mit der DS-GVO. Ist das Verbot der Zweckänderung in Art. 11 Nr. 1 Daten-Governance-Verordnung-E strenger zu verstehen als in der DS-GVO (siehe oben II.1.c)) und warum sollte das notwendig sein? Ferner sollen die Entgelte der Mittler gegenüber den Dateninhabern – also den betroffenen Personen im Sinne der DS-GVO – „fair, transparent und nichtdiskriminierend" sein (Art. 11 Nr. 3 Daten-Governance-Verordnung-E). Was bedeutet das etwa im Vergleich zur Zulässigkeit einer Einwilligung und den dabei aufgestellten Anforderungen (siehe oben II.1.)? Warum dürfen Metadaten nur zur Entwicklung des Dienstes verwendet (Art. 11 Nr. 2 Daten-Governance-Verordnung-E) und nicht auf der Basis einer Einwilligung kommerzialisiert werden, wie es nach der DS-GVO grundsätzlich möglich ist? So ließe sich jede weitere Anforderung in dem Katalog der elf Vorgaben kritisch hinterfragen. Teils geht es um andere Schutzzwecke (etwa die Wahrung des Wettbewerbsrechts, Art. 11 Nr. 9 Daten-Governance-Verordnung-E), so dass keine kritische Überlappung mit der DS-GVO entsteht. Sofern das aber wie aufgezeigt der Fall ist, sollte nochmals näher dargelegt werden, warum es spezifischer zusätzlicher Anforderungen in der Daten-Governance-Verordnung bedarf und worin der Mehrwert liegt. Andernfalls droht die Gefahr, dass die Entwicklung entsprechender Datentreuhänder, die von der Kommission zu Recht begrüßt wird (Erwägungsgrund 22 Daten-Governance-Verordnung-E), eher erschwert wird. Das zeigt auch die missverständliche Aussage, dass die Rechte der DS-GVO nur von der jeweiligen Einzelperson und nicht von Datengenossenschaften ausgeübt werden könnten (Erwägungsgrund 24 Daten-Governance-Verordnung-E). Hier wird der fälschliche Eindruck erweckt, die DS-GVO würde der Ausübung der Rechte der Individualpersonen durch Vertreter entgegenstehen (dagegen bereits oben II.). Insofern hätte eine Bestandsaufnahme der Steuerung der Datentreuhänder durch das geltende Recht als Grundlage für die Entwicklung von Legislativvorschlägen geholfen.

5. Empfehlungen und Leitlinien der Datenschutzaufsichtsbehörden sinnvoll

Während also – jedenfalls mit der DS-GVO überlappende – neue Regeln eher skeptisch zu betrachten sind, besteht Bedarf nach Klarheit bei der Auslegung und Anwendung des bereits geltenden Rechts für Datentreuhänder. So sind insbesondere weitere Aktivitäten der Datenschutzaufsichtsbehörden hilfreich, die in den bisherigen Ausführungen schon zum Teil adressiert wurden. So könnten auf nationaler Ebene die Aufsichtsbehörden bzw. die unabhängigen Datenschutzbehörden des Bundes und der Länder gemeinsam über die Datenschutzkonferenz eine Orientierungshilfe veröffentlichen, um die hier aufgezeigten oder sich im Laufe der Zukunft noch als problematisch erweisenden Aspekte der rechtlichen Einordnung und die Anforderungen an Datentreuhänder näher zu bewerten. Dabei könnten sie beispielsweise – wie bereits vorge-

schlagen (siehe dazu oben III.2.) – klarstellen, in welchen Fällen Datentreuhänder zwingend Datenschutz-Folgeabschätzungen durchzuführen haben. Auf europäischer Ebene wären entsprechende Leitlinien des Europäischen Datenschutzausschusses (EDSA) ebenfalls hilfreich. Ferner könnten auch im Rahmen der Aktualisierung der relevanten Leitlinien die besonderen Probleme von Datentreuhänder-Modellen jeweils bezogen auf entsprechende Teilaspekte thematisiert werden. So hat der EDSA beispielsweise gerade erst Anfang Mai eine aktualisierte Fassung zur Einwilligung veröffentlicht.[64] Diese könnte im Zuge einer späteren erneuten Aktualisierung Hinweise und Beispiele zu den spezifischen Problemen von Datentreuhändern aufnehmen. Bislang existiert auf unionaler Ebene – soweit ersichtlich – nur die sehr allgemein gehaltene Stellungnahme des Europäischen Datenschutzbeauftragten zu PIMS.[65]

VI. Ergebnisse

Datentreuhänder verstanden als Intermediäre zwischen den beiden Hauptakteuren des Datenschutzrechts, nämlich den Datenverarbeitern einerseits und den betroffenen Personen andererseits, können von der betroffenen Person als Vertrauensperson eingesetzt werden, um die informationelle Selbstbestimmung einschließlich kommerzieller Verwertungsinteressen des Persönlichkeitsrechts gegenüber den Verantwortlichen besser wahrzunehmen. So kann der Betroffene angesichts der Vielzahl von Datenverarbeitungsprozessen und einer Vielzahl von datenschutzrechtlich relevanten Aktionen – insbesondere von Einwilligungserklärungen, aber auch der Nutzung von Betroffenenrechten – entlastet werden. Es wurde gezeigt, dass das geltende Recht insbesondere der Datenschutzgrundverordnung der Durchsetzung entsprechender Modelle nicht prinzipiell im Wege steht. So können die wesentlichen datenschutzrechtlichen Gestaltungsrechte auch durch Datentreuhänder ausgeübt werden. In Bezug auf die Einwilligung umfasst das Recht auf informationelle Selbstbestimmung grundsätzlich auch die Befugnis des Einzelnen, zu entscheiden, ob er dieses Recht höchstpersönlich oder unter Einschaltung eines Vertreters ausüben möchte. Auch für Kinder können die Träger elterlicher Verantwortung entsprechend Art. 8 DS-GVO Datentreuhänder einsetzen und sich so von zeitlich aufwendigen und technisch anspruchsvollen Einzelausübungen der diesbezüglichen Gestaltungsrechte entlasten.

Jedoch gelten für die Erteilung einer entsprechenden Vollmacht – soweit übertragbar – die gleichen Voraussetzungen wie sie auch für die Einwilligung selbst gelten. Daher muss auch die Vollmacht insbesondere zweckbestimmt erteilt werden. Eine Generalvollmacht zur umfassenden und unbegrenzten Wahrnehmung des Rechts auf informationelle Selbstbestimmung durch Datentreuhänder wäre wegen Unbestimmtheit unwirksam. Ferner muss die Vollmacht ebenso wie die Einwilligung in informierter Weise erteilt werden – jedenfalls insoweit, als die betroffene Person selbst eine Vorstellung von den grundsätzlichen Rahmenbedingungen haben muss, unter denen der Vertreter eine Einwilligung mit Wirkung für und gegen sie erteilt. Darüber hinaus gilt

[64] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4.5.2020, abrufbar im WWW unter der URL https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (zul. aufgerufen am 1.12.2020).

[65] *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016, S. 6, abrufbar im WWW unter der URL https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (zul. aufgerufen am 1.12.2020); vgl. ferner der Bericht über eine Konsultation der *Europäischen Kommission*, An emerging offer of „personal information management services", 2016, abrufbar im WWW unter der URL https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 (zul. aufgerufen am 1.12.2020).

für die Vollmacht, ebenso wie für die Einwilligung selbst, der Grundsatz der jederzeitigen freien Widerrufbarkeit. Diese rechtlichen Voraussetzungen stellen nicht unerhebliche Anforderungen an die Datentreuhänder, die von diesen durch innovative Ausgestaltungen der Einwilligungserklärungen bewältigt werden müssen, aber auch bewältigbar sind. Diese Entwicklung könnte durch klarstellende Hinweise in entsprechenden aufsichtsbehördlichen Dokumenten auf nationaler Ebene und durch den Europäischen Datenschutzausschuss unterstützt werden.

Darüber hinaus besteht hinsichtlich aller Betroffenenrechte ein relevantes Potenzial für den Einsatz von Datentreuhändern. Rechtlich erhebliche Probleme bei der Geltendmachung dieser Betroffenenrechte durch Datentreuhänder sind nicht ersichtlich. Denn im Ansatzpunkt gilt hier dasselbe wie in Bezug auf die Einwilligung. So gebietet es die informationelle Selbstbestimmung nachgerade, dass diese Rechte grundsätzlich auch über einen Vertreter geltend gemacht werden können. Unter bestimmten Voraussetzungen kann in diesem Zusammenhang der Datentreuhänder auch für seine Nutzer Schadensersatzansprüche geltend machen. Verantwortliche könnten im Übrigen versucht sein, in ihren Allgemeinen Geschäftsbedingungen „Abwehrklauseln" vorzusehen, um die Einschaltung eines Datentreuhänders auf Seiten der betroffenen Person zu verhindern. Derartige Klauseln sind richtigerweise als unwirksam anzusehen.[66]

Für Datentreuhänder sind die Anforderungen an die IT-Sicherheit besonders hoch. Dabei muss der Datentreuhänder den strengen Anforderungen nicht nur genügen, sondern dies auch nachweisen können („Rechenschaftspflicht"). In der Praxis kann der Nachweis vor allem durch eine Zertifizierung gelingen. Datentreuhänder unterfallen unter Umständen der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Hier kann es sinnvoll sein, dass die Aufsichtsbehörden im Rahmen der Erstellung der Liste für Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist, klarstellen, in welchem Umfang dazu auch die Angebote von Datentreuhändern gehören. Schon jetzt kann durch die Art der vom Datentreuhänder verarbeiteten Daten einer der gelisteten Verarbeitungsvorgänge erfasst sein.

Hinsichtlich der Verantwortlichkeit sind Datentreuhänder grundsätzlich als Verantwortliche und nicht als bloße Auftragsverarbeiter zu qualifizieren, da sie ja gerade das überlegene Wissen über die Mittel der Datenverarbeitung haben. Denn die Betroffenen erhoffen sich genau diese Erleichterung durch den Rückgriff auf jenen Intermediär. Es besteht darüber hinaus das Risiko, dass Datentreuhänder, gerade im Fall eines kommerziellen Interesses an der Maximierung von Datenverarbeitungen durch andere Verantwortliche im Rahmen eines kollaborativen Zusammenwirkens mit diesen in die Rolle einer gemeinsamen Verantwortlichkeit hineinwachsen. Allerdings bestehen genügend Gestaltungsmöglichkeiten für den Datentreuhänder, sich gleichsam „im Lager" der betroffenen Person anzusiedeln und an dessen Verarbeitungswünschen orientiert nur Daten der betroffenen Personen an andere Verantwortliche gemäß den Wünschen der betroffenen Personen zu verwalten. Eine gemeinsame Verantwortlichkeit scheidet dann aus. Dasselbe gilt für die Wahrnehmung der Betroffenenrechte: Handelt der Datentreuhänder auch im Interesse anderer Verantwortlicher und stellt sich damit – zumindest auch – in deren „Lager", so wird in vielen Fällen eine gemeinsame Verantwortlichkeit anzunehmen sein. Diese Differenzierung – gleichsam im Sinne einer „Lagertheorie" – kann für Datentreuhänder eine vergleichsweise rechtssichere Orientierung bieten, ob mit den anderen Verantwortlichen eine gemeinsame Verantwortlichkeit besteht oder nicht.

[66] Dazu ausführlich *Sackmann*, Die Zulässigkeit von Abwehrklauseln gegen Datentreuhänder (in Vorbereitung).

Damit sorgt das strenge Haftungsregime der gemeinsamen Verantwortlichkeit zugleich für eine Disziplinierung der Datentreuhänder als Agenten zur Interessenwahrnehmung der sie einschaltenden betroffenen Personen. Verfolgen sie diese nicht konsequent, sondern orientieren sich an den Verarbeitungsinteressen der anderen Verantwortlichen, werden sie folgerichtig zu gemeinsamen Verantwortlichen mit diesen. Das führt in der Konsequenz zu erheblichen Haftungsrisiken. Das durch die gemeinsame Verantwortlichkeit hervorgerufene strenge Haftungsregime schafft daher Anreize, die Interessenkollisionen ausschließen. Datentreuhänder sehen sich aber auch unabhängig von einer gemeinsamen Verantwortlichkeit mit den anderen Verantwortlichen erheblichen Haftungsrisiken ausgesetzt. Bei Verletzung datenschutzrechtlicher Vorschriften drohen erhebliche Bußgelder, die jedoch vor allem von der Höhe des Umsatzes abhängen. Die verhältnismäßig noch größeren Risiken ergeben sich aus der möglichen massenhaften Geltendmachung von Schadensersatzansprüchen durch die Nutzer, gegen die sich Datentreuhänder nach einer Datenschutzverletzung nur schwer verteidigen können. Auch insoweit werden starke Anreize zu einem sorgfältigen Umgang mit den Daten der Betroffenen gesetzt.

Mit Blick auf die etwaige Anpassung des geltenden Rechts ist zunächst zu konstatieren, dass angesichts der sinnvollerweise grenzüberschreitend angelegten Datentreuhänder-Modelle eine flankierende Regelung schon prinzipiell allenfalls auf unionaler Ebene sinnvoll ist. Teilweise sieht die DS-GVO auch gar keine Öffnungsklauseln für mitgliedstaatliche Regelungen in den hier untersuchten datenschutzrechtlichen Regularien vor.

Da sich der Rechtsrahmen grundsätzlich als passend erwiesen hat, sind die von der Europäischen Kommission in der Daten-Governance-Verordnung vorgeschlagenen materiell-rechtlichen Vorgaben für Datentreuhänder fraglich. Sie sollten jedenfalls im weiteren Gesetzgebungsprozess mit den Vorgaben des geltenden Rechts abgeglichen und auf ihre Notwendigkeit geprüft werden. Dabei ist insbesondere zu beachten, dass zusätzliche Regeln nicht zur Verwirrung beitragen. Die Notifizierungspflicht für Datentreuhänder kann dagegen, wenn sie bürokratiearm abgewickelt wird, eine sinnvolle Maßnahme sein, um einen Marktüberblick zu erlangen, Missbrauchsfälle von vornherein effektiv zu unterbinden und so das Vertrauen in die Entwicklung entsprechender Modelle zu stärken.

Erforderlich sind aber davon unabhängig exekutive Konkretisierungen durch nationale Datenschutzaufsichtsbehörden und den Europäischen Datenschutzausschuss. Dies kann in den jeweils relevanten allgemeinen Dokumenten – etwa in den Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung – erfolgen oder in Form eines rechtsproblemübergreifenden Dokuments bezogen auf Datentreuhänder. Aber selbst insoweit muss die weitere Entwicklung entsprechender Modelle weiter beobachtet und situativ reagiert werden.

In the real world, we are increasingly seeing data trustees who act as intermediaries between data processors on the one hand and data subjects on the other. They are rightly seen as having the potential to help data subjects better exercise their informational self-determination, including commercial exploitation interests of privacy rights vis-à-vis data controllers and thus increase both data sovereignty and commercial fairness in the application of privacy law. The article examines whether data protection law – especially the General Data Protection Regulation – provides an appropriate framework for these new actors or whether adjustments are necessary, as recently proposed by the Commission in a „Data Governance Regulation".

Big Data im Strafrecht

Zur datenschutzrechtlichen Dimension der Erfassung von strafrechtlichen Entscheidungen in einer Datenbank

Prof. Dr. Dr. Frauke Rostalski/Malte Völkening[*]

In jüngerer Zeit wird über den Aufbau einer umfassenden Urteilsdatenbank diskutiert, die Aufschluss über die Strafzumessungspraxis geben soll. Strafurteile können aber nicht vollständig anonymisiert werden, weshalb die Vorgaben des Datenschutzrechts zu beachten sind. Das führt zu Konflikten mit dem datenschutzrechtlichen Zweckbindungsgrundsatz. Die notwendige Rechtsgrundlage für die Herausgabe der Urteile findet sich in § 475 Abs. 1, 4 StPO oder in den presserechtlichen Auskunftsansprüchen. Erhebliche Schwierigkeiten bereitet dagegen Art. 10 DSGVO. Danach ist eine gesetzliche Ausnahmeregelung erforderlich, um Daten jenseits behördlicher Aufsicht zu verarbeiten. Eine solche kann bei sehr weiter Auslegung in § 475 Abs. 1, 4 StGB erblickt werden. Dieser kann aber nur auf die Öffnungsklausel in Art. 85 Abs. 2 DSGVO gestützt werden, der Ausnahmen nur für bestimmte Zwecke zulässt. Bei Verfolgung anderer Zwecke bleibt nur der Rekurs auf das Medienprivileg.

Inhaltsübersicht

Die mitunter deutliche Divergenz richterlicher Strafzumessungsentscheidungen ist nicht erst seit dem letzten Deutschen Juristentag (wieder) in aller Munde.[1] Ein Vor-

[*] Die Autorin ist Inhaberin des Lehrstuhls für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung an der Universität zu Köln. Der Autor ist Wissenschaftlicher Mitarbeiter an diesem Lehrstuhl.

[1] Siehe etwa *Kaspar*, Sentencing Guidelines versus freies tatrichterliches Ermessen – Brauchen wir ein neues Strafzumessungsrecht?, 2018; *Kaspar/Höffler/Harrendorf* NK 32 (2020), 35 (36 ff.); *Kudlich/Koch* NJW 2018, 2762.

schlag zur Vermeidung sachlich nicht gerechtfertigter Unterschiede liegt in der Ermöglichung von mehr Transparenz.[2] Diese kann durch eine Datenbank geschaffen werden, die den einzelnen Rechtsanwender in die Lage versetzt, Einblicke in die Strafzumessungsentscheidungen seiner Kollegen in anderen deutschen Gerichtsbezirken zu erlangen.[3] Die vorhandenen juristischen Datenbanken lassen dies nicht zu, weil sie kaum Urteile von Instanzgerichten enthalten. Eine Erfassung und Verarbeitung sämtlicher ausgangsgerichtlicher Entscheidungen scheitert in praktischer Hinsicht schon an mangelnden menschlichen Kapazitäten. Wie an anderer Stelle dargelegt, kann der Einsatz von Künstlicher Intelligenz ein Schlüssel sein, um dieses Defizit auszugleichen.[4]

Neben der technischen Realisierbarkeit stellt sich aber eine weitere Frage, deren Beantwortung sich ganz entscheidend auf die Entwicklung einer umfassenden Datenbanklösung auswirkt: Steht die Katalogisierung von Strafurteilen mit dem europäischen und nationalen Datenschutzrecht in Einklang? Strafurteile enthalten in besonderem Maße sensible Daten von Personen. Ist ihre systematische Erfassung und Verarbeitung in einer Datenbank daher überhaupt zulässig? Es handelt sich dabei um Fragen, die so oder in ähnlicher Weise auch bei anderen Datenbanksystemen, die Strafurteile enthalten (einschließlich beck-online und juris), und teilweise auch darüber hinaus bei jeder (wissenschaftlichen) Befassung mit den Entscheidungen der deutschen Strafgerichte relevant werden. Es wird sich zeigen, dass insbesondere das Inkrafttreten der DSGVO[5] hier zu vielen Problemen geführt hat, deren Einordnung noch ganz am Anfang steht.

I. Anwendbarkeit europäischen und nationalen Datenschutzrechts

Ein Blick ins außereuropäische Ausland zeigt, dass die Erfassung von Strafurteilen in einer Datenbank als Hilfsmittel für richterliche Strafzumessungsentscheidungen kein neuer Gedanke ist. In New South Wales (Australien) ist bereits seit 1990 das sogenannte Sentencing Information System (SIS) im Einsatz:[6] eine Datenbank, „designed to reduce inconsistency"[7]. Genutzt wird es sowohl von Gerichten und Strafverfolgungsbehörden als auch von Verteidigern.[8] SIS bietet Zugang zu Strafzumessungsstatistiken sämtlicher Gerichte des Bundesstaats. Der Nutzer kann in großem Umfang die Volltexte der betreffenden Entscheidungen einsehen. Zusätzlich enthält das Programm Hin-

[2] Dazu *Rostalski/Völkening* KriPoZ 2019, 265 (268 ff.).

[3] Statt vieler *Kaspar/Höffler/Harrendorf* NK 32 (2020), 35 (47 ff.); *Rostalski/Völkening* KriPoZ 2019, 265 (270 ff.); *Streng* StV 2018, 593 (599).

[4] *Rostalski/Völkening* KriPoZ 2019, 265 (271 f.). Entgegen *Greco* RW 2020, 29 (31 Fn. 10) ist dieser Vorschlag nicht mit dem amerikanischen COMPAS-System, das KI-gestützt Rückfallprognosen berechnet, vergleichbar, weil Smart Sentencing nur die vorhandenen Daten klassifiziert und systematisiert, die Bewertung aber den (menschlichen) Rechtsanwendern überlässt.

[5] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016 L 119/1, ber. ABl. L 2016 314/72 und ABl. 2018 L 127/2).

[6] *Potas/Ash/Sagi/Cumines* International Journal of Law and Information Technology 6 (1998), 99 (119 et passim). Vgl. außerdem *Hoven*, FS Sieber (im Erscheinen), II.

[7] *Gleeson*, A Core Value. Vortrag vom 6.10.2006 im Rahmen des Annual Colloquium, Judicial Conference of Australia, Canberra (abrufbar unter: http://jca.asn.au/wp-content/uploads/2013/11/2006-cj6oct06.pdf, zuletzt geprüft am 11.11.2020), S. 4.

[8] *Lumley*, From controversy to credibility: 20 years of the Judicial Commission of New South Wales, 2008 (abrufbar unter: https://www.judcom.nsw.gov.au/wp-content/uploads/2014/07/judcom-20years-web.pdf, zuletzt geprüft am 11.11.2020), S. 7.

weise auf jeweils geeignete Begleitliteratur und zum Strafsystem Australiens.[9] 1996 wurde das SIS in das Programm Judicial Information Research System (JIRS) überführt, das zusätzliche Recherchemöglichkeiten bietet.[10] Auch in Japan gibt es seit 2008 eine Datenbank mit Strafzumessungsentscheidungen, die allerdings auf Verfahren mit Laienrichtern (Saiban'in) beschränkt und nicht öffentlich zugänglich ist.[11]

JIRS und die japanische Strafzumessungsdatenbank könnten als Vorbild einer nationalen Datenbank für Strafurteile dienen. Allerdings hätte sich diese an dem in Deutschland einschlägigen Datenschutzrecht zu messen. In erster Linie ist dabei an die Bestimmungen der DSGVO und der §§ 45 ff. BDSG (iVm § 500 StPO) zu denken. Im deutschen und europäischen Rechtssystem greift der Datenschutz ieS nur für die Verarbeitung personenbezogener Daten (Art. 2 Abs. 1 DSGVO, § 1 Abs. 1 BDSG). Strafurteile enthalten die Namen des oder der Angeklagten, von Zeugen, Sachverständigen, Richtern, Staatsanwälten und so weiter, und sind damit in vielerlei Hinsicht personenbezogen (Art. 4 Nr. 1 DSGVO, § 46 Nr. 1 BDSG).

Diese Informationen spielen für die spätere Rezeption durch Rechtswissenschaft und Rechtspraxis in der Regel keine Rolle. Gemäß dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO, § 47 Nr. 3 BDSG) käme daher eine Anonymisierung infrage.[12] In den bestehenden juristischen Datenbanken und Zeitschriften werden Urteile üblicherweise anonymisiert, indem die Nachnamen der beteiligten Personen (insb. des oder der Angeklagten) bis auf den Anfangsbuchstaben geschwärzt bzw. gelöscht werden. Zu beachten ist jedoch, dass ein Personenbezug gemäß Art. 4 Nr. 1 DSGVO, § 46 Nr. 1 BDSG auch dann noch besteht, wenn die betroffene Person nur indirekt identifiziert werden kann.[13] Strafurteile weisen üblicherweise einen hohen Individualisierungsgrad auf. Selbst wenn die Namen der Beteiligten entfernt werden, ist eine Zuordnung zum Original einschließlich der darin enthaltenen Klarnamen durch einen Textvergleich daher regelmäßig möglich. Gleiches gilt, wenn hinreichende Detailkenntnisse über den zugrundeliegenden Prozess verfügbar sind. Aus Sicht der Verfahrensbeteilig-

[9] Ausführlich zur Funktionsweise *Potas/Ash/Sagi/Cumines* International Journal of Law and Information Technology 6 (1998), 99 (106 ff.); vgl. auch *Miller* Columbia Law Review 105 (2005), 1351 (1375); *Lumley*, From controversy to credibility: 20 years of the Judicial Commission of New South Wales, 2008 (abrufbar unter: https://www.judcom.nsw.gov.au/wp-content/uploads/2014/07/judcom-20years-web.pdf, zuletzt geprüft am 11.11.2020), S. 7.

[10] *Potas/Ash/Sagi/Cumines* International Journal of Law and Information Technology 6 (1998), 99 (105 Fn. 14).

[11] *Schmidt*, Das japanische Saiban'in System und das deutsche Schöffensystem, 2019, S. 157 ff; *Shiroshita* Federal Sentencing Reporter 22 (2010), 243 (246); s. auch *Kaspar/Höffler/Harrendorf* NK 32 (2020), 35 (47 ff.), die die Einführung der Datenbank aber auf 2009 datieren.

[12] Vgl. BeckOK DatenschutzR/*Schantz*, 33. Ed. (1.8.2020), Art. 5 DSGVO Rn. 25.1; ähnlich bereits *Kockler* JurPC 1996, 46 (47, 51); zum Verhältnis von BDSG und DSGVO insofern *Johannes/Weinhold* in HK-BDSG, 2020, § 47 Rn. 24.

[13] Für die Abgrenzung zwischen Anonymisierung und indirekter Bestimmbarkeit ist auf die Möglichkeiten, die der die Daten Verarbeitende oder ein Dritter tatsächlich hat und mit deren Einsatz vernünftigerweise zu rechnen ist, abzustellen (BeckOK DatenschutzR/*Schild*, Art. 4 DSGVO Rn. 18). Es erfolgt eine relative Betrachtung, dazu ausführlich *Hofmann/Johannes* ZD 2017, 221 (225 f.); außerdem *Martini/Weinzierl* NVwZ 2017, 1251 (1252 f.); *Roßnagel* ZD 2019, 157 (159). In diese Richtung auch EuGH Urteil v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 = NVwZ 2017, 213 (215) – Breyer vs. BRD. Zurückhaltend *Karg* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 Rn. 60 ff., dort auch zur Gegenauffassung (Rn. 58). Ähnlich differenzierend *Ziebarth* in HK-EuDSchVO, 2. Aufl. (2018), Art. 4 Rn. 37 ff.

ten und aller Personen, die Zugang zum Originalurteil haben, führt die Schwärzung daher nicht ohne Weiteres zur Anonymisierung der Urteile.[14]

Für Außenstehende (insb. den Betreiber einer Urteilsdatenbank) sind die Originale normalerweise nicht verfügbar,[15] weshalb hier meistens von einer echten (relativen[16]) Anonymisierung auszugehen sein wird. Aber auch dies ist nicht zwingend: Jedenfalls dann, wenn Urteile aufgrund besonderer Sachverhaltskonstellationen nur auf bestimmte Personen bezogen sein können[17] oder eine umfangreiche Presseberichterstattung stattgefunden hat,[18] ist eine Zuordnung auch mit verhältnismäßigem Aufwand möglich.[19] Hinzu kommen Anonymisierungsfehler, die sowohl bei einer händischen als auch bei einer technikgestützten Schwärzung bei hinreichend großen Datenmengen nie ganz auszuschließen sind. Demnach können Strafurteile zwar grundsätzlich anonym sein. Es besteht gleichwohl vor allem bei einer hohen Zahl betroffener Urteile das Risiko, dass sie trotz Schwärzung der Klarnamen auf natürliche Personen bezogen werden können. Da diese Urteile praktisch nicht herausgefiltert werden können,[20] zwingen sie zur Einhaltung der datenschutzrechtlichen Vorschriften in Bezug auf alle verarbeiteten Entscheidungen.

Dabei finden Verarbeitungen im Sinne von Art. 4 Nr. 2 DSGVO, § 46 Nr. 2 BDSG in verschiedenen Stadien der Erstellung einer Strafurteilsdatenbank statt. Die Urteile müssen von den Gerichten (bzw. Staatsanwaltschaften) herausgegeben werden. Anschließend müssen sie, je nach Zweck der Datenbank, gefiltert und klassifiziert werden. Geschieht dies mittels selbstlernender Algorithmen, müssen diese anhand der Daten trainiert werden. Schließlich werden die Urteile in die Datenbank eingepflegt, verknüpft und bei Abfragen ausgegeben. Bei all diesen Vorgängen müssen die Vorschriften des Datenschutzrechts beachtet werden.

II. Wahrung des Grundsatzes der Zweckbindung, Art. 5 Abs. 1 lit. b Var. 2 DSGVO, § 47 Nr. 2 Var. 2 BDSG

Art. 5 DSGVO bzw. § 47 BDSG stellt mehrere Grundsätze für die Verarbeitung personenbezogener Daten auf. Die Erstellung und der Betrieb einer Datenbank bestehend aus Strafurteilen kann vor allem mit dem Grundsatz der Zweckbindung in Konflikt geraten. Art. 5 Abs. 1 lit. b Var. 2 DSGVO und § 47 Nr. 2 Var. 2 BDSG sehen vor, dass personenbezogene Daten nicht in einer Weise weiterverarbeitet werden dürfen,

[14] So auch *Brink/Vogel* NJW 2015, 3710 (3711). Vgl. zu diesem Problem bereits *Rostalski/Völkening* KriPoZ 2019, 265 (272 Fn. 82).

[15] Sie werden im Regelfall zwar öffentlich verkündet (§§ 268 Abs. 2 S. 1, 2 StPO, 169 Abs. 1 S. 1 GVG), jedoch ist vernünftigerweise nicht damit zu rechnen, dass ein Datenbankbetreiber diese Verkündung nutzt, um später erlangte Urteile mit den betroffenen Personen in Verbindung zu bringen.

[16] S. dazu Fn. 13. Die Auffassung von *Ziebarth* in HK-EuDSchVO, Art. 4 Rn. 37 dürfte bei (fach-)öffentlich zugänglichen Urteilsdatenbanken jedoch stets zum Fortbestehen des Personenbezugs führen, da unter den Zugriffsberechtigten auch die (professionellen) Verfahrensbeteiligten sind. Die Frage kann hier offenbleiben, weil auch die im Text vorgenommene enge Auslegung des Begriffs des Personenbezugs nicht von der Beachtung der DSGVO befreit (dazu sogleich).

[17] Vgl. BGH NJW 2018, 3123 (3123 f.) und den „ehemaligen Innenminister des Freistaats T." bei BVerfG NJW 2015, 3708 (3708), dazu *Brink/Vogel* NJW 2015, 3710 (3711).

[18] Vgl. OLG Celle NJW 1990, 2570 (2571); *Brink/Vogel* NJW 2015, 3710 (3711).

[19] IErg ebenso MüKoStPO/*Singelnstein*, 1. Auflage 2019, § 475 Rn. 30.

[20] Zumal auch das Herausfiltern selbst schon eine Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO wäre.

die unvereinbar ist mit den festgelegten, eindeutigen und legitimen Zwecken, zu denen sie erhoben wurden. Erheben meint dabei das Beschaffen von Daten über eine Person.[21]

1. Zweckänderung durch die Verarbeitung in der Datenbank?

Wenn ein Verantwortlicher iSd Art. 4 Nr. 7 DSGVO, § 46 Nr. 7 BDSG Daten von einem Dritten übermittelt bekommt und sie entgegennimmt, liegt eine erneute Erhebung vor[22] und nicht etwa eine (zweckändernde) Weiterverarbeitung der durch den Dritten erhobenen Daten. Die Anforderung der Urteile bei den Gerichten durch den *Datenbankbetreiber* stellt daher eine neue Erhebung mit eigener Zwecksetzung[23] dar, sodass die anschließende Weiterverarbeitung keine Zweckänderung bedeutet. Der Zweckbindungsgrundsatz steht der Verarbeitung insoweit also nicht entgegen.

2. Zweckänderung durch gerichtliche Weitergabe von Entscheidungen?

Indessen sind die in Strafurteilen enthaltenen personenbezogenen Daten, insbesondere im Hinblick auf den Angeklagten, durch die *Gerichte bzw. Staatsanwaltschaften* zum Zweck der Entscheidungsfindung in einem konkreten Strafverfahren erhoben worden. Gemäß Art. 2 Abs. 2 lit. d DSGVO, § 45 S. 1 BDSG iVm § 500 Abs. 1 StPO richtet sich die weitere Verarbeitung einschließlich der Übermittlung dieser Daten an den Datenbankbetreiber daher nicht nach der DSGVO, sondern nach den §§ 45 ff. BDSG in Umsetzung der JI-RL[24].[25]

Zulässig ist gemäß § 49 S. 1 BDSG eine Datenverarbeitung durch die Justiz zu Zwecken der Strafverfolgung[26]. Dagegen erklärt § 49 S. 2 BDSG eine Weiterverarbeitung,

---

[21] *Roßnagel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 4 Nr. 2 Rn. 15 unter Berufung auf § 3 Abs. 3 BDSG a.F.

[22] *Roßnagel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 4 Nr. 2 Rn. 15; vgl. auch *Ernst* in Paal/Pauly, 2. Aufl. (2018), Art. 4 DSGVO Rn. 23.

[23] Vgl. *Roßnagel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 5 Rn. 74.

[24] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. 2016 L 119/89, ber. ABl. 2018 L 127/9), vgl. dazu BeckOK DatenschutzR/*Wolff*, § 45 BDSG Rn. 1; *Schwichtenberg* NK 32 (2020), 91 (92).

[25] Zur Abgrenzung von den §§ 35 ff. DSG NRW s. *Pabst* in Schwartmann/Pabst, DSG NRW, 2020, § 35 Rn. 15 ff; *Braun* in Gola/Heckmann, BDSG, 2019, § 45 Rn. 15 plädiert demgegenüber für ein enges Verständnis des Begriffs der „Verfolgung von Straftaten", sodass die Verurteilung durch die Gerichte nicht davon erfasst ist. Dadurch soll ein „Einklang" mit dem Anwendungsbereich der DSGVO hergestellt werden. *Johannes/Weinhold* in HK-BDSG, § 45 Rn. 53 verweisen insofern auf EG 80 der JI-RL. Dort heißt es jedoch im Gegenteil, dass „diese Richtlinie auch für die Tätigkeit der nationalen Gerichte […] gilt". Diese seien nur (!) von der Zuständigkeit der Aufsichtsbehörden auszunehmen (vgl. Art. 45 Abs. 2 S. 1 JI-RL). Für eine inkongruente Auslegung des Art. 2 Abs. 2 lit. d DSGVO, wie *Braun* sie offenbar befürchtet, gibt es denn auch keine Anhaltspunkte. Dort ist zwar von der Strafverfolgung durch die „zuständigen Behörden" die Rede, von diesem europarechtlichen Begriff sind jedoch auch Gerichte umfasst (vgl. EG 97 der DSGVO und *Petri* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 10 DSGVO Rn. 7; BeckOK DatenschutzR/*Bäcker*, Art. 2 DSGVO Rn. 26; iErg auch *Schwichtenberg* NK 32 [2020], 91 [92]; BeckOK DatenschutzR/*Schild*, Syst. E Rn. 6). Dass EG 20 der DSGVO deren Geltung für die „Tätigkeit der Gerichte" feststellt, steht dem nicht entgegen, da diese Tätigkeit über die Strafverfolgung hinausgeht. §§ 45 ff. BDSG gelten dementsprechend auch für die Datenverarbeitung durch die Strafgerichte einschließlich der Aburteilung.

[26] Genauer nennen § 45 S. 1, 3 BDSG die „Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten" einschließlich des „Schutz[es] vor und d[er] Ab-

die nicht mehr zum Zweck der Strafverfolgung erfolgt, vorbehaltlich einer anderweitigen Regelung für unzulässig.[27] Die Verwendung von Urteilen zur Erstellung einer Datenbank dient nicht länger der Entscheidungsfindung *in diesem konkreten Fall,* was für eine solche Abkehr vom Zweck der Strafverfolgung sprechen könnte.

Allerdings lässt sich die Überlegung anstellen, ob nicht jedwede gerichtliche Entscheidung per se als Teil eines fortlaufenden Prozesses der allgemeinen Rechtsfindung und -verbesserung zu beurteilen ist. Die Datenerhebung in jedem Einzelfall wäre dann in den Gesamtkontext der richterlichen Tätigkeit eingeordnet, die auf die Fortentwicklung oder zumindest Stabilisierung des geltenden Rechts gerichtet ist. Auf dieser Basis ließe sich annehmen, dass auch die Weitergabe des Urteils zu dessen Erfassung in einer Datenbank mit dem ursprünglichen Erhebungszweck in Einklang steht. Denn die spätere Nutzung der Datenbank dient wiederum der Entscheidungsfindung im Hinblick auf andere Sachverhalte und damit der Strafverfolgung.[28]

Entsprechend sieht § 50 S. 1 BDSG die Zulässigkeit der Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder zu statistischen Zwecken „im Rahmen der in § 45 [BDSG] genannten Zwecke" vor[29] – also dann, wenn die wissenschaftlichen usw. Zwecke wiederum der Strafverfolgung dienen.[30] Wissenschaftliche Forschung meint die methodengeleitete und systematische Erzielung neuer Erkenntnisse im Dienste der Allgemeinheit.[31] Hierfür kann eine Urteilsdatenbank eine notwendige Voraussetzung sein, etwa wenn Strafzumessungsentscheidungen statistisch ausgewertet werden sollen, um eine Grundlage für zukünftige Urteile zu schaffen.[32] Dann nimmt bereits die Erstellung der Datenbank an der Privilegierung teil.[33]

§ 49 S. 1 BDSG erlaubt die Weiterverarbeitung unter neuer Zwecksetzung jedoch selbst dann, wenn der neue Zweck ebenfalls in der Strafverfolgung besteht, nur, wenn

---

wehr von Gefahren für die öffentliche Sicherheit". Zumindest die letzteren Zwecke dürften im Rahmen der hier diskutierten Strafurteilsdatenbanken aber keine Rolle spielen, weshalb im Text pauschal von Strafverfolgung gesprochen wird.

[27] Die Vorschrift steht damit im Widerspruch zu § 45 S. 1 BDSG. Diesem zufolge gelten die §§ 45 ff. BDSG für die Strafverfolgungsbehörden nur, „*soweit* sie Daten zum Zweck der Erfüllung dieser Aufgaben [der Strafverfolgung] verarbeiten". § 49 S. 2 BDSG erfasst aber einen Fall, in dem die Behörden Daten gerade *nicht* zu einem der dort genannten Zwecke verarbeiten. Aus der Systematik wird jedoch deutlich, dass die Zweck*änderung* noch von den §§ 45 ff. BDSG erfasst wird. Erst nach erfolgter Änderung greifen die allgemeinen datenschutzrechtlichen Vorschriften insb. der DSGVO. Zum Verhältnis von JI-RL und DSGVO bei der Weitergabe von Daten s. BeckOK DatenschutzR/*Wolff*, § 45 BDSG Rn. 13 ff. und (iErg wie hier) BeckOK DatenschutzR/*Bäcker*, Art. 2 DSGVO Rn. 30 ff.

[28] Vgl. auch OLG Celle NJW 1990, 2570 (2571). Sofern dies auch für die Nutzung durch Dritte (Strafverteidiger, Wissenschaftler etc.) gilt, wäre *Schnabel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 86 Rn. 33 nicht zuzustimmen, demzufolge Daten (durch den Staat) niemals zum Zweck der späteren Offenlegung erhoben werden.

[29] Es handelt sich allerdings nicht um eine eigenständige Rechtsgrundlage, sondern nur um eine Erweiterung des ursprünglichen Zwecks (*Hense* in HK-BDSG, § 50 Rn. 1 f.).

[30] *Hense* in HK-BDSG, § 50 Rn. 2; vgl. *Frenzel* in Paal/Pauly, § 50 BDSG Rn. 2.

[31] Zum Begriff s. *Jarass* GRCh, 3. Aufl. (2016), Art. 13 Rn. 6; *Tinnefeld* in TBPH, Einführung in das Datenschutzrecht, 7. Aufl. (2020), S. 1 (185); *Caspar* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 89 Rn. 11 ff.; *Roßnagel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 5 Rn. 106 mwN.

[32] Vgl. zu einem solchen Projekt *Rostalski/Völkening* KriPoZ 2019, 265 (265 f.) et passim. Derzeit ist eine Machbarkeitsstudie in Arbeit, die klären soll, ob und in welchem Umfang die Rechtsfindung im Bereich der Strafzumessung durch technologiegestützte Auswertungen angeleitet werden kann und darf. Auch das impliziert eine Verarbeitung von Strafurteilen zu wissenschaftlichen Zwecken.

[33] Zur Erstreckung des Begriffs der wissenschaftlichen Forschung auch auf notwendige Vorarbeiten s. *Jarass* GRCh, Art. 13 Rn. 7.

der Verarbeitende hierzu (verwaltungsrechtlich[34]) *befugt* ist. Wenngleich § 50 S. 1 BDSG kein entsprechendes Merkmal enthält, wird aus der Beschränkung auf die „in § 45 [BDSG] genannten Zwecke" einhellig geschlossen, dass sich auch diese Norm nur auf Verarbeitungen durch die zuständigen Strafverfolgungsbehörden (einschließlich der Gerichte) bezieht.[35] Selbst wenn die Weitergabe der Urteile zur Aufnahme in eine Datenbank bzw. der Betrieb und die Nutzung dieser Datenbank nach wie vor (ggf. in wissenschaftlicher Form) der Strafverfolgung dienen, können sie deshalb nur dann auf die §§ 49 S. 1, 50 S. 1 BDSG gestützt werden, wenn die Datenbank von der Justiz selbst betrieben wird und *ausschließlich* den Strafverfolgungsbehörden zu Strafverfolgungszwecken zur Verfügung steht.

Soweit Urteile für eine Datenbank verwendet werden sollen, die nicht durch die Justiz betrieben wird oder sich nicht nur[36] an Strafverfolgungsbehörden, sondern auch an Strafverteidiger, externe Wissenschaftler oder die Öffentlichkeit richtet, ist daher gemäß § 49 S. 2 BDSG eine spezielle Rechtsgrundlage erforderlich. In der Praxis dürfte das für die weit überwiegende Zahl der Urteilsdatenbanken gelten. So gewährt selbst die nichtöffentliche japanische Strafzumessungsdatenbank auch Strafverteidigern Zugriff auf die enthaltenen Daten.[37]

3. Rechtfertigung durch § 475 Abs. 1, 4 StPO

Als spezielle Rechtsgrundlage für die Zweckänderung kommen verschiedene Normen in Betracht. Gemäß § 475 Abs. 1, 4 StPO kann eine Privatperson Auskünfte aus Akten erhalten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, soweit sie hierfür ein berechtigtes Interesse darlegt. Allerdings sind die Auskünfte zu versagen, wenn der hiervon Betroffene daran ein schutzwürdiges Interesse hat. Die Vorschrift gilt nach Auffassung des Bundesgerichtshofs für die Überlassung anonymisierter strafgerichtlicher Entscheidungsabschriften an private Dritte.[38]

---

[34] BeckOK DatenschutzR/*Albers*, § 49 BDSG Rn. 12.

[35] Vgl. BeckOK DatenschutzR/*Schlösser-Rost*, § 50 BDSG Rn. 5; *Krohm* in Gola/Heckmann, § 50 Rn. 5; i.E. auch *Frenzel* in Paal/Pauly, § 50 BDSG Rn. 2, der jedoch auf die Möglichkeit einer Auftragsverarbeitung durch einen Dritten hinweist.

[36] Bei Zweckbündeln ist die Privilegierung durch § 50 S. 1 BDSG auf die privilegierten Zwecke beschränkt. Im Übrigen bleibt der Zweckbindungsgrundsatz vollständig anwendbar (vgl. Art. 89 Abs. 4 DSGVO, dazu *Caspar* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 89 Rn. 67).

[37] Dazu *Schmidt,* Saiban'in System (Fn. 11), S. 159; *Shiroshita* Federal Sentencing Reporter 22 (2010), 243 (246).

[38] BGH NJW 2018 3123 (3123); ebenso *Ritscher/Klinge* in Satzger/Schluckebier/Widmaier, StPO Kommentar, 4. Aufl. (2020), § 475 Rn. 2 und bereits LG Berlin NJW 2002, 838 (838). Demgegenüber leitet der vierte zivilrechtliche Senat eine allgemeine Veröffentlichungspflicht angesichts der hohen Bedeutung der Vorhersehbarkeit richterlicher Entscheidungen aus dem Rechtsstaats-, Demokratie- und Gewaltenteilungsprinzip ab, s. BGH NJW 2017, 1819 (1819 f.); ebenso BVerwG NJW 1997, 2694 (2695); speziell für das Strafverfahren auch *Putzke/Zenthöfer* NJW 2015, 1777 (1777 f.); zum Ganzen BeckOK StPO/*Wittig*, 37. Ed. (1.7.2020), § 475 Rn. 5.1 f. Jedoch ist eine *einfachgesetzliche* Grundlage erforderlich, weil eine Anonymisierung der Urteile den Personenbezug regelmäßig nicht vollständig beseitigt (s.o.), weshalb ein rechtfertigungsbedürftiger Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt. Hierauf stellt letztlich auch BGH NJW 2018, 3123 (3124) ab; vgl. auch BVerfG NJW 2009, 2876 (2876) allgemein zu Aktenauskünften und Akteneinsicht durch Dritte im Strafverfahren. Wie hier MüKoStPO/*Singelnstein*, § 475 Rn. 30.

Soweit die Auskünfte (auch) zu Forschungszwecken erfolgen,[39] findet sich in § 476 Abs. 1 StPO eine weitere Rechtsgrundlage für die Übermittlung von Aktenauskünften, die gemäß ihrem Wortlaut wesentlich strengere Anforderungen an die Aktenauskunft stellt als § 475 Abs. 1, 4 StPO.[40] Werden jedoch neben wissenschaftlichen auch noch andere Zwecke verfolgt, so können entsprechende Auskünfte wegen der strengen Zweckbindung (Abs. 4) nicht auf § 476 StPO gestützt werden. Allerdings ist die Regelung für wissenschaftlich motivierte Auskunftsverlangen nicht abschließend.[41] Gleiches gilt für die Offenlegung personenbezogener Daten.[42] Die Übermittlung nicht (vollständig) anonymisierter Urteile (unter anderem) zu Forschungszwecken kann daher auch auf § 475 Abs. 1, 4 StPO gestützt werden.[43]

Soweit das Betreiben einer Fachdatenbank unter den Pressebegriff fällt[44] und es sich um Entscheidungen der Instanzgerichte handelt (das betrifft beispielsweise die Sammlung von Strafzumessungsentscheidungen), kann außerdem ein presserechtlicher Anspruch auf Übersendung der Urteilsabschriften bestehen, etwa aus § 4 Abs. 1 LPresseG NRW oder aus §§ 55 Abs. 3, 9a Abs. 1 S. 1 RStV.[45] Dessen Verhältnis zu § 475 Abs. 1, 4 StPO ist wiederum stark umstritten.[46] In der Sache laufen die Anspruchsgrundlagen aber ohnehin parallel: Das journalistische Informationsinteresse, das den presserechtlichen Auskunftsansprüchen zugrunde liegt, ist stets auch ein berechtigtes Interesse im

---

[39] S. oben unter II. 2.

[40] Insb. ist der Empfängerkreis auf Forschungseinrichtungen und öffentliche Stellen beschränkt, außerdem statuiert die Norm eine Geheimhaltungsverpflichtung und besondere Organisations- und Verwendungsregeln.

[41] Vgl. *Ritscher/Klinge* in Satzger/Schluckebier/Widmaier, StPO Kommentar, § 475 Rn. 2; *Graalmann-Scheerer* NStZ 2005, 434 (435) zu Anträgen von Doktoranden und Habilitanden.

[42] § 476 StPO bezieht sich zwar nur auf personenbezogene, nicht auf anonymisierte Daten (vgl. § 476 Abs. 1 S. 1 Nr. 2 StPO, *Ritscher/Klinge* in Satzger/Schluckebier/Widmaier, StPO Kommentar, § 476 Rn. 1). Andererseits ist auch § 475 Abs. 1, 4 StPO nicht auf (vollständig) anonymisierte Auskünfte beschränkt (vgl. BeckOK StPO/*Wittig*, § 475 Rn. 11).

[43] Da § 476 StPO wesentlich strengere Anforderungen an die Aktenauskunft stellt als § 475 Abs. 1, 4 StPO, muss er jedoch einen von diesem verschiedenen Anwendungsbereich haben. Wenn eine Unterscheidung anhand des Personenbezugs des Auskunftsgegenstands und der Zwecksetzung nach dem Gesagten nicht möglich ist, bietet es sich an, nach der Bedeutung der Auskunftsgewährung für den davon Betroffenen (den Angeklagten) zu differenzieren. Zu dessen Schutz sieht § 476 StPO zahlreiche Sicherungen vor, die sich nur durch die besondere Sensibilität personenbezogener Daten rechtfertigen lassen. Wenn personenbezogene Daten aber grundsätzlich auch aufgrund von § 475 Abs. 1, 4 StPO herausgegeben werden können, kann die Existenz eines Personenbezugs *allein* nicht ausschlaggebend sein. Die verschärften Voraussetzungen des § 476 StPO sind vielmehr erst dann einzuhalten, wenn eine Aktenauskunft gemäß § 475 Abs. 1, 4 StPO einen unverhältnismäßigen Eingriff in die Rechte des Betroffenen darstellen würde und daher aufgrund *dieser* Norm nicht mehr zulässig wäre. § 476 StPO erlaubt also einen tieferen Eingriff in das Recht auf informationelle Selbstbestimmung als § 475 Abs. 1, 4 StPO.

[44] Dazu noch unten unter IV. 2.

[45] Vgl. BVerwG NJW 2015, 807 (808); BVerfG NJW 2015, 3708 (3709 f.) mit Anm. *Brink/Vogel*; außerdem BGH NJW 2018, 3123 (3124) mit Anm. *Schork*. Für den Bund gibt es keine entsprechende Regelung, hier ergibt sich ein vergleichbarer Informationsanspruch u.U. aber aus Art. 5 Abs. 1 S. 2 GG (BeckOK InfoMedienR/*Engel* , 29. Ed. [1.8.2020], § 4 LPresseG NRW Rn. 8; a.A. etwa *Huber* NVwZ 2013, 1010 [1010 f.]: Anwendbarkeit des Landespresserechts). Zur Subsumtion der Gerichte unter den presserechtlichen Behördenbegriff s. etwa BeckOK InfoMedienR/*Soppe*, § 3 HPresseG Rn. 10.

[46] Für die Spezialität der presserechtlichen Auskunftsansprüche *Ritscher/Klinge* in Satzger/Schluckebier/Widmaier, StPO Kommentar, § 475 Rn. 3; BeckOK StPO/*Wittig*, § 475 Rn. 5 mwN; in diese Richtung wohl auch BVerwG NJW 2015, 807 (811). Das OVG Münster NJW 2001, 3803 (3803) nimmt dagegen offenbar einen Vorrang des § 475 Abs. 1, 4 StPO an. Der VGH Mannheim, Urt. v. 11.9.2013 – 1 S 509/13 wendet beide Anspruchsgrundlagen nebeneinander an. MüKoStPO/*Singelnstein*, § 475 Rn. 12 plädiert für eine gesonderte Regelung *de lege ferenda*.

Sinne des § 475 Abs. 1, 4 StPO.[47] Gemäß § 4 Abs. 2 Nr. 3 LPresseG NRW bzw. §§ 55 Abs. 3, 9a Abs. 1 S. 2 Nr. 3 RStV ist das Interesse an der Herausgabe der Urteile gegen die davon betroffenen schutzwürdigen privaten Interessen abzuwägen. Dies entspricht der Abwägung von berechtigtem Interesse des Anspruchstellers und schutzwürdigem Interesse des Betroffenen im Rahmen des § 475 Abs. 1, 4 StPO.[48]

Fraglich ist damit unabhängig von der Einordnung der Datenbank als Journalismus, ob die Voraussetzungen des § 475 StPO erfüllt sind. Hierfür wäre erforderlich, dass die Erstellung einer solchen Datenbank ein berechtigtes Interesse darstellt und zugleich der Betroffene kein schutzwürdiges Interesse an der Versagung aufweist. Vorausgesetzt ist also eine Abwägung der widerstreitenden Interessen.[49] Dabei streiten zugunsten des Betroffenen – hier insbesondere: des Angeklagten im Strafverfahren – Persönlichkeitsrechte.[50] Strafrechtliche Entscheidungen weisen unabhängig von ihrem spezifischen Ausgang ein hohes Stigmatisierungspotential auf. Bereits die Tatsache, dass ein Strafverfahren gegen eine Person geführt wurde, kann den Betreffenden gesellschaftlich bemakeln, selbst wenn er zuletzt freigesprochen wird. Umso schwerer wiegt es, wenn der Angeklagte verurteilt wird. Mit dem entsprechenden Schuldspruch geht die Aussage einher, dass er sich rechtlich fehlerhaft verhalten hat. Dies betrifft nicht bloß das Verhältnis zwischen Täter und Opfer. Vielmehr nimmt sich der Täter durch die Straftat ein Mehr an Freiheit, das ihm rechtlich nicht zusteht. Auf diese Weise kommt es zu einer Verletzung des Rechts.[51] Die Verantwortung des Betreffenden für sein individuelles Fehlverhalten besteht mithin gegenüber der gesamten Gesellschaft, was auch nachvollziehen lässt, weshalb die Tat einen Eindruck selbst auf Menschen ausübt, die damit unmittelbar nicht in Berührung gekommen sind.[52]

Indem sich aber der Täter in seine Bestrafung fügt und die damit einhergehende Freiheitseinbuße akzeptiert, gelingt es ihm, in den Kreis der übrigen Gesellschaftsmitglieder zurückzugelangen. Durch Verbüßen der Strafe erfolgt ein Ausgleich für die seitens des Täters zu Unrecht angemaßte Freiheit, sodass er im Anschluss daran in jedweder Hinsicht wieder Teil der Rechtsgemeinschaft ist.[53] Er hat dann auch ein be-

[47] Vgl. OVG Münster NJW 2001, 3803 (3803).

[48] Ob eine solche Abwägung im Rahmen des § 475 Abs. 1, 4 StPO erforderlich ist, ist allerdings umstritten, weil der Wortlaut der Versagungsgründe hier von dem im Übrigen weitgehend parallelen § 406e Abs. 2 S. 1 StPO (betreffend das Akteneinsichtsrecht des Verletzten) abweicht („schutzwürdiges Interesse" hier, „*überwiegende* schutzwürdige Interessen" dort). Daraus wird teilweise gefolgert, schon die bloße *Existenz* eines schutzwürdigen Versagungsinteresses führe zum Ausschluss des Auskunftsanspruchs (so BeckOK StPO/*Wittig*, § 475 Rn. 11 mwN). Jedoch ergibt sich aus der insofern eindeutigen Gesetzesbegründung (BT-Drs. 14/1484, S. 27) und dem von der Norm betroffenen Grundrechtskonflikt, der nicht einseitig zulasten der jeweiligen Herausgabeinteressen gelöst werden kann (vgl. BVerfG NJW 2007, 1052 [1052]), dass auch im Rahmen des § 475 Abs. 1, 4 StPO jedenfalls bei der Bestimmung der Schutzwürdigkeit des entgegenstehenden Interesses eine Abwägung mit dem Herausgabeinteresse vorzunehmen ist. Wie hier BVerfG, NJW 2007, 1052 (1052); VerfG Brandenburg, Beschluss v. 15.4.2010 – 37/09; VerfGH Berlin, Beschluss v. 10.2.2009 – 132/08, 132 A/08; VGH Mannheim, Urt. v. 11.9.2013 – 1 S 509/13; LG München I ZD 2015, 483 (484); *Gieg* in Karlsruher Kommentar zur StPO, 8. Aufl. (2019), § 475 Rn. 6. MüKoStPO/*Singelnstein*, § 475 Rn. 28 betont die Ähnlichkeit des Abwägungsmaßstabs zu dem im Rahmen der Landespressegesetze anzulegenden.

[49] S. dazu oben Fn. 48.

[50] BGH NJW 2018, 3123 (3123 f.) mit Anm. *Schork*; *Brink/Vogel* NJW 2015, 3710 (3710 f.).

[51] *Rostalski*, Der Tatbegriff im Strafrecht, 2019, S. 21 f.

[52] Vgl. *Rostalski,* Tatbegriff (Fn. 51), S. 20 ff.

[53] Vgl. *Rostalski,* Tatbegriff (Fn. 51), S. 26, 35 f. Der Täter verliert zu keinem Zeitpunkt seinen Status als Gleicher im Recht. Durch die Tat wird er nicht etwa zum „Feind" der Gesellschaft, weshalb ihm nach wie vor sämtliche Bürgerrechte zustehen (*Rostalski,* Tatbegriff [Fn. 51], S. 22 ff.). Er ist

rechtigtes und schützenswertes Interesse daran, nicht auf seine Eigenschaft als Person, die zu einem früheren Zeitpunkt eine Straftat begangen hat, reduziert zu werden. Zu seiner Resozialisierung gehört es daher, dass die Kenntnisvermittlung der vergangenen Straftatbegehung allein auf Fälle reduziert wird, in denen dies aus überwiegenden Interessen geboten ist (zum Beispiel: Einstellung als Erzieher in einer Kindertagesstätte allein unter Vorlage eines Führungszeugnisses). Im Übrigen muss es aber prinzipiell dem Einzelnen selbst überlassen sein, wem er diesen Teil seiner Vergangenheit offenbart und wem nicht.[54] In diesen Kontext fällt es auch, dass der Täter zu einem gewissen Maße ein schützenswertes Interesse am „Vergessen" hat.[55] Dem liefe es aber zuwider, wenn diejenigen, die bereits früher von der Tat Kenntnis erlangt haben, immer wieder hieran erinnert und dadurch von einer anderenfalls möglichen Neubewertung der Person des Täters abgehalten würden.

Indessen ist zu beachten, dass mit der Erstellung einer Strafurteilsdatenbank allenfalls geringfügige Risiken für das Persönlichkeitsrecht des Einzelnen in der vorgenannten Weise einhergehen. Grund hierfür ist in erster Linie die Anonymisierung der Urteile. Hierdurch ist der Schluss auf die Person des Täters prinzipiell versperrt. Zwar ist zutreffend, dass eine vollständige Anonymisierung etwa bei öffentlicher Medienberichterstattung nicht immer gelingt.[56] Allerdings trägt in solchen Konstellationen die Erfassung der strafgerichtlichen Entscheidung in einer Urteilsdatenbank nicht (weiter) zur Beeinträchtigung der Persönlichkeitsrechte des Angeklagten bei, als dies bereits die Medienberichterstattung selbst tut.[57] Dafür spricht nicht zuletzt die Präsentationsform von Entscheidungen innerhalb einer Datenbank. Diese ist mitnichten darauf gerichtet, Aufmerksamkeit für die Person des Angeklagten zu erzielen. Vielmehr dient die Erfassung dazu, Transparenz in Bezug etwa auf richterliche Strafzumessungserwägungen oder andere *rechtliche* Aspekte der Entscheidung zu schaffen. Dabei sind sämtliche Urteile in ihrem Rang gleichgestellt. Dem hierbei zugrunde liegenden rechtlichen Blickwinkel widerspricht es im Kern, die Aufmerksamkeit des Nutzers auf besonders öffentlichkeitswirksame Faktoren einzelner Entscheidungen zu lenken. Auch trägt die Einordnung der Entscheidungen in den größeren Rahmen der übrigen Rechtsprechung dazu bei, der einzelnen Entscheidung ihre Singularität zu nehmen, was wiederum den Blick von ihren Besonderheiten ablenkt.

Darüber hinaus ist der Nutzerkreis einer Strafurteilsdatenbank in die Abwägung einzubeziehen. Juristische Datenbanken richten sich in erster Linie an Rechtsanwender. Daneben werden sie zu wissenschaftlichen Zwecken genutzt. Die Nutzung ist regelmäßig von einer Gebühr abhängig, was insbesondere einer breiten Öffentlichkeit den Zugang allein dann ermöglicht, wenn sie beispielsweise zugleich bei einer deutschen Hochschule als Studierende eingeschrieben ist. Dieser Adressatenkreis sowie die konkrete Ausgestaltung der Nutzung reduzieren ihrerseits das Risiko einer unzulässigen

---

allerdings dafür verantwortlich, einen Ausgleich für das Mehr an Freiheit zu schaffen, das er sich durch die Tat in ungerechtfertigter Weise genommen hat (*Rostalski,* Tatbegriff [Fn. 51], S. 46 Fn. 105). Nach diesem Ausgleich besteht auch insoweit erneut Gleichheit zwischen ihm und den übrigen Gesellschaftsmitgliedern.

[54] Vgl. auch § 53 Abs. 1 Nr. 2 BZRG, dazu BAG NZA 2014, 1131 (1134 f.).

[55] Zum Recht auf Vergessen bezogen auf strafrechtliche Verurteilungen s. BVerfG NJW 2020, 300 (310 ff.); vgl. außerdem EuGH Urteil v. 13.5.2014 – Rs. C-131/12, ECLI:EU:C:2014:317 = NJW 2014, 2257 (2263 f.) – Google Spain SL u. Google Inc./Agencia Española de Protección de Datos [AEPD] u. Mario Costeja González; BVerfG NJW 2020, 314 (326 ff.).

[56] S. dazu oben unter I.

[57] Vgl. OLG Celle NJW 1990, 2570 (2571).

Persönlichkeitsbeeinträchtigung – insbesondere verglichen mit Medienartikeln, die frei im Internet publiziert werden.

Der Eingriff einer Strafurteilsdatenbank in die Rechte der Betroffenen erweist sich vor diesem Hintergrund als grundsätzlich gering. Dem steht allerdings ein relevantes Interesse an der Erstellung und insbesondere Nutzung eines solchen Instruments gegenüber. Am Beispiel der Strafzumessungsdatenbank: Die gegenwärtige Situation eines erheblichen Auseinanderfallens richterlicher Strafzumessungsentscheidungen ohne ersichtlichen Sachgrund, die sich insbesondere in regionalen Unterschieden ausdrückt,[58] stellt eine ernstzunehmende Gefahr für die gesellschaftliche Akzeptanz von Strafurteilen dar.[59] Ein erhöhtes Maß an Transparenz könnte hier eine Annäherung mit sich bringen. Das Strafrecht ist gerade aufgrund seiner engen Verwobenheit mit gesellschaftlichen Moralvorstellungen von essentieller Bedeutung für das Gemeinwesen. Die von einem Verlust von Akzeptanz durch den Eindruck von Strafungerechtigkeit ausgehende Gefahr darf daher nicht unterschätzt werden. Gemessen an den in dieser Konstellation eher geringfügigen Eingriffen in die Persönlichkeitsrechte Einzelner überwiegt daher das Interesse an der Erstellung einer solchen Datenbank. Ähnliche Überlegungen lassen sich auch zu anderen Verwendungszwecken anstellen.

Im Einzelfall könnte auch die Nichterfassung einer strafrechtlichen Entscheidung zu erwägen sein. Sofern beispielsweise durch ein Strafurteil besonders sensible Informationen über das Privatleben des Angeklagten offenbart werden, die weit über die bisherige Berichterstattung in diesem Fall hinausgehen, ließe sich begründen, von seiner Erfassung abzusehen. Weil es sich dabei um eine Singularität handelt, würde durch diesen punktuellen Eingriff die Aussagekraft und Leistungsstärke der Datenbank nicht grundlegend gemindert. Allerdings würde dies zu einer erheblichen Belastung des Datenbankbetreibers führen, der *sämtliche* erfassten Urteile auf derartige Besonderheiten untersuchen müsste. Praktikabler dürfte demgegenüber eine Möglichkeit sein, entsprechende Urteile aus der Datenbank auf Antrag zu entfernen. Angesichts der in den meisten Verfahren bestehenden uneingeschränkten Öffentlichkeit dürften derartige Fälle ohnehin so selten sein, dass sie die Abwägung insgesamt nicht wesentlich beeinflussen.

Als Zwischenergebnis kann damit festgehalten werden: Da das Interesse des anspruchstellenden Datenbankbetreibers das schutzwürdige Interesse des betroffenen Angeklagten überwiegt, erlaubt § 475 Abs. 1, 4 StPO eine Zweckabweichung durch Herausgabe der Urteilsabschriften. Die eigentliche Weitergabe und die anschließende Verarbeitung durch den Empfänger richten sich dann nach der DSGVO.[60]

III. Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO

Gemäß Art. 6 Abs. 1 DSGVO ist die Verarbeitung von personenbezogenen Daten nur bei Vorliegen einer der dort genannten Bedingungen zulässig. In Betracht kommt eine Rechtfertigung der Verarbeitungen im Rahmen der Verwaltung und Pflege von Datenbanken gemäß Art. 6 Abs. 1 UAbs. 1 lit. e oder lit. f DSGVO. Buchstabe e erklärt die Verarbeitung personenbezogener Daten für rechtmäßig, wenn die Verarbei-

[58] S. etwa *Grundies* in Hermann/Pöge, Kriminalsoziologie, 2018, S. 295 (301 ff.); *Meier*, Strafrechtliche Sanktionen, 4. Aufl. (2015), S. 257; vgl. auch *Streng* StV 2018, 593 (593 f.).

[59] Dazu näher schon *Rostalski/Völkening* KriPoZ 2019, 265 (266); s. außerdem *Kaspar/Höffler/Harrendorf* NK 32 (2020), 35 (36).

[60] S. dazu Art. 9 Abs. 1 S. 2 JI-RL und BeckOK DatenschutzR/*Bäcker*, Art. 2 DSGVO Rn. 30a f.

tung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Buchstabe f macht die Rechtmäßigkeit davon abhängig, dass die Rechte und Interessen des Betroffenen nicht gegenüber den berechtigten Interessen des für die Verarbeitung Verantwortlichen überwiegen.

Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO kann aufgrund der Öffnungsklauseln in den Absätzen 2 und 3 durch die Mitgliedstaaten konkretisiert werden.[61] Eine solche Konkretisierung findet sich landesrechtlich beispielsweise in § 17 Abs. 1 DSG NRW,[62] wonach Datenverarbeitungen bei wissenschaftlicher Zwecksetzung zulässig sind, soweit sie erforderlich und verhältnismäßig sind. Damit dürfte der Anwendungsbereich des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO allerdings nicht erweitert worden sein.[63] Trotz des missverständlichen Wortlauts gilt lit. e nur für Aufgaben, die dem Verantwortlichen durch eine Rechtsnorm *übertragen* worden sind.[64] § 17 Abs. 1 DSG NRW gilt gemäß § 5 Abs. 1 S. 1 DSG NRW nur für öffentliche Stellen (insbesondere für Hochschulen, soweit sie die ihnen nach § 3 HG NRW übertragenen Aufgaben wahrnehmen, § 5 Abs. 5 S. 2 DSG NRW). Praktische Auswirkungen hat diese Beschränkung des personalen Anwendungsbereichs aber nicht, da es sich bei wissenschaftlichen Forschungszwecken im Sinne des § 17 Abs. 1 DSG NRW zugleich um berechtigte Interessen im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO handelt und die übrigen Voraussetzungen (Erforderlichkeit und Interessenabwägung) deckungsgleich sind.[65] Wäre eine Datenverarbeitung daher nach § 17 Abs. 1 DSG NRW zulässig, so wird immer auch eine Zulässigkeit nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO vorliegen.[66] Wie bereits dargelegt, überwiegen in Bezug auf die Erstellung einer Strafurteilsdatenbank die Interessen hieran zumindest im Beispielsszenario die entgegenstehenden Persönlichkeitsrechte des Betroffenen.[67] Dies gilt sowohl für die wissenschaftliche als auch für die nichtwissenschaftliche Nutzung. Die Rechtmäßigkeit der Datenbankerstellung folgt für öffentliche Stellen, soweit sie wissenschaftliche Zwecke verfolgen, in NRW mithin aus Art. 6 Abs. 1 lit. e DSGVO iVm § 17 Abs. 1 DSG NRW, für die Verfolgung nichtwissenschaftlicher Zwecke oder für Private aus Art. 6 Abs. 1 lit. f DSGVO.

IV. Vereinbarkeit mit Art. 10 DSGVO

Die in Strafurteilen enthaltenen personenbezogenen Daten weisen allerdings eine besondere Grundrechtssensibilität auf, weshalb auch die DSGVO hierfür eine Sonderregelung bereithält. Es genügt mithin für die Rechtmäßigkeit der Datenbankerstellung nicht, lediglich auf Art. 6 DSGVO zu rekurrieren. Vielmehr müssen die weitergehenden Anforderungen von Art. 10 DSGVO gewahrt werden. Die Vorschrift sieht in Satz 1

[61] BeckOK DatenschutzR/*Albers/Veit*, Art. 6 DSGVO Rn. 55 ff.

[62] LT-NRW-Drs. 17/1981, S. 143.

[63] *Roßnagel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 6 Abs. 3 Rn. 19.

[64] *Roßnagel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 70, 76; *Assion/Nolte/Veil* in GSSV, DSGVO, 2018, Art. 6 Rn. 106, 111.

[65] Vgl. zum insofern wortgleichen § 27 BDSG BeckOK DatenschutzR/*Schlösser-Rost*, § 27 BDSG Rn. 6. Diese Norm bezieht sich aber ausschließlich auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO und trifft zu Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO keine Aussage.

[66] Überflüssig ist die Norm gleichwohl nicht, da Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO nicht für die Datenverarbeitung durch Behörden gilt (Art. 6 Abs. 1 UAbs. 2 DSGVO, dazu *Schantz* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 96 f.).

[67] S. dazu oben unter II.3.

vor, dass die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten aufgrund von Art. 6 Abs. 1 DSGVO nur unter behördlicher Aufsicht vorgenommen werden darf bzw. dann, wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorsieht, zulässig ist.[68] In Satz 2 der Regelung heißt es ferner: „Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden." Die Vorschrift gilt nur für Daten, die sich auf den Angeklagten, nicht aber für solche, die sich auf sonstige Verfahrensbeteiligte beziehen.[69]

Strafurteilsdatenbanken sammeln in der Regel nur besonders relevante Entscheidungen und sind daher kein (bereichsspezifisch) „umfassendes Register" iSd Art. 10 S. 2 DSGVO.[70] Das gilt aber selbst dann, wenn tatsächlich *alle* Entscheidungen deutscher Strafgerichte gesammelt werden, beispielsweise um die darin zum Ausdruck kommende Entscheidungspraxis wissenschaftlich auszuwerten. Infolge der Anonymisierung zumindest der meisten[71] Urteile bezieht sich eine solche Sammlung nicht durchweg auf die Verurteilungen bestimmter oder bestimmbarer natürlicher Personen. Sie dient daher nicht der Zusammenführung aller Verurteilungen einer bestimmten Person, sondern der insofern personenunabhängigen Auskunft über die Rechtspraxis.[72]

Damit muss sich eine Strafurteilsdatenbank (nur) an der Regelung des Art. 10 S. 1 DSGVO messen lassen. Danach besteht die Möglichkeit, von behördlicher Aufsicht bei der Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen abzusehen, wenn dies nach mitgliedstaatlichem Recht zulässig ist und dieses Recht zugleich eine geeignete Garantie für die Wahrung der Rechte des Betroffenen bereithält. Eine explizite Regelung für wissenschaftliche oder statistische Zwecke findet sich in § 27 BDSG (bzw. § 17 DSG NRW[73]), der sich allerdings auf die Öffnungsklausel des Art. 9 Abs. 2 lit. j DSGVO bezieht[74] und damit gerade *keine* Ausnahme von Art. 10 S. 1 DSGVO vorsieht.

Für die Verarbeitung von Daten über strafrechtliche Verurteilungen ist daher eine andere gesetzliche Ausnahmeregelung erforderlich. Infrage kommen § 475 Abs. 1, 4

---

[68] Die vereinzelt befürwortete teleologische Reduktion des Art. 10 S. 1 DSGVO auf „systematische" Verarbeitungen (*Schwarz* ZD 2018, 353 [356] im Anschluss an *Wybitul/Böhm* CB, Online Update 14.4.2016 [abrufbar unter: http://hoganlovells-blog.de/wp-content/uploads/2016/07/Wybitul_B%C3%B6hm_amended_as_of_14_4_2016.pdf, zuletzt geprüft am 11.11.2020], 1 [7 f.]) ist mit der eindeutigen Systematik nicht vereinbar. Die systematische Registrierung von Straftaten wird (verschärft) von Art. 10 S. 2 DSGVO normiert (was *Schwarz* aaO durchaus anerkennt), weshalb S. 1 in dieser Auslegung praktisch keinen Anwendungsbereich mehr hätte. Entsprechend hat auch der EuGH aufgrund des Wortlautes und des Telos der Vorschrift (der Schutz besonders sensibler Daten) entschieden, dass Art. 10 S. 1 DSGVO jede Form der Datenverarbeitung erfasst, also nicht nur die systematische (EuGH Urteil v. 24.8.2019 – Rs. C-136/17, ECLI:EU:C:2019:773 = EuZW 2019, 906 [908] – ED vs. Commission nationale de l'informatique et des libertés [CNIL]). Konflikten mit gegenläufigen Interessen kann im Rahmen der Öffnungsklauseln in Art. 10 S. 1 Alt. 2, 85 Abs. 2 DSGVO Rechnung getragen werden. Wie hier BeckOK DatenschutzR/*Bäcker*, Art. 10 DSGVO Rn. 3a.

[69] *Gierschmann* in GSSV, DSGVO, Art. 10 Rn. 22; BeckOK DatenschutzR/*Bäcker*, Art. 10 DSGVO Rn. 2; bzgl. Zeugen auch *Petri* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 10 Rn. 11.

[70] Vgl. *Eckhardt* in Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. (2019), Art. 10 DSGVO Rn. 11.

[71] S. oben unter II. 3.

[72] Vgl. *Kampert* in HK-EuDSchVO, Art. 10 Rn. 7; BeckOK DatenschutzR/*Bäcker*, Art. 10 DSGVO Rn. 13.

[73] Zu dieser Norm bereits oben unter III.

[74] BT-Drs. 18/11325, S. 99 (bzw. LT-NRW-Drs. 17/1981 S. 143); bzgl. § 27 BDSG BeckOK DatenschutzR/ *Schlösser-Rost*, § 27 BDSG Rn. 4.

StPO und das sogenannte Medienprivileg (zB aus § 12 S. 4 LPresseG NRW bzw.§§ 9c Abs. 1 S. 4, 57 Abs. 1 S. 4 RStV, ggf. iVm § 51a Abs. 1 LMG NRW). Letzteres beruht auf der Öffnungsklausel in Art. 85 Abs. 2 DSGVO und enthält eine auf journalistische (und literarische) Zwecke beschränkte pauschale Freistellung von weiten Teilen der DSGVO.[75] Die Wahrung der Anforderungen von Art. 10 S. 1 DSGVO hängt daher maßgeblich von der konkreten Ausgestaltung einer Strafurteilsdatenbank ab. Im Folgenden wird zwischen wissenschaftlichen Forschungsprojekten und der Erstellung und Nutzung einer Datenbank in der Rechtspraxis unterschieden.

1. Vereinbarkeit einer Strafurteilsdatenbank mit Art. 10 S. 1 DSGVO bei wissenschaftlicher Ausrichtung

Denkbar ist, neben der Herausgabe auch die anschließende Verarbeitung der Strafurteile auf § 475 Abs. 1, 4 StPO zu stützen. Dann müsste sich der Norm eine entsprechende Erlaubnis entnehmen lassen. Eine nationalstaatliche Vorschrift kann eine solche Ausnahme wegen des Anwendungsvorrangs der DSGVO jedoch nur zulassen, wenn sie sich auf eine Öffnungsklausel in der Verordnung stützen kann.[76] In Betracht kommen Art. 10 S. 1 Alt. 2, 85 Abs. 2 und 86 DSGVO.

a) § 475 Abs. 1, 4 StPO als Erlaubnisnorm

§ 475 StPO ermöglicht seinem Wortlaut nach lediglich die Gewährleistung von Auskünften und Akteneinsicht – von deren Verwendung ist darin keine Rede. Insbesondere enthält die Norm (anders als etwa § 12 S. 4 LPresseG NRW, §§ 9c Abs. 1 S. 4, 57 Abs. 1 S. 4 RStV oder § 27 Abs. 1 BDSG) keine explizite Freistellung von Regelungen der DSGVO. Nun lässt sich einwenden, dass der Erhalt wenig Sinn ergäbe, wenn die Auskünfte anschließend wegen Art. 10 S. 1 DSGVO nicht verwendet werden dürften. Das gilt zwar nur im Rahmen des Anwendungsbereichs der DSGVO, möglich blieben damit aber nur Verwendungen zu ausschließlich persönlichen Zwecken (Art. 2 Abs. 2 lit. c DSGVO) oder in gänzlich unstrukturierter Weise (Art. 2 Abs. 1 DSGVO)[77]. Die meisten relevanten Anwendungsfälle wären demnach ausgeschlossen. Für eine implizite Erlaubnis der Verwendung der von den Gerichten und Staatsanwaltschaften übermittelten Daten spricht auch § 479 Abs. 6 iVm § 32f Abs. 5 S. 2, 3 StPO, demzufolge die aufgrund von § 475 Abs. 1, 4 StPO erlangten Auskünfte grundsätzlich nur, damit aber eben *auch*, für den Zweck verwendet werden dürfen, zu dem sie erteilt worden sind.

Problematisch ist diese Argumentation, wenn es nicht mehr nur um die Verwendung einzelner Entscheidungen geht, sondern um den Aufbau größerer Datenbanken. Diese lassen Aussagen über Straftaten zu, die weit über die Erkenntnisse hinausgehen, die

[75] *Buchner/Tinnefeld* in Kühling/Buchner, 3. Aufl. (2020), Art. 85 Rn. 31 f. Angesichts der durch Art. 85 Abs. 1, 2 DSGVO aufgegebenen Pflicht, die konfligierenden Interessen „in Einklang" zu bringen, ist das kritikwürdig, dazu *Buchner/Tinnefeld* in Kühling/Buchner, Art. 85 Rn. 2, 27, 32; dagegen aber *Cornils* ZUM 2018, 561 (574 ff.). BeckOK DatenschutzR/*Stender-Vorwachs*, Art. 85 DSGVO Rn. 33 ff. hält die Regelung offenbar nunmehr für ausreichend (vgl. die 31. Ed. mit Stand vom 1.2.2020). Das OLG Köln ZD 2018, 434 (435) hat sich kürzlich damit begnügt, die erforderliche Abwägung im Rahmen der Spezialgesetze (insb. des KUG) vorzunehmen. Unklar bleibt, was außerhalb des Anwendungsbereichs solcher Spezialgesetze gilt.

[76] Vgl. *Sydow* in HK-EuDSchVO, Einl. Rn. 36.

[77] Vgl. BeckOK DatenschutzR/*Bäcker*, Art. 2 DSGVO Rn. 4.

aus einer einzelnen Verurteilung abgeleitet werden können. Durch die systematische Analyse, die durch die Erfassung in der Datenbank möglich wird, kann ein eingriffsintensiverer Rückschluss auf Einzelfälle gezogen werden. Angesichts dieser besonderen Grundrechtssensibilität fragt sich, warum der Gesetzgeber keine explizite Regelung derartiger Verarbeitungszwecke in § 475 Abs. 1, 4 StPO aufgenommen hat. Allerdings ist für rechtswissenschaftliche Datenbanken in der Regel die Verwendung anonymisierter Daten ausreichend. Wenngleich diese Anonymisierung nicht vollständig erfolgen kann, wird die Eingriffsintensität dadurch auf ein vertretbares Maß reduziert. Soweit ein Personenbezug (indirekt) hergestellt werden kann, relativiert die Einordnung in den größeren Kontext der Rechtsprechung seine Bedeutung.[78] Insofern wird die besondere Grundrechtssensibilität von Datenbanken durch das Zusammenführen zahlreicher (teil-)anonymisierter Entscheidungen zugleich begründet und gemildert. Hinzu kommt, dass dem Gesetzgeber das Konzept von Online-Datenbanken für Gerichtsentscheidungen bei der Schaffung der Vorschrift im Jahr 2000[79] bereits bekannt gewesen sein wird.[80] Dass er hierfür keine spezialgesetzliche Regelung schuf und eine solche gleichzeitig für erforderlich hielt, ist fernliegend. Aus dem Fehlen einer expliziten Regelung der hier infragestehenden Verarbeitungszwecke kann deshalb nicht auf deren Unzulässigkeit geschlossen werden.

Seinem Sinn und Zweck nach kann § 475 Abs. 1, 4 StPO also entnommen werden, dass nicht nur die Herausgabe der Urteilsabschriften durch die Gerichte und Staatsanwaltschaften, sondern auch deren Verarbeitung durch den Empfänger unter den dort genannten Voraussetzungen zulässig ist. Insofern ist der Norm eine Ausnahme vom Erfordernis behördlicher Aufsicht aus Art. 10 S. 1 DSGVO zu entnehmen.

b) Vereinbarkeit mit der Öffnungsklausel aus Art. 10 S. 1 DSGVO

Allerdings bestehen Zweifel daran, dass § 475 Abs. 1, 4 iVm §§ 479 Abs. 6, 32f Abs. 5 S. 2, 3 StPO „geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen" im Sinne der Öffnungsklausel aus Art. 10 S. 1 DSGVO vorsieht. Dagegen spricht insbesondere der Zweckbindungsgrundsatz des Art. 6 Abs. 4 iVm Art. 5 Abs. 1 lit. b DSGVO, der durch die strafprozessualen Vorschriften noch übertroffen werden müsste.[81] § 479 Abs. 6 iVm § 32f Abs. 5 S. 2, 3 StPO statuiert zwar eine Zweckbindung, sieht aber mit dem hypothetischen Ersatzeingriff eine Ausnahme vor, deren Übertragbarkeit auf den Zweckbindungsgrundsatz der DSGVO problematisch erscheint.[82] Jedenfalls geht der Zweckbindungsgrundsatz an dieser Stelle also nicht über denjenigen der DSGVO hinaus.

Zur geeigneten Garantie der Rechte des Betroffenen wäre es außerdem erforderlich, eine Abstufung des Schutzes nach der Bedeutung der Straftat und gemessen am seitdem vergangenen Zeitraum vorzunehmen.[83] Zwar enthält § 479 Abs. 4 Nr. 2 StPO eine Son-

---

[78] Dazu bereits oben unter II. 3.

[79] Art. 1 Nr. 15 des Gesetzes v. 2.8.2000, BGBl. I S. 1253.

[80] Juris etwa ist seit 1996 über das Internet aufrufbar, s. 30 Jahre Juris – Das Rechtsportal, Jubiläumszeitung (abrufbar unter https://www.juris.de/jportal/cms/remote_media/media/jurisde/pdf/information/2015_juris_jubilaeumszeitung.pdf, zuletzt geprüft am 11.11.2020), S. 3.

[81] BeckOK DatenschutzR/*Bäcker*, Art. 10 DSGVO Rn. 12; vgl. auch *Frenzel* in Paal/Pauly, Art. 10 DSGVO Rn. 8.

[82] Vgl. *Reimer* in HK-EuDSchVO, Art. 5 Rn. 26 mit Fn. 46.

[83] *Frenzel* in Paal/Pauly, Art. 10 DSGVO Rn. 8; vgl. auch *Weichert* in Kühling/Buchner, Art. 10 Rn. 12 f.

derregelung für länger zurückliegende Verurteilungen, die nicht in ein Führungszeugnis für Behörden aufgenommen werden (§ 32 Abs. 2 BZRG). Die Verschärfung besteht aber lediglich darin, dass das berechtigte Interesse an der Auskunft ein rechtliches sein und es nicht mehr nur dargelegt, sondern auch glaubhaft gemacht werden muss.[84] Es handelt sich also insbesondere um eine Beschränkung nur der Auskunfts*erteilung*, nicht der späteren *Verarbeitung*, auf die sich aber Art. 10 S. 1 DSGVO bezieht. Für andere Verurteilungen finden sich überhaupt keine schweregrad- oder zeitabhängigen Beschränkungen. So kann kaum sichergestellt werden, dass dem Verhältnismäßigkeitsgrundsatz als Teil der „geeigneten Garantien" im Sinne des Art. 10 S. 1 Alt. 2 DSGVO[85] genügt wird.[86] Die Garantien, die § 475 Abs. 1 iVm § 479 StPO vorsieht, genügen daher nicht den Anforderungen des Art. 10 S. 1 Alt. 2 DSGVO.[87]

c) Vereinbarkeit mit der Öffnungsklausel aus Art. 86 DSGVO

Art. 86 DSGVO ermöglicht dem nationalen Gesetzgeber, die Offenlegung von personenbezogenen Daten in amtlichen Dokumenten sowie solchen, die sich im Besitz einer Behörde oder einer öffentlichen Einrichtung befinden, durch die Behörde oder Einrichtung zu normieren, um auf diese Weise das Interesse am Zugang zu solchen Dokumenten und das Recht auf Schutz personenbezogener Daten gemäß der DSGVO in Einklang zu bringen. § 475 Abs. 1, 4 StPO lässt sich in seinem originären Anwendungsbereich als Ermächtigungsgrundlage zur Herausgabe von Urteilsabschriften auf diese Klausel stützen.[88] Allerdings bezieht sich die Öffnungsklausel ihrem Wortlaut nach allein auf die Offenlegung, nicht auf die Verwendung der Daten.[89] Selbst wenn Art. 86 DSGVO gleichwohl auch auf die spätere Verarbeitung durch den Informationsempfänger erstreckt würde, wäre immer noch fraglich, ob die Norm gerade auch zu Ausnahmen von Art. 10 S. 1 DSGVO ermächtigt. Dagegen spricht, dass sie, anders als Art. 85 Abs. 2 DSGVO,[90] nicht explizit Ausnahmen von Kapitel II der DSGVO zu-

[84] BeckOK StPO/*Wittig*, § 475 Rn. 17.

[85] BeckOK DatenschutzR/*Bäcker* Art. 10 DSGVO Rn. 12.

[86] Die Bedeutung der Straftat und der zeitliche Abstand können zwar im Rahmen der Interessenabwägung bei der Entscheidung über das Auskunfts*ersuchen* (§ 475 Abs. 1 S. 2 StPO) berücksichtigt werden. Auch auf diese Weise wird jedoch nicht die spätere *Verarbeitung* durch den Anspruchsteller beschränkt. Nur diese ist Bezugspunkt des Verhältnismäßigkeitsgrundsatzes iSd Art. 10 S. 1 DSGVO.

[87] Ein Beispiel für eine detaillierte Regelung von Garantien, wenngleich im Rahmen des Art. 9 Abs. 1 DSGVO und für den Beschäftigtendatenschutz, bietet § 26 Abs. 3 s. 3 iVm § 22 Abs. 2 BDSG.

[88] AA offenbar *Schnabel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 86 DSGVO Rn. 26. Anders als dort behauptet, ist § 475 Abs. 1, 4 StPO jedoch nicht auf Prozessbeteiligte beschränkt. Die Notwendigkeit der Darlegung eines berechtigten Interesses durch den Anspruchsteller trägt nur der Verhältnismäßigkeit des Eingriffs in das Recht auf informationelle Selbstbestimmung Rechnung (MüKoStPO/*Singelnstein*, § 475 Rn. 14) und schränkt den Auskunftsanspruch daher nicht stärker ein als im Rahmen des Art. 86 DSGVO stets erforderlich (vgl. *Schnabel* in Simitis/Hornung/Spiecker genannt Döhmann, Art. 86 Rn. 36; BeckOK DatenschutzR/*Schiedermair*, Art. 86 Rn. 5).

[89] Das gilt zwar auch für § 475 Abs. 1, 4 StPO. Das teleologische Argument, dass dort die extensive Auslegung rechtfertigt, greift bei Art. 86 DSGVO aber nicht, weil sich die Norm nicht nur auf besonders sensible Daten im Sinne des Art. 10 DSGVO bezieht, die ohne gesetzliche Ausnahme durch Private praktisch nicht verarbeitet werden dürfen. Die Erstreckung der Öffnungsklausel auf die Verarbeitung ist also nicht notwendig, um ihre Sinnhaftigkeit zu erhalten. Auch fehlt eine § 479 Abs. 6 iVm § 32f Abs. 5 S. 2, 3 StPO vergleichbare Bezugnahme auf die spätere Verwendung, die eine extensive Auslegung stützen würde.

[90] Hierzu sogleich unter d).

lässt.[91] Auch verweist der Wortlaut auf das „Recht auf Schutz personenbezogener Daten *gemäß dieser Verordnung*". Daraus wird verbreitet sogar die Konsequenz gezogen, dass eine inhaltliche Abweichung von den Garantien der DSGVO *insgesamt* nicht zulässig ist.[92] Ließe Art. 86 DSGVO Ausnahmen von Art. 10 S. 1 DSGVO auch für die Verarbeitung der erhaltenen Daten durch den Empfänger zu, so könnten die Mitgliedstaaten die Verarbeitung sensibler Daten über Straftaten, welche oft auf einer Auskunft durch die Gerichte oder Strafverfolgungsbehörden basieren wird, weitgehend frei regeln. Die sachlichen (Erfordernis „geeignete[r] Garantien für die Rechte und Freiheiten der betroffenen Personen") oder funktionellen Beschränkungen (auf journalistische, wissenschaftliche, künstlerische oder literarische Zwecke) der Öffnungsklauseln in Art. 10 S. 1 und Art. 85 Abs. 2 DSGVO würden so weitgehend unterlaufen. Eine extensive, auch die nachfolgende Verarbeitung umfassende Auslegung des § 475 Abs. 1, 4 StPO fällt daher nicht mehr unter Art. 86 DSGVO.

d) Vereinbarkeit mit der Öffnungsklausel aus Art. 85 Abs. 2 DSGVO

Was bleibt, ist die Öffnungsklausel in Art. 85 Abs. 2 DSGVO. Diese erlaubt explizit Ausnahmen vom II. Kapitel der DSGVO und damit auch von deren Art. 10.[93] Der Anwendungsbereich ist aber auf wissenschaftliche, journalistische, künstlerische und literarische Zwecke beschränkt. Da § 475 Abs. 1, 4 StPO keine derartige Beschränkung enthält, kann eine extensive Auslegung in dieser Allgemeinheit nicht auf Art. 85 Abs. 2 DSGVO gestützt werden. Denkbar wäre hingegen eine Kombination der oben beschriebenen extensiven mit einer unionsrechtskonformen Auslegung:[94] Bei wissenschaftlicher[95] und künstlerischer Zwecksetzung des Anspruchstellers könnte § 475 Abs. 1, 4 StPO extensiv als Erlaubnisnorm für die Verarbeitung der erhaltenen Daten und damit als Ausnahme zu Art. 10 S. 1 DSGVO interpretiert werden.[96] Da eine derartige Interpretation bei anderen, nicht privilegierten Zwecksetzungen nicht mit der DSGVO vereinbar wäre,[97] müsste die extensive Auslegung unionsrechtskonform auf diese Zwecke beschränkt werden. Bei Verfolgung anderer Zwecke könnte § 475 Abs. 1, 4 StPO daher nicht als Ausnahme zu Art. 10 S. 1 DSGVO interpretiert werden, die Verarbeitung der Daten wäre rechtswidrig.

Etwas anderes gilt für journalistische (und literarische) Zwecke. Hierfür kann gemäß Art. 85 Abs. 2 DSGVO zwar ebenfalls eine Ausnahme vorgesehen werden. Von dieser Möglichkeit hat der Gesetzgeber aber mit der Schaffung des Medienprivilegs Gebrauch gemacht (z.B. § 12 S. 4 LPresseG NRW bzw. §§ 9c Abs. 1 S. 4, 57 Abs. 1 S. 4 RStV,

---

[91] Vgl. *Schnabel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 86 DSGVO Rn. 30.

[92] *Specht/Bienemann* in HK-EuDSchVO Art. 86 Rn. 13; *Pauly* in Paal/Pauly Art. 86 DSGVO Rn. 9. *Schnabel* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 86 Rn. 31 plädiert dagegen für einen „Mittelweg".

[93] *Kampert* in HK-EuDSchVO, Art. 10 Rn. 6.

[94] Allgemein zur unionsrechtskonformen Auslegung *Schroeder*, Grundkurs Europarecht, 6. Aufl. (2019), § 16 Rn. 21. Vgl. etwa EuGH Urteil v. 27.6.2000 – verb. Rs. C-240/98 bis C-244/98, ECLI:EU:C:2000:346 = NJW 2000, 2571 (2572 f.) – Océano Grupo Editorial SA vs. Rocío Murciano Quintero u.a.

[95] S. oben unter II. 3. zur Anwendbarkeit des § 475 Abs. 1, 4 StPO auch bei wissenschaftlicher Zwecksetzung.

[96] Zu berücksichtigen wären insofern zusätzlich die Vorgaben des Art. 89 Abs. 1 DSGVO, vgl. *Buchner/Tinnefeld* in Kühling/Buchner, Art. 85 Rn. 30a.

[97] S. die vorstehenden Abschnitte.

ggf. iVm § 51a Abs. 1 LMG NRW). Dieses umfasst auch eine Befreiung von Art. 10 DSGVO,[98] weshalb eine extensive Auslegung des § 475 Abs. 1, 4 StPO als Erlaubnisnorm insofern nicht notwendig ist.[99]

Im Ergebnis wird so die Zulässigkeit der Verarbeitung von Daten über strafrechtliche Verurteilungen bei wissenschaftlicher und künstlerischer Zwecksetzung gemäß § 475 Abs. 1, 4 StPO und bei literarischer und journalistischer Zwecksetzung aufgrund des Medienprivilegs erreicht. Im Übrigen bleibt die Verarbeitung im Anwendungsbereich der DSGVO rechtswidrig. Soweit eine Urteilsdatenbank wissenschaftlichen Zwecken dient,[100] kann ihre Erstellung also auf § 475 Abs. 1, 4 DSGVO gestützt werden, der eine Ausnahme zu Art. 10 S. 1 DSGVO enthält.

2. Vereinbarkeit einer Strafurteilsdatenbank mit Art. 10 DSGVO bei nicht-wissenschaftlicher Ausrichtung

Ob eine Urteilsdatenbank auch bei nicht-wissenschaftlicher Zwecksetzung (etwa bei beabsichtigter Nutzung durch Rechtsanwender) mit Art. 10 S. 1 DSGVO vereinbar ist, hängt folglich davon ab, ob sie unter den Journalismusbegriff fällt und ihre Erstellung damit einen journalistischen Zweck im Sinne des Art. 85 Abs. 2 DSGVO darstellt. Dann kann sie auf das Medienprivileg gestützt werden, in Nordrhein-Westfalen beispielsweise auf die Vorschriften des § 12 S. 4 LPresseG NRW bzw. der §§ 9c Abs. 1 S. 4, 57 Abs. 1 S. 4 RStV, ggf. iVm § 51a Abs. 1 LMG NRW.

Entsprechend der gebotenen funktionalen Betrachtungsweise[101] ist unter Journalismus jede Tätigkeit mit dem Ziel der Verbreitung von Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verstehen.[102] Dabei kann auch eine Datenbank als Presseorgan gelten, wenn sie Aufgaben vergleichbar einer Fachzeitschrift erfüllt.[103] Jedoch muss die redaktionelle Bearbeitung mehr als nur „schmückendes Beiwerk" sein.[104] Die bloße Wiedergabe von Datensammlungen oder amtlichen Mitteilungen soll hierfür nicht genügen.[105] Entscheidend ist, ob ein Beitrag zur individuellen oder öffentlichen Meinungsbildung geleistet wird.[106] Laut Bundesverwaltungsgericht soll das nicht der Fall sein, wenn ungefiltert und möglichst flächendeckend öffentliche Vergabeentscheidungen gesammelt und, mit Schlagworten versehen und kategorisiert, publiziert werden, da hieraus noch keine Rückschlüsse für überindividuell relevante Sachverhalte möglich seien.[107] Anders sei ein Medium zu bewerten, das die öffentliche Vergabe*pra-*

[98] Vgl. *Weichert* in Kühling/Buchner Art. 10 Rn. 9 zu § 57 Abs. 1 RStV und § 41 BDSG a.F.

[99] *Buchner/Tinnefeld* in Kühling/Buchner, 2017, Art. 85 Rn. 33 forderten dementsprechend eine Ergänzung des Medienprivilegs um wissenschaftliche und künstlerische Zwecke. In der aktuellen Auflage wurde diese Forderung gestrichen, ohne dass sich an der Situation (zumindest bezogen auf Strafdaten) etwas geändert hätte (vgl. auch *Frohnecke* ZD 2020, 273 [274]).

[100] Dazu bereits oben unter II. 2.

[101] *Schulz/Heilmann* in GSSV, DSGVO, Art. 85 Rn. 37.

[102] *Specht/Bienemann* in HK-EuDSchVO, Art. 85 Rn. 13.

[103] LG München I, Beschluss v. 19.1.2016 – 6 AR 5/15.

[104] BGH MMR 2009, 608 (610); *Krüger/Wiencke* MMR 2019, 76 (77); ähnlich *Specht/Bienemann* in HK-EuDSchVO, Art. 85 Rn. 13; *Buchner/Tinnefeld* in Kühling/Buchner, Art. 85 Rn. 25.

[105] *Buchner/Tinnefeld* in Kühling/Buchner Art. 85 Rn. 24. In EuGH Urteil v. 16. 12. 2008 – Rs. C-73/07, ECLI:EU:C:2008:727 = EuZW 2009, 108 (110 f.) – Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy u.a., hat der EuGH dagegen den im Wesentlichen unkommentierten Abdruck von nach nationalem Recht öffentlichen Steuerdaten als Journalismus eingestuft.

[106] BVerwG NVwZ 2019, 1283 (1287).

[107] BVerwG NVwZ 2019, 1283 (1287 f.). Insofern zweifelnd, wenngleich iErg zustimmend, *Michel* NVwZ 2019, 1656 (1658).

xis wiederspiegelt und eine Beurteilung von Regelmäßigkeiten und Auffälligkeiten ermöglicht, da die interessierte Öffentlichkeit hierdurch zu einem eigenen Standpunkt finden könne.[108]

Eine Strafurteilsdatenbank kann auf dieser Basis als Journalismus eingestuft werden. Soweit unter den infrage kommenden Urteilen eine inhaltliche Auswahl aufgrund der (angenommenen) Relevanz getroffen wird, dürfte schon hierin eine hinreichende redaktionelle Aufbereitung zu sehen sein.[109] Erfolgt dagegen nur eine ungefilterte Sammlung und Publikation von Urteilen, wie sie etwa für die Information über Strafzumessungsentscheidungen erforderlich wäre, so ist die Beurteilung schwieriger. Die Sammlung ist dort jedoch Teil der systematischen (auch: statistischen) Auswertung,[110] die neben der Information über Entscheidungen in konkreten Einzelfällen die Beurteilung der Strafzumessungspraxis im Ganzen ermöglicht. Hierdurch können zum Beispiel regionale Unterschiede aufgespürt werden. Die Ergebnisse können letztlich Grundlage einer Debatte über die Gewichtung der für die Strafzumessung relevanten Aspekte sein. Diese Aufbereitung ist als Alleinstellungsmerkmal einer solchen Datenbank mehr als nur „schmückendes Beiwerk". Der Betrieb der Datenbank unterfällt daher ebenso wie die Sammlung und Auswertung der Urteile dem Journalismus.[111]

---

[108] BVerwG NVwZ 2019, 1283 (1288).

[109] Zu den Anforderungen an die redaktionelle Gestaltung s. *Lent* ZUM 2013, 914 (916); BeckOK InfoMedienR/*Martini*,§ 1 TMG Rn. 25. Wieso die Gestaltung nur durch natürliche Personen erfolgen können soll, wie *Lent* ZUM 2013, 914 (916) meint, erschließt sich allerdings nicht. Richtig ist zwar, dass bloße „Auflistungen" und „Zusammenstellungen" für sich genommen noch keinen nennenswerten Beitrag zur öffentlichen Meinungsbildung leisten. Angesichts der komplexen Zusammenhänge, die künstliche Intelligenz heute herstellen kann, ist das aber nicht auf das automatisierte Zustandekommen selbst zurückzuführen, sondern schlicht auf die zu geringe Komplexität. Die Beschränkung auf natürliche Personen würde bedeuten, dass es für die Qualifikation als Journalismus entscheidend sein kann, ob ein Mensch dieselben Zusammenhänge händisch oder unter Zuhilfenahme eines Computers herstellt. Entscheidend muss der Beitrag zur Meinungsbildung sein, nicht der Modus des Zustandekommens.

[110] Vgl. *Rostalski/Völkening* KriPoZ 2019, 265 (270).

[111] Der Journalismusbegriff erstreckt sich auf Vorarbeiten, s. *Buchner/Tinnefeld* in Kühling/Buchner, Art. 85 Rn. 17. Gleiches gilt allerdings auch für den Begriff der wissenschaftlichen Forschung, s. Fn. 33. Da letzterer auch die Publikation der Forschungsergebnisse umfasst (BeckOK InfoMedienR/*Cornils*, Art. 85 Rn. 82 f; *Jarass* GRCh, Art. 13 Rn. 7), ist eine trennscharfe Abgrenzung zwischen Wissenschaft und (Fach-)Journalismus in allen Phasen der Tätigkeit schwierig (jedenfalls, soweit Ausarbeitung und Publikation durch denselben Verantwortlichen erfolgen). Vgl. auch *Schulz/Heilmann* in GSSV, DSGVO, Art. 85 Rn. 49, 54 zu Überschneidungen zwischen wissenschaftlichen und literarischen Zwecken. Die Differenzierung im nationalen Recht (sehr weitreichende Ausnahme von datenschutzrechtlichen Pflichten für den Journalismus auf der einen, sehr begrenzte Ausnahmen insbesondere nach § 27 BDSG für die Wissenschaft auf der anderen Seite) ist vor diesem Hintergrund zu pauschal. Vor allem ist eine ausdrückliche gesetzliche Ausnahme zu Art. 10 S. 1 DSGVO für den Bereich der (Strafrechts-)Wissenschaft erforderlich, da nach dem derzeit geltenden Gesetzeswortlaut eine wissenschaftliche Befassung mit Strafurteilen jenseits journalistischer Tätigkeit nur über die beschriebene erweiterte Auslegung des § 475 Abs. 1, 4 StPO möglich ist. Soweit der Befassung keine Aktenauskunft bei einem Gericht oder einer Strafverfolgungsbehörde vorausgeht, fällt auch diese Konstruktion weg. Bis zur – notwendigen – gesetzlichen Regelung des Konflikts muss auf eine Abwägung der betroffenen Grundrechte zurückgegriffen werden (vgl. *Dix* in Simitis/Hornung/Spiecker genannt Döhmann, Datenschutzrecht, Art. 85 Rn. 32). Dabei sind neben dem verfassungsrechtlichen Recht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG) und der Wissenschaftsfreiheit aus Art. 5 Abs. 3 S. 1 GG auch die unionsrechtlichen Entsprechungen (Art. 8 Abs. 1 und Art. 13 GRCh) zu berücksichtigen (dazu *Albrecht/Janson* CR 2016, 500, [502 ff.]). Deshalb steht der Anwendungsvorrang der DSGVO einer solchen Abwägung, anders als *Frohnecke* ZD 2020, 273 (274) meint, nicht entgegen.

Insofern können sich Urteilsdatenbanken auf das Medienprivileg gemäß § 12 S. 4 LPresseG NRW oder § 57 Abs. 1 S. 4 RStV (ggf. iVm § 51a Abs. 1 LMG NRW)[112] stützen, das eine Ausnahme zu Art. 10 S. 1 DSGVO auch bei nicht ausschließlich wissenschaftlicher Zwecksetzung vorsieht.[113]

V. Schluss

Bei der Frage nach der Vereinbarkeit einer Strafurteilsdatenbank mit dem geltenden Datenschutzrecht ist danach zu differenzieren, ob ihre Erstellung wissenschaftlichen Zwecken dient. Ist das der Fall, steht sie grundsätzlich in Einklang mit den europäischen und nationalen Vorschriften zum Datenschutz. Dies betrifft sowohl die Durchführung des Projekts als auch die Publikation der dabei erzielten Ergebnisse. Andernfalls hängt die Zulässigkeit von der konkreten Ausgestaltung ab. Nur bei hinreichender journalistisch-redaktioneller Gestaltung gewährt das Medienprivileg die erforderliche Ausnahme zu Art. 10 S. 1 DSGVO. Das geltende Recht sieht insofern teils schwer nachvollziehbare Differenzierungen von erheblicher Tragweite vor. Vor diesem Hintergrund wäre eine ausdrückliche Regelung der datenschutzrechtlichen Grundlage einer Befassung mit strafrechtlichen Verurteilungen durch die Strafrechtswissenschaft und die Strafrechtspflege wünschenswert.

Big data has arrived in the field of German penalty law. A recent case is the demand for a database shedding light on the routines of sentencing, thus improving transparency and equity. Judgments, however, may not be fully anonymized. This leads to the applicability of privacy law. Conflicts arise from the principle of purpose limitation, since the personal data contained in any judgement have been collected for the purpose of judging, not for being published in databases. Therefore, a special legal basis is needed, which results from § 475 (1), (4) StPO or from the right to information provided by press law. Article 10 GDPR is harder to deal with. It limits the procession of personal data relating to criminal convictions by requiring a legal authorization for handling data beyond the control of official authority. Such authorization can be derived from a broad interpretation of § 475 (1), (4) StPO. It is not supported by the opening clause contained in Article 10 sentence 1 GDPR, though, but by the one in Article 85(2) GDPR – which allows for exceptions only if special, notably academic purposes are concerned. For all other purposes, compliance with privacy law depends on whether the procession of the data can be qualified as journalism. Then, the so-called media privilege grants vast derogations from Chapter II of the GDPR, including Article 10.

[112] Welche Norm einschlägig ist, hängt von der Publikationsform (gedruckt oder digital) und von der Interpretation des Begriffs „Unternehmen der Presse“ in § 57 Abs. 1 S. 1 RStV ab (vgl. LT-NRW-Drs. 17/1565, S. 98). Zur Frage, ob hierunter auch Akteure jenseits redaktioneller Strukturen fallen, s. *Brings-Wiesen* in Spindler/Schuster, § 57 RStV Rn. 4. Ein Unterschied in der Rechtsfolge ergibt sich hieraus (in NRW) aber nicht.

[113] Das gilt nach dem Wortlaut von § 12 S. 4 LPresseG NRW bzw. § 57 Abs. 1 S. 4 RStV auch für Art. 6 Abs. 1 DSGVO, der die Rechtfertigungsbedürftigkeit der Datenverarbeitung normiert. Die Ausnahme ist aber wohl zu pauschal, s. dazu Fn. 75; vgl. andererseits *Buchner/Tinnefeld* in Kühling/Buchner Art. 85 Rn. 28.

Dark Patterns

Phänomenologie und Antworten der Rechtsordnung

Prof. Dr. Mario Martini/Christian Drews/Paul Seeliger/
*Quirin Weinzierl, LL.M. (Yale)**

In der Welt digitaler Benutzeroberflächen begegnen Nutzer immer häufiger sog. „Dark Patterns", die Entscheidungen ihrer Adressaten subtil in eine bestimmte Richtung lenken. Wer Webseiten aufruft, stellt etwa fest, dass es deutlich leichter ist, Berechtigungen für Cookies zu erteilen, als diese zu verweigern. Der Beitrag leuchtet die bestehenden rechtlichen Grenzen, aber auch Lücken für Dark Patterns im Datenschutz-, Vertrags- und Lauterkeitsrecht aus.

Inhaltsübersicht

ZfDR 2021, 47–74

„Das Angebot ist nur noch 60 Sekunden zum angegebenen Preis reserviert!" Bis vor Kurzem sah eine derartige Meldung, wer eine der größten weltweiten Hotelvermittlungs-Websites nutzte. Mutige Kunden, die die Probe aufs Exempel machten und die Warnung ignorierten, merkten jedoch, dass der Zeitablauf keinerlei Konsequenzen nach sich zog.[1] Der geforderte Preis blieb identisch und der Urlauber konnte die Buchung zu denselben Konditionen fortführen. Der Anbieter setzte also darauf, Kunden mit Hilfe vorgetäuschten zeitlichen Drucks dazu zu drängen, einen Vertrag abzuschließen.[2]

Der Fall steht paradigmatisch für viele andere Praktiken, mit denen Anbieter das Verhalten ihrer Nutzer in digitalen Umgebungen zu steuern versuchen. Designmuster wie der Reservierungs-Countdown finden (zumindest international) unter der Bezeichnung „Dark Patterns" vermehrt öffentliche Aufmerksamkeit. Den Begriff prägte der Interfacedesign-Spezialist *Harry Brignull* im Jahr 2010.[3] Die Forschung, vornehmlich aus dem Bereich des Interfacedesigns, richtet ihr analytisches Mikroskop seither immer stärker darauf, lenkende Designmuster anhand von Beispielen zu beschreiben und zu kategorisieren, die Verbreitung und Wirksamkeit der Praktiken zu belegen sowie Techniken zu entwickeln, um Dark Patterns automatisiert zu erkennen.[4]

Bei manchen Behörden und einigen Politikern wirkten diese Untersuchungen als Weckruf. So hat die US-amerikanische *Federal Trade Commission* (FTC) im September 2020 gegen die digitale Lernplattform „Age of Learning" wettbewerbsrechtliche Maßnahmen wegen Dark Patterns ergriffen.[5] Nahezu zeitgleich legte die Datenschutzbehörde des Vereinigten Königreichs (ICO) einen neuen Standard für altersangemessenes Design vor, der spezifische verhaltensbeeinflussende Techniken allgemein verbietet.[6] Auch legislative Maßnahmen zeichnen sich ab: Der sog. DETOUR Act[7], den Senatoren des US-Kongresses parteiübergreifend in den Senat eingebracht haben, ist mit dem Ziel angetreten, Online-Verhaltensbeeinflussungen, insbesondere Dark Patterns, zu verbieten. Kalifornien hat in den *California Privacy Rights Act of 2020* (CPRA) sogar explizit eine Bestimmung aufgenommen, die festschreibt, dass Zustimmungen

---

* *Mario Martini* ist Lehrstuhlinhaber an der DUV Speyer und Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung" am Deutschen Forschungsinstitut für öffentliche Verwaltung. *Christian Drews* und *Paul Seeliger* sind Forschungsreferenten, *Quirin Weinzierl* ist Koordinator in dem „Dark-Pattern-Detection-Project" (Dapde), welches das BMJV fördert. Die Autoren danken *Anton Kamke, Carolin Heinzel, Jule Martenson* und *Ulrike Urbanek* für ihre sehr gute Unterstützung. Soweit nicht anders vermerkt, sind Internetquellen auf dem Stand vom 10.1.2021.

[1] Vgl. auch *Bundeskartellamt*, Sektoruntersuchung Vergleichsportale, 2019, S. 107 f.

[2] Auf Drängen der Europäischen Kommission und der nationalen Verbraucherschutzbehörden hin erklärte der Anbieter schließlich, bis Mitte 2020 auf diese Praxis zu verzichten; vgl. *Europäische Kommission,* Nach Intervention der EU verpflichtet sich Booking.com, die Darstellung von Angeboten und Preisen mit dem EU-Recht in Einklang zu bringen, Pressemitteilung v. 20.12.2019; MMR-Aktuell 2020, 424225.

[3] *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern, abrufbar unter: darkpatterns.org/types-of-dark-pattern, auch mit einer Beispielsammlung.

[4] Etwa *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1.

[5] *Federal Trade Commission,* Regarding Dark Patterns in the Matter of Age of Learning, Inc., Pressemitteilung v. 2.9.2020.

[6] *UK Information Commissioner's Office*, Age Appropriate Design: A Code of Practice for Online Services, 2020, S. 72 ff.

[7] Deceptive Experiences To Online Users Reduction (DETOUR) Act, S. 1084, 116th Cong. (2019). Mittlerweile ist der Gesetzentwurf hinfällig.

zu Datenverarbeitungen, die der Anbieter mit Hilfe von Dark Patterns erlangt hat, unwirksam sind.[8]

In Deutschland hingegen haben Dark Patterns sowohl in der Rechtswissenschaft als auch in der Aufsichtspraxis bisher nur sehr verhaltene Aufmerksamkeit erfahren.[9] Auch hier steht die Rechtsordnung aber vor der Frage, ob und inwieweit Regulierungsbedarf besteht.

I. Das Phänomen „Dark Patterns"

1. Gängiges Begriffsverständnis

Der Terminus „Dark Pattern" ist ein Sammelbegriff, unter dessen Dach sich viele, teils unterschiedliche Phänomene tummeln. Eine einheitliche Definition hat sich bisher (noch) nicht herausgebildet. Ein gemeinsamer Kern schält sich gleichwohl heraus: Bei Dark Patterns handelt es sich um digitale Designmuster, die Nutzer zu Handlungen verleiten, welche ihren „eigentlichen" Interessen zuwiderlaufen oder die sie andernfalls nicht vorgenommen hätten.[10] Neben Countdowns, die Angebote (mitunter scheinbar) zeitlich befristen, sind auch Verweise auf die (vermeintliche) Knappheit und das (vermeintliche) Verhalten anderer Nutzer typische Erscheinungsformen – ebenso wie graphische Hervorhebungen, welche die Aufmerksamkeit lenken. Weitere Anwendungsbeispiele sind voreingestellte Eingabemöglichkeiten sowie suggestive Fragen und Informationen.

Dark Patterns sind besondere Spielarten von *Design Patterns*. Deren Konzept stammt ursprünglich aus der Architektur.[11] Design Patterns beschreiben Vorlagen für häufig wiederkehrende Gestaltungsaufgaben.[12] Designer bedienen sich ihrer etwa, um Oberflächen und Bedienelemente für Nutzer nachvollziehbar zu gestalten (sog. *User-Interface-[UI-]Design)*. Ganze digitale (Um-)Welten basieren auf ihnen.

Ebenso wie andere Designmuster sind Dark Patterns zwar fest in ihre Umgebung eingewoben. Von herkömmlichen Mustern unterscheiden sie sich jedoch dadurch, dass sie Nutzer zu einem Handeln, Dulden oder Unterlassen verleiten, indem sie Reflexionslücken der präferenzgerechten, rationalen menschlichen Entscheidungsfindung ausnutzen.

2. Wirksamkeit und -mechanismen

Aus Anwenderperspektive gilt als „harte Währung" von Dark Patterns ihre Wirksamkeit. Einen Beeinflussungserfolg im Einzelfall setzen Dark Patterns gleichwohl nicht zwingend voraus – schon deshalb, weil unter der Vielzahl adressierter Nutzer einige für Verhaltensbeeinflussung besonders sensibilisiert sein können. Dark Patterns

---

[8] Sec. 14 lit. h CPRA, zur Änderung von Sec. 1798.140 lit. h Nr. 1 *Cal. Civil Code* (*California Consumer Privacy Act* 2018, CCPA). Zum CPRA allgemein *Lejeune,* ITRB 2021, 13 (13 ff.).

[9] So etwa *Hill* DÖV 2020, 205 (206); *Weinzierl* NVwZ-Extra 15/2020, 1 (1 ff.).

[10] Vgl. die Definitionen bei: *Bogenstahl*, Dark Patterns, 2019, S. 1: „die deren eigentlicher Intention zuwiderlaufen", „Nachteile oder negative Konsequenzen"; *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern, abrufbar unter: darkpatterns.org/types-of-dark-pattern: „things that you didn't mean to"; *Forbrukerrådet*, Deceived by Design, 27.6.2018, S. 7: „not in their interest"; *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (1): „not in the user's best interest"; *Luguri/Strahilevitz*, Shining a Light on Dark Patterns, 2019, abrufbar unter: https://ssrn.com/abstract=3431205, S. 11: „things they would not otherwise do".

[11] *Alexander/Ishikawa et al.*, A pattern language, 1977, S. x.

[12] *Gamma/Helm et al.*, Design Patterns, 2015, S. 27 ff.

sollen ihrem Wesen nach auch nicht spezifische Personen, sondern vielmehr eine hinreichende Anzahl von Menschen beeinflussen. Dementsprechend sind Dark Patterns über-individuell zu bestimmen: Es genügt, dass Gestaltungen eine kritische Mindestanzahl menschlicher Entscheidungen im Sinne ihres Verwenders beeinflussen können.

Der Mechanismus, durch den sie wirken, ist demgegenüber sekundär: Sie können manipulieren, täuschen, nötigen oder Nutzer steuern.[13] Der überwiegende Teil der beobachteten Phänomene macht sich verhaltensökonomische bzw. -psychologische Effekte zunutze.[14] *Scarcity*- und *Countdown*-, *Preselection*- sowie *Trick Question*-Patterns etwa instrumentalisieren *Biases* und *Heuristiken* der Entscheider.[15] Andere Dark Patterns basieren auf Elementen der (empirischen) Designforschung[16] oder disziplinübergreifenden Mischgebilden.[17]

Die Wirkmechanismen von Dark Patterns beschränken sich keineswegs auf die digitale Welt. Sie sind bspw. ebenso in Gestalt des Arrangements von Supermarktregalen im Kassenbereich[18] oder des absichtlich verbreiteten Geruchs frischer Backwaren als Kaufanreiz denkbar.[19] Das digitale Umfeld bietet für solche Beeinflussungsstrukturen jedoch ein optimales Ökosystem – insbesondere um Interfacegestaltungen zu erproben. Denn in der digitalen Welt können entscheidungssteuernde Konstrukte tendenziell mächtiger und nuancierter wirken als ihre nicht-digitalen Pendants:[20] Digitale Umgebungen lassen sich nicht nur fast beliebig gestalten, sondern auch kurzfristig sowie zu niedrigen Kosten anpassen. Gerade reichweitenstarke Online-Anbieter können im laufenden Betrieb kleinste Oberflächen-Veränderungen an ihren Nutzern testen und dadurch die Wirksamkeit ihrer Designelemente erhöhen (sog. *A/B-Testing*).[21] Auf diese Weise ist es ihnen möglich, kontinuierlich den Einfluss von Maßnahmen – etwa auf die Verweildauer, die Anzahl der Einwilligungen und Vertragsabschlüsse von Nutzern oder die generelle Reichweite der Seite – zu überprüfen und ggf. zu steigern.

Derartige Tests validieren nicht nur, *ob* Dark Patterns wirken, sondern auch *bei wem*. Sie erzielen nämlich bei Menschen mit verschiedenen Eigenschaften und Hintergründen unterschiedliche Effekte. Attribute wie etwa der Bildungsstatus oder die politische Einstellung[22] sowie (wohl) auch das Geschlecht[23] korrelieren sowohl mit dem Grad der generellen und situativen Beeinflussbarkeit eines Nutzers als auch der Wirksamkeit

[13] *Jaiswal*, Dark patterns in UX: how designers should be responsible for their actions, UX Collective vom 16.4.2018: „manipulate", „tricking"; *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1 (2): „coercing", „steering"; *United States Senator for Nebraska Deb Fischer,* Senators introduce bipartisan legislation to ban manipulative 'dark patterns', Pressemitteilung v. 9.4.2019: „manipulate".

[14] *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (1): „use their knowledge of human behavior"; *United States Senator for Nebraska Deb Fischer* (o. Fn. 13): „drawn from extensive behavioral psychology research".

[15] Vgl. *Baek/Bae et al.,* The Social Science Journal 2014, 523 (528 ff.). Zu den Konzepten *Kahneman/Tversky,* Econometrica 1979, 263; *Tversky/Kahneman,* Science 1974, 1124.

[16] Etwa *Chittaro*, in: Meschtscherjakov/Ruyter/Fuchsberger et al. (Hrsg.), Persuasive Technology, 2016, S. 6 ff.; *Mandel/Johnson,* J Consum Res 2002, 235 (237 ff.).

[17] Auffällig ist zudem, dass Dark Patterns regelmäßig das assoziative und unterbewusste System 1-Denken ansprechen; *Luguri/Strahilevitz* (o. Fn. 10), S. 3. Vgl. *Evans,* Trends in Cognitive Sciences 2003, 454 (454 ff.).

[18] Vgl. *Thaler/Sunstein*, Nudge, 2008, S. 1 f.

[19] Vgl. auch *Hacker*, Verhaltensökonomik und Normativität, 2017, S. 662 f.

[20] Vgl. *Luguri/Strahilevitz* (o. Fn. 10), S. 22.

[21] S. *Narayanan/Mathur et al.,* acmquere 2020, 67 (80); *Susser/Roessler et al.,* Georgetown Law Technology Review 2019, 1 (29 ff.); *Yeung,* Information, Communication & Society 2017, 118 (122).

[22] *Luguri/Strahilevitz* (o. Fn. 10), S. 27 f.

[23] Unterschiedliche Farben auf Webseiten wirken bspw. themenspezifisch bei Männern anders als bei Frauen; *Chittaro*, in: Meschtscherjakov/Ruyter/Fuchsberger et al. (o. Fn. 16), S. 8 ff.

spezieller Patterns. Digitale Tracking-Methoden vereinfachen es Verantwortlichen, diese persönlichen Parameter zu erheben. Perspektivisch ist es dadurch möglich, Web-Oberflächen auf jeden Besucher individuell zuzuschneiden, um maximale Wirksamkeit zu erreichen (sog. *Personalized Dark Patterns*[24]).[25] So lassen sich nicht nur Nutzer mit ihren jeweiligen Schwächen gezielt ansprechen; eine Personalisierung macht es zudem ungleich schwieriger, Dark Patterns aufzufinden und zu verfolgen.

3. Kategorisierung

Die Interfacedesignforschung unternimmt Versuche, verschiedene Arten der Muster zu kategorisieren. *Brignull* selbst beschreibt zwölf verschiedene Typen von Dark Patterns, die er teilweise selbsterklärend (*Trick Question*, *Hidden Costs*, *Disguised Ads*) und in anderen Fällen kreativ (*Privacy Zuckering*[26], *Roach Motel*[27]) benennt.[28] Andere strukturieren und verfeinern *Brignulls* Typen-Katalog, indem sie Oberbegriffe (*Nagging*, *Obstruction*, *Sneaking*, *Interface Interference* und *Forced Action*) und weitere Typen einführen.[29] Aus den vorhandenen Ansätzen lässt sich eine an der Wirkungsweise orientierte konsolidierte Klassifizierung destillieren (s. Tabelle auf der Folgeseite).

4. Abgrenzung zum Nudging

Indem Dark Patterns vielfach auf verhaltensökonomische Steuerungseffekte und Biases zurückgreifen, wohnt ihnen eine Wesensverwandtschaft zum *Nudging* und anderen Phänomenen der Verhaltenssteuerung inne. Sie unterscheiden sich von ihnen aber in ihrem Zweck bzw. Erfolg: *Nudging* will Nutzern zu Entscheidungen verhelfen, die ihren vermuteten eigenen mittel- oder langfristigen Präferenzen entsprechen oder zumindest gesamtgesellschaftliche Ziele fördern.[30] Dark Patterns hingegen setzen sich über individuelle Präferenzen hinweg oder ignorieren sie jedenfalls. Sie beeinflussen menschliche Entscheidungen allein zugunsten der Agenda ihres Verwenders.[31] Man kann daher auch von *Dark Nudging*[32] sprechen.

---

[24] *Weinzierl* NVwZ-Extra 15/2020, 1 (3).

[25] *Susser/Roessler et al.,* Internet Policy Review 2019, 1 (31 f.); *Yeung,* Information, Communication & Society 2017, 118 (121 f.). Entsprechende Auswertungen lassen sich allerdings nicht nur zu kommerziellen Zwecken nutzen; *Roßnagel* MMR 2020, 222 (225).

[26] Verleitung zum extensiven, unbedachten Teilen persönlicher Daten (in Anspielung auf *Mark Zuckerberg*).

[27] „Schabenfalle": Nutzerkontos lassen sich mühelos erstellen, sie zu löschen oder sich von dem Dienst abzumelden, erschwert der Anbieter jedoch durch komplizierte Menüführung oder weitere Handlungserfordernisse, wie eine zwingende telefonische Kontaktaufnahme.

[28] *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern, (o. Fn. 3).

[29] Vgl. *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (4 ff.); *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1. Allen Klassifikationen ist gemein, dass sie nur Näherungswerte abbilden und vielfache alternative Einteilungsformen (zB nach dem Grad der Wirksamkeit oder dem erzielten Nutzerverhalten) denkbar sind. So lässt sich etwa eine *Hidden Subscription* (auch) durch eine Vorauswahl von Häkchen, eine *Trick Question* oder eine Kombination aus beiden erreichen; ob der Mechanismus täuscht, etwas erschleicht oder wegen höherer Transaktionskosten ein zusätzliches Hindernis errichtet, hängt vom Einzelfall ab.

[30] *Thaler/Sunstein* (o. Fn. 18), S. 107 ff.; vgl. auch *Seckelmann/Lamping* DÖV 2016, 189 (193); *Smeddinck* ZRP 2014, 245 (246).

[31] Vgl. *Luguri/Strahilevitz* (o. Fn. 10), S. 3.

[32] Vgl. etwa *Weinzierl* NVwZ-Extra 15/2020, 1 (3).

Kategorie	Druck	Operativer Zwang	Hindernisse	Erschleichen	Irreführen
Wirkungsweise	Ein Designmuster setzt den Nutzer **unter Druck**, eine bestimmte Handlung (nicht) vorzunehmen	**Keine Entscheidungsmöglichkeit** oder (mindestens) eine Entscheidungsalternative ist an **weitere Bedingungen** geknüpft	Bestimmte Entscheidungsmöglichkeiten auszuüben, erfordert **unnötigen/zusätzlichen Aufwand**	Der Nutzer bemerkt die Konsequenzen seiner Handlung aufgrund **heimlicher Änderungen** nicht	Gestaltung der Benutzeroberfläche, die übliche **Erwartungen enttäuscht** bzw. ihnen entgegenläuft
Beispiele[33]	**Nagging** (#): wiederholtes (aggressives) Auffordern, eine bestimmte Handlung vorzunehmen	**Forced Enrollment** (+): Nutzung eines Service nur bei Abschluss eines Abos/Kundenkontos	**Roach Motel** (*, #, +): Anmeldung/Abonnieren wesentlich einfacher als Kündigung	**Sneak into Basket** (*, #, +): Zusätzliches Objekt landet ungewollt im Warenkorb	**Trick Question** (*, #, +): verwirrend formulierte Frage (zB doppelte Verneinung)
	Confirmshaming (*, +): Die Auswahlgestaltung einer Frage löst Schuldgefühle aus	**Forced Continuity** (*, #): automatisches Abonnement; Kündigung erschwert	**Preselection** (#): Auswahlmöglichkeiten sind bereits (abänderbar) getroffen, insbes. durch gesetzte Häkchen	**Hidden Costs** (*, #, +): Zusatzkosten erscheinen erst im letzten Bestellschritt	**Misdirection** (*, +): Design lenkt durch auffällige graphische Elemente vom Inhalt ab
	Countdown (+): Ware/Dienstleistung (angeblich) nur für bestimmte Zeit verfügbar	**Forced Review**: Nutzer können einen Dienst nur dann weiterhin nutzen, wenn sie ad hoc etwa (geänderte) Datenschutzeinstellungen durchsehen und ggf. akzeptieren	**Hidden Information** (#): Für den Nutzer relevante Informationen sind versteckt oder nur schwer verfügbar	**Hidden Subscription** (+): automatisches Abonnieren von Leistungen/Angeboten	**Bait and Switch** (*, #): Klick auf Schaltfläche führt zu anderem Ergebnis als üblicherweise erwartet
	Scarcity (+): Ware/Dienstleistung (angeblich) nur in knapper Zahl verfügbar		**Price Comparison Prevention** (*, #): Preisvergleich erschwert (zB Fremdwährung)		**Disguised Ads** (*, #): als Inhalt oder Steuerungselement getarnte Werbung
	Social Proof (+): direktes Einblenden von (gefälschten) Kundenbewertungen oder dem (vermeintlichen) Verhalten anderer		**Click Fatigue**: Klickwege zu verschiedenen Optionen sind unterschiedlich lang („Klickmüdigkeit")		

5. Kritik an bisherigen Definitionsansätzen und Lösungsvorschlag

Die bisherigen Definitionsansätze zu Dark Patterns bleiben eine klare Antwort auf die Frage schuldig, was das „Dunkle" an ihnen eigentlich ausmacht. Sie lassen insbesondere offen, inwiefern die Wirkung eines bestimmten Designs verwerflicher ist als etwa die (im Grundsatz gesellschaftlich akzeptierte und rechtlich zulässige) werbende Darstellung eines Produkts. Der am häufigsten genutzte Definitionsansatz, der auf die Frustration der „eigentliche[n] Interessen"[34] abstellt, greift insoweit zu kurz. Nicht zuletzt lässt sich nicht immer zuverlässig messen, was im Einzelfall substanziell „gewollt" ist bzw. den „Interessen" der Nutzer entspricht. So können bspw. kurzfristige und langfristige Interessen auseinanderfallen.

Schaut man genauer hin, ist allen Dark Patterns ein Merkmal gemein, das sie von sonstigen Steuerungsmechanismen abgrenzbar macht: Ihre Verwender nutzen die Ge-

[33] Die Bsp. finden sich auch, teilweise unter ähnlichem Namen, bei: (*) *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern (o. Fn. 3); (#) *Gray/Kou et al.,* CHI 2018, Paper 534, 1; (+) *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1.

[34] So etwa *Bogenstahl* (o. Fn. 10), S. 1. Vgl. auch *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (1); *Susser/Roessler et al.,* Internet Policy Review 2019, 1 (7).

staltungsmacht über Benutzeroberflächen unangemessen zum eigenen Vorteil aus; sie lenken nicht nur menschliches Verhalten, sondern agieren zugleich *missbräuchlich*.[35] Dark Patterns setzen die Interessen ihrer Verwender mithin einseitig gegen die Interessen des Nutzers durch – insbesondere um eine höhere Zahl von Vertragsabschlüssen oder -verlängerungen zu generieren, höhere Interaktionsraten zu erreichen oder mehr Daten zu sammeln, die sich letztlich über Werbung monetisieren lassen. Ein Indiz für Missbräuchlichkeit sind solche Gestaltungen, welche die Bedienbarkeit für Nutzer hinsichtlich einer Entscheidungsoption erheblich schmälern und nicht oder nur untergeordnet durch die Funktionalität des Dienstes angezeigt sind.[36] Gleiches gilt für Gestaltungen, die so ungewöhnlich sind, dass der Verbraucher typischerweise nicht mit ihnen zu rechnen braucht.[37]

Missbräuchlichkeit impliziert nicht automatisch ein vorsätzliches Handeln oder gar eine Schädigungsintention, auch wenn einige Definitionsvorschläge[38] zusätzlich eine derartige subjektive Komponente fordern. Dark Patterns können vielmehr ebenso unbeabsichtigt entstehen – insbesondere, wenn Anwender lediglich die Wirkung einzelner Gestaltungselemente (ggf. vollständig automatisiert) erhöhen. Überdies ist von außen betrachtet vielfach nicht erkennbar, ob Vorsatz vorliegt. Zu welchem Grad Dark Patterns Entscheidungen bewusst oder gewollt beeinträchtigen, ist für eine wirkungsorientierte Qualifikation ohnehin unerheblich.[39]

Dark Patterns sind also in conclusio alle Designmuster, die eine kritische Zahl an Nutzern zu einem bestimmten Verhalten verleiten und dabei die Gestaltungsmacht über Benutzeroberflächen einseitig im Interesse ihrer Verwender ausnutzen.

II. Antworten der Rechtsordnung

Die deutsche wie die unionale Rechtsordnung greifen das Phänomen der Dark Patterns bislang nicht explizit auf. Unterschiedliche rechtliche Sphären schieben missbräuchlichen Beeinflussungen durch Oberflächen jedoch zumindest partiell einen Riegel vor. So versagt etwa das Datenschutzrecht Einwilligungen, die das Ergebnis von Dark Patterns sind, uU die Wirksamkeit; das Zivilrecht kann vertragsrechtliche Willenserklärungen für ungültig erklären. Wer Dark Patterns nutzt, ist zudem womöglich lauterkeitsrechtlich belangbar oder riskiert sogar eine Betrugsstrafbarkeit.

1. Verfassungsrecht

Ebenso wie sonstige absatzfördernde Kommunikation, insbesondere Werbung, sind Dark Patterns Ausdruck grundrechtlich geschützten Verhaltens.[40] Der Staat hat die Pri-

[35] Ob und welche Dark Patterns mit Normen kollidieren, ist eine andere Frage (s. dazu u. II.). Die Gestaltungsmacht auszunutzen, haben Dark Patterns mit Allgemeinen Geschäftsbedingungen gemein. Während letztere unmittelbar *Vertragsbestandteil* werden, wirken Dark Patterns, indem sie die Gestaltungsmacht des Anbieters in der Phase der *Vertragsanbahnung* ausnutzen.

[36] Bei einer möglichen Regulierung könnte es dem Verwender obliegen, die Missbräuchlichkeit zu widerlegen.

[37] Vgl. auch den Rechtsgedanken des § 305c Abs. 1 BGB.

[38] *Bogenstahl* (o. Fn. 10), S. 1: „darauf ausgelegt sind"; *Bösch/Erb et al.,* PPET 2016, 237: „intentionally"; *Greenberg/Boring et al.*, in: Wakkary (Hrsg.), DIS '14, 2014, S. 524: „intentionally".

[39] So auch Sec. 3 lit. a Nr. 1 lit. A DETOUR Act: „with the purpose *or* substantial effect"; iErg ebenso *Rieger*/*Sinders*, Dark Patterns, 13.5.2020, S. 17.

[40] *Weinzierl* NVwZ-Extra 15/2020, 1 (6) zum Schutz von Entscheidungsarchitekturen.

vatautonomie sowie die Berufsfreiheit (Art. 2 Abs. 1 und Art. 12 GG; Art. 15 Abs. 1 GRCh bzw. die unternehmerische Freiheit, Art. 16 GRCh) und die Meinungsfreiheit (Art. 5 Abs. 1 GG; Art. 11 GRCh) ihrer Verwender zu respektieren. Gesetzliche Begrenzungen bedürfen daher einer grundrechtlichen Rechtfertigung.

Die Grundrechte der Nutzer, allen voran deren Vertragsfreiheit, können aber ein legitimes Schutzziel, uU sogar eine Schutzpflicht des Staates begründen, derartige Praktiken zu unterbinden. Denn der Staat hat die Voraussetzungen autonomer Entscheidungen im Geschäftsverkehr aktiv zu sichern.[41] Er ist aufgerufen, die Bedingungen freier Selbstbestimmung mit Hilfe seiner Regelungsmacht tatsächlich herzustellen.

Daraus können zwei konkrete Pflichten erwachsen: Der *Gesetzgeber* ist aufgerufen, sich schützend vor Betroffene zu stellen und das Untermaßverbot nicht zu verletzen. Die *Behörden* und *Gerichte* müssen bestehendes Recht im Sinne dieses Schutzauftrags auslegen und anwenden. Diese Pflicht ist insbesondere dort von besonderer Bedeutung, wo bestehenden Normen ein zu idealisiertes Leitbild des menschlichen Entscheidens zugrunde liegt.

2. Datenschutzrecht

Da Dark Patterns vorwiegend ein digitales Phänomen sind,[42] verwundert es nicht, dass sie häufig einen Bezug zu Datenverarbeitungen aufweisen. Insbesondere bei Gestaltungsmustern für Einwilligungserklärungen zur Datenverarbeitung finden sie sich in reicher Zahl. Ihre steuernde Wirkung kann mit den Vorgaben der DSGVO kollidieren.

a) Wirksamkeit von Einwilligungen

aa) Eindeutig bestätigende Handlung

Einwilligungen bedürfen einer „unmissverständlich abgegebene[n] Willensbekundung […] oder […] sonstigen […] bestätigenden Handlung" (Art. 4 Nr. 11 iVm Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO[43]). Zu diesem Gebot stehen jedenfalls *Opt-out*-Gestaltungen, mithin *Preselection*-Patterns, im Widerspruch (Erwgr. 32 S. 3 DSGVO). Ein Anbieter darf bspw. in der Eingabemaske für ein Online-Gewinnspiel nicht standardmäßig davon ausgehen, dass die Teilnehmenden Werbe-Cookies zustimmen.[44]

Zweifel an einer eindeutig bestätigenden Handlung können auch *Trick Question*- und *Misdirection*-Patterns auslösen, die kontraintuitiv zu ihrer tatsächlichen Funktio-

[41] Vgl. hierzu BVerfGE 81, 242 (254 ff.) = NJW 1990, 1469 (1470); *BVerfG* NJW 2020, 905 (Rn. 231 ff.).

[42] S. o. I. 2.

[43] Diese gelten per Verweis in der ePrivacy-RL etwa auch für den besonders praxisnahen Fall von *Cookies*. Art. 5 Abs. 3 iVm Art. 2 S. 2 lit. f ePrivacy-RL verweist insoweit via Art. 2 Abs. 2 lit. h, Erwgr. 17 S. 1 ePrivacy-RL, Art. 94 Abs. 2 S. 1 DSGVO auf die Vorschriften der DSGVO, s. *BGH* NJW 2020, 2540 (Rn. 29 ff., 60 ff.); *GA Szpunar,* ECLI:EU:C:2019:246 = BeckRS 2019, 3909, Rn. 50 ff. In § 15 Abs. 3 TMG ist mit Blick auf Art. 5 Abs. 3 ePrivacy-RL richtlinienkonform ein Einwilligungserfordernis hineinzulesen, *BGH* NJW 2020, 2540 (Rn. 47 ff.). Klarstellend: § 22 Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien sowie zur Änderung des Telemediengesetzes (TTDSG-E), 12.1.2020, abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/P-R/referentenentwurf-zum-gesetz-zur-regelung-des-datenschutzes-und-des-schutzes-privatsphaere.pdf.

[44] *EuGH* ECLI:EU:C:2019:801 = MMR 2019, 732 (Rn. 60 ff.); s. a. *BGH* NJW 2020, 2540 (Rn. 64); *Taeger/Schweda* ZD 2020, 124 (126).

nalität gestaltet sind.[45] Ein solcher Effekt tritt bspw. ein, wenn ein Anbieter für Auswahlmöglichkeiten in einem Bestellvorgang regelmäßig einen grünen Schiebe-Schalter verwendet, die Datenverarbeitungseinwilligung jedoch als erteilt gelten soll, wenn der Schalter in die andere Richtung weist.

Ob und in welchem Umfang das Vertrauen der Nutzer in die Stringenz von Bedienoberflächen (gerade zwischen verschiedenen Anbietern) in diesen Fällen geschützt ist, verrät der Gesetzeswortlaut nicht. Auch die (nicht mit normativ-autoritativer Macht ausgestatteten) Richtlinien des Europäischen Datenschutzausschusses lassen insoweit eine Konkretisierung vermissen; sie verlangen lediglich, Mehrdeutigkeit bei Einwilligungsgestaltungen zu vermeiden.[46] Damit bleibt die Anforderung der eindeutig bestätigenden Handlung derzeit zu abstrakt, um irreführenden Dark Patterns eine echte Hürde entgegenzusetzen.[47]

bb) Freiwilligkeit

Erklärungen, die ein Anbieter durch starke Täuschung oder Drohung mit erheblichen negativen Wirkungen erreicht, sind nicht von der Autonomie des Einwilligenden getragen und deshalb unfreiwillig.[48] Eine konkrete Ausformung dieser normativen Wertung ist das sog. vertikale Kopplungsverbot: Macht der Anbieter die Vertragserfüllung von einer Einwilligung in die Verarbeitung von Daten abhängig, die zu diesem Zweck gar nicht erforderlich ist, stellt das die Freiwilligkeit einer Einwilligung infrage (Art. 7 Abs. 4 DSGVO). Konditionale Patterns aus der Kategorie „operativer Zwang", die etwa eine Verarbeitungsberechtigung dafür ‚einfordern', dass Nutzer ein anderes, inhaltlich unzusammenhängendes Angebot nutzen können, können diesem vertikalen Koppelungsverbot zuwiderlaufen. Das gilt bspw. für eine digitale Bildbearbeitungssoftware, die Nutzern abverlangt, die Standortverfolgung und -speicherung zu aktivieren.[49]

Weniger eindeutig liegt es bei Dark Patterns solcher Kategorien, die aufgrund ihrer subtileren Wirkungsweise die Schwelle der Unfreiwilligkeit nicht derart eindeutig erreichen, etwa dem *Nagging*-Pattern. Als repetitive Bearbeitungsanfrage kann es – gerade, wenn es optisch aggressiv gestaltet ist[50] – den Eindruck erwecken, dass Datenverarbeitungsrechte zu erteilen sind, bevor jemand eine andere, nicht damit im Zusammenhang stehende Anwendung nutzen kann – auch wenn dies objektiv nicht der Fall ist. Ähnlich gelagert sind *Click Fatigue-Patterns*, die etwa die Verweigerung der Einwilligung von weiteren, umständlichen Handlungen abhängig machen.[51] Sie können

[45] Häufig für Cookie-Einwilligungsfelder genutzt. Beratungsunternehmen empfehlen derartige Konstruktionen explizit, vgl. nur *SUCHMEISTEREI GmbH*, Cookie-Consent mit dem Google Tag Manager, 5.8.2020, S. 7.

[46] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, 4.5.2020, S. 19.

[47] Auch das Einwilligungsbewusstsein ist derzeit allenfalls als Untergrenze heranzuziehen; *Buchner/Kühling*, in: dies. (Hrsg.), DSGVO mit BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 56.

[48] *European Data Protection Board* (o. Fn. 46), S. 9. Der Zwang bezieht sich auf den Inhalt der Erklärung, nicht auf den Umstand, dass eine Erklärung ergehen muss; s. a. *Martini/Weinzierl* RW 2019, 287 (308 f.).

[49] Bsp. aus *European Data Protection Board* (o. Fn. 46), S. 8.

[50] Etwa indem (iVm einer *Misdirection*) eine Meldung nur einen großen, farblich unterlegten und zentral positionierten „Zustimmen"-Button sowie ein sehr kleines, graues Kreuzchen bereithält, um die Aufforderung zu schließen, und bis zu einer Interaktion die weitere Nutzung verhindert.

[51] Dazu das – nicht-digitale – Bsp. *EuGH* ECLI:EU:C:2020:901 = BeckRS 2020, 30027: Ein Anbieter erbat bei Vertragsabschluss die Einwilligung, eine Personalausweiskopie zu speichern, ohne

eine Einwilligung kraft ihrer subjektiven Wirkung unfreiwillig machen, weil sie eine „echte oder freie Wahl" verhindern (Erwgr. 42 S. 5 DSGVO).

Wenn Nutzer einzelne Bearbeitungszwecke nicht aus- oder abwählen können, mündet das in eine Coactus-volui-Situation: Solche (quasi-)globalen Einwilligungen zur Datensammlung und -verarbeitung verstoßen gegen das sog. *horizontale Koppelungsverbot* (Art. 7 Abs. 2 S. 1, Erwgr. 43 S. 2 1. Hs. DSGVO).[52]

cc) Informiertheit

Zur *Form,* in der der Verantwortliche Informationen zu geben hat, hält die DSGVO (abgesehen von Art. 7 Abs. 2) kaum explizite Vorgaben vor.[53] Der Unionsgesetzgeber hat damit einen eindimensionalen Ansatz gewählt: Er trifft vorwiegend Informationsvorgaben, klammert aber solche mentalen Abweichungen und Limitationen bei der Informationsverarbeitung aus, auf die Dark Patterns aufsatteln. So setzen *Hidden Information*-Patterns darauf, durch ihre optische Gestaltung Nutzer darüber im Unklaren zu belassen, welche Berechtigungen Anbieter konkret erfragen – etwa indem sie Optionen ausblenden. *Trick Questions*-Patterns können durch ihre Formulierung oder überkomplexe Strukturen Verwirrung über den Umfang von Datenverarbeitungen stiften.[54]

Die Rechtsprechung sucht Wege, um solche verhaltenssteuernden Phänomene zu erfassen. Zielt die konkrete Gestaltung der Bedienoberfläche mit Hilfe einer Vielzahl von Auswahlmöglichkeiten darauf ab, dass der Betroffene sich mit ihren Inhalten gar nicht erst auseinandersetzt, sieht der BGH darin keine informierte Einwilligung „für den bestimmten Fall" (Art. 4 Nr. 11 DSGVO).[55] Das Gericht erkennt damit im Grundsatz an, dass schlecht aufbereitete oder im Übermaß vorhandene Informationen nicht dem Normzweck gerecht werden. Der Verantwortliche verstößt zudem potenziell gegen seine Informationspflichten (Art. 13 Abs. 2 lit. b, c DSGVO), wenn seine Einwilligungsarchitektur den Eindruck vermittelt, Vertragsabschluss und Datenverarbeitungseinwilligung seien nicht unabhängig voneinander,[56] er eine horizontale Kopplung mithin nur vorspiegelt. Die Vorgaben setzen also solchen Gestaltungen Grenzen, die Informationen allzu offensichtlich verschleiern bzw. die Auswahlmöglichkeiten sehr unübersichtlich gestalten.[57]

---

dass dies erforderlich war, um den Vertrag zu schließen. Wer die Zustimmung versagte, musste ein zusätzliches Formular ausfüllen.

[52] Außerdem darf das Menü nicht so gestaltet sein, dass es Nutzer davon abhält, Entscheidungen zu treffen; *BGH* NJW 2020, 2540 (Rn. 32). S. dazu sogleich, I. 2. a) bb).

[53] *European Data Protection Board* (o. Fn. 46), S. 16 f. Die Pflichten des Art. 12 Abs. 1 DSGVO beziehen sich auf Art. 13 ff. DSGVO, also nicht unmittelbar auf die Einwilligung; vgl. auch *Bäcker*, in: Kühling/Buchner (Hrsg.), DSGVO mit BDSG, 3. Aufl. 2020, Art. 13 DSGVO Rn. 63 ff.

[54] Vgl. zu „in Kenntnis der Sachlage" und „für den konkreten Fall" iSd Art. 2 lit. h Datenschutz-RL: *BGH* NJW 2020, 2540 (Rn. 31 f.).

[55] *BGH* NJW 2020, 2540 (Rn. 36). Insofern ist die Informiertheit „das subjektive Gegenstück zur Bestimmtheit", *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DSGVO mit BDSG, 2019, Art. 7 DSGVO Rn. 72.

[56] *EuGH* ECLI:EU:C:2020:901 = BeckRS 2020, 30027 (Rn. 49 f.).

[57] So auch *Böhm/Halim* MMR 2020, 651 (655).

b) *Data Protection by Design* (Art. 25 Abs. 1 DSGVO)

Lenkenden Gestaltungsmustern, die mit Hilfe von Voreinstellungen (und damit unter Ausnutzung des sog. *Default*-Effekts[58]) einseitig die Geschäftsinteressen der Anbieter vor den Privatheitsschutz ihrer Kunden setzen, stellt sich Art. 25 *Abs. 2* DSGVO (*Data Protection by Default*) entgegen. Art. 25 *Abs. 1* DSGVO richtet den Blick über Datenschutzverstöße bei einzelnen *Bearbeitungsvorgängen* hinaus auf die Nutzung grundsätzlich mängelbehafteter *Systeme*: Er schwört die Verantwortlichen auf Datenschutz durch Technikgestaltung (*Data Protection by Design*) ein. Sie sollen den Datenschutz*grundsätzen* (Art. 5 DSGVO) ganzheitlich und von Beginn an bei der Technikgestaltung Raum geben und sie dadurch effektiv umsetzen.[59] Diese Verpflichtung des Verantwortlichen konzipiert die DSGVO als Hebel, um mittelbar auch die Entwickler von Datenverarbeitungssystemen an die Datenschutzziele zu binden.[60] Art. 25 Abs. 1 DSGVO wirkt damit in die Tiefe der Datenverarbeitungsstrukturen hinein.

Zur Technikgestaltung gehört im Grundsatz auch das Design der Anwendungsoberflächen. Denn es repräsentiert die oberste Ebene der technischen Architektur, die den mehrschichtigen Prozess der Datenverarbeitung anleitet: Interfacedesign bahnt den Weg, auf dem sich die technische Gestaltung entfaltet, die die Privatheit schützen soll. Der Wortlaut des Art. 25 Abs. 1 DSGVO lässt sich daher durchaus so verstehen, dass er Design-Muster, zB farbliche Hervorhebungen, als Teil der Technikgestaltung erfasst. Dies geht mit der Philosophie des Data Protection by Design-Gebots, Software insgesamt datenschutzfreundlich auszugestalten, Hand in Hand. Sobald Dark Patterns etwa Nutzer dazu verleiten, größere Datenmengen als erforderlich preiszugeben, konfligieren sie grundsätzlich mit dieser Vorgabe:[61] Art. 25 Abs. 1 DSGVO verweist explizit auf den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO. Der Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DSGVO) gebietet es zudem, Auswahlmöglichkeiten objektiv, neutral und ohne den Einsatz manipulativer Techniken darzustellen.[62]

Allerdings zieht das Data Protection by Design-Prinzip keine klar konturierten Brandmauern für unzulässiges Verhalten ein.[63] Die offene Struktur der Norm trägt ihren Adressaten vielmehr eine Abwägung hinsichtlich der zu ergreifenden Maßnahmen auf. Eine Vielzahl von Variablen, insbesondere der „Stand der Technik", fließen dabei in das Entscheidungskalkül ein.[64] Die Norm ist auf Maßstäbe angewiesen, welche die Grenzen akzeptabler Beeinflussung (ggf. ausgelagert) festschreiben, um vollzugsfähig zu sein. Schon im Lichte des Bestimmtheitsgebots (Art. 49 Abs. 1 S. 1 GRCh) muss mit Blick auf die Bußgeldbewehrung des Verstoßes (Art. 83 Abs. 4 lit. a DSGVO) stets

[58] *Martini*, in: Paal/Pauly (Hrsg.), DSGVO BDSG, 3. Aufl. 2021, Art. 25 DSGVO Rn. 13.

[59] *European Data Protection Board*, Guidelines 4/2019 on Article 25, 2020, S. 6 f.

[60] Dazu Erwgr. 78 S. 4 DSGVO; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DSGVO mit BDSG, 2019, Art. 25 DSGVO Rn. 20 ff.; *Martini*, in: Paal/Pauly (o. Fn. 58), Art. 25 DSGVO Rn. 25 f.

[61] So auch *European Data Protection Board* (o. Fn. 59), S. 18. Vgl. im Weiteren *Baek/Bae et al.,* The Social Science Journal 2014, 523 (528 f.); *Luguri/Strahilevitz* (o. Fn. 10), S. 22 f. sowie *Martini/Weinzierl* RW 2019, 287 (288 f.).

[62] *European Data Protection Board* (o. Fn. 59), S. 18: „No Deception". Zu Recht sah sich der Europäische Datenschutzausschuss im November 2020 zu der Feststellung veranlasst, dass „Dark Patterns […] gegen den Geist von Artikel 25" DSGVO verstoßen, aaO, S. 19; Übersetzung d. Verf.

[63] So auch *Roßnagel* MMR 2020, 222 (227).

[64] *European Data Protection Board* (o. Fn. 59), S. 8 ff.; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (o. Fn. 60), Art. 25 DSGVO Rn. 36 ff. schlägt insoweit Datenbanken vor, die den „Stand der Technik" abbilden.

vorhersehbar sein, welches Verhalten der Unionsgesetzgeber dem Verantwortlichen abverlangt.[65]

Die Norm erfasst jedenfalls besonders starke Beeinflussungsstrukturen hinreichend klar – bspw. sehr intensive *Nagging*-Patterns, die in sehr kurzen Zeitintervallen Kunden Verarbeitungsberechtigungen abringen. Dieses nutzt die Gestaltungsmacht besonders intensiv aus und ist mit den Prinzipien guten Technikdesigns inkompatibel.[66] Für Gestaltungen von geringerer Intensität – zB leichte *Misdirection*-Patterns, wie grüne Ablehnungs- und rote Zustimmungsschaltflächen – ist die Norm hingegen zu abwägungsoffen und konkretisierungsbedürftig, um unmittelbar als scharfes Schwert zu wirken.

So entpuppt sich Art. 25 Abs. 1 DSGVO im Ergebnis zwar als potenzielle normative Waffe gegen Dark Patterns.[67] Erst durch Konkretisierungen kann sie jedoch zu einem wirkungsvolleren Instrument erwachsen.[68]

c) Zwischenergebnis

Das Datenschutzrecht verbietet bereits de lege lata einige Ausprägungen von Dark Patterns.[69] Es sind aber vorwiegend Einzelformen verhaltenssteuernder Lenkung, etwa vorausgewählte Kästchen oder die Verzerrung von Informationen, die mit seinen Vorgaben konfligieren. Die Spielräume des Gesetzeswortlauts versuchen die Gerichte immer wieder zu nutzen, um auch andere verhaltenslenkende Dynamiken, mithin die Essenz von Dark Patterns, zu adressieren. Diese repräsentieren jedoch einen ganz eigenen Gefahrentyp für die Privatautonomie, den die DSGVO nicht explizit adressiert. Immerhin liefert Art. 25 Abs. 1 DSGVO das grundsätzliche normative Rüstzeug dafür, Designgestaltungsformen zu erfassen, die den Datenschutzgrundsätzen widersprechen. Dieses gilt es zu nutzen und Standards herauszuarbeiten bzw. anhand von Fallbeispielen die Schwelle zu definieren, ab der Verwender missbräuchlich vorgehen, also einseitig ihre Gestaltungsmacht über Oberflächen ausnutzen.

Der Wirkradius der datenschutzrechtlichen Vorschriften unterliegt einer weiteren wichtigen Einschränkung: Sie richten sich grundsätzlich nicht gegen bestimmte Ver-

---

[65] Vgl. etwa *EuGH* ECLI:EU:C:2020:455 = BeckRS 2020, 11912 (Rn. 47 ff.); *Jarass*, GRCh, 4. Aufl. 2021, Art. 49 Rn. 11. Ein gefestigter Forschungsstand kann sich in Zertifizierungen iSd Art. 25 Abs. 3 iVm Art. 42 DSGVO manifestieren.

[66] Sec. 13 CPRA, zur Änderung von Sec. 1798.135 lit. c Nr. 4 Cal. Civil Code (CCPA) schreibt eine Sperrfrist von zwölf Monaten fest, in der Verantwortliche keine Erlaubnis zur Datennutzung anfragen dürfen, sofern Verbraucher diese einmal versagt haben; dazu *Lejeune* ITRB 2021, 13 (14).

[67] *European Data Protection Board* (o. Fn. 59), S. 19.

[68] Den allgemeineren Grundsatz „Privacy by Design" effektiv zu konkretisieren, um Dark Patterns auf Cookie-Einwilligungsfeldern zu vermeiden, scheint außerdem der Entwurf der Europäischen Kommission für eine ePrivacy-VO (S. COM(2017) 10 final [ePrivacy-VO-E]) zu intendieren. Er etabliert die Pflicht, in Browsersoftware eine Funktion einzubauen, die Cookies bzw. Tracking allgemein unterdrücken können (Art. 10 ePrivacy-VO-E). Daneben verpflichtet der Entwurf Anbieter für bestimmte Datenverarbeitungen zu einem „deutlichen Hinweis", „in hervorgehobener Weise", etwa durch „standardisierte Bildsymbole", „um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die Erhebung [von Cookies] zu vermitteln", mithin eine Pflicht zu nutzerfreundlicher Designgestaltung und ein Gegenentwurf zu *Misdirection*-Patterns (Art. 8 Abs. 2 ePrivacy-VO-E). Allerdings tendieren die Mitgliedstaaten im Europäischen Rat derweil dazu, diesen Artikel zu streichen, vgl. COD(2020) 9931, S. 76.

[69] Das Recht, eine Einwilligung zu widerrufen (Art. 7 Abs. 3 S. 1 DSGVO), verheißt kaum eine effektive Handhabe gegen Dark Patterns. Denn nach der erteilten Einwilligung (oder Information über andere Verarbeitungsgrundlagen) werden Nutzer idR nicht mit weiteren Konsequenzen ihrer Entscheidung konfrontiert und verspüren typischerweise wenig Anlass dazu, diese zu überdenken – anders als etwa bei gekauften Sachen, bei denen die Übergabe der Kaufsache materialisiert an die Kaufentscheidung erinnert; s. u. II. 3. a) bb).

arbeitungsinhalte, zB bestimmte Vertragsergebnisse: Das Datenschutzrecht soll zwar das Recht auf Schutz personenbezogener Daten verbürgen, dabei aber nicht ein umfassendes Vertragsinhaltsrecht aus der Taufe heben. Dark Patterns, deren Wirkung darin besteht, den Einzelnen zu einem Vertragsabschluss zu bewegen, ohne ihm zugleich mehr Daten als erforderlich abzuringen, vermag das Datenschutzrecht daher grundsätzlich nicht zu greifen.

3. Vertragsrecht

a) Verbrauchervertragsrecht

Für Anbieter kommerzieller (Shopping-)Webseiten[70] sind Dark Patterns ein reizvoller Weg, um die Reichweite oder den Umsatz zu steigern.[71] Sofern die Anbieter dabei mit Verbrauchern in B2C-Geschäften interagieren, setzen ihnen jedoch die Vorschriften des Verbraucherschutzrechts Grenzen. Obgleich deren Vorgaben nicht explizit auf Dark Patterns abzielen, nehmen sie zum Teil doch ähnliche Wirkmechanismen ins Visier.

aa) Transparenz und Information

Das Verbrauchervertragsrecht tritt beeinflussenden Strategien der Verkaufsförderung primär mit Informations- und Transparenzvorgaben entgegen. Es verpflichtet bspw. Unternehmer bei Verbrauchergeschäften, die Gesamtkosten bereits in der Werbephase auszuweisen.[72] Dies soll *Sunk Cost*-Effekte verhindern, die sich etwa *Hidden Costs*-Patterns zunutze machen,[73] indem sie Nutzer erst in einem späten Bestellschritt über zusätzliche Bearbeitungsgebühren oder höhere Lieferkosten informieren.[74] Alle Zahlungspflichten des Verbrauchers, die über die Hauptleistung hinausgehen, sind außerdem explizit vertraglich festzuhalten; im elektronischen Geschäftsverkehr gilt daher – ähnlich wie im Datenschutzrecht[75] – ein *Opt-out*-Verbot (§ 312a Abs. 3 S. 2 BGB[76]).[77] Für einige Bereiche setzen weitergehende spezielle Regelungen Dark Patterns Grenzen; bei Flugbuchungen etwa gilt sogar ein *Opt-in*-Gebot.[78] Gerade *Sneak into Basket*- sowie *Hidden Costs*-, aber auch *Preselection*-Patterns beschränkt das Verbrauchervertragsrecht damit bereits nachhaltig.

---

[70] Vgl. *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1 (11 f.); mind. 11 % von 11000 überprüften Shopping-Webseiten nutzten textbasierte und automatisiert auswertbare Dark Patterns; die tatsächliche Quote liegt möglicherweise höher.

[71] *Narayanan/Mathur et al.,* acmquere 2020, 67 (75). Vgl. etwa zu *Scarcity*-Patterns *Bundeskartellamt* (o. Fn. 1), S. 106 ff.

[72] § 1 Abs. 1, 2 PAngV; dieser setzt Art. 7 Abs. 1, 2, 4 lit. c UGP-RL um; vgl. auch Erwgr. 39 S. 2 RL (EU) 2019/2161. Über § 3a UWG findet die Norm Eingang ins Lauterkeitsrecht; s. dazu u. II. 4.

[73] *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1 (13). Sunk Costs sind bereits getätigte (und daher jedenfalls „verlorene") Aufwendungen. Sie können den Einzelnen psychologisch dazu verleiten, länger an einem Vorhaben festzuhalten als rational sinnvoll, um die eigenen Investitionen vor sich selbst zu rechtfertigen.

[74] Vgl. *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312a Rn. 75.

[75] S. o., I. 2.

[76] Die Vorschrift setzt Art. 22 Verbraucherrechte-RL um.

[77] Darüber hinaus sind einige Nebenkosten (wie unzumutbare Zahlungsmittelentgelte) generell verboten, § 312a Abs. 4 BGB (Art. 19 Verbraucherrechte-RL); s. dazu *OLG Hamburg* GRUR-RS 2020, 33192.

[78] Art. 23 Abs. 1 S. 4 VO (EG) Nr. 1008/2008 (Luftverkehrsdienste-VO); vgl. auch *EuGH* ECLI:EU:C:2020:301 = MMR 2020, 752 (Rn. 16 ff.). Zum Unterschied zwischen *Opt-out-Verbot* und *Opt-in-Gebot* vgl. *Martini/Weinzierl* RW 2019, 287 (295 ff.).

Digitale, entgeltliche[79] B2C-Geschäftsvorgänge muss der Kunde stets mit einer Schaltfläche final bestätigen, die „mit nichts anderem als den Wörtern ‚zahlungspflichtig bestellen' oder einer vergleichbaren Formulierung" versehen ist (§ 312j Abs. 3, 4 BGB)[80]. Diese *Button-Lösung*[81] ist eine gesetzliche Antwort auf die Praxis, kostenlose Abonnements oder Testphasen automatisch kostenpflichtig zu verlängern, ohne diesen Umstand vor Vertragsschluss transparent zu kommunizieren (sog. Abo-Fallen). Wie streng die Rechtsprechung die Vorgaben der Button-Lösung anwendet, illustriert der Fall des Streamingdienstes *Netflix*: Dieser musste die Formulierung „Mitgliedschaft beginnen kostenpflichtig nach Gratismonat" anpassen. Das KG Berlin sah die Gefahr, dass der Passus „Mitgliedschaft beginnen" die Aufmerksamkeit von der einzugehenden Zahlungsverpflichtung ablenkt.[82]

Teil der Button-Lösung ist ebenso die Pflicht, neben der festgelegten Schaltflächengestaltung auch die anderen zentralen Vertragsinhalte übersichtlich vor Vertragsschluss aufzugliedern (§ 312j Abs. 2 BGB iVm Art. 246a Abs. 1 S. 1 Nr. 4 EGBGB[83]),[84] um über den sich anbahnenden Abschluss eines kostenpflichtigen (Dauer-) Schuldverhältnisses zu informieren.[85] Dies beugt jedenfalls faktisch Fällen von *Forced* oder *Hidden Continuity*-Patterns sowie intransparenten, Verbraucher behindernden Preisdarstellungen (*Price Comparison Prevention*-Patterns) vor.[86]

Darüber hinaus adressieren die verbraucherrechtlichen Vorgaben teilweise die Art und Weise, wie erforderliche Informationen bereitzustellen sind („klar und deutlich", „klar und verständlich", § 312j Abs. 1, 2 BGB)[87]. Wie im Datenschutzrecht ergreift die Rechtsprechung dies als Möglichkeit, auch das Design zu berücksichtigen. So hielt der BGH eine Flugbuchungsgestaltung für unzulässig, die eine nicht optierte Reiserücktrittsversicherung erneut durch ein orange unterlegtes Feld mit der Aufschrift „Weiter – Ich möchte abgesichert sein" neben einem nicht farblich unterlegten und in kleinerer

[79] §§ 312, 310 Abs. 3, 13, 14 BGB. „Entgeltlich" ist richtlinienkonform möglichst weit auszulegen; *Wendehorst* NJW 2014, 577 (580).

[80] Art. 8 Abs. 2 S. 2-4 Verbraucherrechte-RL.

[81] BT-Drs. 17/7745, S. 7; *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312j Rn. 22 ff. Bei einem Verstoß kommt kein Vertrag zustande, § 312j Abs. 4 BGB.

[82] *KG Berlin* GRUR-RR 2020, 273 (274).

[83] Die Vorschrift setzt Art. 8 Abs. 2 S. 1, Art. 6 Abs. 1 lit. e, Abs. 6 Verbraucherrechte-RL um. Für Fernabsatzverträge und außerhalb von Geschäftsräumen geschlossene Geschäfte verweist außerdem § 312d Abs. 1 BGB auf Art. 246a EGBGB; § 312e BGB erklärt solche Nebenkosten für unzulässig, die der Anbieter nicht vorab kommuniziert.

[84] BT-Drs. 17/7745, S. 10 f.; *OLG München* MMR 2019, 249 (249 ff.); *Boos/Bartsch et al.,* CR 2014, 119 (122). S. dazu a. §§ 5a, 5b Referentenentwurf eines Gesetzes zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht (GStVSch-E), 4.11.2020, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Verbraucherschutz_Wettbewerbs-_und_Gewerberecht.html, der noch strengere Informationspflichten vorsieht. Zur Systematik der Informationspflichten s. *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312d Rn. 1 ff.

[85] Art. 8 Abs. 2 UAbs. 1 Verbraucherrechte-RL; vgl. BT-Drs. 17/7745, S. 6 f. Zudem erschwert diese strikte Gestaltungsvorgabe es, den finalen Bestätigungs-Button mit anderen Inhalten zu verknüpfen und diesen so zugleich als Einwilligungserklärung auszugestalten, um nicht-erforderliche Daten verarbeiten zu dürfen; mit dieser Idee aber *Moos/Rothkegel* MMR 2019, 732 (738). Ein rechtmäßiger Bestell-Button ist unter den normativen Prämissen so schlicht gestaltet, dass sein rechtsbindender Gehalt nicht mit anderen Angaben auf der Schaltfläche um Aufmerksamkeit konkurriert. Er vermag insofern den Kunden verlässlich dafür zu sensibilisieren, dass ein abzuschließendes Rechtsgeschäft mit Kosten verbunden ist.

[86] Vgl. am Bsp. der Transparenzvorgaben der Luftverkehrsdienste-VO etwa *BGH* GRUR 2017, 283 (294).

[87] Vgl. darüber hinaus Art. 23 Abs. 1 S. 4 Luftverkehrsdienste-VO: „auf klare, *transparente* und eindeutige Art und Weise" (Herv. d. Verf.).

Schrift gehaltenen Feld mit der Aufschrift „Weiter ohne Versicherung“ anbot.[88] Das Urteil verdeutlicht zugleich die Herausforderungen, Dark Patterns mit rechtlichen Mitteln wirksam die Stirn zu bieten: Die im konkreten Fall genutzten faktischen *Misdirection*- und *Preselection*-Patterns zielen nicht darauf ab, Verbrauchern *falsche* Informationen zuzuführen. Sie operieren vielmehr auf einer unterschwelligen Ebene, indem sie eine Auswahloption komplizierter ausformen als die andere.[89] Das normative Handlungsbesteck passt insofern nicht gänzlich zum regulierten Objekt.[90]

Informations- bzw. Transparenzmaßnahmen verhindern zudem nicht per se, dass Anbieter ausgewählte Aspekte in prominenter Weise betonen oder die Aufmerksamkeit der Nutzer auf andere Weise bereits so beanspruchen, dass Verbraucher an die Grenzen ihrer kognitiven Informationsverarbeitungskapazitäten gelangen.[91] Selbst die Button-Lösung mit ihren konkreten Gestaltungsvorgaben für den finalen Bildschirm adressiert ausschließlich die Darstellung zusammenfassender Informationen bzw. des Bestell-Buttons (in ihrem Verhältnis zueinander).[92] *Scarcity*-Banner, die durch ablaufende Zeitanzeigen Bestelldruck aufbauen,[93] oder (willkürlich generierte) *Social Proof*-Hinweise, die zusätzliche Kaufanreize setzen,[94] lassen sich bspw. durch Transparenzvorgaben nur bedingt beim Schopf packen. Informationsvorgaben sind nur begrenzt und nur gegen bestimmte Einflüsse auf Nutzer in Stellung zu bringen. Subtilere Arten der Manipulation, welche Dark Patterns häufig nutzen, bringen das normative System daher schnell an seine Grenzen.

bb) Widerrufsrechte

Als eines seiner wichtigsten verbraucherschutzrechtlichen Instrumente installiert der Gesetzgeber Widerrufsrechte (§ 355 BGB). Sie vermögen Dark Patterns zwar nicht vollständig zu neutralisieren. Sie können aber deren Wirkung rückgängig machen, indem sie Verbrauchern den Weg ebnen, sich von einem Vertrag zu lösen, der unter dem Einfluss von Dark Patterns zustande gekommen ist. Vor allem für zwei Vertragstypen etabliert der Gesetzgeber solche Abwicklungsrechte: für Fernabsatzverträge (§§ 312c, 312g Abs. 1 BGB) und für außerhalb von Geschäftsräumen geschlossene Verträge („AGV“, ehemals Haustürgeschäfte; §§ 312b, 312g Abs. 1 BGB).

Die Vorschriften zu *AGV* lassen die Risikosensibilität des Gesetzgebers hinsichtlich starker, situativer Verbraucherbeeinflussung erkennen, die im Kern auch Dark Patterns auszeichnet.[95] Die Vorschriften zu *Fernabsatzverträgen* folgen demgegenüber einem anderen Grundgedanken: Verbraucher sollen die Möglichkeit haben, Leistungen nach

---

[88] *BGH* GRUR 2017, 283 (283 ff.).

[89] Vgl. *KG Berlin* MMR 2016, 608 (609).

[90] Anders in Bezug auf § 4a Abs. 1 UWG (§ 4 Nr. 1 UWG aF): *OLG Frankfurt/M.* GRUR 2015, 400 (400 f.); *OLG Frankfurt/M.* MMR 2015, 591 (592) und u., II. 4.

[91] Zur Grenze der Aufnahmefähigkeit *Hacker* (o. Fn. 19), S. 118 ff. UU schmälern auch die Informationspflichten selbst – entgegen ihrem Ziel – die Verständlichkeit von Geschäftsabschlüssen, *Föhlisch* MMR 2017, 447 (448).

[92] BT-Drs. 17/7745, S. 10 ff; vgl. auch *KG Berlin* GRUR-RR 2020, 273 (274).

[93] Dies ist vor allem auf Reisewebseiten ein beliebtes Mittel; die Darstellungen sind (mutmaßlich) häufig irreführend oder sogar falsch, *Bundeskartellamt* (o. Fn. 1), S. 99 ff.

[94] Hiergegen richtet sich allerdings das Verbot gefälschter oder irreführender Kundenbewertungen der Nr. 23b, 23c im Anhang zu § 3 Abs. 3 GStVSch-E.

[95] Das Widerrufsrecht erlaubt eine Abkehr von Verträgen, die an Orten zustande kamen, an denen üblicherweise nicht mit einem Vertragsschluss zu rechnen ist. Es adressiert Geschäftsgebaren, welches die (Überrumpelungs-)Dynamik einer konkreten Entscheidungsumgebung ausnutzt, um Verbraucher zu einem Vertragsschluss zu bewegen (Erwgr. 21 S. 2 ff. Verbraucherrechte-RL). *Eidenmüller* AcP 2010, 67 (82 f.).

der Lieferung „in natura“[96] zu begutachten, ohne abschließend an den Vertrag gebunden zu sein. Denn Vertragsobjekte leiden bei Fernabsatzgeschäften generell unter einer beschränkten Darstell- und Erfahrbarkeit.[97]

Obgleich das Widerrufsrecht für Fernabsatzgeschäfte nicht speziell gegen (digitale) Beeinflussungsmöglichkeiten wirken soll, kann es beeinflussten Verbrauchern ein wirksames Schutzrecht gegen Dark Patterns an die Hand geben. Das sub specie seiner gesetzlichen Zielrichtung besser passende AGV-Widerrufsrecht steht ihnen demgegenüber regelmäßig nicht offen, da dieses die physische Anwesenheit der Beteiligten voraussetzt (§ 312b Abs. 1 BGB).

Selbst wenn das Gesetz Betroffenen ein Widerrufsrecht zugesteht, heißt das allerdings nicht, dass sie hiervon in praxi tatsächlich Gebrauch machen, um sich von Geschäften loszusagen, die unter dem Einfluss von Dark Patterns zustande gekommen sind. Denn in das Bewusstsein eines Großteils der beeinflussten Personen gelangt die Wirkung subtil implantierter Dark Patterns nur selten.[98] Zudem haben Verbraucher bei einem Widerruf grundsätzlich die Rücksendekosten zu tragen (§ 357 Abs. 6 S. 1 BGB) und schrecken tendenziell davor zurück, gefühlte Verluste in Kauf zu nehmen, wenn der in Aussicht stehende Mehrwert, wie im Fall von Alltagsgeschäften, gering scheint (sog. *Loss Aversion*[99]).

Bestehende Widerrufsrechte bieten also keine passgenaue Antwort auf vertragliche Bindungen, die unter der Wirkmacht von Dark Patterns zustande gekommen sind. Sie lassen die nötige normative Sensibilität für die praktischen Implikationen von Verhaltensbeeinflussungen noch vermissen.

b) Allgemeines Vertragsrecht

Obgleich Dark Patterns zumindest begrifflich eine moderne Schöpfung sind, begegnet ihnen das allgemeine Vertragsrecht mit seinen altbewährten Instrumenten längst zumindest punktuell. Eine der normativen Grenzen markiert § 123 Abs. 1 Alt. 1 BGB: Ein Vertragspartner kann nicht nur Rechtsgeschäfte wegen Täuschung anfechten, zu denen der Geschäftspartner eindeutig *falsche* Angaben gemacht hat. Er kann auch solchen Verträgen die Wirksamkeit nehmen, die aufgrund *irreführender* Informationen zustande kamen.[100] Solange die (konkludente) Täuschung auf aktivem Handeln beruht, reicht es aus, dass die falsch dargestellten Umstände materiellrechtlich lediglich aus der Sicht des Getäuschten vertragserheblich waren.[101] Eine Willenserklärung, die auf den Eintrag in ein Online-Branchenverzeichnis abzielt, ist daher bspw. anfechtbar, wenn der Vertragspartner sie aufgrund eines *Hidden Costs*-Pattern, namentlich eines im „Kleingedruckten“ verborgenen Hinweises über anfallende Kosten, in der fälschli-

[96] *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312c Rn. 3.

[97] Erwgr. 14 Fernabsatz-RL; *Wendehorst*, in: Krüger (o. Fn. 96), § 312c Rn. 3. Das Widerrufsrecht gleicht also eine Informationsasymmetrie zwischen Unternehmer und Verbraucher aus; *Hacker* (o. Fn. 19), S. 873 f. Vgl. auch *Schmitt*, Das unionsrechtliche Verbraucherleitbild, 2018, S. 389 f.

[98] *Luguri/Strahilevitz* (o. Fn. 10), S. 24 f.; *Susser/Roessler et al.,* Georgetown Law Technology Review 2019, 1 (26). Solange der Unternehmer den Verbraucher nicht (vollständig) über das Widerrufsrecht unterrichtet hat, beginnt die Frist nicht zu laufen (§ 356 Abs. 3 S. 1 BGB). Es erlischt jedoch in jedem Falle nach zwölf Monaten und 14 Tagen (§ 356 Abs. 3 S. 2 BGB).

[99] *Kahneman*, Thinking, Fast and Slow, 2011, S. 283 ff.

[100] *Armbrüster*, in: Säcker/Rixecker/Oetker et al. (Hrsg,), MüKoBGB, 8. Aufl 2018, § 123 Rn. 29.

[101] *BGH* NJW 1991, 1673 (1674); *Armbrüster*, in: Säcker/Rixecker/Oetker et al. (o. Fn. 100), § 123 Rn. 23.

chen Annahme der Kostenfreiheit abgegeben hat.[102] Allerdings trägt der Getäuschte die Beweislast dafür, dass die Täuschung den Vertragsschluss „nach der allgemeinen Lebenserwartung" beeinflusst hat.[103]

Subtil wirkende Dark Patterns wie unwahre *Scarcity*-Patterns als relevante Auswirkungen auf die menschliche Entscheidungsfindung anzuerkennen, versteht sich nicht von selbst. Es wird aber ihrer faktischen Wirkmacht gerecht, in derartigen Dynamiken eine Täuschung iSd § 123 Abs. 1 Alt. 1 BGB zu erkennen. Irreführende oder erschleichende Dark Patterns[104] können bzw. sollten Schuldverhältnisse also grundsätzlich anfechtbar machen. Andere Muster, wie etwa wahre *Social Proof*- oder *Countdown*-Patterns, erfasst § 123 Abs. 1 Alt. 1 BGB hingegen kategorial nicht. Denn diese wirken, ohne Unwahrheiten zu verbreiten.[105]

Wer Dark Patterns einsetzt, verletzt unter Umständen seine vorvertraglichen Wahrheits- und Aufklärungspflichten aus §§ 311 Abs. 2, 241 Abs. 2 BGB und macht sich damit ggf. nach §§ 280 Abs. 1 S. 1, 311 Abs. 2 Nr. 1, 241 Abs. 2 BGB schadensersatzpflichtig. Das kann (als Folge der gesetzlich vorgesehenen Naturalrestitution) zur Aufhebung eines Vertragsverhältnisses führen.[106] Zwar ist die culpa in contrahendo (c.i.c.) bisher vorwiegend in Fällen von Informationsasymmetrien etabliert. Jedoch zeigt sie sich grundsätzlich auch für Fälle von Rationalitätsasymmetrien zwischen Unternehmern und Verbrauchern offen.[107] Ihr (potenzieller) Anwendungsbereich reicht also über denjenigen des § 123 Abs. 1 Alt. 1 BGB hinaus.

4. Lauterkeitsrecht

Das Lauterkeitsrecht schützt nicht nur die Mitbewerber und das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb, sondern auch die Entscheidungsfreiheit der Verbraucher, insbesondere ihre Fähigkeit, eine informierte Entscheidung zu treffen (§ 1 UWG).[108] Diese Entscheidungsfreiheit drohen Dark Patterns zu unterlaufen. Dem Grenzen zu setzen, ist das Lauterkeitsrecht als Instrument prädestiniert.

a) Anwendbarkeit des UWG

Das UWG ist nur auf „geschäftliche Handlung[en]" iSd § 2 Abs. 1 Nr. 1 UWG anwendbar.[109] Der denkbar weite Terminus erfasst sämtliche Maßnahmen, die dem eigenen Geschäftszweck dienen.[110] Er umschließt das Vorfeld und den Nachgang eines kon-

---

[102] Vgl. *AG Miesbach* MMR 2001, 837 (837 f.); *AG Dresden* NJW-RR 2002, 1137 (1138). Dies löst allerdings auch Konflikte mit den Transparenzgeboten des Verbraucherschutzrechts aus, s. o. II. 3. aa).

[103] *BGH* NJW 1995, 2361 (2362); *Asmussen* NJW 2017, 118 (121 f.).

[104] Zu denken ist etwa an *Hidden Subscription*-, *Hidden Information*- oder *Trick Question*-Patterns sowie willkürlich generierte *Social Proof*- oder *Scarcity*-Patterns.

[105] Insofern ebenso *Ebers* MMR 2018, 423 (426).

[106] Zum Verhältnis von Anfechtung und Schadensersatzanspruch aus c.i.c. s. *Armbrüster*, in: Säcker/Rixecker/Oetker et al. (o. Fn. 100), § 123 Rn. 102 ff. mwN.

[107] *Ebers* MMR 2018, 423 (426).

[108] *Sosnitza*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 1 Rn. 27 mit Verweis auf Art. 2 lit. e, k UGP-RL.

[109] *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (Hrsg.), Beck-KK UWG, 39. Aufl. 2020, § 2 Rn. 3.

[110] *Sosnitza*, in: Ohly/Sosnitza (Hrsg.), UWG, 7. Aufl. 2016, § 2 Abs. 1 Nr. 1 Rn. 8. Der Gesetzgeber beabsichtigt allerdings (insbes. zum Schutze „privater Meinungsäußerung" von sog. „Influencern"), den Wortlaut der Norm etwas einzuengen (nun „unmittelbarer", statt „objektiver" Zusammenhang), vgl. GStVSch-E, S. 19. Ob dies an der Auslegung der Norm substanziell etwas ändern

kreten Geschäftsabschlusses, insbesondere die Außendarstellung in Gestalt von Werbung.[111] Das schließt auch die Nutzeroberflächengestaltung einer Webseite oder App ein, die – insbesondere via Werbung – Einnahmen generieren soll, mithin auch den Einsatz von Dark Patterns.

b) Unzulässigkeitstatbestände der „Schwarzen Liste"

Die „Schwarze Liste" des Anhangs zu § 3 Abs. 3 UWG[112] erfasst einige Dark Patterns und schiebt deren Einsatz im geschäftlichen Verkehr damit jedenfalls gegenüber Verbrauchern einen Riegel vor.

Besonders sticht *Nr. 6* der Liste hervor, welche die UGP-RL als *Bait and Switch*-Technik bezeichnet. Der Tatbestand schützt Verbraucher davor, dass der Anbieter eine Nachfrage durch irreführende Angaben gezielt manipulativ umleitet:[113] Er verbietet, eine andere als die beworbene Ware oder Dienstleistung abzusetzen. Auch ein Dark Pattern aus der Kategorie der Irreführung trägt den Namen *Bait and Switch*. Bei diesem führt der Klick auf eine Schaltfläche zu einem anderen als dem üblicherweise erwarteten Ergebnis – etwa indem ein Button durch sein „X"-Design suggeriert, er schließe ein Pop-up-Fenster, stattdessen dem Nutzer aber auf eine unerwartete Seite weiterleitet.[114] Während sich die Nr. 6 des Anhangs nur auf eine sehr spezifische Situation bezieht, ist das *Bait and Switch*-Pattern vielfältiger. Insbesondere beschränkt sich sein manipulatives Umleitungselement nicht auf konkrete „Waren- oder Dienstleistungsangebote". Das Dark Pattern erfasst Nr. 6 daher grds. nicht.

Nr. 7 verbietet unwahre Angaben über die begrenzte Verfügbarkeit von Waren oder Dienstleistungen. Die Vorschrift soll Geschäftspartner vor Entscheidungsdruck schützen, der in möglicherweise unüberlegte Kaufentscheidungen mündet.[115] Dies kann insbesondere *Scarcity*-Patterns Grenzen setzen, die genau diesen Entscheidungsdruck aufbauen. In Gestalt graphisch hervorgehobener Hinweisflächen suggeriert dieses Pattern auf Buchungs- oder Bestellplattformen eine knappe Verfügbarkeit. Der Wirkradius der Nr. 7 unterliegt jedoch einer wichtigen Schranke: Er zielt auf „unwahre", dh objektiv unrichtige Angaben,[116] operiert also in einer Richtig/falsch-Binarität. *Scarcity*-Patterns können diesen Richtig/falsch-Bereich schnell verlassen, etwa durch frei gesetzte Countdowns oder graphische Gestaltungen. Ist ein Gegenstand im virtuellen Warenkorb tatsächlich nur für 15 Minuten reserviert, mag dies zwar willkürlich, aber trotzdem wahr sein.[117] Nicht eindeutig falsch ist etwa die Angabe „*n* Nutzer sehen sich das gerade an"[118], auch wenn sich diese auf das begutachtete Hotel generell und nicht kon-

---

wird, erscheint jedoch zweifelhaft. Denn die Änderung übernimmt lediglich den Wortlaut des (für die Auslegung ohnehin bereits maßgeblichen) Art. 2 lit. d UGP-RL.

[111] *Bähr*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 2 Rn. 121 ff. Vgl. Art. 1 lit. d UGP-RL.

[112] Er entstammt dem weitgehend wortgleichen Anhang I der UGP-RL.

[113] *Obergfell*, in: Fezer/Büscher/Obergfell (Hrsg.), UWG, 3. Aufl. 2016, Anhang zu § 3 Abs. 3 Nr. 6 Rn. 4.

[114] *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (6 f.).

[115] *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (Hrsg.), Beck-KK UWG, 39. Aufl. 2020, Anhang zu § 3 Abs. 3 Rn. 7.6.

[116] Ob die Behauptung ausdrücklich erfolgen muss, ist str.; dafür: *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (o. Fn. 115), Anhang zu § 3 Abs. 3 Rn. 7.3; aA (auch konkludente Behauptungen werden erfasst) *Sosnitza*, in: Ohly/Sosnitza (Hrsg.), UWG, 7. Aufl. 2016, Anhang (zu § 3 Abs. 3) Rn. 25.

[117] Vgl. *Bundeskartellamt* (o. Fn. 1), S. 107 f. Teilweise nehmen derartige Hinweise auf Vergleichsportalen die Hälfte der Bildschirmanzeige ein.

[118] *Bundeskartellamt* (o. Fn. 1), S. 107.

kret im angegebenen Buchungszeitraum bezieht. Die Muster wirken dann nicht durch eine Täuschung, sondern durch eine emotionale oder auf Biases und Heuristiken zielende Steuerung. Deren Wirkungsweise vermag Nr. 7 nicht zu erfassen.

Misdirection-Patterns können gegen die Verbote aus *Nr. 8* (Sprachenwechsel[119]) verstoßen, *Hidden Costs*-Patterns gegen *Nr. 21* (kostenpflichtige Gratisleistungen) und *Sneaking*-Patterns gegen *Nr. 22* (Täuschung über abgegebene Bestellungen). Die UGP-Änderungs-RL[120] nimmt zudem das Verbot gezielt gefälschter sowie als authentisch präsentierter, aber ungeprüfter Verbraucherbewertungen[121] (Fälle des *Social Proof*-Patterns) sowie verdeckte Werbung in Online-Suchergebnissen (*Disguised Ads*-Pattern) in die Schwarze Liste auf.[122]

Gleichwohl zeigt sich, dass die Schwarze Liste des UWG Dark Patterns nicht systematisch erfasst. Gerade Nr. 6 und Nr. 7 machen den Grund dafür beispielhaft deutlich: Ihren Verboten unterfallen verhaltenssteuernde Wirkungsweisen nicht generell, sondern alleine einzelne Ausprägungen.

c) Verbotstatbestände der §§ 4 ff. UWG

Innerhalb der Verbotstatbestände der §§ 4 ff. UWG öffnen insbesondere die verbraucherschützenden §§ 4a, 5, 5a und 7 UWG Einfallstore für Verbote von Dark Patterns.

§ 4a Abs. 1 S. 1 UWG verbietet „aggressive geschäftliche Handlungen", die den Betroffenen zu geschäftlichen Entscheidungen[123] veranlassen, welche er „andernfalls

---

[119] Vgl. die Bezeichnungen der einzelnen Nrn. entnommen aus *Sosnitza*, in: Ohly/Sosnitza (o. Fn. 116), Anhang (zu § 3 Abs. 3) Rn. 7 ff.

[120] RL (EU) 2019/2161, Art. 3 Abs. 7. lit. a, b.

[121] Dazu sollen bereits „Likes" gehören; Erwgr. 49 RL (EU) 2019/2161 (UGP-Änderungs-RL).

[122] Vgl. Art. 1 Nr. 9 GStVSch-E: neue Nrn. 11, 23b u. 23c Anhang zu § 3 Abs. 3 UWG.

[123] Der Begriff (legaldefiniert in § 2 Abs. 1 Nr. 9 UWG) markiert das Pendant zu der „geschäftlichen Handlung" iSd § 2 Abs. 1 Nr. 1 UWG auf Seiten der Verbraucher bzw. sonstigen Marktteilnehmer (*Bähr*, in: Heermann/Schlingloff [o. Fn. 111], § 2 UWG Rn. 362). „Geschäftlich" iSd Norm ist die Entscheidung schon dann, wenn sie mit dem (potenziellen) Abschluss von „Geschäften" bzw. der Ausübung von vertraglichen Rechten in Zusammenhang steht. Dies umschließt rechtsgeschäftliche Handlungen und vorbereitende Realakte, wie das Betreten eines Geschäfts oder das Aufrufen eines kommerziellen Online-Portals (*BGH* GRUR 2016, 1073 [Rn. 34]; *BGH* GRUR 2017, 1269 [Rn. 19]). Das Entscheidungsverhalten der Nutzer, welches Dark Patterns in der digitalen Welt beeinflussen, ist idR eine solche geschäftliche Entscheidung. Weniger eindeutig zu beantworten ist hingegen, ob ein Verbraucherverhalten nur dann „geschäftlich" ist, wenn die bereitgestellten Leistungen entgeltlich sind bzw. sie sich durch potenzielle geldwerte Veränderungen im Vermögen eines Verbrauchers auswirken (*Köhler*, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 156a; aA *Omsels,* WRP 2016, 553, [559])). Bedeutsam ist diese Frage insbesondere mit Blick auf Online-Leistungen, die (vermeintlich) kostenlos erscheinen. Jedenfalls aus der Möglichkeit, kostenpflichtige Zusatzangebote zu buchen, erwächst eine (potenzielle) entgeltliche Vertragsbeziehung (*Köhler*, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 156a). Dies betrifft zB Premium-Accounts oder hinter einer Paywall verdeckte Zeitungsartikel; selbst der Aufruf zum „Spenden" dürfte darunter fallen. Werbung bloß zur Kenntnis zu nehmen, begründet hingegen noch keine „geschäftliche Entscheidung" (*BGH* GRUR 2015, 698 [Rn. 20]). Doch wenn Nutzer mit ihren persönlichen Daten (insbesondere via Cookies oder anderweitige Tracking-Technologien zur personalisierten Werbung) „bezahlen" (können) – folglich ein dreiseitiger Markt besteht – liegt „Geschäftlichkeit" vor (vgl. *Köhler*, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 159): Die eigenen Daten sind den „wirtschaftlichen Interessen der Verbraucher" iSd Art. 1 UGP-Richtlinie zuzurechnen. Schließlich zeichnen sie sich aus Unternehmenssicht durch einen substanziellen wirtschaftlichen Wert aus (vgl. *Mischau,* ZEuP 2020, 335 [337 f.]). Die Entscheidung der Nutzer, diese Daten preiszugeben, ist das marktbezogene Pendant (vgl. *Omsels* WRP 2016, 553 [556 f.]) zur geschäftlichen Handlung der Verwender, Werbe-Tracking einzusetzen – ebenso wie es eine geschäftliche Entscheidung der Nutzer darstellt, persönliche Daten, wie zB die E-Mail-Adresse, im Rahmen von Gewinnspielen zu überlassen (so *Bähr*, in:

nicht getroffen hätte“. Dies kommt der herkömmlichen Definition von Dark Patterns sehr nahe.

Insbesondere Belästigungen, Nötigungen und unzulässige Beeinflussungen beeinträchtigen „die Entscheidungsfreiheit“ iSd Norm (§ 4a Abs. 1 S. 2 UWG). Solche Kategorien von Dark Patterns, die den Nutzer unter Druck setzen (insb. *Nagging*-Patterns), lassen sich als „Belästigung“ einordnen. Die Tatbestände der „unzumutbaren Belästigungen“ (§ 7 UWG), die vor allem auf Werbung abzielen, können weitere Konstellationen von *Nagging*- oder *Obstruction*-Patterns erfassen. Gerade solche Ausgestaltungen, die in Gestalt von Pop-ups oder „Interstitials“[124] den Bildschirm des Nutzers entweder einnehmen oder ihn zum Wegklicken nötigen, können unzumutbar sein. Jedenfalls gilt dies für Pop-ups ohne Schließmöglichkeit.[125] Für spezifische Arten von Werbung erfordert § 7 Abs. 2 Nr. 2, 3 UWG zudem eine „ausdrückliche Einwilligung“, für die dieselben Grundsätze wie unter Art. 7 DSGVO gelten.[126] Dark Patterns, die auf operativen Zwang setzen, lassen sich im Extremfall als „Nötigung“ (§ 4a Abs. 1 S. 2 Nr. 2 UWG) und solche der Kategorie „Irreführen“ als „unzulässige Beeinflussung“ (§ 4a Abs. 1 S. 2 Nr. 3, S. 3 UWG) qualifizieren.

§ 4a Abs. 1 S. 1, 2 UWG setzt jedoch voraus, dass die aggressive Handlung *erheblich* ist. Die Erheblichkeit bemisst sich nach den Kriterien des Abs. 2. Nicht jede Art von Dark Patterns überschreitet diese Schwelle. „Hindernis“-Patterns, wie das *Roach Motel*-Pattern, gehen gleichwohl im Regelbeispiel des § 4a Abs. 2 Nr. 4 UWG auf: Er adressiert „belastende oder unverhältnismäßige Hindernisse nichtvertraglicher Art“, die den Einzelnen davon abhalten, ihm zustehende vertragliche Rechte auszuüben.

§§ 5, 5a UWG können insbesondere Dark Patterns der Kategorien „Erschleichen“ oder „Irreführen“ erfassen. Ebenso wie § 4a Abs. 1 S. 1 UWG rekurriert § 5 Abs. 1 S. 1 UWG auf geschäftliche Entscheidungen des Betroffenen, die er „andernfalls nicht getroffen hätte“. Während die Informations- und Transparenzpflichten des Verbrauchervertragsrechts den Fokus primär auf den *Inhalt* der erforderlichen Informationen sowie deren Bereitstellung richten,[127] gehen §§ 5, 5a UWG darüber hinaus: Ihre Terminologie („Irreführung“, „Täuschung“) erfasst Praktiken, welche die *Informationsverarbeitung* gezielt manipulieren oder erschweren.[128] Das gilt insbesondere – mit Blick auf Dark Patterns – für die 2. Alt. des § 5 Abs. 1 S. 2 UWG: „sonstige zur Täuschung geeigneten Angaben“. Sie verlässt die Richtig/falsch-Binarität und kann damit den subtilen Wirkmechanismen vieler Dark Patterns womöglich die Stirn bieten.[129] So kann § 5

Heermann/Schlingloff [o. Fn. 111], § 2 UWG Rn. 381; Köhler, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 159). Keine „geschäftlichen Entscheidungen“ sind allenfalls Nutzerverhaltensweisen auf nicht-kommerziellen Plattformen oder Webseiten, die sich ausschließlich durch nicht-personalisierte Werbung finanzieren. Reagiert der Nutzer jedoch aktiv auf die (nicht-personalisierte) Werbung, etwa per Klick auf den Werbe-Link, ist dies wiederum – anders als der bloße Konsum der sonstigen Website-Inhalte – eine geschäftliche Entscheidung.

[124] *Interstitials* öffnen anders als Pop-ups kein neues Fenster, sondern überblenden den eigentlichen Seiteninhalt einer Website für einen gewissen Zeitraum mit Werbung.

[125] Teilweise hält die Lit. Pop-ups unabhängig von einer Schließmöglichkeit generell für wettbewerbswidrig; So *Mankowski*, in: Fezer/Büscher/Obergfell (Hrsg.), UWG, 3. Aufl. 2016, Wettbewerbsrecht des Internets (S 12) Rn. 149 mwN.

[126] *BGH* NJW 2020, 2540 (Rn. 31). Vgl. o. I. 2. a).

[127] S. o. I. 3. a) aa).

[128] Vgl. etwa *EuGH* ECLI:EU:C:2015:361 = GRUR 2015, 701 (702); *LG München I* MMR 2016, 257 (259 f.).

[129] Der BGH stuft eine geschäftliche Handlung iSv § 5 Abs. 1 UWG dann als irreführend ein, wenn das Verständnis, das sie bei den Verkehrskreisen, die sie adressiert, erweckt, mit den tatsächlichen Verhältnissen nicht übereinstimmt, s. *BGH* GRUR 2016, 1193 (Rn. 20); *BGH* GRUR 2018, 1263

Abs. 1 S. 2 Nr. 1 UWG („wesentlichen Merkmale der Ware oder Dienstleistung wie Verfügbarkeit") im Gegensatz zu Nr. 7 der Schwarzen Liste (die nur „unwahre Angaben" betrifft) Formen von *Scarcity*-Patterns erfassen, welche eine knappe Verfügbarkeit von Leistungen nicht behaupten, sondern lediglich suggerieren – zB durch einen Countdown, der gar nicht erklärt, was nach Ablauf der Zeit geschieht. Die Art und Weise der Preisberechnung (§ 5 Abs. 1 S. 2 Nr. 2 UWG) können die „erschleichenden" Dark Patterns, wie *Sneaking*- oder *Hidden Costs*-Patterns, betreffen. Zudem bietet Online-Shopping technische Möglichkeiten, mit Hilfe getrackter Daten für den Nutzer individuelle Preise zu generieren, ohne dass der Nutzer dies erkennen kann. Darauf antwortet der Normgeber bislang lediglich außerhalb des Lauterkeitsrechts mit einer Informationspflicht.[130]

§ 5a Abs. 2 UWG stuft es als unlauter ein, wesentliche Informationen vorzuenthalten. Dem steht es gleich, wesentliche Informationen „in unklarer, unverständlicher oder zweideutiger Weise" bereitzustellen (§ 5a Abs. 2 S. 2 Nr. 2 UWG). Die Vorschrift bietet damit einen Schutzschild gegen irreführende Dark Patterns, wie *Trick Question* oder *Hidden Information*-Patterns. Sie erfasst aber auch die Fälle graphischer *Interface*-Manipulation – etwa wenn der Anbieter Buttons oder Text „versteckt", indem er ihn zB ausgraut, verkleinert oder am Rand platziert.[131] Einen Gesamtpreis nicht zu erwähnen – ein Musterbeispiel des *Sneaking*- oder der *Hidden Costs*-Patterns –, erklärt § 5a Abs. 3 UWG explizit für unzulässig. Flugangebote, die Zusatzkosten für Aufgabegepäck verschweigen, verstoßen gegen § 5a Abs. 2, 4 UWG.[132]

Die UGP/UWG-Novelle statuiert zudem neue Informations- und Transparenzpflichten für die Parameter von Rankingergebnissen in Suchmaschinen sowie die Authentizität von Verbraucherbewertungen.[133] *Social Proof*-Patterns, die zwar authentische, aber selektiv positive Bewertungen platzieren, erfasst die Änderung hingegen nicht.

d) Verbrauchergeneralklausel und Rechtsbruchtatbestand

Neben den speziellen Verbotstatbeständen der §§ 4 ff. UWG wirkt die Verbrauchergeneralklausel des § 3 Abs. 2 UWG als Auffangtatbestand wettbewerbsgefährdenden Steuerungen von Verbrauchern entgegen. Ihre zentrale Tatbestandsvoraussetzung ist neben einem Verstoß gegen die unternehmerische Sorgfalt die „wesentliche Beeinflussung des wirtschaftlichen Verhaltens des Verbrauchers". Maßgeblich ist also – ähnlich wie in §§ 4a Abs. 1 S. 1, 5 Abs. 1 S. 1 UWG und entsprechend der üblichen Definition von Dark Patterns –, dass dessen Entscheidung ohne unternehmerische Einwirkung anders ausge-

(Rn. 11). Entscheidend ist letztlich, dass die (durch das Verbraucherleitbild bestimmte) Verkehrsauffassung und die objektive Realität auseinanderfallen. Auch objektiv zutreffende, aber unklare oder mehrdeutige Angaben können irreführend sein: s. *Ruess*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 5 Rn. 184 ff.

[130] Art. 6 Abs. 1 Verbraucherrechte-RL (geändert durch RL (EU) 2019/2161). Um der unionsrechtlichen Vorgabe Rechnung zu tragen, beabsichtigt die Bundesregierung, Art. 246a EGBGB entsprechend zu ergänzen; s. Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuchs und des Einführungsgesetzes zum Bürgerlichen Gesetzbuche in Umsetzung der EU-Richtlinie zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union und zur Aufhebung der Verordnung zur Übertragung der Zuständigkeit für die Durchführung der Verordnung (EG) Nr. 2006/2004 auf das Bundesministerium der Justiz und für Verbraucherschutz, 13.1.2021, abrufbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Bereitstellung digitalerInhalte_2_Modernisierungsrichtlinie.pdf.

[131] Vgl. dazu *LG München I* MMR 2016, 257 (259 f.).

[132] *OLG Dresden* GRUR-RR 2020, 519; s. o., I. 3. a) aa).

[133] Art. 3 RL (EU) 2019/2161; § 5b Abs. 2, 3 UWG nF, vgl. GStVSch-E, S. 30 ff.

fallen wäre. Ob eine Beeinflussung in concreto die Bagatellschwelle der Wesentlichkeit überschreitet, hängt ua von der Häufigkeit, Intensität und Dauer der geschäftlichen Handlung ab.[134] Der weite Wirkradius, den Dark Patterns kraft ihrer örtlichen und zeitlichen Entgrenzung im Internet entfalten, indiziert eine solche Spürbarkeit grundsätzlich.

Der Rechtsbruchtatbestand des § 3a UWG ermöglicht es ferner, mit lauterkeitsrechtlichen Mitteln gegen Rechtsverstöße aus *anderen* Rechtsgebieten, wie Verletzungen berufs-, produkt- oder vertriebsbezogener[135] Normen, vorzugehen.[136] Mit seiner Hilfe können Wettbewerber und Verbraucherschutzorganisationen insbesondere gegen *Hidden Information*- sowie *Hidden Costs*-Dark Patterns intervenieren, die gegen Informationspflichten, etwa aus der PAngV oder der Luftverkehrsdienste-VO[137], aus § 5 TMG oder aus §§ 312a,[138] 312d Abs. 1, 312i BGB[139] verstoßen.[140]

e) Zwischenergebnis

Dark Patterns fallen grundsätzlich in den sachlichen Anwendungsbereich des UWG. Es adressiert diese zwar ebenso wie das sonstige Recht nicht als solche; seine Schwarze Liste wirft vielmehr eher zufällig und ohne phänomenspezifisches Gesamtkonzept Schlaglichter auf einzelne seiner Spielarten. Einige Ansätze des UWG erfassen ihre Wirkprinzipien allerdings zumindest partiell. Dies gilt insbesondere für die Kategorien der Druck ausübenden (über §§ 4a, 7 UWG) sowie der erschleichenden und irreführenden Dark Patterns (über §§ 5, 5a UWG).

Der Schutz der individuellen Entscheidungsautonomie („Entscheidungen", die man ohne einen bestimmten externen Einfluss „nicht getroffen hätte"), durchzieht das UWG wie ein roter Faden.[141] Es schützt zumindest deren *äußere* Komponente, dh die äußere Handlungsfreiheit, indem es Informationspflichten verankert. Viele Dark Patterns greifen jedoch vornehmlich die *innere* Handlungsfreiheit an,[142] indem sie die Art und Weise der Informationswahrnehmung und -verarbeitung manipulieren und dabei verhaltenspsychologische Schwächen ausnutzen. Ob der Unionsgesetzgeber auch den Schutz der inneren Handlungsfreiheit im Blick hatte, ist unklar.[143] In einigen Referenzfällen hat die

---

[134] *Sosnitza*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 3 Rn. 129. Dies bedeutet im Umkehrschluss aber nicht, dass eine unlautere Handlung schon deshalb nicht spürbar ist, weil sie nur einmal oder nur für kurze Zeit vorgenommen worden ist: so *BGH* GRUR 2011, 842 (Rn. 21). Auch nur vereinzelt eingesetzte, dafür aber umso wirkmächtigere Dark Patterns können demnach spürbar sein.

[135] Vgl. die Fallgruppen bei *Ohly*, in: Ohly/Sosnitza (Hrsg.), UWG, 7. Aufl. 2016, § 3a Rn. 31 ff.

[136] Neben einer das Marktverhalten regelnden Tendenz muss der Rechtsverstoß aber im Einzelfall eine *spürbare* Beeinträchtigung der Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern zur Folge haben. Die Kriterien für eine solche Spürbarkeit entsprechen denen der „Wesentlichkeit" iSd § 3 Abs. 2 UWG. Vgl. *Ohly*, in: Ohly/Sosnitza (o. Fn. 135), § 3a Rn. 30c.

[137] So auch der BGH im Reiserücktrittsversicherungs-Fall (s. o. Fn. 88).

[138] *OLG Hamburg* GRUR-RS 2020, 33192.

[139] *Mankowski*, in: Fezer/Büscher/Obergfell (o. Fn. 125), Wettbewerbsrecht des Internets (S 12), Rn. 182, 205, 223.

[140] Im Anwendungsbereich der UGP-RL dürfte daneben ohnehin § 5a Abs. 2, 4 UWG einschlägig sein. Ob er § 3a UWG sogar verdrängt, darüber gehen die Meinungen auseinander, jedenfalls ist die Norm insoweit richtlinienkonform auszulegen, vgl. *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (Hrsg.), Beck-KK UWG, 39. Aufl. 2020, Vorbemerkungen PAngV Rn. 5; *Ohly*, in: Ohly/Sosnitza (o. Fn. 135), § 3a Rn. 75.

[141] Vgl. §§ 2 Abs. 1 Nr. 8, 4a Abs. 1 S. 1, 5 Abs. 1 S. 1, 5a Abs. 2 Nr. 2, Abs. 6 UWG.

[142] Vgl. zur Abgrenzung von innerer und äußerer Handlungsfreiheit *Micklitz/Namysłowska*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, UGP-Richtlinie Art. 1 Rn. 9.

[143] Vgl. *Micklitz/Namysłowska*, in: Heermann/Schlingloff (o. Fn. 142), UGP-Richtlinie Art. 1 Rn. 10. Immerhin spricht der Gesetzgeber zB im Rahmen des § 4a UWG mittlerweile von „psychisch

deutsche Rechtsprechung immerhin eine Unlauterkeit mit der mangelhaften *Art und Weise* der Informationsbereitstellung durch Designpraktiken im digitalen Raum begründet.[144] Eine *systematische* Aufarbeitung des internen Entscheidungsfindungsprozesses – und damit der subtilen Wirkmechanismen von Dark Patterns – findet dagegen nicht statt.[145]

5. Sonstige einfachgesetzliche Rechtsmaterien, insbesondere Medienrecht

Neben dem Datenschutz-, Vertrags- und Lauterkeitsrecht berühren Dark Patterns eine Vielzahl weiterer Rechtsbereiche – vom Strafrecht (etwa wegen tatbestandlicher Täuschungshandlung iSd § 263 Abs. 1 StGB durch Abo-Fallen)[146] bis hin zum Recht der Telemedien. Das TMG wird vergleichsweise konkret: Es trägt Diensteanbietern Kennzeichnungspflichten auf, die „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar" ausgestaltet sein müssen (§ 5 Abs. 1). Das ermöglicht es, das Design besonders in den Blick zu nehmen und so *Hidden Information* und *Click Fatigue*-Patterns normativ zu greifen. So hat die Rechtsprechung bereits längere oder verschlungene Klickwege für unzulässig erachtet[147] – ebenso wie eine „kleine, blasse und drucktechnisch nicht hervorgehobene Schrift"[148]. Ähnliche Formulierungen („leicht zugänglich"; „öffentlich und leicht verfügbar"), welche die Informations- und Transparenzpflichten flankieren, verwendet die neue P2B-Verordnung – etwa für die Offenlegung von Ranking-Parametern durch Suchmaschinen oder die Zugänglichkeit eines Beschwerdemanagementsystems.[149] Weitere derartige Vorschriften finden sich im NetzDG („leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Verfahren")[150], im ePrivacy-VO-E („leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form", Art. 8 Abs. 3)[151] sowie im Medienstaatsvertrag („leicht wahrnehmbar, unmittelbar erreichbar und ständig verfügbar", §§ 85, 93 Abs. 1 MStV). Der MStV adressiert überdies explizit die nutzerfreundliche Designgestaltung. Er definiert den Begriff der „Benutzeroberfläche" (§ 2 Nr. 15 MStV) und hält Regelungen vor, die Medienangebote (leicht) auffindbar machen sollen. So hat der „in einer Benutzeroberfläche vermittelte Rundfunk in seiner Gesamtheit auf der ersten Auswahlebene unmittelbar erreichbar und leicht auffindbar zu sein" und darf die Auffindbarkeit einzelner Angebote nicht „unbillig behinder[n]" (§ 84 Abs. 3, 2 MStV). Der MStV verfolgt damit allerdings nicht das Ziel, Verbraucher vor verhaltenssteuernden Maßnahmen zu schützen, sondern Medienvielfalt und einen fairen Wettbewerb der Meinungen sicherzustellen.

---

vermittelten Zwang", ohne aber näher auf die psychologischen Wirkmechanismen einzugehen: vgl. GStVSch-E, S. 18 f.

[144] Vgl. *LG Berlin* MMR 2005, 778 (779); *LG München I* MMR 2016, 257 (259 f.).

[145] Vgl. *Omsels* WRP 2016, 553 (Rn. 19).

[146] *BGH* NJW 2014, 2595 (2596 ff.). S. zu Abo-Fallen II. 3. a) aa).

[147] *LG Düsseldorf* MMR 2003, 340; vgl. auch *OLG Düsseldorf* MMR 2014, 393.

[148] *OLG Frankfurt/M.* K&R 2009, 197.

[149] Art. 5 Abs. 2, 10 Abs. 1, 11 Abs. 1 UAbs. 2, Abs. 4 UAbs. 1 VO (EU) 2019/1150 (P2B-VO).

[150] § 3 Abs. 1 NetzDG. Dieses Verfahren soll nach einem Regierungsentwurf in Zukunft zudem „leicht bedienbar" sein, vgl. Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes, 1.4.2020, abrufbar unter: https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html, S. 3, 48.

[151] COM(2017) 10 final (ePrivacy-VO-E).

III. Herausforderungen bei der Rechtsdurchsetzung

Dark Patterns sind typischerweise sehr subtil konstruiert. So können die Hintergrundgestaltung von Webseiten oder vorsichtig gestaltete beeinflussende Entscheidungsarchitekturen bereits eine erhebliche Wirkung entfalten, ohne Nutzer sonderlich zu irritieren.[152] Das erschwert die Bemühungen, wirksam gegen sie vorzugehen.

Selbst wenn der aufmerksame Nutzer ein unzulässiges Dark Pattern dechiffriert hat, schränken Probleme bei der Beweissicherung nicht selten die Möglichkeiten der Rechtsdurchsetzung ein:[153] Dark Patterns sind oft flüchtig und für den Einzelnen schwer reproduzierbar. Ihre Wirkung ist häufig prozessbezogen und lässt sich dann nicht ohne Weiteres in Bildern einfangen. Beweissichere Methoden erfordern eine hohe technische Kompetenz.[154]

Verbandsklagen nach dem UWG oder UKlaG[155] (bzw. in Zukunft auf Grundlage der neuen Verbandsklage-RL[156]) sowie ggf. der öffentliche Pranger[157] können dieser strukturellen Hilflosigkeit des Einzelnen ein Stück weit abhelfen. Sofern Verbraucherschutzbehörden von Amts wegen tätig werden, ermöglicht die CPC-Verordnung[158] ein koordiniertes, unionsweites Vorgehen. Über diesen Weg erwirkte bspw. die federführende niederländische Datenschutzbehörde gegenüber dem Portal Booking.com, auffällige verbraucherschutzwidrige Praktiken einzustellen[159] – darunter auch (wenngleich nicht als solche bezeichnete) Dark Patterns. Zudem stehen den Aufsichtsbehörden Nachforschungsbefugnisse, wie Auskunftsbegehren, gegenüber den Verantwortlichen zu (Art. 58 Abs. 1 lit. a DSGVO). Auf diese Weise könnten sie (in den Grenzen ihrer datenschutzrechtlichen Kompetenzen) etwa in Erfahrung bringen, ob ein Anbieter Dark Patterns testet oder gar personalisiert. Die novellierte UGP-RL droht Anbietern nun auch höhere, umsatzabhängige Bußgelder an.[160] Sie verlangt zudem einen Zugang zu angemessenen und wirksamen Rechtsbehelfen, einschließlich Schadensersatz.[161] Dies eröffnet Verbrauchern und ihren Schutzorganisationen grundsätzlich einen Weg, um gegen Dark Patterns vorzugehen.

Die Heterogenität der individuellen menschlichen Reaktionsmuster erschwert die Aufgabe der Rechtsdurchsetzung allerdings weiter. Denn Dark Patterns wirken bei Menschen mit verschiedenen Eigenschaften und Hintergründen unterschiedlich und lassen sich angepasst an individuelle Schwächen ausspielen.[162] Platzieren Anbieter ge-

---

[152] *Luguri/Strahilevitz* (o. Fn. 10), S. 24 ff.; *Mandel/Johnson,* J Consum Res 2002, 235 (240 ff.).

[153] Vgl. *Ebers* MMR 2018, 423 (427).

[154] *Mankowski*, in: Fezer/Büscher/Obergfell (o. Fn. 125), Wettbewerbsrecht des Internets (S 12) Rn. 314 ff. Dies gilt umsomehr, als einfache Ausdrucke oder Screenshots von Webseiten sich leicht manipulieren lassen und daher nur eingeschränkte Beweiskraft entfalten.

[155] Dazu *Uebele* GRUR 2019, 694 (697 ff.).

[156] Die RL (EU) 2020/1828 ersetzt die alte Unterlassungsklage-RL (2009/22/EG), vgl. Art. 21. Verbraucher können dadurch über qualifizierte Einrichtungen leichter gegen (grenzüberschreitende) Verstöße gegen verbraucherschützendes Unionsrecht und der DSGVO (vgl. Anhang I der RL). Dazu näher *Augenhofer* NJW 2021, 113.

[157] Etwa https://twitter.com/darkpatterns.

[158] VO (EU) 2017/2394.

[159] MMR-Aktuell 2020, 424225. Weitere Beschwerden wegen Dark Patterns sind bereits anhängig, u.a. gegen Amazon (wegen erschwerter Kündigungsmöglichkeit von Amazon Prime [Roach Motel]) und Google (Standort-Tracking), vgl. *Forbrukerrådet*, Amazon manipulates customers to stay subscribed, 14.1.2021, abrufbar unter: https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/.

[160] Art. 3 Nr. 6 RL (EU) 2019/2161. Vgl. auch Art. 1 Nr. 5, 7 GStVSch-E.

[161] Art. 3 Nr. 5 RL (EU) 2019/2161. Vgl. auch Art. 1 Nr. 5 GStVSch-E.

[162] S. o., I. 1.

zielt personalisierte Inhalte, birgt das insbesondere für Minderheiten oder marginalisierte Gruppen Gefährdungspotenzial.[163] Um wirksam gegen Dark Patterns vorzugehen, ist daher eine besonders hohe Sensibilität hinsichtlich ihrer Wirkweise und Spezifika angezeigt. Eine starke institutionelle Koordination sowie technischer Sachverstand sind hierfür die condicio sine qua non.

IV. Schlussfolgerungen und Ausblick

1. Dark Patterns de lege lata und Regulierungsansätze

Das Phänomen „Dark Patterns" ist seit mehr als einer Dekade bekannt. Weder der deutsche noch der unionale Gesetzgeber sind gegen sie bisher explizit tätig geworden. Nichtsdestotrotz setzt das Recht bereits heute implizit einigen Designmustern Grenzen, mit deren Hilfe Verwender ihre Gestaltungsmacht einseitig zu ihrem Vorteil ausnutzen. Insbesondere das Lauterkeits- und Verbraucherschutzrecht unterbinden diverse Dark Patterns, wie *Hidden Information*, *Preselection*, *Price Comparison Prevention* oder *Hidden Costs*. Dass diese in der internationalen wissenschaftlichen Diskussion über Dark Patterns gleichwohl so viel Aufmerksamkeit erfahren, gründet auch auf die international unterschiedliche Gesetzeslage: In Übersee sind die Schutzlücken größer als in Europa.

Regulierungsbedarf verursacht hierzulande vor allem die Kategorie „(gefühlter) Druck". Denn für *Confirmshaming*- oder *Social Proof*-Patterns ist das gesetzgeberische Bewusstsein bisher nicht besonders ausgeprägt.[164] Ihre Relevanz springt auch nicht unmittelbar ins Auge. Ähnlich wie irreführende Oberflächengestaltungen sind sie zudem ein qualitativ graduelles Phänomen, dem kein pauschaler Verwerflichkeitsgrad anhaftet.

Dass sich das Recht bislang nur punktuell Dark Patterns in den Weg stellt, legt ein strukturelles Regelungsdefizit offen: Das vielerorts vorherrschende Leitbild des informationsbedürftigen und informierbaren Verbrauchers sowie das daran anknüpfende Regulierungskonzept des „Informationsmodells"[165] wirkt häufig als zu enger normativer Flaschenhals für verhaltensökonomische und psychologische Erkenntnisse über menschliche Entscheidungswege.[166] Zwar kann es etwa in Fällen der Preisintransparenz gleichsam als Schutzkorken gegen Dark Patterns wirken, indem es dem Verbraucher die notwendigen Informationen an die Hand gibt.[167] Doch zeigt sich, dass situative Informationen oft nicht dazu in der Lage sind, die Steuerungswirkung konkreter Designelemente zu unterbinden. Das gesetzliche Verbraucherleitbild vernachlässigt insbesondere innere Restriktionen der menschlichen Entscheidungsfindung, die von kognitiven, emotionalen oder situativen Faktoren ausgehen.[168] Dies gilt umso mehr, als solche Einflüsse grundsätzlich nicht nur bei besonders verletzlichen Personengruppen, sondern bei jedermann wirken können.[169] Erfolg versprechende Maßnahmen gegen Dark Patterns müssen den regulativen Fokus deshalb verstärkt auf solche Umstände menschlicher Entscheidungs-

[163] Vgl. *O'Neil*, Weapons of Math Destruction, 2017, S. 66 ff.
[164] Zumindest hinsichtlich unwahrer *Social Proof*-Patterns verspricht aber Nr. 23b, 23c Anhang zu § 3 Abs. 3 GStVSch-E Abhilfe.
[165] S. hierzu *Tamm*, Verbraucherschutzrecht, 2011, S. 150; *Weber,* ZRP 2020, 98.
[166] Vgl. *Weinzierl* NVwZ-Extra 15/2020, 1 (9).
[167] *Micklitz/Rott*, in: Dauses (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 50. Aufl. 2019, Rn. 119.
[168] *Hacker* (o. Fn. 19), S. 432 ff.; *Rischkowsky/Döring,* J Consum Policy 2008, 285 (309); *Schmitt* (o. Fn. 97), S. 548 f.
[169] Vgl. *Weber* ZRP 2020, 98 (101).

findung erweitern sowie die Interpretation bestehender Normen stärker am tatsächlichen menschlichen Verhalten ausrichten.

Das vergleichsweise junge Datenschutzrecht leidet als Schutzinstrument gegen Dark Patterns an vielen Stellen an ähnlichen strukturellen Defiziten wie das Verbraucher- und Wettbewerbsrecht. Das allgemeine Vertragsrecht scheint durch seine am Einzelfall orientierte Perspektive demgegenüber weniger anfällig für pauschalisierende Verbraucherbilder und damit in der Lage, individuelle Entscheidungsschwächen aufzugreifen. Doch löst es diese Erwartung letzten Endes nicht vollständig ein: Fallen Dark Patterns in die Kategorien „irreführend" oder „erschleichend", können Verträge zwar ggf. anfechtbar sein; allerdings harrt diese Auslegung zum einen noch einer Anpassung der Rechtsprechung an verhaltensökonomische sowie psychologische Erkenntnisse. Zum anderen wirken zahlreiche Dark Patterns, ohne Unwahrheiten zu verbreiten (zB mit Hilfe sozialen Drucks).

Den vielversprechendsten Ansatzpunkt für die Maßnahmen gegen Dark Patterns bieten generalklauselartige Tatbestände, wie die c.i.c. im Schuldrecht oder der *Data Protection by Design*-Grundsatz im Datenschutzrecht. An diesen Stellen weist das Gesetz jeweils eine – ausfüllungsfähige und -bedürftige – regulatorische Flexibilität auf. Allerdings haftet dieser generalklauselartigen Struktur notwendig Rechtsunsicherheit an. Jedenfalls für Konstellationen, die im auslegungstechnischen „Graubereich" liegen, sollte der Gesetzgeber daher missbräuchlichen Patterns mit weiteren Spezialregelungen explizit entgegentreten und verhaltensökonomische Erkenntnisse stärker in Gesetzesbegründungen bzw. Erwägungsgründe einfließen lassen.

Anstelle einer „großen Lösung" in Gestalt eines umfassenden Gesetzes, das Verhaltensmanipulation im digitalen Raum ins Visier nimmt, kann der Gesetzgeber mit kleinem Räderwerk gezielt nachsteuern, indem er etwa zusätzliche Typen oder Kategorien von Dark Patterns in die „Schwarze Liste" des UWG bzw. der UGP-RL aufnimmt. Ein gangbarer Weg besteht auch darin, allgemeinere lauterkeitsrechtliche Verbotstatbestände stärker auf die Wirkweisen von Dark Patterns zuzuschneiden. Zudem wären bestehende Informationspflichten oder Beschwerdemanagementsysteme durch explizite Gebote, eine klare und verständliche Art und Weise der Informationsbereitstellung nicht durch irreführende, ablenkende oder unnötigen Aufwand erzeugende Designmethoden zu umgehen, zu flankieren.[170] Im Datenschutzrecht könnte der Gesetzgeber die Anforderungen an eine wirksame Einwilligung nachschärfen. Möglich wäre eine Ergänzung etwa des Art. 7 DSGVO durch ein Erfordernis, dass bei einer Wahlsituation sämtliche Entscheidungsoptionen auch hinsichtlich ihres Designs gleich zu behandeln sind[171] oder in Art. 9 Abs. 2 lit. a DSGVO die Voraussetzung „[ausdrücklich] und ohne steuernden Einfluss".[172]

Richtig ist es zugleich, nicht generell Dark Patterns (etwa jegliche verwirrend formulierte Frage) nach dem Rasenmäherprinzip pauschal für unzulässig zu erklären. Ein wirksamer Schutz vor Dark Patterns sollte sich vielmehr auf die Regulierung solcher Erscheinungsformen begrenzen, die eine kritische Schwelle der Ausnutzung privatautonomer Gestaltungsfreiheit überschreiten. Darüber hinaus sollte der Gesetzgeber bei den Methoden ansetzen, die Dark Patterns ihre besondere Wirkmacht verleihen: der Möglichkeit gezielten Testens. Dass solche Tests zum Einsatz kommen, ließe sich

[170] Vgl. auch *Baumgartner/Hansch,* ZD 2020, 435 (438); *Weinzierl* NVwZ-Extra 15/2020, 1 (10).
[171] Die französische Datenschutzbehörde CNIL fordert dies bereits in Bezug auf Cookie-Banner, s. *Baumgartner/Hansch* ZD 2020, 435 (438).
[172] *Weinzierl* NVwZ-Extra 15/2020, 1 (10).

durch Informationsansprüche gegen Verwender digitaler Oberflächen zumindest transparent machen. Denkbar ist eine Pflicht, die Ergebnisse von A/B-Tests bei berechtigtem Interesse offenzulegen und/oder deren Durchführung betroffenen Nutzern generell kundzutun.[173] Dieses Wissen wäre ein Grundstein, um die bestehende Informations- und Machtasymmetrie zugunsten von Verbrauchern abzutragen. Denkbar sind daneben ergänzende technische Vorkehrungen oder Apps, die Dark Patterns aufdecken oder gar unterdrücken.

2. Abhilfe in Sicht?

Dark Patterns sind im digitalen Raum omnipräsent. Im günstigsten Fall sind sie nur lästig, im schlimmsten Fall untergraben sie sublim und strukturell die Entscheidungsautonomie des Einzelnen. Staatliche Behörden und der Gesetzgeber erkennen die Problematik erst allmählich. Hat die Europäische Union im Bereich des Datenschutzes mit der DSGVO noch weltweit Pionierarbeit geleistet, kommen die ersten legislativen Vorstöße zum Umgang mit Dark Patterns mit dem DETOUR Act sowie dem novellierten California Privacy Rights Act nun aus den USA. Das geplante Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) korrigiert in Bezug auf Cookie-Einwilligungen bisher lediglich die bis dato unzureichende Umsetzung des Art. 5 Abs. 3 e-Privacy-RL im Nachgang der *Planet 49*-Urteile.[174] Die Novelle der UGP-RL[175] beschränkt sich weitgehend auf Informationspflichten und Rankings von Suchergebnissen. Die Digitale-Inhalte-Richtlinie[176] adressiert wiederum vertragliche Rechte in Zusammenhang mit digitalen Produkten, nicht hingegen verhaltenssteuernde Praktiken außerhalb eines Vertragsverhältnisses.

Die Europäische Kommission hat derweil aber ein Legislativpaket vorgelegt, das den europäischen Rechtsrahmen für digitale Dienste (der seit der E-Commerce-RL aus dem Jahre 2000 keine Veränderung erfahren hat) umfassend neu abstecken soll: Der *Digital Services Act* (DSA) adressiert den Umgang mit „illegalen Inhalten" sowie mit Meinungsfreiheit und Falschinformationen auf digitalen Plattformen.[177] Der *Digital Markets Act* (DMA)[178] versucht flankierend, die Marktmacht der Digitalriesen („Torwächterfunktion") zu begrenzen. Der DSA adressiert zwar grundsätzlich auch die Problematik manipulativer Verhaltenssteuerung.[179] Darauf, dass nicht nur Dritte, sondern Facebook und Co. *selbst* flächendeckend mittels Dark Patterns manipulieren, gehen beide Entwürfe – trotz Problembewusstseins der Kommission[180] – bisher nicht direkt ein. Sie verpassen damit eine Chance. Lobenswerte Ansätze finden sich immerhin

[173] Vgl. auch Sec. 3 lit. b DETOUR Act; *Weinzierl* NVwZ-Extra 15/2020, 1.
[174] Vgl. TTDSG-E (s. Fn. 43), S. 31 ff.
[175] S. a. GStVSch-E.
[176] RL (EU) 2019/770; s. a. Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, 13.1.2021, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Bereitsstellung_digitaler_Inhalte.html.
[177] COM(2020) 825 final, S. 2 ff.
[178] COM(2020) 842 final.
[179] Vgl. Erwgr. 32, 63, 68, Art. 26 Abs. 1 lit. c COM(2020) 825 final.
[180] Vgl. *Ms Jourová on behalf of EU Commission*, Question E-000774/19 to the Commission. Das Europäische Parlament operiert zwar ebenfalls mit dem Begriff, thematisiert das Phänomen im Vorfeld des DSA aber eher am Rande: vgl. *Europäisches Parlament*, REPORT with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), 7.10.2020; *Europäisches Parlament, Fachabteilung Wirtschaft, Wissenschaft und Lebensqualität*, New aspects and challenges in consumer protection, April 2020, S. 23, 36.

in Bezug auf die Transparenzpflichten, insbesondere im Zusammenhang mit personalisierter Werbung und Empfehlungsalgorithmen.[181]

Die Gefahren, die von Dark Patterns ausgehen, sollten den europäischen und den nationalen Gesetzgeber sowie die zuständigen Verwaltungen anspornen, nach passgenauen Lösungen zu suchen. Um Dark Patterns gleichsam aus der rechtlichen Dunkelheit zu holen, müssten die zuständigen Entscheidungsträger den regulatorischen Scheinwerfer nicht nur auf Teilphänomene, sondern auf sämtliche Typen und Kategorien, insbesondere gefühlten Druck, richten. Einstweilen bleibt der Eindruck: „[…] die einen sind im Dunkeln und die andern sind im Licht, und man siehet die im Lichte, die im Dunkeln sieht man nicht."[182] Solange diese Grundregel für die manipulative Gestaltung digitaler Oberflächen gilt, tappt jeder verbraucherpolitische Schutzmechanismus gegen Dark Patterns im Dunkeln.

V. Ergebnisse

1. Dark Patterns sind Designmuster, die eine kritische Zahl an Nutzern zu einem bestimmten Verhalten verleiten und dabei die Gestaltungsmacht über Benutzeroberflächen einseitig im Interesse ihrer Verwender ausnutzen.
2. Das Datenschutz- und Verbrauchervertragsrecht verbietet ebenso wie das Lauterkeitsrecht bereits einige Ausprägungen von Dark Patterns; diese lediglich punktuellen Verbote zeigen jedoch eine systemische Schwachstelle auf: Das zugrunde liegende Verbraucherleitbild erkennt die vielfältigen Steuerungsmöglichkeiten nicht.
3. Um bestehende gesetzliche Lücken zu schließen, ist es einerseits nötig, die Auslegungsmethoden an aktuelle verhaltensökonomische und -psychologische Erkenntnisse anzupassen und andererseits explizite Regelungen zu schaffen, die unterschwellige Beeinflussungen abseits der Informationsebene stärker adressieren.

The advancing digitization of commercial interactions creates ever growing possibilities to influence human decision making. So-called "Dark Patterns" allow designers of digital user-interfaces to steer users into taking decisions they would not have made otherwise. Although Dark Patterns constitute a relatively recent development, data protection, consumer protection as well as fair trading law already prohibit some of their manifestations. Nevertheless, these legal regimes are often based on the model of the rational consumer. The subliminal effects of Dark Patterns however reveal the particular risks boundedly-rational actors face. This finding indicates legal adjustments.

[181] Vgl. Art. 24, 29, 30 COM(2020) 825 final.
[182] *Bertolt Brecht*, Dreigroschenoper, Schlussstrophe.

Kommerzialisierung personenbeziehbarer Daten

Das Datenschutzrecht als Maßstab für die rechtliche Anerkennung von Daten als Wirtschaftsgüter

Dr. Alexander Bijok[*]

Für personenbeziehbare Daten wird oft der Vergleich zu einem „Rohstoff" bemüht, da sie für viele informationswirtschaftliche Geschäftsmodelle zentral für ihre Wertschöpfung sind. Faktisch werden diese Daten somit zu Wirtschaftsgütern, ohne dass die Rechtsordnung, namentlich das Datenschutzrecht, nennenswert auf diese Entwicklung anders reagiert als mit Skepsis. Der „Rohstoff" liegt für die Betreiber der entsprechenden Gecshäftsmodelle somit praktisch kostenlos zur Abschöpfung bereit, ohne dass der Betroffene an dieser Wertschöpfung beteiligt wird. Dieser Aufsatz soll zunächst die für den Betroffenen entstehenden Kosten näher beleuchten. Darauf aufbauend werden Preisbildung, Vertragsrecht sowie ein etwaiges, damit verbundenes Ausschließlichkeitsrecht („Dateneigentum") untersucht.

Inhaltsübersicht

[*] Der Autor ist derzeit Rechtsreferendar am Kammergericht. Er wurde zum Thema „Kommerzialisierungsfester Datenschutz" durch die Universität Regensburg unter der Betreuung von Prof. Dr. Jürgen Kühling promoviert.

ZfDR 2021, 75–96

A. Einleitung

Die EU-Kommission geht davon aus, dass die europäische Datenwirtschaft bis zum Jahr 2025 einen Wert von 829 Milliarden Euro haben und somit 5,8 Prozent des Bruttoinlandproduktes ausmachen wird.[1] Auch – oder gerade – personenbeziehbare Daten sind ein wichtiger Faktor für die Informationswirtschaft. Im Mittelpunkt steht dabei jedoch keineswegs ihre persönlichkeitsrechtliche Relevanz, sondern ihr wirtschaftlicher Nutzwert für die jeweiligen Geschäftsmodelle. Ganz im Sprachbild des „Rohstoffs des 21. Jahrhunderts“[2] erfolgt diese Abschöpfung direkt vom Nutzer als „Mining“[3] oder gar als „Exploitation“[4].

Dieses wirtschaftliche Selbstverständnis steht im krassen Gegensatz zum grundrechtlichen Ansatz und dem Fokus auf die Persönlichkeitsrechte seitens des Datenschutzrechts, das dieses Streben nach Datenmaximierung zu dämpfen versucht. Der allgegenwärtigen und für den Nutzer unsichtbaren Datenerhebung kann er sich nicht entziehen, ohne sich unzumutbarer Weise der digitalen Abstinenz hinzugeben.

Die scheinbar hemmungslose Datenpreisgabe ist nicht etwa Ausdruck einer Gleichgültigkeit gegenüber der eigenen Privatsphäre,[5] sondern vielmehr Ergebnis einer Kontrolllosigkeit, in der letztlich auch die Schwäche im rechtlichen Schutz von Daten erkennbar wird. Es stellt sich insofern die Frage, wie das Datenschutzrecht adäquat auf eine Kommerzialisierung personenbeziehbarer Daten, die es nicht zu verhindern vermag, reagieren kann.

[1] https://ec.europa.eu/germany/sites/germany/files/docs/eu_nachrichten_04b_2020web.pdf (abgerufen zuletzt am 08.01.2021).

[2] Vgl. zum Beispiel *Dammann* ZD 2016, 307 (313); *Dickmann* r+s 2018, 345 (348); *Härting* CR 2016, 646 (648); *Riehm* VersR 2019, 714; *Spiekermann et al.* Electronic Markets 2015, 91; *Wandtke* MMR 2017, 6; kritischer *Kühling*/*Sackmann* ZD 2020, 24 (25).

[3] Dazu *Bunk*, In: Stiftung Datenschutz [Hrsg.], Dateneigentum und Datenhandel, 2019, 29.

[4] *Miller*/*Mork* IEEE IT-Professional 2013, 57.

[5] So sehen 51 Prozent der EU-Bürger die Datenherausgabe nach dem Geschäftsmodell Daten gegen Leistung als Problem, Special Eurobarometer Report 359 (2011), 33; vgl. auch *Dienlin*/*Trepte* EJSP 2015, 285 (286).

B. Die Präventionslogik des Datenschutzes

I. Auseinanderfallen von Regelungs- und Schutzgegenstand

Dass die Datenschutz-Grundverordnung in Art. 4 Nr. 1 die Begriffe Daten und Informationen synonym benutzt, muss als bedauerlich bezeichnet werden. Nicht nur gehört die Unterscheidung in vielen Wissenschaftsbereichen zum absoluten Standard, sondern die Differenzierung ist auch notwendig, um die Gefahren der Datenabschöpfung für den Betroffenen überhaupt konkret erfassen zu können.

Daten sind formalisiert darstellbare Zeichen[6] und an sich weder von Wert noch von irgendeinem Belang. Sie sind bloße Bytes, Pixel, Zahlen- oder Buchstabenfolgen. Damit sie ihre Bedeutung, ihren wirtschaftlichen Wert, ihre Persönlichkeitsrechtsrelevanz entfalten, müssen sie verarbeitet werden.[7] Ein Text ist bedeutungslos, wenn er in einer Sprache geschrieben ist, die der Leser – auch mit Hilfe Dritter – nicht entziffern kann.

Hier zeigt sich die erste Besonderheit des Datenschutzrechts. Daten haftet keine Personenbezogenheit als inhärente Eigenschaft an. Ob sie personenbeziehbar sind, muss durch den Blick des potenziellen Verarbeiters festgestellt werden.

Schutzgegenstand ist also die personenbezogene Information. Was ein Datenverarbeiter aus ihm vorliegenden Daten an Informationen gewinnt, wie er sie interpretiert und sie kontextualisiert, entzieht sich allerdings der Regulierbarkeit.[8] Anders ist dies mit Daten. Sie werden Regelungsgegenstand des Datenschutzrechts. Dieses bestimmt, unter welchen Rahmenbedingungen der Datenverarbeiter sie zu seiner Verarbeitungsgrundlage machen darf. Die synonyme Verwendung von Daten und Informationen macht diese zentrale Stellung der Datenverarbeitung allerdings nahezu unsichtbar.

II. Präventionslogische Unschärfe

Im Auseinanderfallen von Regelungs- und Schutzgegenstand zeigt sich bereits die zweite Besonderheit des Datenschutzrechts, nämlich die ihm innewohnende Präventionslogik. Soll eine spezifische Informationsgewinnung unterbunden werden, so muss der Datenverarbeiter präventiv daran gehindert werden, bestimmte Daten verarbeiten zu können. Dies stellt das Datenschutzrecht vor eine große Herausforderung. Es muss ex ante eine Prognose aufstellen, ob und welche persönlichen Informationen von dem Datenverarbeiter aus den Daten gewonnen werden können. Ein Datum ist personenbeziehbar, wenn eine solche Informationsgewinnung mit hinreichender Wahrscheinlichkeit anzunehmen ist. Jeder Prävention wohnt dabei eine Unschärfe inne, auch tatsächlich zu schützen, was sie schützen soll.

Neben den Verarbeitungsmethoden spielt für die Informationsgewinnung auch die Kontextualisierung eine Rolle. Je mehr Informationen der Verarbeiter bereits über eine Person hat, desto leichter fällt es, neue Informationen erkenntnisbringend einzuordnen. Dies lässt sich mit einem Puzzle vergleichen: sind nur wenige Puzzleteile bekannt, so fällt es schwer, sich das restliche Motiv zu erschließen und neue Puzzleteile zuzuordnen. Je vollständiger das Puzzle bereits ist, desto besser kann das Motiv erschlossen werden.

---

[6] Anstatt vieler *Albers*, Informationelle Selbstbestimmung, 2005, S. 89.

[7] Wegen dieser Ungenaugikeit wurde der Versuch unternommen, die Materie als „Informationsschutzrecht" zu bezeichnen, BT-Drs. 11/3730, 28, was schlicht an der Einbürgerung des Begriffs „Datenschutzrecht" scheiterte.

[8] Vgl. *Stiglitz* QJE 2000, 1441 (1449); *Grimm* JZ 2013, 585 (586); *Simitis* NJW 1984, 398 (402); pointiert klingt dies auch bereits bei *Schlink* NVwZ 1986, 249 (252) an.

Durch diese Präventionslogik wird auch der Kontrollverlust aus Sicht des Betroffenen greifbar. Nicht nur erfolgt die Datenerhebung oftmals derart unsichtbar, dass er kaum überblicken kann, welche und wie viel Daten über ihn erhoben werden. Selbst wenn er das wüsste, fiele es ihm schwer, abzuschätzen, welche vielleicht tiefgreifenden Erkenntnisse daraus über ihn gewonnen werden können. Dadurch wirkt nicht nur der tatsächliche Privatheitsverlust persönlichkeitsrechtlich beeinträchtigend auf den Betroffenen, sondern bereits die Ungewissheit über Möglichkeit und Umfang des Privatheitsverlustes.

Die Ungewissheit gilt zunächst auch für den Datenverarbeiter. Er weiß nicht, welche Informationen er aus Daten gewinnt, bevor er sie verarbeitet hat. Zum einen motiviert dies den kommerziell tätigen Datenverarbeiter zu einer möglichst umfangreichen Datenverarbeitung. Zum anderen hat er gegenüber dem Betroffenen bessere Prognosebedingungen, da er seine Verarbeitungsmethoden und seinen bisherigen Erkenntnisstand besser kennt als der Betroffene. Diese Asymmetrie betrifft insbesondere den Wert der erhobenen Daten für das jeweilige Geschäftsmodell, aber auch das Maß des individuellen Privatheitsverlustes, mit dem infolge der Erhebung und Verarbeitung zu rechnen ist.

C. Daten als „Allmende-Gut“

I. Rivalität und Exklusivität

Zunächst kennzeichnen sich Güter durch ihre Knappheit.[9] Dies setzt voraus, dass eine vermehrte Nutzung zu einer Qualitätseinbuße führt. So lässt sich ein Laib Brot nicht zweimal verzehren, sondern nur aufteilen. Daten wird dagegen ein nicht-rivalisierender Charakter zugeschrieben, da sie sich unbegrenzt duplizieren und stets erneut vollumfänglich nutzen ließen.[10] Dem ist zwar zuzustimmen, für private Informationen gilt dies jedoch nicht. Eine Information verliert ihre Privatheit, wenn sie geteilt wird.[11] Die Kosten für diesen Verlust liegen dabei stets bei demjenigen, der die Privatheit für sich in Anspruch nimmt. Es wäre ein Widerspruch, anzunehmen, dass eine Information ohne Einbuße privat ist, wenn jeder auf sie Zugriff hätte.

Weder Daten noch Informationen sind hingegen exklusiv. Eine natürliche Exklusivität liegt für Güter vor, bei denen der Inhaber Andere an der Nutzung faktisch hindern kann.[12] Ein Laib Brot kann durch Gewahrsam vor dem Zugriff Dritter geschützt werden. Der Zugang zu einem Fischschwarm im Meer hingegen lässt sich nicht mit vertretbarem Aufwand kontrollieren. Daten und Informationen können zwar exklusiv bleiben, wenn ihre Kommunikation vollständig unterbleibt. Sobald sie jedoch kommuniziert werden, bricht diese natürliche Exklusivität vollständig zusammen.[13] Zwar lässt sich eine fehlende natürliche graduell durch eine rechtliche Exklusivität ausgleichen,[14] wie dies etwa im Urheberrecht der Fall ist.

---

[9] *Metzger* AcP 2016, 817 (827).

[10] *Heymann* CR 2016, 650 (653); *Hoeren* MMR 2019, 5 (6); *Zech* CR 2015, 137 (139).

[11] *Hoofnagle*/*Whittington* UCLA L. Rev. 2014, 606 (637 ff.); *Samuelson* Stan. L. Rev. 2000, 1125 (1126).

[12] *Towfigh*/*Petersen-Morell*, Ökonomische Methoden im Recht, 2017, 79.

[13] *Zech* CR 2015, 137 (140); vgl. auch *Riehm*, VersR 2019, 714 (719).

[14] *Towfigh/Petersen-Magen*, Ökonomische Methoden im Recht, 2017, 125.

II. Allmede-Problematik in der Datennutzung

Ein rivalisierendes Gut mit nicht-exklusivem Charakter ist ein Allmende-Gut. Ein solches kann faktisch durch jeden genutzt werden, obwohl seine Nutzung zu Qualitätseinbußen führt. Es entstehen Übernutzungsrisiken einerseits, aber auch ein Übernutzungsanreiz, da die Kosten für die Nutzung nicht vom Kostenverursacher getragen werden.[15] Ein Fischer hat keinerlei persönlich-ökonomischen Anreiz, seine Fischfangmenge zu begrenzen. Auch wenn eine zu hohe Fischfangquote zu einer Überfischung der Meere führt.

Informationswirtschaftliche Datenverarbeiter generieren Umsatz aus der Erhebung und Verarbeitung von Daten. Sind ihre Geschäftsmodelle auf Angebotspersonalisierung bzw. eine Querfinanzierung durch Werbepersonalisierung angelegt oder profitieren sie von einer individualisierten Risikokalkulation, ist der Nutzwert an die Personenbeziehbarkeit von Daten gekoppelt. Kosten entstehen dem Datenverarbeiter nicht für die Daten, sondern ausschließlich in begrenztem Umfang für ihre Speicherung, sowie den Einsatz von Erhebungs- und Verarbeitungswerkzeugen.[16] Die Kosten für die Datenhergabe trägt der Betroffene durch den potenziellen Verlust seiner Privatheit, der sich in der späteren Informationsgewinnung realisiert.[17]

III. Verantwortung für die Kostentragung

Der Betroffene trägt die Kosten seiner Datenhergabe durch den Verlust eigener Privatheit. Dabei stellt sich die Frage, ob und inwieweit er hierfür zu kompensieren ist. Klassische Stimmen aus dem Datenschutzrecht verweigern sich gegen den Gedanken einer Kompensation, da Daten aufgrund ihrer Persönlichkeitsrechtsrelevanz keine Wirtschaftsgüter sein dürften. Andernfalls drohe ein Ausverkauf der Persönlichkeit.[18]

Dieser Gedanke erweist sich trotz seiner betroffenenschützenden Intention als äußerst betroffenenschädlich und ist deshalb zurückzuweisen. Der Betroffene wird nicht dadurch geschützt, dass man die Augen vor der Realität der Datenkommerzialisierung verschließt. Er kann nur geschützt werden, wenn das Recht auf die reellen Gefahren der Datenkommerzialisierung antwortet; erforderlich ist insofern ein „Schutz vor Kommerzialisierung durch Kommerzialisierung".[19]

Die Datenverarbeitung aus kommerzieller Motivation zu verhindern ist außerdem gar nicht das Ziel des Datenschutzrechts. Vielmehr strebt das Datenschutzrecht gerade gegenüber Privaten eine Situation an, bei der der Betroffene in Selbstbestimmung, d.h. Privatautonomie, über seine Daten entscheiden kann.[20]

---

[15] *Hardin* Science 1968, 1243 (1243 f.); vgl. auch *Berberich*/*Golla* PinG 2016, 165 (168).

[16] *Miller*/*Mork* IEEE IT-Professional 2013, 57.

[17] Ausführlicher zur Allmendeproblematik siehe *Bijok*, Kommerzialisierungsfester Datenschutz, 2020, 96, näher zu den Privatheitskosten 280 ff.

[18] So etwa *Simitis* NJW 1998, 2473 (2477 f.); dazu auch *Langhanke*, Daten als Leistung, 2018, 157.

[19] *Götting*/*Schertz*/*Seitz*, Handbuch des Persönlichkeitsrechts, 2008, 200.

[20] Vgl. *Buchner*, Informationelle Selbstbestimmung, 2006, 202; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 387; *Masing* NJW 2012, 2305 (2308).

1. Formelles Autonomieverständnis

Legt man dem Selbstbestimmungsrecht ein formelles Autonomieverständnis[21] zugrunde, so gilt der Grundsatz „stat pro ratione voluntas".[22] Jede Fehlentscheidung, Informationsasymmetrie, kognitive Verzerrung und präferenzwidrige Verhaltensweise des Einzelnen liegt in seiner Verantwortung und berührt die Gültigkeit einer Datenpreisgabe nicht. Wäre ihm an einer Kompensation für seine Datenpreisgabe und des damit verbundenen Privatheitsverlustes gelegen, so müsse er diese einfordern.[23] Entsprächen die Privatheitskosten, die mit der Nutzung eines Internetdienstes einhergingen, nicht seiner Präferenz nach Privatheit, so könne er die Einwilligung verweigern und auf den Dienst verzichten.

Aus dieser Grundprämisse und dem Befund, dass es keinen monetären Datenmarkt gibt, an dem Betroffene selbst partizipieren, wird daher stellenweise gefolgert, dass Betroffene offenbar keinen Wert in ihren Daten sähen[24] oder keine Präferenz nach Privatheit hätten.[25]

2. Materielles Autonomieverständnis

Dies widerspricht jedoch wiederum dem vielfach untersuchten Befund des sogenannten „Privacy Paradox".[26] Demnach lässt sich beobachten, dass Nutzer sehr freigiebig ihre Daten preisgeben und Erhebungen zulassen, obwohl sie zugleich eine hohe Präferenz nach dem Erhalt ihrer Privatheit haben. Bei Zugrundelegung eines materiellen Autonomieverständnisses löst sich ferner auch das scheinbar Paradoxe an diesem Befund auf: Den Betroffenen gelingt es nicht, präferenzgerecht zu handeln.[27] Wird das Autonomieverständnis materialisiert, so zählt nicht allein die formelle Möglichkeit des Handelns für die Annahme autonomen Handelns, sondern es müssen die realen Rahmenbedingungen berücksichtigt werden, unter denen eine Entscheidung getroffen wird.[28]

Die Datenerhebung findet überwiegend passiv, d.h. ohne direktes Zutun des Betroffenen statt und wird dadurch nahezu unsichtbar.[29] Dies macht es schwer, nachzuvollziehen, welche und wie viele Daten einem Verarbeiter vorliegen. Die präventionslogische Unschärfe erschwert darüber hinaus, die Risiken für die Privatheit adäquat abzuschätzen. Abzuschätzen, welche Informationen der Datenverarbeiter zur Verknüpfung und Kontextualisierung heranziehen und wie leistungsfähig er Informationen aus

---

[21] Vgl. zu diesem dem homo oeconomicus verschriebenen „klassischen" Konzept *Canaris*, FS Lerche, 1993, 871 (881); *Wolf*, Rechtsgeschäftliche Entscheidungsfreiheit, 1970, 78.

[22] *Flume*, FS DJT 1960, 141.

[23] *Wandtke* MMR 2017, 6 (8) meint, allein der Marktmechanismus entscheide über die vermögensrechtliche Qualität von Daten.

[24] *Bull* CR 2018, 425 (427).

[25] *Smith et. al.* MIS Quarterly 2011, 989 (1007).

[26] *Acquisti*/*Brandimarte*/*Loewenstein* Science 2015, 509 (510); *Eling*, Der Wert von Nutzerinformationen, 2018, 10; *Hui*/*Teo*/*Lee*, MIS Quaterly 2007, 19 (21); *Palmetshofer*/*Semsrott*/*Alberts*, Wert persönlicher Daten, 2017, 13; *Sandfuchs*, Privatheit wider Willen, 2015, 216 f.; *Smith et. al.* MIS Quarterly 2011, 989 (993); in kritischer Analyse *Dienlin*/*Trepte*, EJSP 2015, 285 (286 ff.).

[27] So ist etwa darauf hinzuweisen, dass je intransparenter die Risiken für den Betroffenen sind, seine Hingabebereitschaft umso höher ausfällt, *Acquisti*/*John*/*Loewenstein*, J. Leg. Stud. 2013, 249 (251); *Metzger* AcP 2016, 817 (830).

[28] Zu diesem Konzept, das dem Gedanken der „begrenzten Rationalität" folgt etwa *Drexl*, Selbstbestimmung des Verbrauchers, 1998, 96; *Hacker*, Verhaltensökonomik, 2017, 71; *Singer*, Willenserklärungen, 1995, 30.

[29] Vgl. *Acquisti*/*Brandimarte*/*Loewenstein* Science 2015, 509.

neuen Daten gewinnen kann, ist essenziell.[30] Ein Großteil der die konkreten Kosten beeinflussenden Faktoren liegt allerdings in der alleinigen Kenntnissphäre des Verantwortlichen.

D. Rechtliche Lösungsansätze

I. Bepreisung von Daten

Anzudenken ist, den Betroffenen dadurch besserzustellen, indem die Datenhergabe für kommerzielle Zwecke bepreist wird. Dabei stellt sich insbesondere die umstrittene Frage, ob bzw. inwieweit dies mit dem Persönlichkeitsrechtsschutz vereinbar ist und ob das Datenschutzrecht hierfür einen rechtlichen Maßstab bilden kann.

1. Datenkommerzialisierungsschutz

Bekommt die Bepreisung von Daten rechtliche Relevanz, so würde hieraus nicht nur die Anerkennung resultieren, dass personenbeziehbare Daten kommerziell verwendet werden können, sondern auch, dass an ihrer Hingabe ein Vermögensinteresse bestehen kann. Dies würde etwa eine rechtliche Prüfung nach einer „angemessenen Vergütung" ermöglichen.

Wie bereits erörtert, lassen sich kommerzielle Übernutzungsrisiken für den Betroffenen nicht rechtlich entschärfen, wenn bereits die Möglichkeit der kommerziellen Nutzung personenbeziehbarer Daten bestritten wird. Nunmehr stellt sich jedoch die über eine Duldung der Kommerzialisierung hinausgehende Frage, ob sich aus den Grundsätzen des Datenschutzrechts auch Rahmenbedingungen für eine kommerzielle Datenverarbeitung ableiten lassen, die sich mithilfe der Datenschutz-Grundverordnung durchsetzen lassen.

Hier wird zum Teil entgegengehalten, dass das Datenschutzrecht nicht zum Ziel habe, die kommerzielle Datenverwertung zu schützen. Es schütze vor einer Gefährdungslage für die Persönlichkeitsrechte, die mit einer Kommerzialisierung verschärft würde. Dem muss entgegengehalten werden, dass das Datenschutzrecht die Motivation, aus der eine Datenhergabe erfolgt, gar nicht bewertet.[31] Das Datenschutzes soll den Datenverkehr weder einschränken noch verbieten, wie Art. 1 Abs. 3 DSGVO bereits klarstellt. Wenn die Maxime eine Selbstbestimmungssituation bei der Datenhergabe ist, muss das Datenschutzrecht umgekehrt auch aktiv dafür Sorge tragen, dass wenn die Hergabe aus kommerzieller Motivation erfolgt, dies in einer bewussten und freiwilligen Weise der Fall ist und auch möglich ist.

Das Datenschutzrecht muss insofern auch Rahmenbedingungen bieten, unter denen ein wirtschaftlicher Datenverkehr möglich ist und die den Betroffenenbelangen hinreichend Rechnung tragen. Auch die Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen geht in Art. 3 Abs. 1 davon aus, dass personenbeziehbare Daten Bezahlung[32] einer

[30] *Hoofnagle*/*Whittington* UCLA L. Rev. 2014, 606 (635 ff.).

[31] Mit dem Hinweis, dass das Datenschutzrecht keine „erziehende Funktion" übernehme *Buchner* DuD 2010, 39 (40).

[32] Dazu *Metzger* JZ 2019, 577 (579); der Begriff „Bezahlen mit Daten" taucht mehrmals im Referentenentwurf des BMJV vom 05.10.2020 zur Umsetzung der Richtlinie auf, 35 f.

Dienstleistung sein können, die mit der Datenschutz-Grundverordnung in Einklang stehen kann.

Dass sich etwa die Datenethikkommission gegen die Bezeichnung „Gegenleistung" in diesem Zusammenhang sträubt,[33] ist nicht nachvollziehbar.[34] Selbst der deutsche Gesetzgeber geht davon aus, dass eine Datenhingabe als Entgelt verstanden werden kann.[35] Die Möglichkeit einen Betrachtung als Gegenleistung anzuerkennen, sie aber nicht beim Namen nennen zu dürfen, ist nicht nur unverständlich, sondern verschleiert die Realität informationswirtschaftlicher Gefährdungslagen zulasten des Betroffenen. Auf die Spitze getrieben würde das durch die abwegige und völlig systemwidrige Konstruktion, dass sich Betroffene zur Datenhingabe verpflichten, aber gleichzeitig die Inanspruchnahme von Dienstleistungen eine Schenkung darstellte.[36]

2. Die Kopplung von Daten und Geld

Ausgangspunkt für die Betrachtung der Datenhergabe als „Bezahlung" ist ihre Kopplung an eine Gegenleistung. Dabei stellt sich die Frage, wo das Datenschutzrecht Grenzen für ein Austauschverhältnis mit einer Leistung sieht. Rechtsgrundlage für eine entsprechende Datenerhebung ist stets die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Sind Daten für die Vertragserfüllung erforderlich, so sind diese Zwecke keine kommerzielle Nutzung.[37] Es entstehen Privatheitskosten, die sich anders, als mit einer Einwilligung rechtfertigen lassen und deshalb auch nicht kompensiert werden müssen. Hierauf wird nochmal unter dem Punkt des Datenvertragsrechts zurückzukommen sein.

a) Freiwilligkeit

Bereits der Grundsatz der Privatautonomie, hier konkretisiert als Selbstbestimmungsrecht im informationellen Bereich, setzt voraus, dass der Betroffene freiwillig entscheiden kann, ob und unter welchen Voraussetzungen er einer Datenpreisgabe als Gegenleistung zustimmt. Sowohl ein Kopplungsverbot[38] als auch ein faktischer Kopplungszwang schließen die Freiwilligkeit daher aus.[39] Mit Art. 4 Nr. 11 DSGVO wird dieses Erfordernis nochmals explizit für die Einwilligungskonstellation der Datenpreisgabe aufgegriffen. Damit wird verdeutlicht, dass der Grundsatz der Privatautonomie auch hier gilt.[40]

Beispielhaft für ein Freiwilligkeitsdefizit wird etwa in Erwägungsgrund 43 S. 1 DSGVO eine Machtasymmetrie genannt. Solche Asymmetrien können zu Zwangssituationen führen, wenn dem Betroffenen faktisch keine Möglichkeit bleibt, die Forderung der Datenpreisgabe auszuschlagen, etwa weil er auf die dafür angebotene Gegen-

[33] Datenethikkommission, Gutachten 2019, 105; ähnlichlautende Kritik auch EDPS, Opinion 4/2017, 3.

[34] So auch *Versaci*, ERCL 2018, 374 (380 f.).

[35] BT-Drs. 17/13951, 72; vgl. auch *Czajkowski*/*Müller-ter Jung* CR 2018, 157 (160); *Schmidt-Kessel*/*Grimm* ZfPW 2017, 84 (107).

[36] *Riechert* PinG 2019, 234 (237); so auch der Referentenentwurf des BMJV vom 05.10.2020 zur Umsetzung der Digitale Inhalte-Richtlinie, 18 – die Konstruktion wird umso unverständlicher bei der Formulierung des Wortlautes des § 516a Abs. 1 BGB-E, der darauf hinweist, dass der Beschenkte, seine Daten dem Schenker „bereitstellt oder sich hierzu verpflichtet".

[37] *Czajkowski*/*Müller-ter Jung* CR 2018, 157 (160).

[38] Ursprünglich sah das deutsche Recht in § 28 Abs. 3b BDSG a.F. ein solches vor.

[39] Vgl. zum Kopplungsverbot als Kontrahierungszwang *Krohm*/*Müller-Peltzer* ZD 2017, 551 (555).

[40] Dazu *Langhanke*, Daten als Leistung, 2018, 136; *Hacker* ZfPW 2019, 149 (164 f.).

leistung angewiesen ist. Gerade bei „Take-it-or-leave-it"-Situationen, wenn also eine Angebotsausschlagung automatisch den Dienstverzicht (etwa bei sozialen Netzwerken) oder Technologieverzicht (etwa bei Smartphones) zur Folge hätte, ist die Freiwilligkeit zweifelhaft.[41]

Ein Verständnis der Freiwilligkeit, welchem dem Betroffenen die freie Wahl ließe, ob er überhaupt für eine Dienstleistung eine Gegenleistung zu erbringen habe, kann damit jedoch schlechthin nicht verbunden sein. Im Gegensatz zu personenbeziehbaren Daten haftet Geld jedoch keine Persönlichkeitsrechtsrelevanz an. Mit dem datenschutzrechtlichen Freiwilligkeitsgrundsatz müsste es insofern vereinbar sein, dass dem Betroffenen jederzeit eine Alternative zur Datenpreisgabe verbleiben muss.[42] Hier bietet sich insbesondere an, die Datenpreisgabe jederzeit durch eine Geldleistung ersetzen zu können.

b) Nachteilsverbot und Alternativleistung

Einen Unterfall der Freiwilligkeit stellt das Nachteilsverbot in Erwägungsgrund 42 S. 5 DSGVO dar. Wenn eine Datenpreisgabe durch eine Geldleistung ersetzt werden kann, stellt sich die Frage, ob diese alternative Geldleistung mit dem Nachteilsverbot kollidiert. Dieses sieht vor, dass eine Hingabesituation nur dann als freiwillig anzusehen ist, wenn der Betroffene keine Nachteile durch eine Verweigerung erleidet.

Hier zeigt sich deutlich die Auswirkung einer rechtlichen Kommerzialisierungsanerkennung. Zuweilen wird es als Nachteil gesehen, die Datenpreisgabe nur gegen Geld verweigern zu können.[43] Im Abgleich mit der informationswirtschaftlichen Praxis ist dies bereits deshalb unsachgerecht, da ein solches Verständnis die entsprechenden Geschäftsmodelle unmöglich machen würde,[44] die nur deshalb entgeltfrei angeboten werden können, weil sie ihren Umsatz aus der Datenverarbeitung generieren. Das Resultat wäre somit – mangels Freiwilligkeit – ein Verbot der Datenforderung und eine zwangsläufige, entgeltliche Kostenpflichtigkeit der entsprechenden Dienste. Ein Verbot der Datenpreisgabe würde jedoch ebenfalls keine Selbstbestimmung über das Ob einer Datenpreisgabe gewährleisten.

Der Verbraucher hat keinen Anspruch auf kostenlose Leistungen, wohl aber auf eine Transparenz der Kosten. Der Freiwilligkeit muss dadurch Rechnung getragen werden können, dass der Betroffene frei darin ist, für welche Art der Leistung er sich entscheidet. In den Fokus rückt somit das Verhältnis zwischen den beiden angebotenen Alternativen. Hier kann das Datenschutzrecht nun gar nicht mehr anders, als Daten mit Geld zu vergleichen. Denn die relevante Frage ist nun, wie hoch der Alternativgeldpreis sein darf, damit der Betroffene noch eine freie Wahl hat, ob er diesen zahlt, oder stattdessen lieber seine Daten preisgibt. Daten- und Geldleistung müssen verhältnismäßig zueinander sein.

Das Nachteilsverbot definiert hierbei den Verhältnismäßigkeitsmaßstab. Dieser ist nur gewahrt, solange die geforderte Geldleistung nicht den Wert der geforderten Datenleistung übersteigt. Andersherum bleibt es dem Verantwortlichen aber unbenommen, eine gegenüber dem geforderten Datenwert niedrigere Geldleistung zu fordern. Der Verhältnismäßigkeitsmaßstab wird zudem zu einer Leistungstrias erweitert. Denn

---

[41] *Dickmann* r+s 2018, 345 (355); *Rosenberg* UCLA Journal of Law & Technology 2016, 1 (27).

[42] *Buchner* DuD 2010, 39 (41); *Krohm*/*Müller-Peltzer* ZD 2017, 551 (553); *Langhanke*, Daten als Leistung, 2018, 132; *Richter* PinG 2018, 6 (7).

[43] *Hoofnagle*/*Whittington* UCLA L. Rev. 2014, 606 (662); zur „Zweiklassen-Datengesellschaft" auch *Härting* CR 2016, 646 (648); *Rosenberg* UCLA Journal of Law & Technology 2016, 1 (19).

[44] *Schantz* NJW 2016, 1841 (1845).

bereits nach ganz allgemeinen privatrechtlichen Maßstäben erfolgt auch das Verbot eines zu krassen Missverhältnisses zwischen Geldforderung und Dienstleistung, etwa im Wege einer Wucherprüfung. Mittelbar wird dadurch bereits verhindert, dass die geforderten Daten in einem zu krassen Missverhältnis zur Querfinanzierung des entsprechenden Geschäftsmodells stehen.[45]

c) Kopplungsregel

Auftrieb für eine Ablehnung hinsichtlich von Bezahlmodellen gibt scheinbar der berüchtigte Art. 7 Abs. 4 DSGVO, in den zuweilen ein „Kopplungsverbot" hineingelesen wird. Überschätzt werden sollte diese Regelung allerdings nicht. Dies begründet sich bereits darin, dass das Verhältnis des Datenschutzrechts zur Informationswirtschaft bereits im Gesetzgebungsprozess heftig umkämpft war,[46] was sich schlussendlich in dieser Vorschrift entladen hat.

Der Wortlaut der Norm erweckt den Eindruck, dass die Beurteilung der Freiwilligkeit davon abhinge, inwieweit die Datenerhebung erforderlich sei. Dies ist gleich in doppelter Hinsicht unsachgerecht. Zum einen richten sich Kopplungskonstellationen, bei denen die Datenerhebung erforderlich für die Vertragserfüllung ist, überhaupt nicht nach der Einwilligung im Sinne des Art. 6 Abs. 1 lit. a DSGVO, sondern nach der Vertragserforderlichkeit gemäß Art. 6 Abs. 1 lit. b DSGVO. Zum anderen sind (objektive) Erforderlichkeit und (subjektive) Freiwilligkeit maßstäbliche Gegensätze.[47] Statt in Art. 7 Abs. 4 DSGVO ein Verbot von Kopplungssituationen zu sehen, überzeugt vielmehr, die Norm als „Aufhänger" für den Prüfungsmaßstab der Alternativleistung heranzuziehen bzw. hierin eine gesetzliche Ersetzungsbefugnis zu verorten.

3. Transparenz

Eine Bepreisung von Daten hat vor allem den Vorteil, die tatsächlich anfallenden Kosten für den Betroffenen in Form eines Privatheitsverlustes zu beziffern und offenzulegen. Ein maßgeblicher Faktor für den durch das Privacy Paradox empirisch belegten, präferenzwidrig freigiebigen Umgang vieler Betroffener mit ihren Daten liegt auch in der „Umsonst-Illusion",[48] also dem Eindruck, dass die in Anspruch genommenen Dienste kostenlos seien. Dieser Eindruck wird ausgerechnet die Rechtsprechung unterstützt, wenn etwa das Landgericht Berlin[49] (bestätigt durch das Kammergericht)[50] das Vorbringen einer Klägerin zurückweist, dass die Werbung Facebooks, es sei und bleibe kostenlos, lauterkeitsrechtlich irreführend sei und daher unterbleiben müsse. Die Datenpreisgabe entspreche, so das Kammergericht, nicht dem allgemeinen Verständnis anfallender Kosten.

Genau hierin liegt aber das Problem – die Verschleierung von persönlichkeitsrelevanten Kosten.[51] Werden Daten aufgrund ihrer Persönlichkeitsrechtsrelevanz nicht als

[45] Ansatzweise bereits bei *Krohm*/*Müller-Peltzer* ZD 2017, 551 (553); *Golland* CR 2020, 186 (190); ausführlich zur Konzeption einer doppelten Missverhältnisprüfung *Bijok*, Kommerzialisierungsfester Datenschutz, 2020, 187.

[46] Hierzu *Krohm*/*Müller-Peltzer* ZD 2017, 551 (552 f.).

[47] Vgl. *Ohly*, Einwilligung im Privatrecht, 2002, 208; *Radlanski*, Das Konzept der Einwilligung, 2016, 207.

[48] *Lewinski*, In: Stiftung Datenschutz [Hrsg.], Dateneigentum und Datenhandel, 2019, 209 (218).

[49] LG Berlin MMR 2018, 328.

[50] KG MMR 2020, 239.

[51] *Hoofnagle*/*Whittington* UCLA L. Rev. 2014, 606 (657), ebenfalls unter Bezug auf den Slogan „Facebook ist und bleibt kostenlos".

Wirtschaftsgüter anerkannt, geht hiermit auch ein Freifahrtschein für die Geschäftsmodellbetreiber einher, diese Gefährdungen für das Persönlichkeitsrecht für den eigentlich zu schützenden Betroffenen zu verschleiern. Aus der Intention von Betroffenenschutz wird unwillentliche Betroffenenschädigung.

Den langjährige Werbespruch entfernte Facebooks Mitte 2019 von seiner Webseite.[52] Nicht also als Reaktion auf die 2018 in Kraft getretene Datenschutz-Grundverordnung, sondern mutmaßlich als Reaktion auf die kurz zuvor verabschiedete Richtlinie (EU) 2019/770, die die Frage des möglichen Gegenleistungscharakters von Daten zwischen den Zeilen[53] bejaht.[54] Es liegt nun am deutschen Gesetzgeber, bei der Umsetzung dieser Richtlinie den möglichen Fortschritt auszuschöpfen und nicht hinter dem Regelungspotenzial aus Art. 3 Abs. 1 der RL zurückzubleiben. Die klare Benennung, dass Daten „Gegenleistung" oder gar „Bezahlung" sein können, wäre aus Transparenzgesichtspunkten ein bedeutender Gewinn.

Das oben erläuterte Nachteilsverbot bei einer Gegenüberstellung von Geld- und Datenleistung brächte hier einen weiteren Vorteil. Der Wert der Daten müsste durch die Verantwortlichen – die schließlich einen Prognosevorteil hinsichtlich der gewinnbaren Informationen haben – klarer umrissen werden. Wendungen, wie dass die Daten keinen bedeutenden Geldwerten hätten,[55] würden sich hiermit gegen die Geschäftsmodellbetreiber wenden. Denn wären die Daten für den Verantwortlichen tatsächlich kaum etwas wert, wären auch äußerst niedrige Alternativgeldleistungen die Folge. Dies wiederum könnte für viele Betroffenen ein ernsthafter Anreiz sein, die Alternativgeldleistung einer Datenpreisgabe vorzuziehen. Brächte eine äquivalente Umrechnung hingegen äußerst hohe Alternativgeldleistungen hervor, so rückte die Wucherkontrolle zur angebotenen Dienstleistung in den Vordergrund.

4. Informiertheit

Für den Betroffenen liegt ein Informationsdefizit vor, wenn er nicht über ausreichend Informationen verfügt, um die für ihn entstehenden Privatheitskosten abschätzen zu können. Ein Mehr an Informationen führt jedoch zumeist nicht zu einem Gewinn hinsichtlich der Informiertheit. Datenschutzerklärungen und Einwilligungsgesuche dürften in der Praxis etwa ähnlich häufig gelesen werden, wie Allgemeine Geschäftsbedingungen.[56]

Abschätzbarkeit ist nicht positives Wissen. Die Privatheitsrisiken, die mit einer Datenpreisgabe verbunden sind, ließen sich durch eine Bezifferung als Geldwert verständlich aufbereiten und machte in dieser Hinsicht zudem verschiedene Geschäftsmodellbetreiber untereinander näherungsweise vergleichbar, ohne dies mühsam über die Lektüre gleich mehrerer Datenschutzerklärungen zu versuchen. Die Sichtbarkeit eines solchen äquivalenten Geldwertes könnte zudem auch einen starken Einfluss auf das Bewusstsein für den Wert der eigenen Daten haben.[57]

---

[52] https://www.derstandard.de/story/2000107888172/kein-ist-und-bleibt-kostenlos-mehr-face book-aendert-heimlich-slogan (abgerufen zuletzt am 08.01.2021).

[53] In COM(2015) 634 final war noch explizit der Begriff „Gegenleistung" zu lesen, der jedoch nach der Kritik EDPS Opinion 4/2017, S. 3 entfernt wurde, *Metzger* JZ 2019, 577 (579).

[54] Vgl. etwa *Staudenmayer* NJW 2019, 2497; *Indenhuck*/*Britz* BB 2019, 1091 (1095); *Metzger* AcP 2016, 817 (833 f.); *Riechert* PinG 2019, 234 (235).

[55] Dazu *Dickmann* r+s 2018, 345 (348).

[56] *Lewinski* PinG 2013, 12; *Richter* PinG 2018, 6 (7) vergleicht das Wegklicken entsprechender Texte sogar mit einer Abwehrreaktion.

[57] Sogar die Datenethikkommission, Gutachten 2019, 105 räumt einen solchen positiven Effekt auf das Bewusstein trotz äußerst kritischer Haltung ein.

II. Datenvertragsrecht

In der Literatur ist überwiegend die Bezeichnung entsprechender Geschäftsmodelle als eine Konstellation „Daten gegen Leistung“[58] anzutreffen, vereinzelt aber auch „Einwilligung gegen Leistung“[59]. Dies legt nahe, dass zentrales Regelungsregime für den Datenumgang in der Informationswirtschaft zunächst das Vertragsrecht ist.

1. Leistungscharakter

Vertragsrechtlich kann sowohl die Datenpreisgabe selbst als auch die Einwilligung zur Datenerhebung nach § 241 Abs. 1 BGB eine Leistung darstellen.[60] Fraglich ist jedoch die Konsequenz dieser Einordnung.

a) Bindungswirkung der Kopplung

Ob Daten und Einwilligungen auch als Gegenleistung fungieren, also in ein synallagmatisches Vertragsverhältnis eingebunden werden können, hängt von der Anerkennung direkter Kopplungssituationen ab.

Gegen die Annahme einer synallagmatischen Kopplung könnten etwa Freiwilligkeitsgrundsatz und, zumindest für die Einwilligung, deren freie Widerrufbarkeit angeführt werden. Zuweilen wird auch eine Konditionalkopplung angedacht,[61] da auch der Verantwortliche kein Interesse an einer Rechtsdurchsetzung habe, die Folge eines Synallagmas wäre. Nicht nur würde die Datenqualität der zwangsweise erhobenen Daten leiden, sondern es drohte auch wettbewerblich ein erheblicher Reputationsverlust, wenn die Nutzer zum Privatheitsverlust gezwungen würden. Daher werden die Datenhergabe bzw. Einwilligungserteilung als Bedingung nach § 158 Abs. 1 BGB gesehen, die zwar suspendieren, aber eben nicht zwingen. Dem Verantwortlichen bliebe daher das Recht der Leistungsaussetzung, sobald die Datenpreisgabe ausbliebe. Unmittelbare Auswirkungen auf die Wirksamkeit eines Vertrags hätte dies jedoch nicht.

Dies überzeugt bei genauerer Betrachtung nicht. Denn aus der – sicherlich zutreffenden – Annahme, dass der Verantwortliche kein Interesse an der Erzwingung der Datenpreisgabe hat, kann nicht abgeleitet werden, dass er überhaupt kein Interesse an einer Gegenleistung hätte. Mit diesem Ansatz lässt sich auch das Entgegenstehen des Freiwilligkeitsgrundsatzes bzw. der freien Widerruflichkeit der Einwilligung entschärfen. Denn besteht die Möglichkeit der jederzeitigen Ersetzbarkeit der Leistung des Betroffenen durch eine Geldleistung unter Wahrung von Freiwilligkeitsgrundsatz und Nachteilsverbot, so ließe sich eine Kopplungssituation mit der Annahme eines Synallagmas vereinbaren. Der Betroffene hat keinen Anspruch auf die Kostenlosigkeit einer Dienstleistung, sondern muss freiwillig darüber entscheiden können, ob er die Entstehung von Privatheitskosten in Kauf nehmen möchte. Auch die Gleichstellung einer Geldzahlung und der Bezahlung mit personenbeziehbaren Daten legt ein Synallagma nahe.

b) Daten und Einwilligung als Leistungsgegenstand

Wenn es um personenbeziehbare Daten geht, könnten zunächst auch Daten als Gegenstand der Kopplung zu betrachten sein. Gleichwohl hat der Verantwortliche nicht

[58] Statt aller *Langhanke*, Daten als Leistung, 2018.

[59] *Buchner* DuD 2010, 39; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 41 ff.; *Specht* JZ 2017, 763 (767).

[60] *Krohm*/*Müller-Peltzer* ZD 2017, 551 (554); *Schmidt-Kessel*/*Grimm* ZfPW 2017, 84 (89).

[61] *Hacker* ZfPW 2019, 149 (173); *Schweitzer*, In: Torsten Körber, Jürgen Kühling [Hrsg.], Regulierung – Wettbewerb – Innovation, 2017, 269 (290).

allein ein Interesse an der bloßen Datenerhebung, sondern an einer rechtmäßigen Datenerhebung nach der Datenschutz-Grundverordnung.[62] Würde explizit eine Datenerhebung entgegen ihrer Rechtmäßigkeit vereinbart werden, stellte dies einen Verstoß gegen § 134 BGB dar.[63]

Insofern besteht ein Interesse an der Erlangung der Legitimität, Daten für bestimmte Zwecke kommerziell verwerten zu dürfen. Ist diese Legitimität bereits inhärent dem Vertrag anhaftend – wenn sich diese also datenschutzrechtlich aus Art. 6 Abs. 1 lit. b DSGVO ergibt – kommen lediglich Daten als möglicher Leistungsgegenstand in Betracht. Eine zusätzlich eingeholte datenschutzrechtliche Einwilligung könnte die Legitimation nicht mehr konstitutiv herstellen[64] und taugte daher nicht als Leistungsgegenstand.

In Konstellationen, die nach Art. 6 Abs. 1 lit. a DSGVO zu beurteilen sind, kann im Vertrag allerdings auch zur Einwilligung verpflichtet werden. Dies ist nach deutscher Rechtsdogmatik nur denkbar, wenn die Einwilligung vom Vertrag insoweit zu trennen ist, dass die Einwilligung nicht bei Verbindung mit einem Vertrag in diesem als „Gestattungsvertrag" aufginge.[65] Letzteres wäre eine Folge der Einordnung der Einwilligung als Realakt.[66] Wird die Verpflichtung zur Erteilung einer datenschutzrechtlichen Einwilligung als tauglicher Leistungsgegenstand betrachtet, so kann weitergehend sogar von einem Vertrag über Datenverwertungsrechte, mithin einem datenschutzrechtlichen Lizenzmodell, gesprochen werden.[67]

Wird die Einwilligung zum Leistungsgegenstand, so bleibt die parallele Einstufung der Daten als Leistungsgegenstand zwar problemlos möglich. Fraglich ist jedoch, ob sie auch notwendig bleibt oder von der Einwilligung verdrängt wird. Denn wird vertraglich die Erteilung einer Einwilligung vereinbart, dass der Verantwortliche bestimmte Daten zu bestimmten (kommerziellen) Zwecken erheben und verarbeiten darf, wären die entsprechenden Daten rechtlich gesehen akzessorisch mitumfasst.[68] Dies käme insbesondere der Praxis nahe, dass die meisten Daten passiv erhoben werden, d.h. ohne das Zutun des Betroffenen und diese zudem bei Vertragsschluss auch an sich noch unbestimmt sind.

Die kumulative Erfassung von Daten als Leistungsgegenstand machte bei Einwilligungskonstellationen dort Sinn, wo die (aktive) Bereitstellung ganz bestimmter Daten notwendig würde, etwa beim Ausfüllen eines Nutzerprofils.[69] Ist dies nicht der Fall, so reicht die Bezeichnung der Konstellation als „Einwilligung gegen Leistung" aus, um das Leistungsgepräge treffend zu erfassen.

2. Leistungslegitimation

Zwar können Daten und die Einwilligung Leistungsgegenstand sein. Fraglich bleibt jedoch, auf welchen Zulässigkeitstatbestand die Leistung datenschutzrechtlich gestützt werden kann.

---

[62] *Langhanke*/*Schmidt-Kessel* EuCML 2015, 218 (220).
[63] *Langhanke*, Daten als Leistung, 2018, 111.
[64] Vgl. *Schmidt-Kessel*/*Grimm* ZfPW 2017, 84 (90).
[65] *Frömming*/*Peters* NJW 1996, 958; vgl. auch *Bräutigam* MMR 2012, 635.
[66] *Peifer*, Individualität im Zivilrecht, 2001, 314; *Ohly*, Einwilligung im Privatrecht, 2002, 168.
[67] Vgl. dazu schon *Lessig* Soc. Res. 2002, 247 (254 f.); *Samuelson* Stan. L. Rev. 2000, 1125 (1158); vgl. weiterhin *Grünberger* AcP 2018, 213 (267); *Wandtke* MMR 2017, 6 (11).
[68] So etwa *Melan*/*Pfeiffer* DStR 2017, 1072 (1073).
[69] Dazu *Metzger* AcP 2016, 817 (834).

a) Einwilligung

Trotz zahlreicher Unkenrufe bleibt die datenschutzrechtliche Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO das „Königsinstrument" zur Rechtfertigung der Datenerhebung und der Selbstbestimmung im informationellen Bereich.[70] Neben der Vertragserforderlichkeit nach Art. 6 Abs. 1 lit. b DSGVO stellt sie den einzigen Zulässigkeitstatbestand dar, der die willentliche Mitwirkung des Betroffenen erfordert. Hier bietet sich, insbesondere zur Abgrenzung gegenüber der Vertragserforderlichkeit, eine Differenzierung entlang der Charakterisierung als Haupt- und Nebenleistung an.

Eine Hauptleistung ist solch eine Leistung, die dem Schuldverhältnis ihr charakteristisches Gepräge gibt und als essentialia negotii im Vertrag selbst bestimmt ist.[71] Im informationswirtschaftlichen Sinne sind hier insbesondere datenbetriebene Geschäftsmodelle zu verorten, bei denen sich das Austauschverhältnis auf Seiten des Betroffenen auf nichts anderes bezieht als die Datenpreisgabe bzw. die Legitimation zur Datenerhebung. Dies sind die Konstellationen, bei denen Daten erhoben werden, um durch ihren Einsatz die Angebote zu quersubventionieren. Die Daten dienen somit der Bezahlung des Angebots.[72]

Unerheblich ist dabei, ob es sich um reine datenbetriebene Modelle handelt, oder Mischmodelle. Zum einen können dies Freemium-Modelle sein,[73] die auf Datenpreisgabe basieren, aber die Datenerhebung für eine Geldzahlung reduzieren. Zum anderen können dies Rabatt-Modelle sein,[74] die grundsätzlich auf Geld basieren und einen Nachlass dafür bieten, dass Daten erhoben werden können (z.B. bei Telematik-Tarifen[75] oder in Kundenbindungssystemen[76]). Da Geld- und Datenpreisgabe als funktionales Äquivalent anzusehen sind, können beide auch kumulativ die Hauptleistung der Bezahlung darstellen.

Maßgeblich für die Einstufung als Hauptleistung und somit als Einwilligungskonstellation ist somit die Verwendung der Daten für wirtschaftliche Zwecke. Denklogisch kann auch gefragt werden, ob eine Datenpreisgabe gegen Geld ersetzbar ist, ohne dass die Leistung des Verantwortlichen nicht mehr erbringbar wäre.

b) Vertragserforderlichkeit

In der Schlussfolgerung liegt nahe, dass ein Nebenleistungscharakter zu einem Rückgriff auf die Vertragserforderlichkeit nach Art. 6 Abs. 1 lit. b DSGVO berechtigt.[77] Dieser Zulässigkeitstatbestand ist attraktiver, als eine Einwilligung, da die Legitimation für die Datenerhebung keinen eigenständigen Rechtsakt (die Einwilligungserteilung) benötigt, sondern bereits in den Vertragsschluss eingearbeitet werden kann. Im Gegensatz zur datenschutzrechtlichen Einwilligung ist dies auch konkludent möglich.

Würde ein lockerer, rein wirtschaftlicher Maßstab für die Vertragserforderlichkeit angesetzt werden, böte dies die Möglichkeit einer „Flucht in die Erforderlichkeit" für den Verantwortlichen.[78] Da der Vertragszweck frei gewählt werden kann, könnten so-

[70] *Richter* PinG 2018, 6.
[71] *Medicus*/*Lorenz*, Schuldrecht I, 21. Auflage 2015, Rn. 108.
[72] So auch bereits der 71. Deutscher Juristentag in Essen 2016, Thesen zum Zivilrecht, 5 Ziff. 3.
[73] *Schweitzer*, In: Torsten Körber, Jürgen Kühling [Hrsg.], Regulierung – Wettbewerb – Innovation, 2017, 269 (272 f.).
[74] *Hacker* ZfPW 2019, 149 (187).
[75] *Brand* VersR 2019, 725 (732).
[76] *Acquisti*, Economics of Privacy, 2014, 6.
[77] Vgl. auch *Czajkowski*/*Müller-ter Jung* CR 2018, 157 (160).
[78] *Vendrell*/*Schulze*, Verträge über digitale Inhalte, 2018, 26; *Graf von Westphalen* IWRZ 2018, 9 (11).

mit umfangreiche Datennutzungen schlicht für erforderlich erklärt werden und bedürften keiner Einwilligung oder einer Kompensation. Es empfiehlt sich jedoch, einen engen und objektivierenden Maßstab anzusetzen – vertragserforderlich können nur Daten sein, die keine Bezahlung sind und demgemäß auch nicht hypothetisch durch eine Geldzahlung ersetzt werden könnten. Die Daten haben lediglich eine die Hauptleistung unterstützende Funktion, die der ordnungsgemäßen Vertragsdurchführung dienen.[79] Die Heranziehung vertragsrechtlicher Maßstäbe erweist sich dabei als vorteilhaft, insbesondere um ein datenschutzrechtliches „Schattenvertragsrecht"[80] zu vermeiden, bei der eine Vertragsrechtsdogmatik in die Datenschutz-Grundverordnung hineingelesen werden muss.

Die Wirtschaftlichkeit des Geschäftsmodells scheidet daher kategorisch aus. Auch die Optimierung des Angebots scheidet aus, da dies vom Geschäftsrisiko der Wirtschaftlichkeit umfasst ist. Wird andererseits jedoch ein Kaufvertrag mit Liefervereinbarung geschlossen, so dürften Liefer- und Rechnungsdaten zweifelsfrei vertragserforderlich und mithin nicht durch Geldzahlung ersetzbar sein.

Schwieriger wird dies, wenn die Datenerhebung nicht mehr von der Hauptleistung isolierbar ist, etwa bei der Nutzung eines smarten Kühlschranks, der ohne datenerhebende Funktionen gar nicht funktionstüchtig wäre.[81] Hier muss jedoch genau geprüft werden, ob einerseits ein smarter Kühlschrank als aliud zu einem herkömmlichen Kühlschrank gelten kann, oder ob das Gebot der Privatheit durch Technikgestaltung nach Art. 25 DSGVO zu einer Isolierbarkeit zwingt, womit die smarte Funktion schlechthin nicht länger als vertragserforderlich gelten kann. Vertragsleitbilder könnten hier eine Typisierung erleichtern, andernfalls muss die Abgrenzung im Einzelfall erfolgen.[82]

Unproblematischer hingegen ist eine Zweckmehrheit in der Datenerhebung. Werden vertragserforderliche Daten auch für kommerzielle Zwecke genutzt, so steht dies für die Zwecke der kommerziellen Erhebung einem Einwilligungserfordernis nicht im Wege. Erheben etwa Apps allein vertragserforderliche Daten, so dienen die Daten als Bezahlung, soweit sie über die vertragserforderlichen Zwecke hinaus verwendet werden. Hierfür sind sie durch Geldzahlung ersetzbar.

c) Wahrung berechtigter Interessen

Aufgrund zahlreicher defizitärer Einwilligungslagen wird zum Teil vorgebracht, dass der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO eine höhere, wenn nicht gar zentrale Bedeutung beigemessen werden müsse.[83] Dies ist aber entschieden zurückzuweisen. Neben den gesetzlichen Rechtfertigungstatbeständen erfordert die Wahrung berechtigter Interessen keinerlei Mitwirkung des Betroffenen. Dieser hat somit keinerlei Einflussmöglichkeit auf die Datenerhebung, indem er etwa einen Vertrag ausschlägt oder eine Einwilligung versagt.

Die Selbstbestimmung als Maxime des Datenschutzrechts bleibt dem Betroffenen hiermit versagt.[84] Als Entlastungstatbestand für die Einwilligung kann dieser Tatbestand lediglich als Bagatellschranke in Betracht kommen. Keinesfalls kann er die zentrale Bedeutung von Mitwirkungselementen im Datenschutzrecht verdrängen.

---

[79] In Anlehnung an die Defintion der Nebenleistung nach *Medicus*/*Lorenz*, Schuldrecht I, 21. Auflage 2015, Rn. 109.

[80] *Indenhuck*/*Britz* BB 2019, 1091.

[81] *Hacker* ZfPW 2019, 149 (162); ferner *Melan*/*Pfeiffer* DStR 2017, 1072 (1077).

[82] Dazu *Grünberger* AcP 2018, 213 (249).

[83] So *Veil* NVwZ 2018, 686 (695); *Golland* CR 2020, 186 (194).

[84] *Zech*, Information als Schutzgegenstand, 2012, 215.

3. Leistungspflicht des Datenschuldners

Wird bei den Modellen „Daten gegen Leistung" oder „Einwilligung gegen Leistung" von einer synallagmatischen Kopplungssituation ausgegangen, stellt sich die Frage nach den konkreten Leistungspflichten auf Seiten des Betroffenen und ihrer datenschutzrechtlichen Begrenzung.

Die Verpflichtung zur Erteilung einer Einwilligung weist Züge eines Lizenzmodells auf, bei dem sich der Betroffene verpflichtet, dem Verantwortlichen Datenverwertungsrechte zu erteilen. Dabei kann der Betroffene nur eine Handlung, nämlich die Einwilligungserteilung schulden, nicht jedoch den Erfolg, dass daraufhin auch bestimmte Daten rechtmäßig erhoben werden können.

Dies wird besonders deutlich bei mehrrelationalen Daten.[85] Mehrrelational ist ein Datum, wenn der Datenverarbeiter mit hinreichender Wahrscheinlichkeit personenbezogene Informationen über mehrere Personen gewinnen kann. Dies sind typischerweise Gruppenfotos oder ein Freundschafts- bzw. Beziehungsstatus. Nach Art. 7 Abs. 1 DSGVO obliegt es dem Verantwortlichen, die Einwilligung des bzw. jedes Betroffenen nachzuweisen. Somit kann ein Betroffener auch nicht verpflichtet werden, mehrrelationale Daten rechtmäßig preiszugeben, wenn der Verantwortliche nicht sicherstellen kann, dass er auch über die Einwilligung der anderen Betroffenen verfügt.

Hinsichtlich einer Pflicht zur Datenpreisgabe zeigt weiterhin die Aufteilung zwischen Daten und Informationen weitere Auswirkungen. So ist insbesondere eine Pflicht zu „wahren" Datenangaben problematisch. Da Daten lediglich Verarbeitungsgrundlage zur Informationsgewinnung mittels Kontextualisierung und Interpretation sind, erscheint es nahezu unmöglich, ein preisgegebenes Datum als „wahr" oder „falsch" einzustufen.[86] Was bei aktiv gegebenen Angaben, wie z.B. einer Namenseingabe noch gelingen dürfte, dürfte sich bei passiven Verhaltensdaten als nicht nachprüfbar herausstellen. Bei aktiven Angaben wiederum stellt sich die Frage der Statthaftigkeit.[87]

Während bei Vertragserforderlichkeit noch eine Pflicht zur Unterlassung treuwidriger Vereitelung der Informationsgewinnung angenommen werden kann, erscheint dies gerade bei Einwilligungskonstellationen fraglich, etwa bei der Klarnamenpflicht.[88] Diese dürfte gerade aus den Gesichtspunkten des Privatheitsschutzes eine Besonderheit darstellen. Die Nutzung eines Pseudonyms stellt nicht automatisch Anonymität her. Entsprechende Profile ließen sich für den Anbieter noch immer individualisieren. Lediglich für Dritte stellt ein Pseudonym ein anonymes Datum dar – bei sozialen Netzwerken also einer breiteren Öffentlichkeit.

Die Kosten für den Privatheitsverlust des Einzelnen wären also sehr hoch im Vergleich zum Erkenntnisgewinn für den Verantwortlichen. Gemäß dem Prinzip der Datenminimierung erscheinen solche spezifischen Pflichten zur Angabe konkreter Daten also schwieriges Terrain zu sein und bedürfen einer genaueren Betrachtung. Denkbar erscheint, dass solche Konstellationen durch die Schaffung von AGB-Klauselverboten[89] gesetzgeberisch adressiert werden, beispielsweise durch ein Verbot der Forderung von Klarnamen.

---

[85] Dazu *Langhanke*, Daten als Leistung, 2018, 123 ff.
[86] Zu diesem Problem *Floridi*, The Philosophy of Information, 2011, 45.
[87] Für eine mögliche Verpflichtung *Metzger* AcP 2016, 817 (834).
[88] Ablehnend *Caspar* ZRP 2015, 233 (234 ff.).
[89] So auch Datenethikkommission, Gutachten 2019, 102.

4. Ersetzungsbefugnis des Datenschuldners

Das Datenschutzrecht verhindert aus Erwägungen des Persönlichkeitsrechtsschutzes, dass ein Betroffener zur Preisgabe von Daten oder zur Erteilung einer Einwilligung gezwungen werden kann. Wenn solche Preisgabe- oder Erteilungspflichten jedoch bestehen, stellt sich die Frage ihrer Durchsetzbarkeit.

Wie bereits angesprochen, erscheint hier eine durch die Datenschutz-Grundverordnung abgesicherte Ersetzungsbefugnis[90] ein passendes Rechtsinstitut zu sein. Dem Nutzer muss freigestellt werden, ob er eine Einwilligung für kommerzielle Zwecke erteilt und seine Daten zur Kommerzialisierung preisgibt oder ob er lieber einen äquivalenten Geldpreis zahlt. Die Ersetzungsbefugnis ist ein Gestaltungsrecht,[91] welches dem Berechtigten einräumt, die Primärleistungspflicht – also Daten bzw. eine Einwilligung – durch eine Ersatzleistungspflicht zu ersetzen – hier Geld – die schließlich in das bestehende Synallagma einrückt. Sie führt nicht zu einer Erfüllung, ist aber eine Leistung an Erfüllungs Statt (vgl. § 364 BGB).[92] Auch nach getroffener Auswahl behält der Berechtigte dabei das Recht, den Leistungsgegenstand zu wechseln.[93]

Der Wechsel des Leistungsgegenstands lässt sich in Art. 7 Abs. 3 DSGVO mit der freien Widerrufbarkeit der Einwilligung verorten. Auch hier bleibt der Freiwilligkeitsgrundsatz nur durch ein Geldäquivalent gewahrt, wenn der geforderte Geldpreis also nicht den zuvor geforderten Datenwert übersteigt. Die Ausübung des Widerrufs der Einwilligung berührt insofern die Wirksamkeit des Vertrags nicht, sondern ist lediglich Ausübung der Ersetzungsbefugnis der geschuldeten Leistung. Insofern muss die Bezeichnung „Widerruf" als unglücklich angesehen werden, da sich bei dieser Betrachtung zeigt, dass der Widerruf im Sinne des Datenschutzrechts und der (Verbraucher-) Widerruf zwei Rechtsinstitute ohne Berührungspunkte zueinander sind, die nicht verwechselt[94] werden sollten.[95]

Die Nichterteilung der Einwilligung, ihr Widerruf oder die unterbleibende Datenpreisgabe an sich stellen insofern keine Pflichtverletzung dar, obwohl zu ihnen verpflichtet werden kann. Erst wenn auch die Ersatzleistung verweigert wird, läge eine Pflichtverletzung vor, die den Verantwortlichen zu Konsequenzen berechtigen kann.

Besondere Vertragsbeendigungsrechte, wie eine Kündigung, wenn die Datenpreisgabe unterbleibt, bedarf es daher nicht. Liegt jedoch eine Pflichtverletzung vor, da auch keine Geldleistung gezahlt wird, kann auf das bereits bestehende Rechtsregime des allgemeinen Schuldrechts zurückgegriffen werden. Die Implementierung besonderer Kündigungsrechte[96] wegen unterbleibender Datenpreisgabe oder Einwilligungserteilung würde insofern dem Nachteilsverbot nicht in gleicher Weise Rechnung tragen; der Betroffene würde sich vermutlich eher davon abschrecken lassen, eine Einwilligung zu widerrufen, wenn dies mit einer Kündigung in einem sozialen Netzwerk einherginge, als wenn er stattdessen aufgefordert würde, einen monatlichen Beitrag zu zahlen.

---

[90] Ausführlicher *Bijok*, Kommerzialisierungsfester Datenschutz, 354 ff.

[91] *Hahn*, Die zivilrechtliche Ersetzungsbefugnis, 2011, 40.

[92] Vgl. BGH NJW 1967, 553; *Wiese*, Alternativität in Schuldverhältnissen, 2017, 12.

[93] *Wiese*, Alternativität in Schuldverhältnissen, 2017, 12 m.w.N.; a. A. dagegen *Hahn*, Die zivilrechtliche Ersetzungsbefugnis, 2011, 75.

[94] Etwa so *Czajkowski*/*Müller-ter Jung* CR 2018, 157 (164); *Staudenmayer* NJW 2019, 2497 (2498).

[95] *Schulze*, Datenschutz und Verträge über digitale Inhalte, 2018, 130.

[96] Vgl. *Langhanke*/*Schmidt-Kessel* EuCML 2015, 218 (222); *Metzger* AcP 2016, 817 (859 f.); Referentenentwurf des BMJV vom 05.10.2020 zur Umsetzung der Digitale Inhalte-Richtlinie, 14 – § 327q Abs. 2 BGB-E.

III. Dateneigentum

Die rechtliche Debatte um ein Dateneigentum kann als kurz und intensiv bezeichnet werden. Während in den 1990er Jahren zunächst im anglo-amerikanischen Raum[97] und später dann versprengt auch in der deutschen Literatur[98] ein solches Eigentumsrecht diskutiert wurde, nahm die Diskussion erst in der zweiten Hälfte der 2010er Jahre an Fahrt auf,[99] wurde intensiv unter rechtspolitischen Erwägungen geführt und wird zuweilen sogar übereilt für beendet[100] erklärt.

Letztlich handelt es sich bei „Dateneigentum" jedoch um ein vielfältiges Schlagwort, das zahlreiche Facetten hat, die der Übersicht halber nicht zusammengeworfen werden sollten. Dazu zählt insbesondere eine Differenzierung von Ansätzen über ein Eigentum an sogenannten „Maschinendaten"[101] vor dem Hintergrund der Industrie 4.0 sowie den Ansatz, das Datenschutzrecht nicht als Begrenzung des erstgenannten anzusehen,[102] sondern ganz im Gegenteil das Dateneigentum aus dem Datenschutzrecht heraus zu begründen.

1. Betroffenheit als Zuordnungskriterium

Ein „Recht am eigenen Datum" kann sein Zuordnungskriterium vernünftigerweise nur in der Betroffenheit finden. Eine Anknüpfung an Leistung bzw. Investitionsschutz käme für personenbeziehbare Daten deshalb nicht in Betracht, da diese auch dem Verantwortlichen zufallen und sich die Rechtsposition somit gegen den Betroffenen wenden könnte.[103] Auch bei der Heranziehung des Skripturaktes entsteht diese Gefahr, wenn etwa die Erzeugung nicht vom Betroffenen veranlasst wird – aufgrund der überwiegend passiven Datenerhebung in der Informationswirtschaft sogar der Regelfall.[104] Kritisch wäre bei der Skripturakttheorie zudem, dass die Duplizierung eines Datums entgegen der Interessenlage zu der Entstehung eines neuen Rechtsgegenstandes führen könnte. Insbesondere aus Publizitätsgesichtspunkten muss dies zurückgewiesen werden.[105]

Wird die Betroffenheit zuordnend herangezogen, entsteht diese Gefahr nicht. Insbesondere führt die Duplizierung von Daten nicht zur Entstehung eines neuen Rechtsgegenstandes, da die Zuordnung an denjenigen erfolgt, auf den das Datum beziehbar ist. Das Datum ist wie eingangs erläutert zwar Regelungsgegenstand, aber eben nicht Schutzgegenstand. Die Kritik, dass dem Datum durch eine eigentumsrechtliche Betrachtung unverhältnismäßig stark in den Fokus rücke,[106] verfängt somit nicht. Die Zuweisung entlang der Betroffenheit würde zudem mit der Vermögenswerthaltigkeit von Daten zusammenfallen, die sich für den Betroffenen aus dem Wert der durch sie vermittelten Privatheit speist.

---

[97] *Mell* BTLJ 1996, 1 (76); *Lessig*, Code and other Laws of Cyberspace, 1999, 130; *Samuelson* Stan. L. Rev. 2000, 1125 (1134); *Schwartz*, Harv. L. Rev. 2004, 2056 (2069 ff.).

[98] *Götting*, Persönlichkeitsrechte, 1995, 144; spezifischer dann *Buchner*, Informationelle Selbstbestimmung, 2006, 209.

[99] Zuletzt etwa Datenethikkommission, Gutachten 2019, 104.

[100] Vgl. *Graf von Westphalen* IWRZ 2018, 9 (14)

[101] *Drexl et. al.* GRUR Int. 2016, 914; *Riehm*, VersR 2019, 714 (715); *Wiebe* CR 2017, 87 (89).

[102] Vgl. *Zech* GRUR 2015, 1151 (1160).

[103] Deutlich etwa Bundesministerium für Verkehr und digitale Infrastruktur, „Eigentumsordnung" für Mobilitätsdaten?, 2017, 14.

[104] *Riehm*, VersR 2019, 714 (715).

[105] So auch *Hoeren* MMR 2019, 5 (7).

[106] *Albers*, Informationelle Selbstbestimmung, 2006, 144 f.

2. Die Allmende-Problematik als Zuordnungsgrund

Über die entstehenden informationellen Privatheitskosten mangelt es für ein Dateneigentum nicht an der dafür nötigen Rivalität. Gleichwohl ist anzumerken, dass die mangelnde natürliche Exklusivität zu einer Allmende-Eigenschaft führt, die im Kontext der Informationswirtschaft und zahlreicher auf der Verwertung personenbeziehbarer Daten aufbauenden Geschäftsmodelle Übernutzungsrisiken nach sich zieht. Nachteilhaft ist dies für den Betroffenen, dessen präferenzwidriger Verlust seiner Privatheit durch die Unternehmen nicht kompensiert wird, obwohl diese gewinnbringenden Umsatz aus den Daten generieren.

Die gegenteilige Sorge vor einer „Anti-Allmende“,[107] also einem Unternutzungsrisiko, ist dem Datenschutzrecht hingegen völlig fremd. Das Datenschutzrecht dient nicht der Ankurbelung der digitalen Wirtschaft, sondern soll einen selbstbestimmten Umgang des Betroffenen mit seinen Daten ermöglichen. Das „Recht am eigenen Datum“ stellte eine besondere Verdeutlichung dieser Maxime dar, die eine mangelnde natürliche Exklusivität durch konstitutives Eigentum, d.h. rechtlicher Exklusivität, ausgliche. Anknüpfungspunkt hierfür wäre folglich auch das Datenschutzrecht, genauer: die betroffenenschützende Rechtsposition aus der Datenschutz-Grundverordnung, die ihren Kern im Einwilligungstatbestand findet.

Ebenfalls zurückzuweisen ist die Kritik, dass ein Dateneigentum begrenzt sein müsse und deshalb ein Eigentumsrecht zurückzuweisen sei.[108] Die Sozialbindung von Eigentum zwingt dazu, das Eigentum mit seinen Schranken zusammenzudenken. Aus der Notwendigkeit dieser Begrenzung kann aber nicht dessen pauschale Unverhältnismäßigkeit abgeleitet werden. In diesem Lichte kann in den Zulässigkeitstatbeständen des Art. 6 Abs. 1 DSGVO auch eine Inhalts- und Schrankenbestimmung erkannt werden. Während der Betroffene insbesondere dort über sein Eigentum verfügen kann, wo Dritte nur mit seiner Einwilligung Daten nutzen dürfen, ergeben sich Grenzen des Rechts dort, wo der Eingriff entweder bagatellartig ausfiele oder durch Gesetz, lebenswichtige Interessen anderer, rechtliche Verpflichtungen bzw. eine Vertragsdurchführung gerechtfertigt werden kann. Dies würde weiterhin im Gleichlauf mit dem bereits weiter oben erläuterten Recht auf eine faire Vergütung stehen, das sich auf Einwilligungskonstellationen konzentrierte.

3. Die Einwilligung als Zuordnungsnorm

Aus der Reichweite absoluter Rechte ergibt sich ein numerus clausus-Prinzip[109] solcher Rechtspositionen, die insofern aus konkreten Rechtsnormen abzuleiten sind. Herleitungsversuche aus dem BGB,[110] KUG,[111] UrhG,[112] GeschGehG[113] oder gar dem StGB[114] gelingen nicht in überzeugender Weise. Für die Einwilligung ist dabei fraglich,

---

[107] So *Esken*, Dateneigentum und Datenhandel, 2019, 79.

[108] So etwa *Determann* ZD 2018, 503 (508).

[109] *Jänich*, Geistiges Eigentum, 2002, 242; *McGuire*, Die Lizenz, 2012, 274 ff.; vgl. auch *Berberich*/*Golla* PinG 2016, 165 (175); *Eichberger* VersR 2019, 709 (712 f.); *Klüber*, Persönlichkeitsschutz und Kommerzialisierung, 2007, 82; *Wiebe*/*Schur*, ZUM 2017, 461 (464).

[110] Vgl. etwa *Hoeren*/*Völkel*, Eigentum an Daten, 2014, 37; *Härting* CR 2016, 646 (647); *Riehm* VersR 2019, 714 (716).

[111] Dazu *Buchner*, Informationelle Selbstbestimmung, 2006, 215.

[112] *Grützmacher* CR 2016, 486 (487 f.).

[113] Vgl. *Graf von Westphalen* IWRZ 2018, 9 (14).

[114] *Hoeren* MMR 2019, 5 (7).

ob hinter der zuvor betrachteten schuldrechtlichen Ebene auch eine absolute Ebene liegen könnte.

Dabei fällt auf, dass im Zuge der Betrachtung des Geschäftsmodells „Daten bzw. Einwilligung gegen Leistung" zwischen der schuldrechtlichen Einwilligungsverpflichtung und der eigentlichen Einwilligungserteilung unterschieden werden kann. Die Einwilligungsverpflichtung ist der rein schuldrechtliche Akt, bei dem ein Vertrag geschlossen wird. Der Betroffene verpflichtet sich dabei, seine Einwilligung zu erteilen, um dadurch dem Verantwortlichen die Datenerhebung rechtlich zu ermöglichen und im Gegenzug eine Dienstleistung von diesem in Anspruch zu nehmen. Die Leistungspflicht kann dabei im Wege der Ersetzungsbefugnis durch eine Geldleistung ausgetauscht werden. Die Einwilligungserteilung bzw. ihr Widerruf sind die Durchführung dieser Pflicht oder Ausübung der Ersetzungsbefugnis nach alleiniger Maßgabe des Datenschutzrechts.

Immer wieder werden Eigentumsrechte an Daten dabei mit dem Lizenzmodell in Verbindung gebracht, also dass entsprechende Ausschließlichkeitsrechte über Lizenzen vergeben werden. Da sich das Wort „Lizenz" vom lateinischen „licet", d.h. „Erlaubnis" ableitet,[115] liegt es nahe, eine etwaige absolute Wirkung in der datenschutzrechtlichen Einwilligung zu suchen. Versuche, dafür das Recht auf Datenübertragbarkeit zu bemühen,[116] überzeugen hingegen nicht. Zwar wird versucht, in Art. 20 DSGVO einen vindikationsähnlichen Herausgabeanspruch zu erkennen. Gleichwohl folgt ein Vindikationsanspruch dem Eigentum, begründet es aber nicht.

Die Nähe der Einwilligung zur Lizenz schimmert immer häufiger auch in Praxis[117] und Rechtsprechung[118] durch. So geht der BGH in seiner Entscheidung zum digitalen Nachlass davon aus, dass Erben sogar als Vertragspartei in einen Nutzungsvertrag aufrücken können, der auf dem Austausch von Daten bzw. einer Einwilligung gegen Leistung beruht, ohne selbst Betroffene zu sein.[119] Dennoch gingen die Betroffenenrechte auf sie über. Diese Kontrolle über persönliche Inhalte wird sogar direkt mit einer Verfügungsbefugnis in Verbindung gebracht.[120] Zwar besteht nach Erwägungsgrund 27 DSGVO kein postmortaler Datenschutz, gleichwohl kann sich dieser aber aus nationalem Vertragsrecht ergeben. Persönlichkeitsinteressen und Vermögensinteressen sind somit auch keine Gegenspieler, sondern fließen beide in einer einheitlichen Rechtsposition zusammen.[121]

4. Umfang der Herrschaftsposition an Daten

Ziel eines absoluten Rechts an eigenen Daten ist die Auflösung der Allmende-Problematik durch die Stärkung der Kontrollfähigkeit persönlicher Informationen. Einerseits kann dies durch die Selbstbestimmung der Datenhingabe selbst gefördert werden. Andererseits muss diese Kontrollfähigkeit auch noch graduell vorhanden bleiben, nachdem personenbeziehbare Daten preisgegeben wurden. Andernfalls bliebe dem Betroffenen nur die Möglichkeit zwischen dem Ausbleiben von Kommunikation und der Akzeptanz seines Kontrollverlustes infolge von Kommunikation.

---

[115] *McGuire*, Die Lizenz, 2012, 31.
[116] Vgl. *Jülicher*/*Röttgen*/*Schönfeld* ZD 2016, 358 (361).
[117] Hierzu *Kutscher*, Der digitale Nachlass, 2015, 31 f.; *Jülicher* ZIP 2015, 2063 (2066), Fn. 37.
[118] BGH NJW 2018, 3178 = BGHZ 219, 243 (254, 260); OLG Düsseldorf, K&R 2012, 819.
[119] BGH NJW 2018, 3178 = BGHZ 219, 243 (259 f.); dazu *Martini*/*Kienle* JZ 2019, 235 (237).
[120] BGH NJW 2018, 3178 = BGHZ 219, 243 (274).
[121] *Langhanke*, Daten als Leistung, 2018, 156; *Wandtke* MMR 2017, 6 (9); vgl auch *Buchner*, Informationelle Selbstbestimmung, 2006, 214.

Ein Recht an den eigenen Daten als Herrschaftsposition würde sich dadurch kennzeichnen, dass diese „Informationsherrschaft" nicht nur deskriptiv eine faktische Herrschaftsmöglichkeit über die eigenen Daten nachzeichnet, sondern darüber hinaus auch normativ den Herrschaftswillen über die eigenen Daten absichert. Eine solche Konzeption findet sich auch bei anderen absoluten Rechten, wie etwa mit der „Sachherrschaft" im Sachenrecht oder der „Werkherrschaft"[122] im Urheberrecht. Diese Konzeption einer Informationsherrschaft legt zudem nahe, dass ein Recht an den eigenen Daten Assoziationen zur Idee des Besitzes weckt. Diese Assoziation wird auch bereits in der Literatur andiskutiert,[123] wenngleich sie noch stark von der Idee des sachenrechtlichen Besitzes im Sinne des §§ 854 ff. BGB geleitet wird. Der Vergleich mit den §§ 854 ff. BGB sollte allerdings nicht überstrapaziert werden, da im Sachenrecht dem Besitz an sich keine zuordnende Funktion zukommt, sondern dieses einem Recht zum Besitz überlassen bleibt, welches sich seinerseits durch das Eigentum legitimieren muss.[124]

Während die Sachherrschaft allein nur Besitz, aber kein Eigentum begründen kann, sieht dies für die Werkherrschaft im Urheberrecht und die Informationsherrschaft im Daten(schutz)recht freilich anders aus. Entscheidender Unterschied ist, dass es sich beim sachenrechtlichen Eigentum um ein solches handelt, welches eine natürliche Exklusivität anerkennt, ein Dateneigentum hingegen die Exklusivität rechtlich erst schafft. Die Informationsherrschaft dient als eben dieses konstitutive Element.

Dass eine solche Herrschaftsposition dem Leitgedanken des Datenschutzes entspricht, zeigt sich etwa im Recht der Datenübertragbarkeit aus Art. 20 DSGVO in Verbindung mit dem Recht auf Löschung aus Art. 17 DSGVO. Mit diesen beiden Rechten ausgestattet ist es dem Betroffenen möglich, auch nach der Datenhingabe zu bestimmen, wer Inhaber seiner Daten sein darf. Beide Ansprüche in Kombination können als eine Art „Datenherausgabeanspruch" gesehen werden,[125] bei dem der Betroffene bestimmt, wer neuer Inhaber der anspruchsgegenständlichen Daten wird und dass der Anspruchsgegner gleichzeitig seine Inhaberschaft über die Daten verliert. Diese Informationsherrschaft kann sogar dergestalt ausgeübt werden, dass der Betroffene die Daten nicht an sich, sondern an einen Dritten übertragen lässt. Eine Möglichkeit, die in der Informationswirtschaft ein wichtiges Instrument sein kann, um ganze Nutzerprofile zwischen verschiedenen Dienstanbietern zu verschieben – oder wieder an sich zu ziehen. Dass dieses Instrument oft im Lichte des Wettbewerbsrechts gesehen wird,[126] verdeutlicht nochmals den mit den Daten verbundenen, für zahlreiche Geschäftsmodelle wettbewerbsrelevanten Vermögenswert.

Die Frage nach dem Verbleib von Daten in der Insolvenz stellt eine weitere „Gretchenfrage" dar, die eine umfängliche Herrschaftsposition erkennen lässt. Konkret betrifft dies beispielsweise eine Konstellation, bei der personenbeziehbare Daten in der Sphäre des Verantwortlichen gespeichert sind – beispielsweise einem Clouddienstanbieter – und dieser insolvent geht.[127] Welche Ansprüche hat der Betroffene im Hinblick auf seine Daten? Führt der Insolvenzverwalter ein bestehendes Vertragsverhältnis nach § 103 InsO nicht fort, so kann der Betroffene nach § 45 S. 1 InsO nur den Geldwert seiner Daten geltend machen – vorausgesetzt, ein solcher wird von der Rechtsordnung

[122] Vgl. *Jänich*, Geistiges Eigentum, 2002, 197 f.
[123] *Hoeren* MMR 2019, 5 (6).
[124] *Michl* NJW 2019, 2729 (2731 ff.).
[125] Vgl. *Graef*/*Husovec*/*Purtova* GLJ 2018, 1359 (1369).
[126] So etwa *Hoffmann* JZ 2019, 960 (968).
[127] *Jülicher* ZIP 2015, 2063 ff.; vgl. *Eichberger* VersR 2019, 709 mit dem Verweis auf eine dahingehend gerichtete kleine Anfrage an die Bundesregierung BT-Drs. 19/8108.

anerkannt. Geht ein solcher „Herausgabeanspruch“ allerdings über die vertragsrechtliche Ebene hinaus und offenbart eine dahinterliegende absolute Wirkung, so wären Daten nach § 47 S. 1 InsO aussonderungsfähig und könnten direkt herausverlangt werden.

Bemerkenswert ist, dass etwa Luxemburg schon 2013 auf diese Frage reagierte, indem es in Art. 567 Code de Commerce einen solchen Herausgabeanspruch in der Insolvenz kodifizierte.[128] Auch die Praxis versucht zuweilen, das Problem mit expliziten „Dateneigentumsklauseln“ zu lösen[129] – was aufgrund der Relativität einer vertraglichen Vereinbarung allerdings nicht dieselbe Wirkung erzielen kann.

E. Ergebnisse

1. Die Defizite des Datenschutzrechts liegen einerseits in einer allgemein zu kurz greifenden Rechtsrelevanz des Datenverarbeitungsprozesses und andererseits darin, dass die althergebrachten Regelungsmaximen des Datenschutzrechts speziell in der Informationswirtschaft nicht anschlagen und den Betroffenen somit de facto schutzlos stellen. Die Betonung der Persönlichkeitsrelevanz wird dem Datenschutzrecht letztendlich zum Verhängnis.
2. Die Gefährdungslagen des Betroffenen in der Informationswirtschaft lassen sich auf Selbstbestimmungsdefizite zurückführen, Dies äußert sich in mangelndem Bewusstsein für die eingegangen Privatheitsrisiken, dem Verhältnis dieser zu den Vorteilen der im Gegenzug angebotenen Dienstleistungen und einer mangelnden Kontrollfähigkeit, wenn die Daten einmal hergegeben wurden.
3. Aufgabe der Datenschutzrechtsordnung muss sein, diese Gefährdungslagen im Kern zu adressieren. Grundvoraussetzung für einen Schutz vor Gefährdungslagen ist jedoch, dass diese Gefährdungslagen zunächst als legitim und existent anerkannt werden. Wer sich weigert, Daten als Wirtschaftsgüter anzuerkennen, kann auch nicht vor den Gefahren schützen, die gerade aus dieser Eigenschaft erwachsen.
4. Der Betroffene hat zumeist kein ausgeprägtes Wissen um die wirtschaftliche Bedeutung seiner Daten für die Informationswirtschaft; und wenn er es weiß, so fehlt es am alltäglich vorhandenen Bewusstsein hierfür. Sowohl die rechtliche Anerkennung von Datenwerten würde dem Betroffenen dies ins Bewusstsein rufen als auch der Zuspruch durch die Rechtsordnung, dass es letztlich um *seine*[130] Daten geht – eine Zuordnung, die längst gesellschaftlich in der Datenschutzdebatte angekommen ist.

Often personal data is compared to a „raw material“, in regard to its crucial role for business models in the information economy. Hence, this data becomes a commodity, without the legal system, especially information privacy law, reacting to this development different from scepticism. It seems that data as „raw material“ can be mined by businesses for free. Data subjects on the other hand do not participate in any profits made. This paper first examines accruing privacy costs for data subjects due to data disclosure. Based on this, it discusses formation of prices, contract law and an eventual exclusive right („data property“) related to personal data.

[128] *Jülicher* ZIP 2015, 2063 (2066); vgl. auch *Hoffmann* JZ 2019, 960 (968).
[129] *Jülicher* ZIP 2015, 2063 (2066, Fn. 37).
[130] Selbst in BVerfG NJW 1984, 419 ist stets von „seinen“ personenbezogenen Daten die Rede, wenn es um den Betroffenen geht. Einzig, als es um Ausschließlichkeitsrechte geht, wird diese sprachliche Zuordnung überhaupt in Anführungszeichen gesetzt.

Jetzt 3 Monate ZD kostenlos testen und Geschenk sichern!

IHR GESCHENK

SONDERAUSGABE DER AUSKUNFTS-ANSPRUCH NACH ART. 15 DS-GVO

Die große Zeitschrift zum Datenschutz

Die ZD informiert umfassend über die relevanten datenschutzrechtlichen Aspekte aus allen Rechtsgebieten und begleitet die nationale sowie internationale Gesetzgebung und Diskussion um den Datenschutz. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B. ‣ Konzerndatenschutz ‣ Beschäftigtendatenschutz ‣ Datenschutz-Folgenabschätzung ‣ Compliance ‣ Kundendatenschutz ‣ Telekommunikation ‣ Soziale Netzwerke ‣ Datentransfer in Drittstaaten ‣ Vorratsdatenspeicherung ‣ Informationsfreiheit ‣ Profiling und Scoring ‣ Tracking.

Geschaffen für die Unternehmenspraxis

Jedes Heft enthält ein Editorial, Aufsätze mit Lösungsvorschlägen, Angaben zur Lesedauer, Abstracts in Deutsch und Englisch, Schlagwortketten, Entscheidungen mit Anmerkungen und aktuelle Meldungen.

Alles inklusive:

- Online-Modul ZDDirekt – vollständiges Online-Archiv ab ZD 1/2011
- 14-täglicher Newsdienst ZD-Aktuell
- Homepage www.zd-beck.de
- Fundstellen-Recherche in beckonline.

3 Hefte gratis

Bestellen Sie das kostenlose Schnupperabo unter www.beck-shop.de/go/ZD.

ZD – Zeitschrift für Datenschutz

11. Jahrgang. 2021. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 279,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 219,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 15,– jährlich.

beck-shop.de/go/ZD

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

Der Schlüssel zum optimalen Umgang mit dem Datenschutzrecht.

Der bewährte Handkommentar

erläutert die vielfältigen Anwendungsfragen von DS-GVO und BDSG **fundiert und praxisnah.** Er überzeugt dabei durch **leichte Handhabung** und **hohe Relevanz** sowohl **für Praktiker** als auch **für Wissenschaftler.** Erfahrene Expertinnen und Experten aus Praxis, Wissenschaft und Aufsichtsgremien erläutern die komplexen Regelungen und deren Auswirkungen.

Die 3. Auflage

berücksichtigt topaktuell das Thema **»COVID-19-Pandemie und Datenschutzrecht«:** Datenschutz im Home-Office, Corona-Apps, Datenerhebungen von Versammlungsteilnehmern, Möglichkeiten einer pandemiebedingten Flexibilisierung der in der DS-GVO vorgegebenen Fristen (z.B. bei der Bearbeitung von Auskunftsanfragen nach Art. 15 DS-GVO) und andere Aspekte der Corona-Pandemie werfen vielfältige datenschutzrechtliche Fragen auf, für die der Kommentar erste Antworten bietet.

Darüber hinaus werden die Gesetzesänderungen durch das **2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU** berücksichtigt:

- Änderung der §§ 1, 4, 9, 16, 19, 22, 26, 38 BDSG
- neuer § 86 BDSG (Verarbeitung personenbezogener Daten für Zwecke staatlicher Auszeichnungen und Ehrungen)

Neue Rechtsprechung

Außerdem sind zahlreiche neue datenschutzrechtliche Gerichtsentscheidungen eingearbeitet, z.B. das **EuGH-Urteil Schrems II** und die BVerfG-Entscheidungen Recht auf Vergessen I und II.

Paal/Pauly
DS-GVO BDSG · Datenschutz-Grundverordnung Bundesdatenschutzgesetz

3. Auflage. 2021. XLV, 1560 Seiten.
Gebunden € 139,–
ISBN 978-3-406-75374-9
Neu im Januar 2021

beck-shop.de/30829288

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 172495
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK