MMR

Zeitschrift für IT-Recht und Recht der Digitalisierung

in Kooperation mit: Bitkom · davit im DAV · eco · game · Legal Tech Verband · VAUNET

AUS DEM INHALT

www.mmr.de

twitter.com/MMRZeitschrift

de.linkedin.com/showcase/zeitschriftmmr

7/2021

Seiten 521–600
24. Jahrgang · 15. Juli 2021
Verlag C.H.BECK München

1850202107

Deutsche Stiftung für Recht und Informatik

DSRI-HERBSTAKADEMIE 2021

Im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt

Die nunmehr 22. Herbstakademie 2021 wird von der DSRI in Verbindung mit der DGRI gemeinsam mit dem wissenschaftlichen interdisziplinären Zentrum für Recht der Informationsgesellschaft (ZRI) der Universität Oldenburg veranstaltet.

Die virtuelle 22. DSRI-Herbstakademie stellt ab dem 1.9.2021 etwa 57 Vorträge zu aktuellen Themen des Informationstechnologierechts als Videos nebst Folien auf ihrer Webseite online. Neben den in einem Review-Prozess ausgewählten Beiträgen werden in den »Updates« von Experten Überblicke über die Rechtsentwicklung des letzten Jahres in wichtigen Bereichen des IT-Rechts gegeben.

Live-Eröffnung am 1.9.2021, 19:00 Uhr, Oldenburger Schloss

Annie Heger, MusikComedy auf Platt und Hoch
Prof. Dr. Louisa Specht-Riemenschneider, Lösungsoption Datentreuhand
Oliver Thomsen, DSRI-Vorstand, Vergabe des Best Paper Award
Interaktives Cocktail-Mixen mit BARprofi Kim Kalinski

THEMENÜBERBLICK

DATENSCHUTZ

- Einwilligung bei Dark Pattern
- Marketing-Einwilligungen
- Dark Pattern
- Cookies und die Einwilligung
- Datenschutzkonforme Due Diligence
- Kündigung bei DSGVO-Verstoß
- Privacy by Design
- Automatisierte Entscheidungsfindung
- Datenschutzmanagement
- Gesundheitsdaten
- Verantwortliche bei Blockchains
- Datenschutz in der Insolvenz
- Restschuldbefreiung nach Privatinsolvenz
- Online-Prüfungssoftware
- Sprachassistenten
- Datenübermittlung im Kfz
- Datenschutz-Zertifizierung
- Update Datenschutz

IT-RECHT

- Blockchain und Smart Contracts
- Non-fungible Tokens
- Software als digitales Produkt
- Mängelrechte bei digitalen Produkten
- B2B-AGB in SW-Verträgen
- LegalTech-Inkasso
- Agile IT-Projekte
- Update IT-Vertragsrecht

STEUERRECHT

- Digitalisierung im Steuerrecht
- Nationales Steuerrecht
- Internationales und europäisches Steuerrecht

DATENSICHERHEIT

- IT-Sicherheitslücken
- Bewertung von IT-Sicherheitsvorfällen
- Hacking autonomer Kfz
- Update IT-Sicherheit

SOZIALE MEDIEN

- Betreiberverantwortlichkeit
- Daten-Governance
- Barrierefreiheit
- Kommunikationsplattform

SMART CITY

- Urban Air Mobility – Die Paketdrohne
- Smart Building

KÜNSTLICHE INTELLIGENZ

- AIaaS Compliance
- EU-Regulierung von KI
- Unrechtmäßige Nutzung von KI-Trainingsdaten
- ePerson mbH
- KI und Produkthaftung
- Gesetz zum autom. Fahren

IMMATERIALGÜTERRECHT / TK-RECHT

- Update Immaterialgüterrecht
- Update TK-Recht

Deutsche Stiftung für Recht und Informatik (DSRI)

Tel.: (0441) 798 - 4093 / - 4135
Fax: (0441) 798 - 4136
Mail: herbstakademie@dsri.de

Postanschrift:
Kurwickstr. 14/15
26122 Oldenburg

Tagungsentgelt – Die Freischaltung des Zugangs zu Vorträgen und Eröffnungsabend ist kostenpflichtig. Im Entgelt in Höhe von 115,00 € sind enthalten: Zugangscodes zu den Videodateien und Vortragsfolien zu den ab 1.9.2021 freigeschalteten Vorträgen, Teilnahme an der Live-Eröffnungsveranstaltung am 1.9.2021 und der Tagungsband im Wert von 69,80 €. Pro Person kann ein Cocktail-Paket (Basis für 3 Cocktails) zum subventionierten Preis von 30,00 € portofrei bestellt werden.

Buchung und Freischaltung der Vorträge auf der Website **www.dsri.de**.

Detaillierte Informationen zum Programm, zum Ablauf der virtuellen Tagung und zur FAO-Bescheinigung finden Sie unter **www.dsri.de**.

Die Veranstaltung wird unterstützt von:

CBH Rechtsanwälte, Köln • CSW Rechtsanwälte, München • DLA Piper, Köln/München • EpicWork AG, Hannover • Luther Rechtsanwaltsgesellschaft, Köln • Meinicke & Berthel RAe/FAe, Hamburg • Osborne Clarke, Hamburg • reuschlaw LegalConsultants, Saarbrücken • Scheja und Partner Rechtsanwälte mbB, Bonn • Schürmann Rosenthal Dreyer, Berlin • Taylor Wessing, Hamburg • tecLEGAL Habel | LLP Law, München • Witzel Erb Backu & Partner RAembB, München • WP Dr. Widmer & Partner, Bern

Medienpartner:

CR · DATENSCHUTZ-BERATER · InTeR · Kommunikation & Recht · MMR Zeitschrift für IT-Recht und Recht der Digitalisierung · ZD Zeitschrift für Datenschutz

MMR
Zeitschrift für IT-Recht und Recht der Digitalisierung
TK · IT-Security · Medien · Robotik · KI · Datenschutz · Games
twitter.com/MMRZeitschrift
de.linkedin.com/showcase/zeitschriftmmr
7/2021
Seiten 521–600

INHALT

Jörg Ukrow EDSA: Leitlinien zum Targeting von Nutzern sozialer Netzwerke verabschiedet MMR-Aktuell 2021, 439463

Eine bedeutende digitale Kommunikationsentwicklung während der 2010er-Jahre war der Aufstieg der sozialen Medien. Immer mehr Menschen nutzen soziale Medien, um mit Familie und Freunden in Kontakt zu bleiben, um sich beruflich zu vernetzen oder um sich über gemeinsame Interessen und Ideen zu verbinden. Zu den Hauptmerkmalen sozialer Medien gehört die Möglichkeit für Einzelpersonen, sich zu registrieren, um „Konten" oder „Profile" für sich selbst zu erstellen, miteinander zu interagieren, indem sie nutzergenerierte oder andere Inhalte teilen, und Verbindungen und Netzwerke mit anderen Nutzern aufbauen.

Als Teil ihres Geschäftsmodells bieten viele Social-Media-Anbieter Targeting-Dienste an. Diese ermöglichen es dem „Targeter", bestimmte Botschaften an die Nutzer sozialer Medien zu übermitteln, um kommerzielle, politische oder andere Interessen zu fördern. Ein kennzeichnendes Merkmal des Targeting ist die wahrgenommene Anpassung zwischen der Person oder Gruppe, auf die abgezielt wird, und der Botschaft, die übermittelt wird. Die zu Grunde liegende Annahme ist, dass, je besser diese Anpassung ist, desto höher die Empfangsrate (Conversion) und damit die Effektivität der Targeting-Kampagne (Return on Investment) ist.

Die Mechanismen für das Targeting von Social-Media-Nutzern sind im Laufe der Zeit immer ausgefeilter geworden. Organisationen haben nun die Möglichkeit, Personen auf der Basis einer Vielzahl von Kriterien anzusprechen. Solche Kriterien können auf der Grundlage von persönlichen Daten entwickelt worden sein, die Benutzer aktiv zur Verfügung gestellt oder geteilt haben, wie z.B. ihr Beziehungsstatus. Zunehmend werden Targeting-Kriterien jedoch auch auf der Grundlage von personenbezogenen Daten entwickelt, die entweder vom Social-Media-Anbieter oder von Dritten beobachtet oder abgeleitet und von der Plattform oder von anderen Akteuren (z.B. Datenbrokern) gesammelt (aggregiert) wurden, um Ad-Targeting-Optionen zu unterstützen. Mit anderen Worten: Das Targeting von Social-Media-Nutzern beinhaltet nicht nur den Akt der „Auswahl" der Einzelpersonen oder Gruppen von Einzelpersonen, die die beabsichtigten Empfänger einer bestimmten Nachricht sind (das „Zielpublikum"), sondern einen gesamten Prozess, der von einer Reihe von Akteuren durchgeführt wird und zur Übermittlung bestimmter Nachrichten an Einzelpersonen mit Social-Media-Konten führt.

Die Kombination und Analyse von Daten, die aus verschiedenen Quellen stammen, zusammen mit der potenziell sensiblen Natur personenbezogener Daten, die im Zusammenhang mit sozialen Medien verarbeitet werden, schafft Risiken für die Grundrechte und -freiheiten von Personen. Aus Sicht des Datenschutzes beziehen sich viele Risiken auf den möglichen Mangel an Transparenz und Nutzerkontrolle. Für die betroffenen Personen ist die zu Grunde liegende Verarbeitung personenbezogener Daten, die zur Übermittlung einer gezielten Nachricht führt, oft undurchsichtig. Darüber hinaus kann es zu unerwarteten oder unerwünschten Verwendungen personenbezogener Daten kommen, die nicht nur datenschutzrechtliche Fragen aufwerfen, sondern auch in Bezug auf andere Grundrechte und -freiheiten problematisch sind. In letzter Zeit hat das Targeting in sozialen Medien zudem im Zusammenhang mit demokratischen Entscheidungsfindungs- und Wahlprozessen an öffentlichem Interesse und regulatorischer Kontrolle gewonnen.

Vor diesem Hintergrund hat der durch die DS-GVO eingerichtete *Europäische Datenschutzausschuss (EDSA)* am 13.4.2021 Leitlinien zum Targeting von Nutzern sozialer Netzwerke angenommen. Unter Berücksichtigung der Rechtsprechung des *EuGH* sowie der Bestimmungen der DS-GVO in Bezug auf die gemeinsam für die Verarbeitung Verantwortlichen und ihre jeweilige Rechenschaftspflicht bieten die Leitlinien eine Orientierungshilfe für das Targeting von Social-Media-Nutzern, insbesondere im Hinblick auf die Verantwortlichkeiten von Targeting-Anbietern und Social-Media-Anbietern. Wo eine gemeinsame Verantwortlichkeit besteht, versuchen die Leitlinien anhand von Praxisbeispielen zu klären, wie die Verteilung der Verantwortlichkeiten zwischen Zielpersonen und Social-Media-Anbietern aussehen könnte. Das Hauptziel der Leitlinien ist daher die Klärung der Rollen und Verantwortlichkeiten zwischen dem Social-Media-Anbieter und dem Targeter. Zu diesem Zweck werden in den Leitlinien auch die potenziellen Risiken für die Rechte und Freiheiten natürlicher Personen, die Hauptakteure und ihre Rollen identifiziert und die Anwendung der wichtigsten Datenschutzanforderungen (wie Rechtmäßigkeit und Transparenz, Datenschutz-Folgenabschätzung usw.) sowie die Schlüsselelemente der Vereinbarungen zwischen Social-Media-Anbietern und den Zielpersonen behandelt.

Die Leitlinien unterstreichen u.a., dass wenn polarisierende oder unwahre (Desinformations-)Botschaften auf bestimmte Personen abzielen, ohne dass diese in einen bestimmten Kontext gestellt werden oder die Personen andere Standpunkte kennenlernen, der Einsatz von Targeting-Mechanismen dazu führen kann, dass der demokratische Wahlprozess untergraben wird – ein Aspekt, der auch in der laufenden Rechtsetzung i.R.d. Europäischen Aktionsplans für Demokratie besondere Beachtung verdient.

■ Vgl. auch *Delventhal*, ZD-Aktuell 2021, 05014; *Ebers*, MMR 2018, 423 und *Rauer/Ettig*, ZD 2021, 18.

Dr. Jörg Ukrow, LL.M.Eur.,
ist geschäftsführendes Vorstandsmitglied des Instituts für Europäisches Medienrecht e.V. (EMR) und stellvertretender Direktor der Landesmedienanstalt Saarland (LMS).

EU: Schärfere Regeln für internationalen Online-Handel MMR-Aktuell 2021, 439417

Anfang Juli 2021 sollen neue EU-Steuerregeln für Bestellungen bei außereuropäischen Online-Händlern in Kraft treten, so Medienberichte. Wichtigste Änderung sei dabei der Wegfall der bisherigen Freigrenze von 22,– EUR für Direktimporte.

Dadurch soll auf alle Päckchen 19% Einfuhrumsatzsteuer fällig werden. Die neue Freigrenze wird faktisch bei 5,23 EUR liegen. Außerdem müssen die Händler künftig für alle Sendungen eine Zollerklärung ausfüllen. Diese Steuerreform soll einen fairen Wettbewerb zwischen europäischen und ausländischen E-Commerce-Marktteilnehmern ermöglichen. Für Verbraucher*innen kann dies bedeuten, dass das Online-Shoppen von Waren aus China entsprechend teurer wird.

Christina Etteldorf Portugal: Datenschutzbehörde stoppt Datentransfer in die USA auf Basis von Schrems II

MMR-Aktuell 2021, 439471

Mit Entscheidung v. 27.4.2021 hat die portugiesische Datenschutzbehörde *(Comissão Nacional de Protecção de Dados – CNPD)* gegenüber dem *Instituto Nacional de Estadística (INE)* – dem portugiesischen Statistikinstitut, das u.a, für die Durchführung der Volkszählung zuständig ist – angeordnet, alle Datenübertragungen an in den USA oder in anderen Drittländern ansässige Dienstleister zu stoppen. Das stützt die *CNPD* auf das im Juli 2020 ergangene Urteil des *EuGH* im Schrems-II-Verfahren (MMR 2020, 597 m. Anm. *Hoeren* = ZD 2020, 511 m. Anm. *Moos/Rothkegel*), in dem bedeutende Feststellungen zur Rechtmäßigkeit von und Verantwortlichkeit für Datenübertragungen in die USA getroffen wurden.

I.R.d. Volkszählung hatte das hiermit betraute *INE* Anfang 2021 Briefe an portugiesische Haushalte verschickt, die einen Code und ein Passwort enthielten, um auf der vom *INE* betriebenen Webseite „censos2021.ine.pt" einen Online-Fragebogen zu beantworten, in dem u.a. auch personenbezogene Daten wie Namen angegeben werden sollten. Auf der Webseite sind verschiedene Sicherheits- und Content-Delivery-Dienste von *Cloudflare*, einem Dienstleister mit Hauptsitz in den USA, eingebunden. Der Dienst von *Cloudflare* verwendet dabei Anycast, eine Adressierungsart in Computernetzen, um den eingehenden Datenverkehr an das dem Nutzer am nächsten gelegene Rechenzentrum zu leiten, wobei IP-Adressen verwendet werden, die in den Vereinigten Staaten registriert sind.

Nach Auffassung der *CNPD* garantiert der Algorithmus, der den Datenverkehr weiterleitet, indem er den nächstmöglichen Server wählen soll, nicht, dass die Daten nicht an andere Server im Ausland gesendet werden. Insbesondere sehen die – vom *INE* akzeptierten – AGB von *Cloudflare* auch vor, dass personenbezogene Daten über jeden der 200 von *Cloudflare* verwendeten Server (u.a. in den USA, Südafrika, China, Indien, Jordanien, Mexiko, Russland, Singapur) übertragen werden können. Bei einer Übermittlung von personenbezogenen Daten von Unionsbürger*innen in ein Drittland außerhalb der EU fordert Art. 44 DS-GVO allerdings, dass sichergestellt sein muss, dass im Empfangsland ein vergleichbares Schutzniveau besteht. Sofern für das betreffende Drittland kein Angemessenheitsbeschluss der *EU-Kommission* vorliegt, darf eine Übermittlung nur erfolgen, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Bislang wurden solche geeigneten Maßnahmen darin gesehen, dass für die Übermittlung die Geltung der von der *EU-Kommission* entwickelten Standarddatenschutzklauseln zwischen den Beteiligten vereinbart wurde. In seinem Schrems-II-Urteil aus dem Jahr 2020 hatte der *EuGH* allerdings u.a. festgestellt, dass für die Verarbeitung Verantwortliche, die die Standardvertragsklauseln aus 2018 für Datenübermittlungen verwenden, dennoch weiterhin verpflichtet sind, Schutzmaßnahmen zu ergreifen, um ein gleichwertiges Schutzniveau in Drittländern zu gewährleisten.

Dieser Verpflichtung ist das *INE* als für die Datenverarbeitung Verantwortlicher nach Auffassung der *CNPD* nicht nachgekommen. Weder sei die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung getroffen und der Rat der *Datenschutzbehörde* eingeholt worden, noch seien die getroffenen Maßnahmen zur Gewährleistung der Cybersicherheit ausreichend. Zwar lege der Vertrag mit *Cloudflare* die Geltung der Standardvertragsklauseln der *EU-Kommission* zu Grunde, weitere, in diesem Fall erforderliche Maßnahmen seien aber nicht getroffen. Dabei merkt die *CNPD* insbesondere an, dass, wie das Schrems-II-Urteil zeigt, die Übermittlung von Daten in die USA zu Verletzungen von Grundrechten führen kann, da die US-Gesetzgebung den Zugriff der *Regierung* auf die Daten aus Gründen der nationalen Sicherheit und des öffentlichen Interesses erlaubt, ohne dabei klare und präzise Regeln für die Beschränkung dieses Zugriffsrechts oder die Durchsetzung von Betroffenenrechten vorzusehen. Daher wies die *CNPD* das *INE* an, innerhalb von zwölf Stunden nach Erlass der Entscheidung jegliche Verarbeitung personenbezogener Daten für die Volkszählung in den USA oder einem anderen Drittland ohne angemessenes Schutzniveau auszusetzen.

Diese Entscheidung zeigt, dass auch durch die Behörden langsam Konsequenzen aus der Schrems-II-Entscheidung gezogen werden. Im vorliegenden Fall betrifft dies den besonderen Fall, dass die Verarbeitung staatlich veranlasst ist und die Bürger*innen gesetzlich zur Teilnahme an der Volkszählung verpflichtet sind. Allerdings hat das Fehlen (rechts)sicherer Möglichkeiten, digitale Dienstleistungen und Produkte EU-ausländischer Anbieter einzubinden, sofern damit eine Datenverarbeitung auf Servern im Ausland verbunden ist, auch für den privaten Sektor eine ganz erhebliche Bedeutung.

■ Vgl. auch *Czeszak*, ZD-Aktuell 2020, 07250; *Henrich*, MMR-Aktuell 2020, 431928; ZD-Aktuell 2020, 07236; *Blasek*, ZD-Aktuell 2021, 05210; *Sörup-Parvez*, ZD 2021, 291 und *Kuntz*, ZD-Aktuell 2021, 05133 mwN.

Ass. iur. Christina Etteldorf
ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken/Brüssel.

OLG Frankfurt/M.: Äußerung zu Shitstorm als Tatsachenbehauptung

MMR-Aktuell 2021, 439419

Das *OLG Frankfurt/M.* (B. v. 11.5.2021 – 16 W 8/21) hat sich mit der Aussage befasst, jemand habe einen riesigen „Shitstorm" geerntet. Nach dem Verständnis eines durchschnittlichen Lesers handelt es sich bei einem Shitstorm um einen Sturm der Entrüstung. Nur wenige negative Stellungnahmen reichen nicht aus, um sie als „riesigen Shitstorm" zusammenzufassen. Die Ast., eine Sängerin, wendete sich u.a. gegen die Äußerung „Auch seine ehemalige Bandkollegin ... kommentiert, spricht von Demenz und erntet einen riesigen Shitstorm" in den sozialen Medien. Die *Vorinstanz* hatte den auf Unterlassung gerichteten Eilantrag noch zurückgewiesen. Die hiergegen gerichtete Beschwerde vor dem *OLG Frankfurt/M.* hatte teilweise Erfolg: In der Äußerung, dass die Antragstellerin einen riesigen Shitstorm geerntet habe, liege eine unwahre Tatsachenbehauptung. Bei dem Begriff „Shitstorm" handele es sich nach dem Verständnis eines durchschnittlichen Lesers um einen Sturm der Entrüstung. Wenige negative Stellungnahmen reichten nicht aus, um sie als „riesigen Shitstorm" zusammenzufassen.

■ Vgl. auch *Remmertz*, MMR 2018, 507; *Holznagel*, MMR 2018, 18 und MMR-Aktuell 2018, 400754.

BGH: Wettbewerbswidrige Bestpreisklauseln von Booking.com

MMR-Aktuell 2021, 439346

Der *BGH* (B. v. 18.5.2021 – KVR 54/20; MMR wird die Entscheidung demnächst veröffentlichen) hat entschieden, dass die von Booking.com bis 2016 eingesetzten und schon 2015 vom *Bundeskartellamt (BKartA)* als kartellrechtswidrig eingestuften „engen Bestpreisklauseln" wettbewerbswidrig sind.

Das Hotelportal Booking.com ermöglicht seinen Kund*innen die direkte Buchung von Hotels über die Website. Dazu schloss Booking.com mit verschiedenen Hotels Vermittlungsverträge, die vor 2016 in ihren AGB sog. „enge Bestpreisklauseln" vorsahen. D.h., dass die kooperierenden Hotels ihre Zimmer zwar unter bestimmten Voraussetzungen offline und auf anderen Plattformen billiger anbieten dürfen, nicht jedoch auf ihrer eigenen Website. Hier durften sie die angegebenen Preise auf Booking.com nicht unterschreiten.

Schon 2015 hatte das *BKartA* die Kartellrechtswidrigkeit solcher Klauseln festgestellt und den weiteren Einsatz ab 1.2.2016 untersagt, woraufhin Booking.com die Klauseln nicht mehr nutzte. In der weiteren gerichtlichen Auseinandersetzung hob das *OLG Düsseldorf* die Verfügung auf und entschied am 4.6.2019, dass solche Klauseln nicht kartellrechtswidrig seien, sondern eine notwendige Nebenabrede von Plattformen wie Booking.com sein können. Als solche sind sie nicht vom Kartellverbot des Art. 101 Abs. 1 AEUV und § 1 GWB erfasst.

Der *BGH* hob nun die Entscheidung des *OLG Düsseldorf* auf und stellte klar, dass solche Bestpreisklauseln zunächst wettbewerbswidrig sind. Durch die Beschränkung der Verfügungsbefugnis über die Preisangabe auf der eigenen Website wird den teilnehmenden Hotels insbesondere die Möglichkeit genommen, Kund*innen dadurch zu werben, dass sie die eingesparte Vermittlungsprovision bei interner Buchung an die Kund*innen direkt weitergeben und günstigere Preise anbieten können. Zugleich stellte der *BGH* klar, dass auch die Anwendung des Kartellverbots nach Art. 101 Abs. 1 AEUV nicht ausgeschlossen ist, weil eine notwendige Nebenabrede der Vermittlungsverträge vorliege, da es hier auf eine objektive Notwendigkeit für die Durchführung ankomme, die sich auch nach der weiteren Entwicklung von Booking.com ohne die Klauseln so nicht bestätigen konnte. Auch eine Freistellung nach Art. 2 Abs. 1 Vertikal-GVO oder eine Einzelfreistellung nach Art. 3 Abs. 1 Vertikal-GVO führen nach Ansicht des *BGH* nicht zu einer Ausnahme vom Verbot des Art. 101 Abs. 1 AEUV.

■ Vgl. auch *OLG Düsseldorf* MMR 2020, 794 (Ls.); MMR-Aktuell 2015, 365211 und *BKartA* MMR-Aktuell 2014, 358047 (Ls.).

DAV: Stellungnahme zum DSA

MMR-Aktuell 2021, 439260

Der *Deutsche Anwaltsverein (DAV)* begrüßt in seiner Stellungnahme durch die Ausschüsse Geistiges Eigentum und Informationsrecht den Verordnungsvorschlag der EU-Kommission für den *Digital Services Act (DSA)* in weiten Teilen.

Der *DAV* stellt fest, dass die Art. 3 bis 9 DSA kohärent auf die Regelungen der Art. 12 bis 15 RL 2000/31/EG (E-Commerce-RL) aufbauen und die Regelungsstruktur der Haftungsprivilegien entsprechend nicht grundlegend neugestaltet werden sollte. Dabei begrüßt der *DAV* insbesondere die grundsätzliche Beibehaltung der Haftungsprivilegien für Intermediäre, sodass europäische Unternehmen im internationalen Markt wettbewerbsfähig bleiben können, ohne dabei zu großen Haftungsrisiken ausgesetzt zu sein. Hier habe sich das Notice-and-Take-Down-Prinzip (Hinweis- und Löschprinzip) über die letzten Jahre bewährt.

Das Prinzip wurde allerdings durch mitgliedstaatliche Regelungskomplexe durchbrochen, so z.B. in Deutschland für Beseitigungs- und Unterlassungsansprüche, sodass die Regelungen der Art. 12 ff. E-Commerce-RL nach und nach durch komplizierte Rechtsprechung zur Störerhaftung überlagert wurden und die erstrebte Rechtssicherheit nur teilweise erreicht werden konnte.

Die Rechtsprechung des *EuGH* differenzierte bei den Haftungsprivilegien der Intermediäre zwischen reinen Intermediären und solchen mit einer „aktiven Rolle", auf die die Art. 12 bis 15 E-Commerce-RL nicht anwendbar sind (vgl. *EuGH* MMR 2011, 596 m. Anm. *Hoeren*) Zur Stärkung der Rechtssicherheit fordert der *DAV* für den DSA klarstellende Regelungen, die die *EuGH*-Rechtsprechung zu einer haftungsbegründenden „aktiven Rolle" der Provider berücksichtigen. Der *DAV* schlägt insbesondere im Hinblick auf Art. 6 DSA eine Klarstellung vor, dass der DSA eine Vollharmonisierung erreichen will und ausdrücklich auch die Haftung von Providern auf Beseitigung und Unterlassung erfasst. So soll praktischen Rechtsunsicherheiten vorgebeugt werden, die dadurch entstehen können, dass mit der deutschen Störerhaftung und den Grundsätzen der E-Commerce-RL sonst zwei schwer abzugrenzende Haftungsregime bestehen.

■ Vgl. auch *Grünwald/Nüßing*, MMR 2021, 283; *Schmid/Grewe*, MMR 2021, 279; MMR-Aktuell 2021, 438167 und MMR-Aktuell 2021, 438406.

Rezensionen · Tagungsberichte · Termine · Rezensionen · Tagungsberichte ·

NEU AUF DER HOMEPAGE

www.mmr.de

Rezensionen

- **Sina Dörr** David Nink, Justiz und Algorithmen, Berlin (Duncker & Humblot) 2021, ISBN 978-3-428-18106-3, 119,90 EUR
- **Dr. Konrad Duden** Martin Ebers / Christian Heinze / Tina Krügel / Björn Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik, Rechtshandbuch, München (C.H.BECK) 2020, ISBN 978-3-406-74897-4, 199,– EUR

Tagungsbericht

- **Quirin Weinzierl** FTC Workshop: Bringing Dark Patterns to Light

Jörg Ukrow UK: Draft Online Safety Bill zur Bekämpfung illegaler Online-Inhalte vorgestellt

MMR-Aktuell 2021, 439472

Der am 12.5.2021 veröffentlichte Entwurf eines Gesetzes zur Online-Sicherheit (Draft Online Safety Bill) enthält – in Anlehnung an neuere Rechtsetzungsvorschläge der *EU* wie den geplanten Digital Services Act – Entwürfe von Gesetzesänderungen, die schädlichen Online-Praktiken ein Ende setzen und gleichzeitig eine neue Ära der Rechenschaftspflicht und des Schutzes der demokratischen Debatte einläuten sollen. Die vorgesehenen Regelungen sollen die Rechte der Menschen stärken, sich online frei zu äußern, und gleichzeitig den Journalismus und die demokratische politische Debatte in Großbritannien schützen. Weitere Bestimmungen betreffen die Bekämpfung von weitverbreiteten Online-Betrügereien wie Romance Fraud, bei denen Menschen manipuliert wurden, um Geld an gefälschte Identitäten auf Dating-Apps zu senden. Hier sollen Online-Unternehmen für die Bekämpfung von betrügerischen nutzergenerierten Inhalten verantwortlich werden.

Social-Media-Sites, Websites, Apps und andere Dienste, die nutzergenerierte Inhalte hosten oder es Menschen ermöglichen, sich online mit anderen auszutauschen, soll nach dem Entwurf eine Sorgfaltspflicht gegenüber ihren Nutzer*innen treffen, sodass das, was offline inakzeptabel ist, auch online inakzeptabel sein wird. Sie müssen die Risiken berücksichtigen, die ihre Websites für die jüngsten und schutzbedürftigsten Menschen darstellen können, und handeln, um Kinder vor unangemessenen Inhalten und schädlichen Aktivitäten zu schützen. Sie müssen robuste Maßnahmen ergreifen, um illegalen Missbrauch zu bekämpfen, einschließlich schneller und effektiver Maßnahmen gegen Hassverbrechen, Belästigung und Drohungen gegen Einzelpersonen, und sie müssen ihre Versprechen gegenüber den Nutzer*innen hinsichtlich ihrer Standards einhalten.

Die größten und populärsten Social-Media-Seiten (Dienste der Kategorie 1) müssen nach dem Entwurf gegen Inhalte vorgehen, die zwar rechtmäßig, aber dennoch schädlich sind, z.B. Missbrauch, der unter der Schwelle einer Straftat liegt, Ermutigung zur Selbstschädigung und Fehlinformationen/Desinformation.

Plattformen der Kategorie 1 werden in ihren Geschäftsbedingungen explizit angeben müssen, wie sie gegen diese rechtmäßigen Schädigungen vorgehen.

Der Gesetzentwurf will zugleich sicherstellen, dass die Menschen in Großbritannien sich online frei äußern und an pluralistischen und wichtigen Debatten teilnehmen können. Alle Unternehmen, die unter das Gesetz fallen, müssen bei der Erfüllung ihrer Pflichten Schutzmaßnahmen für die freie Meinungsäußerung berücksichtigen und einführen. Diese Sicherheitsvorkehrungen werden von der britischen Regulierungsbehörde *Ofcom* in Verhaltenskodizes festgelegt, könnten aber z.B. beinhalten, dass menschliche Moderatoren in komplexen Fällen, in denen der Kontext wichtig ist, Entscheidungen treffen. Nutzer*innen müssen Zugang zu effektiven Beschwerdemöglichkeiten haben, wenn Inhalte ohne triftigen Grund entfernt wurden, und Unternehmen müssen diese Inhalte wiederherstellen, wenn sie ungerechtfertigt entfernt wurden. Nutzer*innen werden auch in der Lage sein, sich mit Beschwerden an die *Ofcom* zu richten. Dienste der Kategorie 1 werden nach dem Entwurf zusätzliche Pflichten haben. Sie müssen aktuelle Bewertungen ihrer Auswirkungen auf die freie Meinungsäußerung durchführen und veröffentlichen sowie nachweisen, dass sie Schritte unternommen haben, um jegliche negativen Auswirkungen zu mildern. Diese Maßnahmen sollen das Risiko begrenzen, dass Online-Unternehmen restriktive Maßnahmen ergreifen oder Inhalte übermäßig entfernen, um ihren neuen Online-Sicherheitspflichten nachzukommen. Ein Beispiel hierfür könnten KI-Moderationstechnologien sein, die harmlose Inhalte fälschlicherweise als schädlich kennzeichnen, wie etwa Satire.

Inhalte auf Websites von Nachrichtenverlagen fallen nicht in den Anwendungsbereich des Gesetzespakets. Dies umfasst sowohl ihre eigenen Artikel als auch Nutzerkommentare zu diesen Artikeln. Auch Artikel von anerkannten Nachrichtenverlagen, die auf Diensten, die in den Geltungsbereich fallen, geteilt werden, sind vom Anwendungsbereich ausgenommen. Unternehmen der Kategorie 1 sollen verpflichtet sein, den Zugang britischer Nutzer zu journalistischen Inhalten, die auf ihren Plattformen geteilt werden, zu schützen. Das bedeutet, dass sie bei der Moderation von Inhalten die Bedeutung des Journalismus berücksichtigen müssen, ein schnelles Einspruchsverfahren für entfernte Inhalte von Journalist*innen haben und von *Ofcom* für die willkürliche Entfernung von journalistischen Inhalten zur Rechenschaft gezogen werden können. Die Inhalte von Bürgerjournalist*innen sollen dabei den gleichen Schutz genießen wie die Inhalte von professionellen Journalist*innen.

Ofcom soll die Befugnis erhalten, Unternehmen, die gegen die neue Sorgfaltspflicht verstoßen, mit Geldstrafen von bis zu 18 Mio. GBP oder 10% des weltweiten Jahresumsatzes zu belegen, je nachdem, welcher Betrag höher ist, und den Zugang zu Websites zu sperren.

Das Gesetzespaket soll auch Bestimmungen enthalten, die Unternehmen dazu verpflichten, Inhalte über sexuelle Ausbeutung und Missbrauch von Kindern (Child Sexual Exploitation and Abuse), die in ihren Diensten identifiziert werden, zu melden. Dies soll sicherstellen, dass Unternehmen den Strafverfolgungsbehörden die qualitativ hochwertigen Informationen zur Verfügung stellen, die diese zum Schutz der Opfer und zur Ermittlung der Täter benötigen.

■ Vgl. auch *Ukrow*, MMR-Aktuell 2021, 438549; *ders.*, MMR-Aktuell 2019, 417643; *Schmid/Greve*, MMR-Aktuell 2021, 435431; *dies.*, MMR 2021, 279; *Höferlin/Widlock*, MMR 2021, 277 und *Schindler*, ZD-Aktuell 2021, 05097 mwN.

Dr. Jörg Ukrow, LL.M.Eur.,
ist geschäftsführendes Vorstandsmitglied des Instituts für Europäisches Medienrecht e.V. (EMR) und stellvertretender Direktor der Landesmedienanstalt Saarland (LMS).

Völkerrecht im Cyberraum

MMR-Aktuell 2021, 439254

Die *Bundesregierung* sieht in ihrer Antwort (BT-Drs. 19/29615) keinen Bedarf einer umfassenden Neuregelung auf Völkerrechtsebene bezogen auch auf Cyber-Sachverhalte. Nach Auffassung der *Bundesregierung* ist das „Völkerrecht des Netzes" ein untechnischer Sammel- und Oberbegriff für eine Vielzahl völkerrechtlicher Normen mit Relevanz für und Anwendbarkeit auf Cyber-Sachverhalte, die bereits Teil der existierenden Völkerrechtsordnung seien. Gleichwohl bringe sich die *Bundesregierung* in die laufende internationale Diskussion ein, „wie das geltende Völkerrecht, z.B. die UN-Charta, das im Wesentlichen vor dem Cyberraum entstanden ist, Anwendung findet".

■ Vgl. auch MMR-Aktuell 2011, 322757.

MMR

Zeitschrift für IT-Recht und Recht der Digitalisierung

TK · IT-Security · Medien · Robotik · KI · Datenschutz · Games

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

7/2021

EDITORIAL

IT-Schlichtungsverfahren – eine Lösung für den Corona-bedingten Verfahrensstau

Lesedauer: 10 Minuten

Professor Dr. Axel Metzger

Zora Witte

Seit Beginn der Corona-Pandemie sehen sich die staatlichen Gerichte mit zahlreichen Einschränkungen der Verfahrensabläufe konfrontiert. So wurden auf Grund des zunächst herrschenden Notbetriebs an den Gerichten, zusätzlicher Corona-bedingter Verfahren und der geltenden Abstandsregelungen viele Verfahren vertagt. Zwar arbeiten die Gerichte den Bedingungen angepasst weiter, allerdings mangelt es oft an Platz für die Durchführung von Verhandlungen unter Einhaltung der Corona-Regeln. Es wird zunehmend versucht, virtuelle Gerichtsverhandlungen zu ermöglichen, doch fehlt häufig noch die Ausrüstung für Video-Verhandlungen. Die Verfahrensbeteiligten befinden sich somit in der Situation, dass zwar Klage eingereicht und möglicherweise schon erwidert wurde, die Verhandlungstermine allerdings abgesagt wurden und noch keine neuen Termine angesetzt werden konnten. Die sinkenden Infektionszahlen werden in den kommenden Wochen zwar zu einer schrittweisen Rückkehr in die Normalität bei Gericht führen. Bis die aufgestauten Verfahren abgearbeitet sind, wird es aber noch einige Monate dauern.

Gerade bei rechtlichen Auseinandersetzungen i.R.v. IT-Projekten, wie Softwareerstellung, Outsourcing oder der Einführung oder Migration von Unternehmenssoftware, sind die Verfahrensbeteiligten jedoch auf eine rasche Klärung ihrer Streitigkeit angewiesen. Die meisten IT-Projekte beruhen auf aufwändigen Planungen und IT-Dienstleister wie Auftraggeber benötigen Planungssicherheit hinsichtlich einer weiteren Zusammenarbeit oder eines Wechsels des Dienstleisters. Ein ins Stocken geratenes Gerichtsverfahren kann zu Verzögerungen und zum Scheitern von IT-Projekten führen.

Vor diesem Hintergrund kann es für die Parteien IT-rechtlicher Streitigkeiten von Vorteil sein, eine außergerichtliche Streitbeilegung zu versuchen. Anders als bei der Mediation bewerten die Schlichter im Rahmen eines Schlichtungsverfahrens den Vortrag der Parteien und unterbreiten Einigungsvorschläge. Die Schlichter können flexibel und schnell auf die Corona-Regeln reagieren. Es gibt zahlreiche branchenspezifische Schlichtungsstellen. Ein etabliertes Schlichtungsverfahren für den IT-Sektor wird von der *DGRI (Deutschen Gesellschaft für Recht und Informatik)*, einer

unabhängigen wissenschaftlichen Fachgesellschaft für IT-Recht, angeboten. Die *DGRI* betreibt eine eigene Schlichtungsstelle, um ein speziell auf Fragen technischer Sachverhalte zugeschnittenes Verfahren zur Lösung rechtlicher Konflikte anzubieten. Den inhaltlichen und zeitlichen Schwerpunkt der Arbeit der *Schlichtungsstelle IT der DGRI* stellen die Vorbereitung, die Besetzung und Begleitung der Schlichtungsverfahren dar. Typische Streitfragen, die bei der Schlichtungsstelle eingehen, betreffen IT-Projektverträge unterschiedlicher Art, Softwareentwicklung, ERP-Systeme, Service Level Agreements, Fragen des gewerblichen Rechtsschutzes und Urheberrechts, Datenschutz und IT-Security, Softwarelizenzierung, Websites und Domains sowie E-Commerce.

Während das Gericht letztlich nur rein rechtlich entscheiden kann und (außer beim Vergleich) an die Anträge der Parteien gebunden ist, kann eine Schlichtung eine rechtliche und fachliche Lösung herbeiführen, die wesentlich zielführender ist. Dies wird gerade dadurch ermöglicht, dass das Schlichtungsteam im *DGRI*-Verfahren in der Standardkonstellation aus einem Juristen und einem Sachverständigen besteht. Die informelle Atmosphäre und die räumliche Flexibilität erlauben kurzfristige Ortstermine und eine zügige Konzentration des Verfahrens auf die wesentlichen Streitpunkte. Gerade bei laufenden Projekten und langjährigen Geschäftsbeziehungen erweist sich die beratende Rolle des Schlichtungsteams als erheblicher Vorteil. Während das gerichtliche Verfahren auf die endgültige Bewertung eines bestimmten Klagebegehrens aus der Vergangenheit gerichtet ist, kann die Schlichtung durch zukunftsorientierte, technisch und wirtschaftlich sinnvolle Kompromissvorschläge einen Projektverlauf positiv beeinflussen und eine weitere, konstruktive Zusammenarbeit der Parteien ermöglichen.

Auch nach Klageerhebung kann noch ein Schlichtungsantrag eingereicht werden, sofern kein obligatorisches Schlichtungsverfahren vor Klageerhebung vorgesehen ist und auch keine diesbezügliche Vereinbarung der Parteien vorliegt. Das bereits anhängige Gerichtsverfahren berührt das Schlichtungsverfahren nicht. Andersherum hat auch die Einreichung eines Schlichtungsantrags zunächst keine Auswirkungen auf das staatliche Gerichtsverfahren. Für die Möglichkeit, ein Schlichtungsverfahren auch nach Klageerhebung durchführen zu können, spricht insbesondere die Pflicht der Zivilgerichte, in jeder Verfahrenslage auf eine gütliche Einigung hinzuwirken. Das staatliche Gerichtsverfahren kann zur Ermöglichung einer außergerichtlichen Schlichtung ausgesetzt werden. Die Ergebnisse des Schlichtungsverfahrens können nach dessen Beendigung in das Gerichtsverfahren überführt werden. Wurde ein Schlichtungsvergleich erzielt, kann dieser als Anwaltsvergleich im Sinne der Zivilprozessordnung vor Gericht geschlossen werden. Erfolgt ein Schlichtungsspruch, kann dieser in das Gerichtsverfahren eingeführt werden. Das Gerichtsverfahren kann dadurch beendet werden, dass der außergerichtliche Vergleich zu einem Prozessvergleich gemacht wird. Dies hat zur Folge, dass sich die Begründetheit der Klage nach dem außergerichtlichen Vergleich richtet und der Beklagte auf Grundlage des Vergleichs anerkennen kann. Darüber hinaus besteht die Option einer beiderseitigen Erledigungserklärung oder einer Klagerücknahme durch den Kläger.

Ein Beispiel aus der Praxis der *Schlichtungsstelle IT* aus dem letzten Jahr verdeutlicht den effizienten Verfahrensablauf des Schlichtungsverfahrens:

Die Antragstellerin, ein Verlag, hat mit der Antragsgegnerin, einem Unternehmen, das Branchensoftware im Verlagswesen anbietet, einen Projektvertrag über die Lieferung von Software geschlossen. Im Verlauf der Zusammenarbeit kommt es zu Streitigkeiten hinsichtlich der Qualität der Dienstleistung. So bemängelt die Antragstellerin die Konzeption der Schnittstellen und die Programmierung des Systems. Mehrere Aussprachen zwischen Antragstellerin und Antragsgegnerin bleiben ergebnislos, sodass die Antragstellerin einen Schlichtungsantrag bei der *Schlichtungsstelle IT* einreicht. Dies ist ohne Weiteres möglich, da die Parteien die Schlichtungsklausel der *DGRI* in ihrem Projektvertrag aufgenommen haben.

Nach Eingang des Schlichtungsantrags Mitte September 2020 geht das Verfahren kurze Zeit später auf die Schlichter über. Die Verhandlungen finden per Videokonferenz unter Einsatz eines juristischen und eines technischen Schlichters statt. Anfang März 2021, und somit weniger als fünf Monate nach Verfahrensübergang, kann ein einvernehmlicher Schlichtungsvergleich erzielt werden.

Der geschilderte Fall aus der Praxis der *Schlichtungsstelle* steht beispielhaft für die Verfahrensabläufe der letzten Zeit. DGRI-Schlichtungsverfahren dauern im Schnitt 6,8 Monate. (vgl. hierzu näher *Metzger/Klein*, CR 2017, 73 (75)) Die staatlichen Gerichte, bei denen schon die erste Instanz oft über ein Jahr braucht und auch Schiedsverfahren nach Maßgabe der üblichen Schiedsordnungen, etwa der DIS, dauern im Durchschnitt deutlich länger.

Im Vergleich zu den Vorjahren bestand im Jahr 2020 ein gesteigertes Interesse an der Tätigkeit der *Schlichtungsstelle IT*. Während im Jahr 2019 drei Schlichtungsanträge eingingen, wurden im Jahr 2020 sechs Schlichtungsanträge eingereicht. In drei der Verfahren aus 2020 konnte ein Schlichtungsvergleich unterzeichnet werden, sodass die Verfahren bereits zu einem Abschluss gebracht werden konnten. Im Vergleich zu den Vorjahren setzt sich die Tendenz steigender Verfahrenszahlen fort. Die Schlichtungsteams und die künftigen Parteien profitieren von diesen aktuellen Erfahrungen aus der Durchführung von Schlichtungsverfahren unter Pandemiebedingungen.

Die bei der *Schlichtungsstelle IT* durchgeführten Verfahren führen in weit mehr als der Hälfte der Fälle zu einer Einigung der Parteien. Kann eine einvernehmliche Lösung nicht erzielt werden, so können zumindest die mit dem Sachverhalt befassten IT-Sachverständigen in weitergehenden Verhandlungen oder im Rahmen eines gerichtlichen Verfahrens eingesetzt werden.

Mithin kann eine außergerichtliche Einigung unter Zuhilfenahme der Dienste einer Schlichtungsstelle Abhilfe für die momentanen Verzögerungen staatlicher Gerichtsverfahren schaffen. Dabei ist, wie bereits dargestellt, so vorzugehen, dass das staatliche Gerichtsverfahren für die Dauer des Schlichtungsverfahrens ausgesetzt und ein Schlichtungsantrag bei einer Schlichtungsstelle eingereicht wird. Das Ergebnis des Schlichtungsverfahrens kann im Anschluss in das Gerichtsverfahren eingeführt werden und für dessen Beendigung sorgen. Dies erfordert allerdings, dass die Parteien den Streit im Rahmen einer Schlichtung beenden wollen. Ohne Zustimmung beider Seiten ist dieser Weg versperrt.

Die Schlichtung in IT-Rechtsstreitigkeiten bietet sich gerade in der aktuellen Situation eines eingeschränkten Betriebs bei den staatlichen Gerichten an. Durch das schlanke Verfahren, die Einbindung eines IT-Sachverständigen und die auf die Zukunft gerichtete Arbeitsweise ist die Schlichtung aber auch nach der Corona-Pandemie eine sinnvolle Alternative – gerade für streitige IT-Projekte.

Berlin, im Juli 2021

Professor Dr. Axel Metzger
ist Inhaber des Lehrstuhls für Bürgerliches Recht und Immaterialgüterrecht, insbesondere Gewerblicher Rechtsschutz an der Humboldt-Universität zu Berlin.

Zora Witte
betreut die Schlichtungsstelle am Lehrstuhl für Bürgerliches Recht und Immaterialgüterrecht, insbesondere Gewerblicher Rechtsschutz an der Humboldt-Universität zu Berlin.

THOMAS HOEREN / REINER MÜNKER

Geheimhaltungsvereinbarung: Rechtsnatur und Vertragsprobleme im IT-Sektor

Gestaltungs- und Vertragsmuster für die Beratung

Vertraulichkeit

Seit Inkrafttreten des Geschäftsgeheimnisgesetzes spielen Geheimhaltungsvereinbarungen eine konstitutive Rolle bei der Begründung des Geheimnisschutzes. Noch ist allerdings in der Praxis wenig darüber bekannt, wie man ein solches „Confidentiality Agreement" verfassen soll. Der Beitrag beleuchtet die Klippen für den beratenden Anwalt bei der Gestaltung und zeigt erste Denkansätze bis hin zu möglichen Vertragsklauseln.

Lesedauer: 20 Minuten

I. Einleitung

Im Rahmen der Aufnahme von Vertragsverhandlungen werden Beteiligte bereits früh mit Geschäftsgeheimnissen konfrontiert. Grundsätzlich besteht eine Nebenpflicht aus dem vorvertraglichen Schuldverhältnis, diese auch vertraulich zu behandeln.[1] Diese Pflicht ist jedoch meist nicht hinreichend bestimmt,[2] sodass es sich etabliert hat, die Partei, der Geschäftsgeheimnisse dargelegt werden, durch eine Geheimhaltungsvereinbarung (auch Vertraulichkeitsvereinbarung genannt) zur vertraulichen Behandlung zu verpflichten.

Geheimhaltungsvereinbarungen haben mit Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen eine ganz neue Bedeutung im deutschen Recht erlangt. Hat bisher ein bloßer Geheimhaltungswille gereicht um den Anforderungen der §§ 17 ff. UWG zu genügen, wird nun gem. § 2 Nr. 1 lit. b GeschGehG gefordert, dass angemessene Geheimhaltungsmaßnahmen getroffen wurden.[3] Dabei herrscht Einigkeit darüber, dass eine Geheimhaltungsvereinbarung ein Kernelement dieser Voraussetzung darstellt.[4]

Damit eine Information ein Geschäftsgeheimnis i.S.d. § 2 Nr. 1 GeschGehG ist und dessen Schutz genießt, muss sie u.a. geheim sein (§ 2 Nr. 1 lit. a GeschGehG) und ihr rechtmäßiger Inhaber angemessene Geheimhaltungsmaßnahmen (§ 2 Nr. 1 lit. b GeschGehG) treffen. Eine Geheimhaltungsvereinbarung kann zur tatsächlichen Geheimhaltung beitragen und eine angemessene Geheimhaltungsmaßnahme darstellen.[5] Eine pauschale Aussage darüber, wie die Maßnahmen genau auszugestalten sind, lässt sich jedoch nicht treffen.[6] Für einen umfassenden Schutz müssen u.U. mit dieser rechtlichen Maßnahme auch technische und organisatorische Geheimhaltungsmaßnahmen einhergehen.[7] Wird keine Geheimhaltungsvereinbarung geschlossen, bedeutet dies nicht automatisch, dass das Geschäftsgeheimnis nicht mehr geschützt ist, jedoch ist eine Vereinbarung immer zu empfehlen, um als Geheimnisinhaber so weit wie möglich abgesichert zu sein.[8]

II. Arten

Bei Geheimhaltungsvereinbarungen ist zwischen ein- und zweiseitigen zu unterscheiden. Bei einer einseitigen Geheimhaltungsvereinbarung unterliegt nur die Partei einer Geheimhaltungspflicht, die mit Geschäfts- und Betriebsgeheimnissen der anderen Partei in Berührung kommt. Zweiseitige Vereinbarungen kommen meist zustande, wenn zwei Parteien zusammenarbeiten und durch diese Zusammenarbeit gegenseitig Geschäftsgeheimnisse ihres Vertragspartners erfahren.[9] Beide Parteien verpflichten sich dadurch zur gegenseitigen Geheimhaltung.[10] Ferner ist bei Geheimhaltungsvereinbarungen darauf zu achten, ob sie mit einem Arbeitnehmer oder Geschäftspartner geschlossen werden und daher insbesondere den arbeits- oder wettbewerbsrechtlichen Anforderungen genügen müssen.[11]

III. Bestandteile einer Geheimhaltungsvereinbarung

Geheimhaltungsvereinbarungen sind zumeist vorformulierte Vertragsbedingungen, die dem anderen Teil bei Vertragsschluss vom Verwender gestellt und nicht ausgehandelt werden und daher Allgemeine Geschäftsbedingungen i.S.d. § 305 Abs. 1 BGB sind.[12] Als solche müssen Geheimhaltungsvereinbarungen einer Inhaltskontrolle der §§ 307 ff. BGB standhalten. Dabei ist maßgeblich auf § 307 Abs. 2 Nr. 1 BGB abzustellen.[13]

Eine Geheimhaltungsvereinbarung[14] sollte insbesondere die folgenden Punkte abdecken:

- Definition von vertraulichen Informationen und Geschäftsgeheimnissen
- Geheimnisschutzpflicht
- Nutzungsverbot/Reverse Engineering
- Verhältnis zu Dritten
- Hinweise auf Fehlverhalten/Whistleblowing
- Sanktionen und ggf. Hinweis auf Haftung/Strafbarkeit
- Zuständigkeit und anwendbares Recht

1 *Westermann,* in: MüKoBGB, 8. Aufl. 2019, § 453 Rn. 37.
2 *Heusel*, in: Nägele/Apel, Beck'sche Online-Formulare IT- und Datenrecht, 6. Ed. 2021, 3.4 Rn. 3.
3 *BGH* GRUR 2003, 356 (358) – Präzisionsmessgeräte; *Hille,* WRP 2020, 824, Rn. 3 f.; *Böning*, in: Hoeren/Münker, GeschGehG, 2021, § 1 Abs. 3 Nr. 3 und 4 Rn. 26 (i.E.).
4 *Hille,* WRP 2020, 824, Rn. 4; *Partsch/Rump*, NJW 2020, 118 (120).
5 *LAG Düsseldorf* MMR 2021, 181 (184), Rn. 80.
6 *Baranowski/Glaßl*, BB 2016, 2563 (2565); *Dann/Markgraf*, NJW 2019, 1774 (1775).
7 *Heinzke*, CCZ 2016, 179 (182).
8 *Jansen/Hofmann*, BB 2020, 259 (262).
9 Vgl. *Becker/Kussnik*, RAW 2018, 119 (124).
10 *Thalhofer/Zdanowiecki*, in: Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 19 Rn. 13.
11 S. dazu auch: *BGH* GRUR 1963, 367.
12 *Heusel* (o. Fußn. 2), Rn. 2.
13 *Hoeren*, in: Hoeren/Münker (o. Fußn. 3), Vorb §§ 1-2 Rn. 12.
14 *Heusel* (o. Fußn. 2), 3.3 und 3.4; *Kirchner/Prasse/Steinbach-Martens*, in: Schulze/Grziwotz/Lauda, BGB: Kommentiertes Vertrags- und Prozessformularbuch, 4. Aufl. 2020, § 311 Rn. 6; *Alexander*, WRP 2017, 1034 (1044), Rn. 121; s.a. das Muster in: *Hoeren/Münker* (o. Fußn. 3), S. 519.

1. Definition von vertraulichen Informationen und Geschäftsgeheimnissen

Die Definition der geheimzuhaltenden Information bildet zusammen mit der Geheimnisschutzpflicht das Kernstück jeder Geheimhaltungsvereinbarung.[15] In der Praxis wurde in der Vergangenheit üblicherweise aufgelistet, welche Informationen als vertraulich zu behandeln sind.[16] Nach Einführung des GeschGehG wäre nun denkbar, sich am Wortlaut von § 2 Nr. 1 GeschGehG zu orientieren und die Definition des Geschäftsgeheimnisses zu übernehmen. Dabei sollte jedoch stets auf das Kriterium der „angemessenen Geheimhaltungsmaßnahmen" geachtet werden. Sofern auf die Definition in § 2 Nr. 1 GeschGehG verwiesen wird, sollte in der Vereinbarung deutlich zur Sprache gebracht werden, dass Geschäftsgeheimnisse trotzdem geschützt sind, wenn der Schutzbereich des § 2 Nr. 1 GeschGehG mangels „angemessener Geheimhaltungsmaßnahmen" nicht eröffnet ist.[17] Abzulehnen ist in jedem Fall eine zu enge Definition, um Schutzlücken zu vermeiden. Gerade wenn konkrete Fallgruppen genannt werden, bietet dies auch gleichzeitig Risiken, da kaum möglich ist, sämtliche Konstellationen zu erfassen.[18] Es ist ratsam, diese Definition mit einem Katalog von vertraulichen Informationen zu kombinieren. Dabei bieten sich verschiedene Möglichkeiten an, diesen Katalog zu erstellen.

a) Positiv benennen (eng)

Das Geschäftsgeheimnis wird z.B. durch Nennen und Anfügen einer Anlage konkret bezeichnet. Dies ist nicht immer möglich, da zu Beginn einer Geschäftsbeziehung regelmäßig unklar ist, welche konkreten Informationen die andere Partei im Laufe der Zusammenarbeit erhalten wird.[19] Dieser Ansatz wird meist bei Franchise-Vereinbarungen oder Lizenzverträgen, etwa für Patente oder Marken, genutzt, da er sich dafür eignet sicherzustellen, dass konkrete Informationen, wie z.B. Patentunterlagen, unzweifelhaft von der Vereinbarung umfasst sind.[20]

b) Negativ benennen (weit)

Eine abschließende Liste aller nicht geheimer Informationen bzw. Informationsarten wird erstellt und alle anderen Informationen unterfallen der Geheimhaltung.[21]

c) Verweis (differenziert)

Es wird auf die Kennzeichnung und Geheimhaltungsmaßnahmen der konkreten Dokumente/Informationen verwiesen. Dies setzt ein umfassendes Kennzeichnungs- bzw. Maßnahmensystem voraus.[22] Dementsprechend liegt die angemessene Geheimhaltungsmaßnahme dann erst in dieser Kombination vor.[23]

Denkbar sind auch Kombinationen aus positivem und negativem Nennen und Verweisen auf Kennzeichnungen. Die Informationen müssen weiterhin als geheimhaltungsbedürftig eingestuft sein. Dies entschied auch das *ArbG Trier*[24], was das *LAG Rheinland-Pfalz* wiederum in einem U. v. 21.2.2013 bestätigte, in welchem es den Verstoß einer Geheimhaltungspflicht verneinte, da kein berechtigtes betriebliches Interesse an der Geheimhaltung der Information bestand.[25]

Darüber hinaus muss diese Definition, sofern sie unter die AGB fällt, der Inhaltskontrolle standhalten. Klauseln, durch welche demjenigen, dem die Informationen offengelegt werden, pauschal die Pflicht auferlegt wird das „Know-how" oder „Geschäftsgeheimnisse" des Vertragspartners zu schützen, verstoßen mangels einheitlicher Definitionen dieser unbestimmten Begriffe gegen das Transparenzgebot aus § 307 Abs. 1 S. 2 BGB.[26] Klauseln, in denen zur Geheimhaltung aller dem Vertragspartner bekannt gewordenen Tatsachen verpflichtet wird, sog. „Catch All"-Klauseln, sind als unangemessene Benachteiligung des Vertragspartners gem. § 307 Abs. 1 S. 1 BGB unwirksam.[27]

Im IT-Bereich besteht insofern wenigstens Klarheit, dass der Quellcode regelmäßig als Betriebsgeheimnis einzustufen ist. Dies hat zumindest der *Oberste Gerichtshof in Österreich* in seiner E. v. 10.12.2020 ausdrücklich anerkannt.[28] Auch in der deutschen Rechtsprechung und Literatur wird dies zumeist angenommen.[29]

Als Beispiel für eine entsprechende Klausel könnte man folgende Formulierung wählen:

> Der Geschäftspartner verpflichtet sich aus diesen Gründen zur strikten und unbedingten Geheimhaltung sämtlicher Tatsachen, Informationen und Unterlagen (in mündlicher, gedruckter oder maschinenlesbarer Form), welche den in der Präambel bezeichneten Geschäftsbetrieb der XXX betreffen (im Weiteren als „vertrauliche Informationen" bezeichnet). Zu den vertraulichen Informationen zählen insbesondere
> - die von der XXX-Gruppe entwickelten Technologien und Datenmodelle zur computergestützten Analyse von Finanzmärkten,
> - die von der XXX-Gruppe zur Analyse entwickelte Software, einschließlich des Source Codes, Object Codes, der Programmdokumentation, der Datenflusspläne, der Benutzerdokumentation und sonstiger technischer Grundlagen,
> - die Identitäten von XXX-Kunden, Partnern, Zulieferern und Vertriebsunternehmen,
> - die finanziellen und strategischen Rahmenbedingungen der XXX-Gruppe,
> - die der Kooperation zwischen Kunden und XXX zu Grunde liegenden Informationen hinsichtlich der wirtschaftlichen Aktivitäten der Kunden und
> - die Finanzinformationen, die XXX ihren Kunden übermittelt oder zu übermitteln beabsichtigt.

2. Geheimnisschutzpflicht

Die Geheimhaltungsvereinbarung sollte genaue Regelungen hinsichtlich des Umfangs der Geheimnisschutzpflicht enthalten.[30] Verpflichtungen und Ausnahmetatbestände sollten dabei klar definiert werden. Auch hier kann auf § 2 Nr. 1 lit. b GeschGehG verwiesen werden, indem sich der Beteiligte dazu verpflichtet selbst angemessene Geheimhaltungsmaßnahmen zu treffen.[31]

In der Geheimhaltungsvereinbarung sollte nicht nur die Pflicht, Geheimnisse nicht an Dritte weiterzugeben zum Ausdruck gebracht werden, sondern darüber hinaus auch die Pflicht, Geheimnisse nicht für andere als im Vertrag geregelte Zwecke zu verwenden, um z.B. Fälle zu vermeiden, in denen ein ehemaliger Arbeitnehmer sich selbstständig macht.[32]

---

15 *Becker/Kussnik*, RAW 2018, 119 (122).
16 *Jansen/ Hofmann*, BB 2020, 259 (263); vgl. *Hille,* WRP 2020, 824 (828), Rn. 37.
17 *Jansen/ Hofmann*, BB 2020, 259 (263).
18 *Becker/Kussnik*, RAW 2018, 119 (124).
19 *Becker/Kussnik*, RAW 2018, 119 (124).
20 *Hille,* WRP 2020, 824 (828).
21 Vgl. *Kirchner/Prasse/Steinbach-Mertens* (o. Fußn. 14).
22 *Hille,* WRP 2020, 824 (828 f.).
23 *Becker/Kussnik*, RAW 2018, 119 (125).
24 *ArbG Trier* U. v. 2.8.2012 – 2 Ca 526/12.
25 *LAG Rheinland-Pfalz* ZD 2013, 460.
26 Vgl. *Hille,* WRP 2020, 824 (827 f.).
27 *Greßlin/Römermann,* BB 2016, 1461 (1464); *Holthausen*, NZA 2019, 1377 (1379 f.).
28 *ÖOGH* MMR 2021, 549 – in diesem Heft.
29 BGHZ 93, 191 (206) – Druckbalken; *BGH* GRUR 2002, 1046 (1048 f.) – Faxkarte; *OLG Celle* CR 1989, 1002 (1003); *Graf*, in: MüKoStGB, 3. Aufl. 2017, § 202a Rn. 31, 88, 92; *Hauck*, in: Hoeren/Münker (o. Fußn. 3), § 16 Rn. 37; *Maaßen*, GRUR 2019, 352 (356).
30 *Jansen/Hofmann*, BB 2020, 259 (263).
31 *Jansen/Hofmann*, BB 2020, 259 (263).
32 *McGuire*, WRP 2019, 679 (684), Rn. 36.

Weiterhin kann in einer Geheimhaltungsvereinbarung keine bedingungslose Geheimhaltungsverpflichtung ohne entsprechende Ausnahmen auferlegt werden.[33] Eine der Geheimhaltungsverpflichtung widersprechende gesetzliche oder behördliche Offenbarungsverpflichtung kann z.B. nicht durch eine vertragliche Vereinbarung ausgeschlossen werden.[34] Hingegen muss die Erfüllung solcher Offenbarungsverpflichtungen immer von der Verschwiegenheitsverpflichtung ausgenommen werden. Dies gilt auch für die Weitergabe von Informationen an den Betriebsrat oder Steuerberater durch den Arbeitnehmer.[35]

Klausel:

Diese Verpflichtung entfällt für Informationen, die
- der Öffentlichkeit vor der Mitteilung an den empfangenden Partner bekannt oder allgemein zugänglich waren oder
- der Öffentlichkeit nach der Mitteilung an den empfangenden Partner ohne Mitwirken oder Verschulden desselben bekannt oder allgemein zugänglich werden oder
- dem empfangenden Partner bei Erhalt der Information bereits bekannt waren oder
- dem empfangenden Partner zu irgendeinem Zeitpunkt von einem Dritten ohne Auferlegung einer Vertraulichkeitsverpflichtung offenbart oder zugänglich gemacht werden oder
- von einem Mitarbeiter des empfangenden Partners ohne Kenntnis der Information entwickelt wurde.

Sollte die Offenlegung geheimhaltungsbedürftiger Informationen von einer Behörde oder einem Gericht zwingend angeordnet werden, so ist der empfangende Partner insoweit zur Offenlegung gegenüber der Behörde oder dem Gericht befugt. Der empfangende Partner hat den mitteilenden Partner über eine solche Anordnung unverzüglich zu informieren, soweit dies rechtlich zulässig ist.

Das *LAG Mecklenburg-Vorpommern* hat mit U. v. 21.10.2009 darüber hinaus entschieden, dass auch Klauseln, durch welche es dem Arbeitnehmer verwehrt wird, sich mit anderen Arbeitnehmer*innen über seine Arbeitsvergütung auszutauschen, unwirksam sind. Dem Arbeitnehmer wird durch eine solche Regelung die Möglichkeit genommen, eine etwaige Ungleichbehandlung aufzudecken und diese gegenüber dem Arbeitgeber geltend zu machen.[36] Für den Fall der Beendigung der Zusammenarbeit bzw. der Geheimhaltungsvereinbarung ist regelmäßig eine Pflicht zur Rückgabe von Unterlagen und zur Vernichtung bzw. Löschung von Informationen, die Teil der Geheimhaltungsvereinbarung waren, vorgesehen.[37]

Die Geheimnisschutzpflicht könnte wie folgt lauten:

- Ohne ausdrückliche schriftliche Zustimmung der XXX darf der Geschäftspartner die vertraulichen Informationen weder für eigene Zwecke noch zu Gunsten Dritter sammeln, kopieren, aufbewahren oder in irgendeiner Art verwenden. Manuskripte für wissenschaftliche Veröffentlichungen und Vorträge, die mit dem Tätigkeitsbereich der XXX-Gruppe in Verbindung stehen, sind der XXX zur Freigabe vorzulegen. Eine Freigabe erfolgt, sofern berechtigte betriebliche Interessen einer Publikation nicht entgegenstehen.
- Der Geschäftspartner verpflichtet sich dazu, die vertraulichen Informationen innerhalb der XXX nur an diejenigen weiterzugeben, die diese Informationen zur Durchführung ihrer jeweiligen Arbeitsaufgabe im XXX-Bereich unbedingt benötigen. Dabei sind die Vorgaben der Geschäftsleitung in Bezug auf die jeweiligen Arbeitsaufgaben und die jeweils für Datenzugriffe in einzelnen Abteilungen bestehenden Regelungen nach Maßgabe der DS-GVO und ergänzender TOMs zu beachten.
- Der Geschäftspartner ist zur Einhaltung des aktuellsten Standes der Technik, was Datensicherheit und den Schutz von Informationen angeht, verpflichtet. Er wird die XXX auf bestehende und drohende Sicherheitslücken hinweisen. Er wird bei der Auswahl und Bestellung von Wartungs-, Pflege- und sonstigem technischem Personal darauf achten, dass die jeweils tätigen Personen ihrerseits den aktuellsten Stand der Datensicherheit beachten und in all ihren Aktivitäten der vertraulichen Natur von XXX-Informationen Rechnung tragen.
- Der Geschäftspartner verpflichtet sich in der Kommunikation innerhalb des Unternehmens und im Verkehr nach außen zur Einhaltung höchster Vertraulichkeitsstandards. Insbesondere wird er Informationen nicht unverschlüsselt über Internet-Dienste übertragen. Er wird auf den Einsatz geeigneter Firewall-Systeme sowie eine stets auf aktuellem Stand befindliche Virenkontrolle achten. Er trägt auch Sorge dafür, dass die von ihm benutzten Rechner nicht unbefugt zugänglich, insbesondere gegen Zugriff durch Dritte durch effiziente technische Schutzsysteme, gesichert sind. Besondere Sorgfaltspflichten treffen den Geschäftspartner auch hinsichtlich des sicheren Umgangs mit Passwörtern.

3. Nutzungsverbot/Reverse Engineering

Durch die gesetzliche Zulassung des Reverse Engineerings, welche nach dem Wortlaut von § 3 Abs. 1 Nr. 2 GeschGehG auch Geschäftspartnern, die schon vor Markteintritt im rechtmäßigen Besitz der Information sind, es gestattet, Gebrauch von einer solchen Produktanalyse zu machen, sind neue Probleme für Geheimnisinhaber entstanden.[38] Um zu vermeiden, dass Arbeitnehmer oder Geheimnismitwisser einen unfairen Vorteil erlangen, ist es daher durchaus ratsam, Reverse Engineering vertraglich auszuschließen, um sich auf § 3 Abs. 1 Nr. 2 GeschGehG berufen zu können.[39]

In dem Fall, dass der Geheimnisinhaber dem Geschäftspartner die Nutzung des Geschäftsgeheimnisses auf vertraglicher Basis erlaubt, muss in der Geheimhaltungsvereinbarung darauf hingewiesen werden, dass durch diese Erlaubnis keine Kontrollbefugnis i.S.d. § 2 Nr. 2 GeschGehG entsteht.[40]

Eine Klausel könnte etwa lauten:

Der empfangende Partner verpflichtet sich zudem, geheimhaltungsbedürftige Informationen eines offenbarenden Partners nicht zurückzuentwickeln (Reverse Engineering), zu dekompilieren, zu disassemblieren oder in sonstiger Weise auf deren Zusammensetzung und/oder Herstellung zu untersuchen, sofern dies nicht für das Vorhaben erforderlich ist und der offenbarende Partner dem zuvor ausdrücklich schriftlich zugestimmt hat.

4. Verhältnis zu Dritten

Überdies muss in Geheimhaltungsvereinbarungen eine Erstreckung der Geheimhaltungsverpflichtungen auf Dritte geregelt werden. Der Kreis derjenigen, denen bestimmte Informationen weitergegeben werden, muss eingeschränkt werden. In einer Geheimhaltungsvereinbarung sollte daher eine entsprechende Klausel eingearbeitet werden, in der z.B. geregelt wird, dass ge-

33 *Holthausen*, NZA 2019, 1377 (1380).
34 *Holthausen*, NZA 2019, 1377 (1380); *Preis/Reinfeld*, ArbuR 1989, 361 (365).
35 *Holthausen*, NZA 2019, 1377 (1380).
36 *LAG Mecklenburg-Vorpommern* U. v. 21.10.2009 – 2SA 237/09.
37 *Kirchner/Prasse/Steinbach-Mertens* (o. Fußn. 14).
38 *Strobel*, in: Hoeren/Münker (o. Fußn. 3), § 3 Abs. 1 Nr. 2 Rn. 30.
39 *Becker/Kussnik*, RAW 2018, 119 (127); *McGuire*, WRP 2019, 679 (684), Rn. 40.
40 Zur dahinterstehenden Problematik: *McGuire*, WRP 2019, 679 (683) mwN.

schützte Informationen an Mitarbeiter*innen nur soweit weitergegeben werden dürfen, wie dies für ihre Tätigkeit unbedingt notwendig ist.[41] Weiterhin sollte der Empfänger der Geheimhaltungspflicht durch eine entsprechende Regelung dazu verpflichtet werden, seine Angestellten, Mitarbeiter*innen und externen Dienst- und Werkleister wiederum vertraglich zur Geheimhaltung zu verpflichten.[42] Auch sollte eine Geheimhaltungsvereinbarung eine Verpflichtung zum vorherigen Einverständnis des Geschäftsgeheimnisinhabers vorsehen, in dem Fall, dass der Verpflichtete es für notwendig erachtet, einen Dritten in die Vereinbarung einzubeziehen.[43]

Da auch das Erhalten rechtswidrig weitergegebener Geschäftsgeheimisse vom GeschGehG sanktioniert wird, sollte zum eigenen Schutz eine Versicherung eingefügt werden, dass so erlangte Geschäftsgeheimnisse Dritter an einen selbst nicht weitergegeben werden.[44]

5. Hinweise auf Fehlverhalten/Whistleblowing

Auf Grund der Tatsache, dass viele rechtswidrige Informationen, die durch Whistleblowing preisgegeben werden (z.B. Kartellabsprachen), mangels Handelswert kein Geschäftsgeheimnis darstellen, ist die Bedeutung des Whistleblowings für den Geheimnisschutz auf die Offenlegung von Informationen i.R.v. Hinweisen auf Fehlverhalten begrenzt.[45] In so einem Fall hat der Hinweisgeber die Möglichkeit, sich gem. § 5 Nr. 2 GeschGehG unter bestimmten Voraussetzungen auf eine Rechtfertigung zu berufen. In der Praxis hat sich etabliert, dass ein Hinweisgeber zunächst interne Steuerungs- und Kontrollsysteme nutzen muss und sich anschließend an öffentliche Stellen zu wenden hat.[46] Ein Kontakt mit den Medien sollte das letztmögliche Mittel darstellen.[47] Um dies zu verdeutlichen, sind Geheimnisinhaber gehalten, Kontroll- und Kommunikationssysteme zu schaffen und explizit auf diese in der Geheimhaltungsvereinbarung hinzuweisen.[48]

6. Sanktionen und Hinweise auf Haftung/ Strafbarkeit

Auf Grund der schwierigen Beweisbarkeit von Schäden wegen einer Verletzung aus einer Geheimhaltungspflicht sind insbesondere Vertragsstrafen ratsam.[49] Letztlich können diese als Druckmittel dienen, den zur Verschwiegenheit verpflichteten Teil auf die Einhaltung seiner Pflichten hinzuweisen.[50]

Solche Vertragsstrafen müssen jedoch den Anforderungen des § 309 Nr. 6 BGB entsprechen. Indem die Höhe der Vertragsstrafe in das Ermessen des Geheimnisinhabers bzw. des ursprünglichen Informationsinhabers gestellt wird, der wiederum die Vergütung des anderen Vertragsteils und die Schwere des Pflichtverstoßes berücksichtigt, sind solche Regelungen durchsetzbar.[51] Die Vereinbarung von Schadensersatzpauschalen, die den Nachweis eines Schadens entbehrlich machen, ist jedoch ebenfalls schwierig durchzusetzen.[52] Dabei darf gem. § 309 Nr. 5 BGB die Pauschale nicht höher als der regelmäßig zu erwartende Schaden sein und dem anderen Vertragsteil muss die Möglichkeit eingeräumt werden, nachzuweisen, dass der Schaden nicht eingetreten ist oder niedriger ist als die Pauschale.[53] Wichtig ist auch, dass die Pönale an konkrete Tatbestände knüpft. Eine zu unbestimmte Vertragsstrafe fällt dem Verdikt der Transparenz nach § 307 Abs. 1 Nr. 2 BGB anheim.

Problematisch sind Vertragsstrafen auch in internationalen Kontexten. US-amerikanische Gerichte wehren sich gegen die Vorstellung einer Vertragsstrafe, sog. „contractual penalties" sind ausnahmslos unwirksam.[54] Wirksam sind hingegen Klauseln über sog. „liquidated damages", durch die die Parteien mit Vertragsschluss bereits im Vorfeld die schadensersatzrechtlichen Folgen eines potenziellen Vertragsbruchs festlegen.[55] Auf Grund der generellen Unwirksamkeit von Vertragsstrafen und der genauen Prüfung der tatsächlichen Rechtsnatur einer vertraglichen Klausel durch die Gerichte, orientiert sich die Gestaltung von Verträgen in den USA an der Abgrenzung von „contractual penalties" und „liquidated damages".[56] Die Unterscheidung zwischen Vertragsstrafe und pauschalisiertem Schadensersatz ist auch in Großbritannien essenziell. Nach englischem Recht ist eine vertragliche Abrede nichtig, soweit sie als Vertragsstrafe zu qualifizieren ist.[57] Nach Rechtsprechung des *englischen Supreme Courts* ist allerdings eine Ausnahme des strengen Verbots von Vertragsstrafen anzunehmen, wenn eine Partei keine Möglichkeit zur Vereinbarung einer Schadenspauschale hat, weil es diesem Rechtsbehelf an hinreichender Effektivität mangeln würde. Dies ist im Einzelfall abzuwägen. Diese durch die Rechtsprechung etablierte Flexibilität in der Abgrenzung zwischen Vertragsstrafe und pauschalisiertem Schadensersatz führt zur diesbezüglichen Annäherung des englischen Rechts an das kontinentale Recht.[58]

Zu beachten ist bei der Festlegung der Vertragsstrafe ebenfalls § 9 GeschGehG, wodurch die Möglichkeit geschaffen wird, gegen Rechtsfolgen mit dem Einwand vorzugehen, sie seien im konkreten Fall unverhältnismäßig.[59] Demnach ist es immer ratsam zu prüfen, bei welchem Verhalten eine Vertragsstrafe in welcher Höhe eintritt und ob dies insbesondere mit arbeitsrechtlichen Vorgaben im Einklang steht. Denkbar ist auch eine Regelung, in der ein Geheimnisinhaber die Höhe der Vertragsstrafe anhand der Umstände bestimmen kann, diese aber durch ein Gericht, sollte Uneinigkeit bestehen, untersucht werden kann.[60]

Neben einer Vertragsstrafe drohen dem Verletzer jedoch noch weitere Rechtsfolgen arbeitsrechtlicher, zivilrechtlicher und strafrechtlicher Natur.[61]

Eine sinnvolle Regelung zu Vertragsstrafen könnte heißen:

> Der Geschäftspartner wird darauf hingewiesen, dass jede Verletzung dieser Vertraulichkeitsvereinbarung hohe Schadensersatzansprüche der XXX gegen ihn, mindestens aber eine Vertragsstrafe in Höhe von Betrag XXX auslösen kann (alternativ: in angemessener Höhe, wobei der Inhaber die Höhe nach billigem Ermessen i.S.v. § 315 BGB bestimmen wird und die Angemessenheit der Vertragsstrafe im Streitfall

41 *Becker/Kussnik*, RAW 2018, 119 (123).
42 *Kirchner/Prasse/Steinbach-Mertens* (o. Fußn. 14).
43 *Kirchner/Prasse/Steinbach-Mertens* (o. Fußn. 14).
44 *Becker/Kussnik*, RAW 2018, 119 (127); *McGuire*, WRP 2019, 679 (684 f.), Rn. 42; vgl. *Hoeren/Münker*, CCZ 2018, 85 (86 f.).
45 *Beyerbach*, in: Hoeren/Münker (o. Fußn. 3), § 5 Nr. 1 Rn. 47; *Kalbfus*, GRUR 2016, 1009 (1011); *McGuire*, WRP 2019, 679 (685), Rn. 44.
46 *Baranowski/Glaßl*, BB 2016, 2563 (2566); *Brammsen*, in: MüKoLauterkeitsrecht, 2. Aufl. 2014, § 17 Rn. 57; *McGuire*, WRP 2019, 679 (685), Rn. 45; *Reinhardt-Kasperek,* in: Hoeren/Münker (o. Fußn. 3), § 5 Nr. 2 Rn. 20.
47 *McGuire*, WRP 2019, 679 (685), Rn. 45.
48 *Wirth/Krause*, CB 2015, 27 (31).
49 *Alfes*, in: Krauß/Weise, Beck'sche Online-Formulare Vertrag, 56. Ed. 2021, 20.2 Rn. 3; *Heusel* (o. Fußn. 2), Rn. 14.
50 *Mayer*, MDR 2018, 245 (247).
51 *Heusel* (o. Fußn. 2), Rn. 14.
52 *Söbbing*, GWR 2010, 237 (239).
53 *Fischl*, in: Auer-Reinsdorff/Conrad (o. Fußn. 10), § 17 Rn. 130.
54 *Nodoushani*, VersR 2005, 1623.
55 *Nodoushani*, VersR 2005, 1623.
56 *Nodoushani*, VersR 2005, 1623.
57 *Beale*, IWRZ 2017, 68 (68).
58 *Beale*, IWRZ 2017, 68 (72).
59 S. dazu auch: *Pohl*, in: Hoeren/Münker (o. Fußn. 3), § 9; *Tochtermann*, WRP 2019, 688.
60 *Voigt/Herrmann/Grabenschröer*, BB 2019, 142 (145).
61 *Gaugenrieder/Unger-Hellmich,* WRP 2011, 1364 (1379 f.).

von dem zuständigen Gericht überprüft werden kann). Auch wird er bereits jetzt auf die denkbaren strafrechtlichen Folgen einer unbefugten Offenbarung, insbesondere im Hinblick auf § 23 GeschGehG hingewiesen.

7. Zuständigkeit, anwendbares Recht und mehr

Ebenso kann es empfehlenswert sein, Vereinbarungen über den Gerichtsstand und das anzuwendende Recht in den Vertrag aufzunehmen. Im Rahmen einer Gerichtsstandsvereinbarung ist § 38 Abs. 1 ZPO einzuhalten, der die Zuständigkeit eines Gerichts durch Vereinbarung nur ermöglicht, wenn es sich bei den Vertragsparteien um Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen handelt.[62] Gem. § 1029 ZPO kann auch die Zuständigkeit eines Schiedsgerichts vereinbart werden. Nach Absatz 2 kann dies sowohl im Rahmen einer selbstständigen Vereinbarung als auch in Form einer Klausel in einem Vertrag erfolgen. Eine solche Schiedsgerichtsvereinbarung bringt insbesondere den Vorteil, die Öffentlichkeit eines ordentlichen Gerichtsprozesses zu vermeiden.[63] Zusätzlich kann eine salvatorische Klausel hinzugefügt werden, um den Bestand der Vereinbarung bei Unwirksamkeit eines Teils derselben sicherzustellen.

Zuletzt bietet es sich an, eine doppelte Schriftformklausel aufzunehmen, die jedoch so gestaltet sein muss, dass sie einer AGB-Kontrolle nach § 307 BGB standhält, insbesondere nach der Rechtsprechung des *BAG*[64] darf dadurch der Vertragspartner nicht unangemessen benachteiligt werden und der Eindruck entstehen, dass eine abweichende mündliche Individualabrede unwirksam sei.[65]

IV. Besonderheiten bei Verträgen mit Arbeitnehmern

Daraus ergibt sich ein klares Leitbild für eine Geheimhaltungsvereinbarung mit Geschäftspartnern im IT-Bereich, das jedoch nicht unbesehen auf eine Geheimnisabrede mit Arbeitnehmer*innen übertragen werden kann. Bei diesem Klientel sind Vertragsstrafen regelmäßig nicht zulässig, wenn diese zu hoch ausfallen.[66] Denkbar wäre bei Arbeitnehmer*innen auch ein Wettbewerbsverbot, um einen Wechsel zu konkurrierenden Unternehmen unter Mitnahme von Geschäftsgeheimnissen zu untersagen.[67] Bei einem solchen Verbot fällt aber nach § 74 Abs. 2 HGB eine Karenzentschädigung an, die während der gesamten Zeit des Wettbewerbsverbots drohende Schäden oder Einbußen des Arbeitnehmers kompensiert. Fällt die Karenzentschädigung nicht angemessen hoch aus, ist der Arbeitnehmer auch nicht an die Vereinbarung über das Wettbewerbsverbot gebunden.[68] Effektiver ist hier ein Abwerbeverbot zwischen Geschäftspartnern, um gerade im hochsensiblen Bereich der Übernahme fremder Programmierer das Softwarehaus vor Abwerbeversuchen zu schützen.[69] Allerdings ist dabei § 75f HGB zu bedenken, wonach eine gerichtliche Durchsetzbarkeit solcher Abwerbeverbote von Arbeitnehmer*innen[70] grundsätzlich nicht besteht. Sinn dieser Norm ist gerade, dass die Pflicht zur Zahlung einer Karenzentschädigung nicht umgangen wird, um das Recht auf berufliche Selbstbestimmung gem. Art. 12 Abs. 1 GG zu schützen.[71] Jedoch hat der *BGH* in seiner E. v. 30.4.2014 bekräftigt, dass vertragliche Verbote der Abwerbung wichtiger Schlüsselpersonen für eine Dauer bis zu zwei Jahren nach Abschluss des Projekts zulässig und im Wege einer verfassungskonformen einschränkenden Auslegung des § 75f HGB einklagbar sein können.[72] Voraussetzung dafür ist außerdem das Vorliegen einer definierten Fallgruppe. Die abwerbende Handlung muss entweder nach dem UWG eine unlautere geschäftliche Handlung darstellen[73] oder das Abwerbeverbot ist eine Nebenbestimmung und nicht Hauptzweck der Vereinbarung, welche auf einem besonderen Vertrauensverhältnis oder einer besonderen Schutzbedürftigkeit basiert.[74]

Klausel:

> Jede Partei verpflichtet sich, während sowie bis zwei Jahre nach Beendigung dieses Vertrags keine Mitarbeiter*innen der anderen Partei direkt oder indirekt abzuwerben. Für jeden Fall einer Zuwiderhandlung gegen die Bestimmung in Satz 1 zahlt die verstoßende Partei an die andere Partei eine Vertragsstrafe in Höhe von XXX.

V. Fazit

Die Abfassung einer Geheimnisschutzvereinbarung im IT-Bereich ist kein Teufelszeug. Schwierig ist nur die gewissenhafte Prüfung, was unter eine solche Vereinbarung fallen soll. Sorgfalt ist auch bei der Präzisierung der Tatbestände für eine Vertragsstrafe geboten. Ansonsten kann sich ein Muster eventuell an beiliegendem Raster entwickeln lassen, das mit aller Bedacht empfohlen werden kann, aber noch an die Bedürfnisse des Rechtsgestalters angepasst werden muss.

Schnell gelesen ...

- Geheimhaltungsvereinbarungen müssen sorgfältig geplant werden.
- Besonderes Augenmerk gilt vor allem der genauen Bezeichnung, was geheimhaltungsbedürftig ist. Dabei müssen auch Datensicherheits- und Datenschutzfragen einbezogen werden.
- Eine Geheimhaltungsvereinbarung kann mit Vertragsstrafen verbunden werden, sofern die Vorgaben des AGB-Rechts eingehalten werden und der Strafschadensersatz nicht zu hoch festgesetzt wird.
- Eine Vereinbarung zu Reverse Engineering kann sinnvoll sein.
- Besonderer Problemfall ist eine Geheimhaltungsvereinbarung in Arbeitsverhältnissen, u.a. wegen der Karenzentschädigung.

62 *Heusel* (o. Fußn. 2), Rn. 16.
63 *Heusel* (o. Fußn. 2), Rn. 16.
64 *BAG* NZA 2008, 1233.
65 *Heusel* (o. Fußn. 2), Rn. 17.
66 *Hoeren* (o. Fußn. 13), § 2 Rn. 52.
67 *Böning*, in: Hoeren/Münker (o. Fußn. 3), § 1 Abs. 3 Nr. 3 und 4 Rn. 35 f.
68 *Böning*, in: Hoeren/Münker (o. Fußn. 3), § 1 Abs. 3 Nr. 3 und 4 Rn. 35 f. mwN.
69 *Hoeren* (o. Fußn. 13), § 2 Rn. 53.
70 Nicht nur Handlungsgehilfen fallen unter § 75f HGB: *BGH* NJW 1974, 1282 (1283); BAGE 22, 125 (134).
71 *BGH* NJW 1984, 116 (117).
72 *BGH* NZA 2015, 111 ff.
73 *BGH* NZA 2015, 111 (114).
74 *BGH* NZA 2015, 111 (114).

Professor Dr. Thomas Hoeren
ist Direktor des ITM an der Universität Münster und Mitherausgeber der MMR.

Dr. Reiner Münker
ist Hauptgeschäftsführer der Wettbewerbszentrale Bad Homburg.

GERALD SPINDLER

Ausgewählte Rechtsfragen der Umsetzung der digitalen Inhalte-Richtlinie in das BGB

Schwerpunkt 2: Rechtsbehelfe, Beweislastregelungen und Regress zwischen Unternehmern

Digitale Produkte

Die Richtlinie über digitale Inhalte steht kurz vor ihrer Umsetzung ins deutsche Recht. Im Anschluss an den Beitrag zum Anwendungsbereich und Mangelbegriff (MMR 2021, 451) beleuchtet dieser Beitrag die verschiedenen Umsetzungsbestimmungen mit Schwerpunkt auf Rechtsbehelfen, insbesondere der Nacherfüllung, den Auswirkungen auf datenschutzrechtliche Einwilligungen und weiteren Änderungen, insbesondere des Verhältnisses von Update-Pflichten zu Änderungsmöglichkeiten des Händlers, sowie des zwingenden Regresses. Dabei zeigt der Beitrag noch bestehende Defizite auf, etwa in internationalen Lieferketten, aber auch die nach wie vor bestehenden Diskrepanzen hinsichtlich des Verhältnisses von schuldrechtlichen Pflichten und datenschutzrechtlichen Rechtsbehelfen.

Lesedauer: 24 Minuten

I. Einleitung

Die Richtlinie über digitale Inhalte (DI-RL) wird demnächst umgesetzt und enthält neben den Mangelbegriffen und Update-Pflichten[1] auch zahlreiche Detailregelungen zu den Rechtsbehelfen, einschließlich des schwierigen Verhältnisses von datenschutzrechtlichen Vorgaben zur Behandlung von Daten i.R.d. schuldrechtlichen Leistungsaustauschs, ferner zum Regress zwischen Unternehmern und zur Beweislastregelung, die im Folgenden näher untersucht werden.

II. Rechtsbehelfe

Hinsichtlich der Rechtsbehelfe enthalten die DI-RL und § 327i BGB-RegE[2] wenig Überraschendes, indem die Beendigung des Vertrags (Rücktritt, Kündigung), die Nacherfüllung und die Preisminderung aufgeführt werden. Darüber hinaus hat der deutsche Gesetzgeber an dem Schadensersatz festgehalten, was die DI-RL den Mitgliedstaaten überlassen hat. Auch die gewohnte Hierarchie der Gewährleistungsrechte wird beibehalten, indem der Verbraucher zunächst die Nacherfüllung geltend machen muss, § 327m Abs. 1 Nr. 1, 2 BGB-RegE, was sich indirekt aus Art. 14 Abs. 1 u. Abs. 4 DI-RL ergibt.

1. Nacherfüllung

Für die Nacherfüllung gibt § 327l Abs. 1 BGB-RegE dem Unternehmer die Wahlfreiheit, wie er die Vertragsmäßigkeit wiederherstellt – anders als nach Art. 13 Abs. 2 Warenkauf-RL bzw. § 439 Abs. 1 BGB, die dem Verbraucher die Wahl überlassen. Die Nachbesserung muss unentgeltlich erfolgen, wovon aber z.B. Kosten der Datenübermittlung ausgenommen sein sollen, die der Verbraucher nur als Schaden geltend machen könne.[3] Ferner sieht § 327l Abs. 1 BGB-RegE zwar eine angemessene Frist zur Nachbesserung nach Inkenntnissetzung durch den Verbraucher über den Mangel vor, nicht aber, dass der Verbraucher diese auch setzen muss.[4] Schließlich stellt § 327l Abs. 1 S. 2 BGB-RegE die Nacherfüllung unter den Vorbehalt der Unannehmlichkeiten für den Verbraucher, worunter der Gesetzgeber z.B. nötige Veränderungen der digitalen Umgebung oder Auswirkungen auf die Funktionalität anderer digitaler Produkte erfassen will.[5]

Unterschiede zum geltenden Gewährleistungsrecht ergeben sich ferner hinsichtlich der Unmöglichkeit für den Unternehmer zur Nacherfüllung: Zwar muss der Unternehmer bei einer tatsächlichen oder rechtlichen Unmöglichkeit (Erwägungsgrund 65 DI-RL) nicht mehr nacherfüllen, sodass § 327l Abs. 2 BGB-RegE auf § 275 Abs. 1 BGB verweisen kann; jedoch gilt dies nicht für die in § 275 Abs. 2, 3 BGB vorgesehenen Abwägungen zwischen Schuldner- und Gläubigerinteresse, die die DI-RL nicht kennt.[6] Ferner kann der Anspruch auf Nacherfüllung wegen Unverhältnismäßigkeit der Kosten für den Unternehmer ausgeschlossen sein, wobei auf die Rechtsprechung zu § 439 Abs. 4 S. 2 BGB zurückgegriffen werden kann. In diesem Rahmen sollen auch Synergieeffekte des Unternehmers zu berücksichtigen sein, etwa wenn eine verbesserte Version des digitalen Produkts auf Grund einer Mängelbeseitigung hergestellt wird.[7]

2. Vertragsbeendigung

Auf Grund der Gleichstellung von einmaligen und dauerhaften Bereitstellungen von digitalen Produkten musste der Gesetzgeber die Differenzierung zwischen Rücktritt und Kündigung zu Gunsten des Terminus „Vertragsbeendigung" aufgeben. Nach § 327m Abs. 1 Nr. 1 BGB-RegE kommt die Vertragsbeendigung insbesondere bei dem Ausschluss der Nacherfüllung nach § 327l Abs. 2 BGB-RegE in Betracht, wobei allerdings keine ausdrückliche Erklärung des Unternehmers erforderlich ist. In der Praxis wird der Verbraucher aber den Unternehmer auffordern, sich zu erklären.[8] Auch für den Fall, dass der Unternehmer die Nachbesserung nicht innerhalb einer angemessenen Frist vorgenommen hat, sieht § 327m Abs. 1 Nr. 2 BGB-RegE das Recht zur Vertragsbeendigung vor; wiederum verlangt weder Art. 14 Abs. 4 lit. b DI-RL noch § 327m Abs. 1

1 RL (EU) 2019/770 des Europäischen Parlaments und des Rates v. 20.5.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. ABl. 2019 L 136, 1 ff.; vgl. zum Anwendungsbereich, Mangelbegriff und Update-Pflichten bereits *Spindler*, MMR 2021, 451.

2 Begr. zum Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen v. 17.3.2021, BT-Drs. 19/27653 (im Folgenden: Begr. RegE), abrufbar unter: https://dip21.bundestag.de/dip21/btd/19/276/1927653.pdf.

3 Begr. RegE, BT-Drs. 19/27653, 66.

4 Begr. RegE, BT-Drs. 19/27653, 66.

5 Begr. RegE, BT-Drs. 19/27653, 66.

6 Begr. RegE, BT-Drs. 19/27653, 67.

7 Begr. RegE, BT-Drs. 19/27653, 67; zur Unverhältnismäßigkeit der Kosten gem. § 439 Abs. 4 S. 2 BGB siehe u.a. *BGH* B. v. 14.1.2009 – VIII ZR 70/08; *BGH* U. v. 4.4.2014 – V ZR 275/12; *OLG Braunschweig* B. v. 4.2.2003 – 8 W 83/02.

8 Darauf weist zutr. Begr. RegE, BT-Drs. 19/27653, 67 f. hin.

Nr. 2 BGB-RegE eine Nachfristsetzung mit der Androhung der Ablehnung.[9]

Ferner gibt § 327m Abs. 1 Nr. 3 BGB-RegE dem Verbraucher das Recht zur Vertragsbeendigung, falls sich nach der Nachbesserung ein Mangel zeigt, der nicht notwendigerweise den gleichen Mangel betrifft, weswegen der Verbraucher die Nachbesserung geltend gemacht hatte, und der zudem noch nicht erkennbar war bei Bereitstellung; denn das Vertrauen des Verbrauchers in die Nachbesserung des Unternehmers sei in diesem Fall erschüttert.[10] Als Vertragsbeendigungsgrund kommt neben dem schwerwiegenden Mangel auch die Weigerung des Unternehmers zur Nachbesserung in Betracht, wobei es nicht darauf ankommt, ob die Weigerung berechtigt war oder nicht.[11]

Nur bei unerheblichen Mängeln kann der Verbraucher kein Recht auf Vertragsbeendigung geltend machen – wovon wiederum die Verträge, die nur Daten „als Gegenleistung" vorsehen, ausgenommen sind, § 327m Abs. 2 S. 2 BGB-RegE.[12]

Für Paketverträge enthält § 327m Abs. 4 BGB-RegE eine dem § 327c Abs. 6 BGB-RegE vergleichbare Regelung für die Vertragsbeendigung: Wenn der Mangel eines Vertragsbestandteils das Interesse des Verbrauchers an dem gesamten Paketvertrag entfallen lässt, erstreckt sich die Vertragsbeendigung auch auf den ganzen Paketvertrag. Ähnliche Regelungen sieht § 327m Abs. 5 BGB-RegE im Hinblick auf Verträge über Sachen vor, die mit digitalen Produkten verbunden sind und denen kein Kaufvertrag zu Grunde liegt (§ 327c Abs. 6 BGB-RegE), und bei denen sich auf Grund des Mangels die Sache nicht mehr zur gewöhnlichen Verwendung eignet. Dabei handelt es sich auf Grund der eigenständigen Regelung der Bedingungen für die Vertragsbeendigung um eine Rechtsfolgenverweisung.[13]

3. Minderung

Anstelle der Vertragsbeendigung kann der Verbraucher im Falle von Verträgen, für die er einen Preis entrichtet, eine Minderung nach § 327n Abs. 1 BGB-RegE verlangen, wobei die Einschränkung auf unerhebliche Mängel hier nicht in Betracht kommt. Für die Berechnung der Minderung verweist § 327n Abs. 2 BGB-RegE – wie sonst auch – auf das Verhältnis des Werts eines mangelfreien digitalen Produkts zum wirklichen Wert des Produkts; abgewichen wird allerdings hinsichtlich des Zeitpunkts, der in Umsetzung von Art. 14 Abs. 5 DI-RL auf die Bereitstellung verweist, im Gegensatz zum sonst im Kauf- und Werkvertragsrecht verwandten Zeitpunkt des Vertragsschlusses, §§ 441 Abs. 3 S. 1, 638 Abs. 3 S. 1 BGB.[14] Einzelheiten zur Frist, innerhalb derer der Unternehmer dem Verbraucher einen zu viel gezahlten Preis zu erstatten hat, regelt § 327n Abs. 4 BGB-RegE. Ein Nutzungsersatz wie nach § 441 Abs. 4 BGB mit Verweis auf §§ 346 Abs. 1, 347 Abs. 1 BGB wird ausgeschlossen, da diesen Art. 17 Abs. 3 DI-RL ausschließt.[15]

4. Schadensersatz

Neben der Vertragsbeendigung[16] gewährt § 327m Abs. 3 BGB-RegE dem Verbraucher auch nach §§ 280 Abs. 1, 283 S. 1 und 311a Abs. 2 S. 1 BGB das Recht, Schadensersatz statt der Leistung oder nach § 284 BGB Ersatz vergeblicher Aufwendungen zu verlangen. Damit wird aber auch die Anwendung von § 281 BGB ausgeschlossen, ebenso von §§ 283 S. 2 und 311a Abs. 2 S. 2, 3 BGB für den Schadensersatz wegen Unmöglichkeit der Nacherfüllung.[17]

Im Gegensatz zu anderen Rechtsbehelfen können diese Regelungen allerdings abbedungen werden, was § 327s Abs. 4 BGB-RegE klarstellt, wobei natürlich wiederum die Grenzen, die durch §§ 307 ff. BGB gezogen werden, zu beachten sind.[18] Da die §§ 327a ff. BGB gesetzliche Leitbilder darstellen, werden auch hier Abweichungen auf den Prüfstand z.B. der Kardinalpflichten gestellt werden; jedenfalls müssen die gleichen Bedingungen eingreifen wie für Schadensersatzansprüche bei sonstigen schuldrechtlichen Verträgen, etwa im Kauf- oder Werkvertragsrecht.[19]

5. Ausübung des Rechts auf Vertragsbeendigung und Rechtsfolgen

§ 327o BGB-RegE setzt Art. 15, 16 DI-RL um. Für die Erklärung zur Beendigung des Vertrags verlangt § 327o Abs. 1 BGB-RegE lediglich eine – formlose – Erklärung des Verbrauchers, die auch konkludent erfolgen kann; die Deinstallation allein soll indes nicht genügen[20] – was nachvollziehbar erscheint, da die Erklärung eine empfangsbedürftige Willenserklärung ist, die zu einer Umgestaltung des Rechtverhältnisses führt. § 351 BGB über die Unteilbarkeit des Rücktrittsrechts wird sinngemäß angewandt, damit auch für die Kündigung und für die Minderung.

Hinsichtlich der Rechtsfolgen hält § 327o Abs. 2, 3 BGB-RegE zunächst die aus dem Rücktrittsrecht bekannte Pflicht des Unternehmers fest, alle Zahlungen bzw. bei einem Dauerschuldverhältnis anteilig dem Verbraucher die Zahlungen zu erstatten, die auf den Zeitraum der Mangelhaftigkeit entfallen.

§ 327p BGB-RegE fasst Art. 16, 17 DI-RL zusammen, indem weitere Pflichten nach Vertragsbeendigung geregelt werden, etwa die Pflicht des Verbrauchers, das digitale Produkte nicht mehr weiter zu nutzen, wobei § 327p Abs. 1 S. 2 BGB-RegE dem Unternehmer ausdrücklich das Recht einräumt, die Nutzung zu unterbinden, etwa durch DRM-Systeme. Ob dieses Recht auch Eingriffe in die digitale Umgebung des Verbrauchers umfasst, wird weder durch die DI-RL noch § 327p BGB-RegE adressiert; angesichts des damit verbundenen erheblichen Eingriffs ist ein solches Recht abzulehnen.[21]

Ferner regelt § 327p Abs. 2 BGB-RegE in fast wortgetreuer Umsetzung von Art. 16 Abs. 3 DI-RL die Pflicht des Unternehmers, weiter nicht-personenbezogene Daten des Verbrauchers nicht zu nutzen, mit den in § 327p Abs. 2 Nr. 1 bis 4 BGB-RegE vorgesehenen Ausnahmen. Die Vorschrift gilt explizit nicht für personenbezogene Daten, für die sich alle Pflichten, insbesondere Löschungspflichten, allein aus der DS-GVO ergeben. Auch soll § 327p Abs. 2 BGB-RegE für alle Inhalte, also auch nicht-digitale Inhalte gelten, die der Verbraucher bei der Nutzung der digitalen Inhalte erstellt oder bereitgestellt hat;[22] hierunter dürften in erster Linie 3D-Drucke fallen, die mit Hilfe digitaler Inhalte bzw. Baupläne erstellt wurden. Der Anwendungsbereich erscheint mit Blick auf die Beschränkung auf nicht-personenbezogene

9 Vgl. *Spindler/Sein,* MMR 2019 488 (490); s.a. *Gsell*, in: Schulze/Staudenmayer, EU Digital Law, 1. Aufl. 2020, Art. 14 DCD Rn. 49, die darauf zu Recht hinweist, dass der Verbraucher das Recht zur Ablehnung der zweiten Andienung bzw. die Rechtsbehelfe der Minderung und Vertragsbeendigung haben muss.

10 So Begr. RegE, BT-Drs. 19/27653, 68.

11 Begr. RegE, BT-Drs. 19/27653, 69: Im Falle der unberechtigten Verweigerung hat der Verbraucher die Wahl zwischen Geltendmachung des Nachbesserungsanspruchs oder der Vertragsbeendigung.

12 Zu Verträgen mit Daten als Gegenleistung s. *Spindler*, MMR 2021, 451.

13 Zutr. *Rosenkranz*, ZUM 2021, 195 (200).

14 Begr. RegE, BT-Drs. 19/27653, 70, wonach sich in der Praxis aber keine großen Unterschiede ergeben sollen.

15 Begr. RegE, BT-Drs. 19/27653, 71.

16 Begr. RegE, BT-Drs. 19/27653, 69.

17 Begr. RegE, BT-Drs. 19/27653, 69.

18 S. zur Anwendbarkeit der §§ 305 ff. BGB *Spindler*, MMR 2021, 451.

19 Zur AGB Inhaltskontrolle im Kaufvertragsrecht s. *Fehrenbach*, in: BeckOGK, Stand: 1.3.2021, BGB § 307 Gewährleistungsklausel Rn. 26 ff.; *Schulte-Nölke*, in: HK-BGB, 10. Aufl. 2019, § 307 Rn. 18; *Faust*, in: BeckOK BGB, 57. Aufl., Stand: 1.2.2021, § 476 Rn. 29 f.; *Wurmnest*, in: MüKoBGB, 8. Aufl. 2019, § 307 Rn. 90 ff. jew. mwN.

20 Begr. RegE, BT-Drs. 19/27653, 71.

21 I.E. wohl ebenso *Twigg-Flesner*, in: Schulze/Staudenmayer (o. Fußn. 9), Art. 16 DCD Rn. 77.

22 Begr. RegE, BT-Drs. 19/27653, 73.

Daten verengt, da schon Metadaten einen Personenbezug auslösen können.[23] Der Unternehmer darf jedoch die nicht-personenbezogenen Daten weiter nutzen, wenn diese keinen Nutzen mehr außerhalb des vom Unternehmer bereitgestellten Kontextes haben, § 327p Abs. 2 S. 2 Nr. 1 BGB-RegE, wozu insbesondere die digitalen Umgebungen z.B. bei Computerspielen gehören; allerdings betont die Begründung zu Recht, dass diese Regelung nicht gelten kann, wenn der digitale Inhalt des Verbrauchers einfach konvertiert und in anderen digitalen Umgebungen weiterverwandt werden kann.[24]

Eine für die Praxis weitere wichtige wesentliche Ausnahme betrifft die aggregierten Daten, die vom Unternehmer nur mit unverhältnismäßigem Aufwand wieder disaggregiert werden können, § 327p Abs. 2 S. 2 Nr. 3 BGB-RegE, da solche Daten meist auch nicht mehr den Personenbezug nach der DS-GVO aufweisen. Für die Frage, wann ein unverhältnismäßiger Aufwand vorliegt, soll auf die Verdoppelung der Kosten für die Disaggregation zurückgegriffen werden[25] entsprechend Art. 2 Abs. 2 S. 2 VO 2018/1807[26] bzw. der entsprechenden Leitlinie der *EU-Kommission*.[27] Schließlich darf der Unternehmer digitale Inhalte, die von Nutzer*innen (nicht notwendigerweise Verbraucher*innen) gemeinsam erstellt wurden, weiterhin nutzen, gem. § 327p Abs. 2 S. 2 Nr. 4 BGB-RegE, sofern andere Verbraucher*innen diese Inhalte nutzen, wie etwa gemeinsam erstellte Spiellandschaften.[28]

Ähnlich wie Art. 20 DS-GVO sieht § 327p Abs. 3 BGB-RegE auch für nicht-personenbezogene Daten das Recht für den Verbraucher vor, vom Unternehmer in einem gängigen und maschinenlesbaren Format die Inhalte unentgeltlich übertragen zu bekommen – allerdings nicht diejenigen nach § 327p Abs. 2 S. 2 Nr. 1 bis 3 BGB-RegE, sodass vor allem die aggregierten Daten sowie die in einer proprietären Umgebung erstellten Inhalte nicht erfasst werden. Allerdings bleibt schon wie bei der DI-RL unklar, woher bei fehlendem Personenbezug der Daten der Unternehmer wissen soll, ob der Verbraucher tatsächlich genau diese Daten herausverlangen darf.

Die Auslegung der Begriffe unentgeltlich und gängiges Format können sich dabei an den Leitlinien des *Europäischen Datenschutzausschusses* bzw. *Art. 29-Datenschutzgruppe* zu Portabilität nach Art. 20 DS-GVO[29] orientieren.[30] Für die angemessene Frist kann auf Art. 12 Abs. 3 S. 1 DS-GVO zurückgegriffen werden, der höchstens einen Monat nach Antragseingang vorsieht. § 327p Abs. 3 S. 1 BGB-RegE normiert einen eigenständigen Anspruch des Verbrauchers, sodass eine Löschung der Inhalte vor Ablauf der Frist einen Schadensersatzanspruch des Verbrauchers auslösen kann.[31] Allerdings sieht § 327p Abs. 3 S. 1 BGB-RegE auch keine Frist vor, innerhalb derer der Verbraucher seine Rechte geltend machen muss; da aber der Anspruch mit der Vertragsbeendigung entsteht, sollte hier, entsprechend der Verjährungsfrist nach § 327j Abs. 3 BGB-RegE im Gewährleistungsbereich, eine zweimonatige Frist eingreifen.[32]

6. Auswirkung auf datenschutzrechtliche Erklärungen

Auf Grund des Auseinanderfallens der schuldrechtlichen Bindung des Verbrauchers hinsichtlich der Preisgabe seiner Daten und der Rechte nach der DS-GVO, insbesondere der freien Widerrufbarkeit der Einwilligung und des Widerspruchs, sieht sich der Gesetzgeber genötigt, in § 327q BGB-RegE nochmals die Unabhängigkeit der datenschutzrechtlichen Rechte zu betonen. So bleibt die Wirksamkeit des Vertrags durch die Ausübung von datenschutzrechtlichen Betroffenenrechten unberührt, § 327q Abs. 1 BGB-RegE.

Für die Fälle der wiederkehrenden Bereitstellungen gem. § 327b Abs. 5 S. 1 BGB-RegE oder der dauerhaften Bereitstellung nach § 327b Abs. 5 S. 2 BGB-RegE sieht § 327q Abs. 2 BGB-RegE ein in der DI-RL nicht explizit vorgesehenes Kündigungsrecht für den Unternehmer vor, das von einer Abwägung der Interessen des Unternehmers und derjenigen des Verbrauchers abhängt; nur wenn dem Unternehmer im Hinblick auf die nach Widerruf oder Widerspruch noch zulässigen Datenverarbeitungen die Fortsetzung des Vertragsverhältnisses unzumutbar ist, soll er das Kündigungsrecht ausüben können.[33] Die Regelung ist auch nicht abdingbar, § 327s Abs 1 BGB-RegE. Allerdings ist der Hinweis des Gesetzgebers, dass beim Widerruf der Einwilligung der Unternehmer die weitere Datenverarbeitung auf andere Rechtfertigungstatbestände nach der DS-GVO stützen könne,[34] in dieser Form jedenfalls nach – umstrittener[35] – Auffassung der Aufsichtsbehörden unzutreffend, da beim Wegfall der Einwilligung der Datenverarbeiter sich nicht auf andere Rechtfertigungstatbestände stützen können soll.[36]

§ 327q Abs. 3 BGB-RegE flankiert die Sicherung der freien Ausübung der datenschutzrechtlichen Betroffenenrechte weiter, indem jedwede Ersatz- oder Vergütungsansprüche des Unternehmers für den Entfall der Datenverarbeitung zwingend ausgeschlossen werden, einerlei ob sie auf vertraglichen oder gesetzlichen Ansprüchen beruhen wie z.B. Schadensersatzansprüche[37] oder Nutzungsersatzansprüche aus § 812 Abs. 1 S. 1 BGB.[38] Damit weicht der RegE explizit von einer Strömung in der Literatur ab, die ein strengeres Vorgehen zur Vermeidung von Missbrauch gefordert hatte, etwa Regeln zum Nutzungsersatz oder ein (bedingungsloses) Kündigungsrecht in den Fällen des Einwilligungswiderrufs.[39] Auch jedweder Diskussion um eine mögliche Einschränkung des Widerrufsrechts in diesen Fällen wird damit ein Riegel vorgeschoben.[40]

---

23 S.a. Begr. RegE, BT-Drs. 19/27653, 71; zum möglichen Personenbezug von Metadaten: *Ernst*, in: Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 14; *Albers/Veit*, in: BeckOK DatenschutzR, 35. Aufl., Stand: 1.5.2020, DS-GVO Art. 9 Rn. 19; *Schiff*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 65-68, so schon zur Auslegung des personenbezogenen Datums i.S.d. DS-GVO Vorgängers der RL 95/46/EG: *Art. 29-Datenschutzgruppe*, Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken (WP 215) v. 10.4.2014, S. 5.

24 Begr. RegE, BT-Drs. 19/27653, 73 f.

25 So Begr. RegE, BT-Drs. 19/27653, 74.

26 VO (EU) 2018/1807 des Europäischen Parlaments und des Rates v. 14.11.2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (ABl. L 303 v. 28.11.2018, S. 59).

27 Gliederungspunkt 2.2 der Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union v. 29.5.2019 (COM(2019) 250 final).

28 Begr. RegE, BT-Drs. 19/27653, 74, dies soll dagegen nicht für das Kommentieren von Inhalten bei sozialen Netzwerken gelten.

29 Leitlinien zum Recht auf Datenübertragbarkeit der *Art. 29-Datenschutzgruppe* v. 13.12.2016 i.d.F. v. 5.4.2017 (16/DE WP 242 rev.01, S. 18).

30 Zutr. Begr. RegE, BT-Drs. 19/27653, 75.

31 Begr. RegE, BT-Drs. 19/27653, 74.

32 S. aber auch *Twigg-Flesner* (o. Fußn. 21), Rn. 53 f., der nur eine „reasonable time after excersing the right to terminate the contract" annimmt.

33 Ähnl. i.E. schon *Hacker*, Datenprivatrecht, 2020, S. 226 ff.

34 Begr. RegE, BT-Drs. 19/27653, 76.

35 Gegen die Sperrwirkung der widerrufenen Einwilligung: *Albers/Veit* (o. Fußn. 23), Art. 6 Rn. 27; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 11; *Borges/Steinrötter*, in: BeckOK IT-Recht, 1. Aufl., Stand: 1.9.2020, DS-GVO Art. 6 Rn. 7; *Taeger*, in: Taeger/Gabel, DSGVO – BDSG, 3. Aufl. 2019, DS-GVO Art. 6 Rn. 41; dafür: *Uecker*, ZD 2019, 248 (249).

36 *Datenschutzkonferenz (DSK)*, Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, Stand: 22.2.2019, S. 3; *Art. 29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gem. VO 2016/679 (WP259 rev.01) v. 10.4.2018, S. 27.

37 Dazu *Hacker* (o. Fußn. 33), S. 211 f.

38 Begr. RegE, BT-Drs. 19/27653, 76.

39 Etwa *Kumkar*, ZfPW 2020, 306 (330 f.); für strengere Regeln auf Grund von Missbrauchsgefahr auch *Specht*, JZ 2017, 763 (769).

40 Zu dieser Möglichkeit *Kumkar*, ZfPW 2020, 306 (330 f.); *Specht*, JZ 2017, 763 (769); umfassend *Hacker* (o. Fußn. 33), S. 208 ff., der Einschränkungen strikt ablehnt.

Insgesamt handelt es sich beim § 327q BGB-ReGE auf den ersten Blick zwar um eine gute Kompromisslösung.[41] Auf der einen Seite sollte dem Umstand Rechnung getragen werden, dass personenbezogene Daten denselben Stellenwert wie monetäre Gegenleistungen[42] einnehmen, auf der anderen Seite musste dem Datenschutz genüge getan werden, indem es weiterhin zumindest überwiegend nachteilsfrei möglich bleiben soll, seine datenschutzrechtlichen Betroffenenrechte auszuüben. Doch wird als Ergebnis dieses Spagats mit § 327q BGB-RegE zwischen dem Vertrag und der datenschutzrechtlichen Einwilligung eine harte Trennung eingeführt.

Dadurch wird das grundlegende Problem, dass die DS-GVO keine vertragsrechtlichen Ansätze kennt,[43] auf geschickte Art und Weise umgangen,[44] was auf den ersten Blick auch interessengerecht erscheint; betrachtet man Tatbestand und Rechtsfolgen des Kündigungsrechts des Unternehmers aber genauer, wird deutlich, dass weiterhin Probleme bestehen. So ist nach § 327q Abs. 2 BGB-RegE zunächst eine Abwägung durchzuführen, um das Bestehen des Kündigungsrechts zu prüfen. Weiterhin ist nicht abschließend geklärt, welche Gewährleistungsrechte ab Einwilligungswiderruf und bis zu einer etwaigen Kündigung des Unternehmers bestehen.

Offen bleibt zudem die grundlegende Frage, was bei einem synallagmatischen Vertrag die Leistungspflicht des Datenbereitstellers (des Verbrauchers) ausmacht, etwa ob die Erteilung der Einwilligung in die Verarbeitung oder die bloße Bereitstellung der Daten geschuldet wird, insbesondere ob ein Anspruch auf Datenbereitstellung durchsetzbar wäre[45] – was letztlich der strikten Trennung nach § 327q BGB-RegE widersprechen dürfte.

III. Änderung von dauerhaft bereitgestellten digitalen Produkten

Schließlich regelt § 327r BGB-RegE die Voraussetzungen und Rechtsfolgen bei Änderungen i.R.v. Verträgen über die dauerhafte Bereitstellung von digitalen Produkten, auch solche ohne Bezahlung durch einen Preis,[46] aber nicht der wiederkehrenden Bereitstellung. Keine Anwendung findet § 327r BGB-RegE gemäß Absatz 6 auf Paketverträge mit Bestandteilen eines Internet-Zugangsdienstes oder rufnummerngebundenen Kommunikationssystems, was Art. 3 Abs. 6 UAbs. 3 DI-RL entspricht.

Die Regelung hindert nicht den Abschluss eines neuen Vertrags, Erwägungsgrund 75 DI-RL, sondern wirkt nur im Rahmen eines bestehenden Vertrags. Auch bei einer Änderung muss das digitale Produkt im Kern erhalten bleiben.[47] Schwierigkeiten können sich hinsichtlich der Abgrenzung zu den Pflichten zu Updates bzw. Aktualisierungen ergeben, die nur die Vertragsmäßigkeit aufrechterhalten sollen, § 327e Abs. 2 Nr. 3, Abs. 3 Nr. 5 BGB-RegE. Demgemäß kann es für Änderungen nach § 327r BGB-RegE nur um solche Updates gehen, die über die Vertragsmäßigkeit hinausgehen und die vertraglich geschuldete Leistung ändern sollen.[48]

Daher müssen sog. Funktions-Updates, die die Möglichkeiten z.B. eines Programms erweitern, aber auch Sicherheits-Updates enthalten, aufgespalten werden in solche, die die ursprünglichen vertraglich geschuldeten Funktionen erhalten sollen, und solche, die diese Funktionen erweitern; nur für Letztere ist § 327r BGB-RegE einschlägig.

Die Änderungsmöglichkeit muss ferner vertraglich vorgesehen sein, § 327r BGB-RegE gibt kein gesetzliches Änderungsrecht;[49] zudem bleibt die Inhaltskontrolle nach § 308 Nr. 4 BGB unberührt.[50] Änderungen sollen u.a. nur bei triftigem Grund nach § 327r Abs. 1 Nr. 1 BGB-RegE möglich sein, wobei Erwägungsgrund 75 DI-RL Änderungen infolge neuer technischer Umgebungen (z.B. geänderte Betriebssysteme), erhöhte Nutzerzahlen oder allgemein wichtige betriebstechnische Gründe erwähnt. Der triftige Grund muss im Vertrag spezifiziert sein.[51] Allerdings sind gerade hier Zweifel an der Abgrenzung zu den Updates zur Erhaltung der Vertragsmäßigkeit, gerade bei geänderten digitalen Umgebungen,[52] nicht zu verhehlen. Anders als im Fall nachteiliger Veränderungen muss der Verbraucher nicht im Vorhinein informiert werden; eine mit der Änderung vorgenommene zeitgleiche Information genügt.[53]

Bei für den Verbraucher nachteiligen Änderungen müssen zunächst die Gründe nach § 327r Abs. 1 BGB-RegE vorliegen; er muss darüber hinaus aber auch „innerhalb einer angemessenen Frist vor dem Zeitpunkt der Änderung mittels eines dauerhaften Datenträgers informiert" werden. Die angemessene Frist soll sich dabei einzelfallabhängig bestimmen,[54] die Nachteiligkeit anhand eines objektiven Maßstabs entsprechend § 327e Abs. 3 Nr. 2 BGB-RegE wiederum in Abhängigkeit von der Art des Produkts etc. Die Information des Verbrauchers muss Angaben über die Merkmale und den Zeitpunkt der Änderung ebenso wie über die Rechte des Verbrauchers enthalten einschließlich einer etwaigen Möglichkeit zur unveränderten Fortsetzung des Vertrags, § 327r Abs. 2 S. 2 Nr. 1, 2 BGB-RegE. Stimmt die Information nicht mit der Änderung überein, liegt keine Befugnis zur Änderung vor, sodass das digitale Produkt nicht mehr vertragskonform ist.[55]

Dem Verbraucher steht unabhängig von der Information durch den Unternehmer[56] jedenfalls das Recht zur Vertragsbeendigung ab dem Zeitpunkt der Änderung (und wiederum unabhängig von der Information) zu, sofern die Änderung nicht unerheblich ist, § 327r Abs. 3 BGB-RegE. Als unerheblich sieht der Gesetzgeber etwa eine lediglich grafische Änderung der Nutzeroberfläche ohne Einfluss auf die Funktionalität an.[57]

Das Beendigungsrecht des Verbrauchers wird jedoch ausgeschlossen, wenn der Unternehmer dem Verbraucher die Weiternutzung der aktuellen Version ohne Änderung einräumt, § 327r Abs. 4 BGB-RegE. Bezugspunkt ist immer die jeweils aktuelle

41 Dazu auch *Sattler*, NJW 2020, 3623 (3627 ff.).
42 Obwohl der Datenhandel in den Anwendungsbereich der Richtlinie fällt, wird im Bezug auf Daten bewusst auf den Begriff „Gegenleistung" verzichtet, dies war im Kommissionsentwurf noch anders, vgl. Art. 3 Abs. 1 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final und ist wohl Ergebnis der Kritik des europäischen Datenschutzbeauftragten s. *European Data Protection Supervisor (EDPS)*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (14.3.2017), 9 f.; ausf. zur Frage, wann Daten als Gegenleistung kategorisiert werden können *Hacker*, ZfPW 2019, 148 (159 ff.).
43 Krit. dazu auch: *Staudenmeyer*, ZEuP 2019, 663 (676); *Sattler*, CR 2020, 145 (152).
44 *Sattler*, NJW 2020, 3623 (3628).
45 Dazu *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221); *Kumkar*, ZfPW 2020, 306 (327).
46 Begr. RegE, BT-Drs. 19/27653, 77 in Klarstellung zu § 327r Abs. 1 Nr. 2 BGB-RegE.
47 Zutr. *Möllnitz,* MMR 2021, 116 (118).
48 Begr. RegE, BT-Drs. 19/27653, 77; *Möllnitz,* MMR 2021, 116 (117).
49 Begr. RegE, BT-Drs. 19/27653, 77; *Schulze*, ZEuP 2019, 695 (716); *Staudenmayer*, NJW 2019, 2497 (2501), näher zur Funktion des Änderungsrechts: *Wendland*, in: Schulze/Staudenmayer (o. Fußn. 9), Art. 19 DCD Rn. 1 f., 8.
50 Anders offenbar *Möllnitz,* MMR 2021, 116 (119), die § 327r BGB-RegE hier als abschließend ansieht, jedenfalls hinsichtlich des Transparenzgebots.
51 *Spindler/Sein,* MMR 2019, 488 (493); *Möllnitz,* MMR 2021, 116 (119).
52 S. aber *Möllnitz,* MMR 2021, 116 (118), die auch dies offenbar unter die Änderung einbeziehen will.
53 Begr. RegE, BT-Drs. 19/27653, 78 unter Verweis auf Art. 19 Abs. 1 DI-RL.
54 Begr. RegE, BT-Drs. 19/27653, 78.
55 Anders offenbar *Möllnitz,* MMR 2021, 116 (120), die dann einen geänderten Vertragsinhalt auf Grund der gegebenen Information annehmen will.
56 Begr. RegE, BT-Drs. 19/27653, 78.
57 Begr. RegE, BT-Drs. 19/27653, 79.

Version, die der Verbraucher akzeptiert hat; ein Wahlrecht zwischen verschiedenen vorhergehenden, von ihm übersprungenen Versionen hat der Verbraucher nicht,[58] ebenso wenig einen Anspruch auf Beibehaltung der unveränderten Version.[59] Bei zulässiger Änderung ist der Verbraucher vielmehr zur Duldung verpflichtet; eine eigenständige Eingriffsbefugnis in die digitale Umgebung wird dem Unternehmer allerdings auf Grund der tiefgreifenden Folgen nicht zuzugestehen sein.[60]

Die Rechtsfolgen bei Beendigung richten sich gem. § 327r Abs. 5 BGB-RegE nach den speziellen Normen für digitale Produkte, hier der §§ 327o, 327p BGB-RegE mit der Möglichkeit Schadensersatz nach § 327m Abs. 3 BGB-RegE zu verlangen.

IV. Verjährungsfrist

§ 327j BGB setzt Art. 11 Abs. 2, Abs. 3 DI-RL um und unterscheidet im Gefolge der Ferenschild-Entscheidung des *EuGH*[61] zwischen den Fristen der Gewährleistung und der Verjährung der Ausübung der Rechte. Demgemäß beträgt die Gewährleistungsdauer bei einer einmaligen Bereitstellung mindestens zwei Jahre ab der Bereitstellung, bei einer dauerhaften Bereitstellung mit Ende des entsprechenden Zeitraums, § 327j Abs. 1, Abs. 2 BGB-RegE. Eine Sonderregelung hat die Verjährung für Aktualisierungspflichten bei einmaligen Bereitstellungen erfahren, die erst mit dem Ablauf des Zeitraums beginnt, innerhalb dessen Verbraucher die Updates erwarten können (§ 327f Abs. 1 S. 3 Nr. 2 BGB-RegE), womit die normale Verjährungsfrist erheblich verlängert werden kann und etlichen Ungewissheiten unterliegt.[62] Der deutsche Gesetzgeber konnte aber angesichts der Regelungen in der DI-RL auf Grund ihres vollharmonisierenden Charakters nicht hiervon abweichen.

Im Sinne der sog. Ferenschild-Entscheidung des *EuGH* beträgt die nach Art. 11 Abs. 2 UAbs. 3 DI-RL dem Mitgliedstaat überlassene Verjährungsfrist für die Geltendmachung der Gewährleistungsrechte zwei Monate nach Auftreten des Mangels[63] – daraus können sich faktisch längere „Gewährleistungsfristen", aber auch kürzere ergeben, da der Beginn der Verjährungsfrist auf das erste Auftreten des Mangels abstellt.

Für die Gestaltungsrechte der Vertragsbeendigung und Minderung verweist § 327j BGB dagegen auf die entsprechende Anwendung des § 218 BGB, der sonst nur für den Rücktritt gilt, womit ein Gleichklang der Gewährleistungsfristen erreicht wird. [64]

V. Beweislast

§ 327k BGB-RegE dient der fast wortgetreuen Umsetzung der Regelungen in Art. 12 DI-RL und differenziert danach, ob es sich um einmalige und wiederkehrende Bereitstellungen handelt, hier eine Beweislastumkehr ein Jahr ab der Bereitstellung, oder ob es sich um eine dauerhafte Bereitstellung handelt, für die eine Beweislastumkehr für den Zeitraum der Bereitstellung gilt. Anders als Art. 12 DI-RL, der generell auf die Vertragswidrigkeit nach Art. 5 DI-RL verweist, bezieht § 327k Abs. 1, Abs. 2 BGB-RegE sich nur auf §§ 327e, g BGB, mithin nicht auf die Aktualisierungspflichten nach § 327f BGB; auch der Begründung lässt sich hierfür kein entsprechender Anhaltspunkt für diese Auslassung entnehmen. In europarechtskonformer Auslegung muss es aber für die Verpflichtungen zur Aktualisierung ebenso auf die Differenzierung nach einmalig oder dauerhaft bereitgestellten Inhalten ankommen, mit der Folge, dass die Beweislastumkehr für fehlgeschlagene Updates für einmalig bereitgestellte Inhalte ein Jahr nach deren Bereitstellung endet.

Nach § 327k Abs. 3, Abs. 4 BGB bzw. Art. 12 Abs. 4, Abs. 5 DI-RL greift die Beweislastumkehr der § 327k Abs. 1, Abs. 2 BGB-RegE nicht ein, wenn die digitale Umgebung des Verbrauchers zum jeweils relevanten Zeitpunkt nicht kompatibel war, sofern der Unternehmer den Verbraucher vor Vertragsschluss klar und deutlich über die technischen Anforderungen des Produkts oder seine Obliegenheit zur Mitwirkung informiert hat, § 327k Abs. 4 BGB-RegE.[65] Diese Obliegenheit umreißt § 327k Abs. 3 Nr. 2 BGB-RegE dahingehend, dass der Verbraucher eine notwendige und ihm mögliche Mitwirkung zur Feststellung der digitalen Umgebung nicht vornimmt und der Unternehmer dafür das den Verbraucher am geringsten belastende technische Mittel einsetzen wollte. Dabei umfasst die digitale Umgebung die gesamte Hard- und Software des Verbrauchers bis hin zu seinen Netzwerkverbindungen.[66]

Die Probleme, die sich hieraus aus der DS-GVO und auch Überlegungen zur IT-Sicherheit ergeben, liegen demgegenüber auf der Hand und werden vom Gesetzgeber nur ansatzweise adressiert,[67] indem die Übermittlung von automatisch erstellten Fehlerberichten erwähnt wird, für die aber der deutsche Gesetzgeber zu Recht darauf hinweist, dass hier eine aktive vorherige Zustimmung durch den Verbraucher erforderlich ist.[68] Ob z.B. eine vorab erteilte generelle Zustimmung zur Übermittlung von Fehlerdiagnoseberichten den Maßstäben der DS-GVO standhält, erscheint angesichts der durchaus verschiedenen Fehlermöglichkeiten zweifelhaft. Dies gilt erst recht für Fernwartungen („remote access"), die dem Unternehmer einen uneingeschränkten Zugriff auf die digitale Umgebung des Verbrauchers ermöglichen.

VI. Regress zwischen Unternehmern

Die einzige auf Verträge zwischen Unternehmern konzipierte Regelung enthält § 327u BGB-RegE, der einen zwingenden, nicht abdingbaren Regress für den Unternehmer gegenüber Vorlieferanten in Gestalt eines Aufwendungsersatzanspruchs im Falle digitaler Produkte vorsieht und Art. 20 DI-RL umsetzt, der allerdings den Mitgliedstaaten einen erheblichen Spielraum belässt. Nach § 327u Abs. 6 BGB-RegE gilt dies aber nicht nur im ersten „Endglied" der Vertriebskette, sondern gegenüber jedem Vertriebspartner in der Lieferkette, also im Prinzip bis zum ersten Lieferanten, sog. Kettenregress.[69] Nur Open-Source-Anbieter bleiben ausgenommen.[70]

Der Aufwendungsersatzanspruch bezieht sich zum einen auf die unterbliebene Bereitstellung des digitalen Produkts gem. § 327c Abs. 1 S. 1 BGB-RegE, zum anderen auf Aufwendungen i.R.v. Gewährleistungsansprüchen des Verbrauchers gegenüber dem Unternehmer. Allerdings muss der Mangel zum Zeitpunkt der Bereitstellung für den Verbraucher vorgelegen haben – wovon die Pflicht zu Aktualisierungen nach § 327f Abs. 1 BGB-RegE ausgenommen ist, § 327u Abs. 1 S. 2 BGB-RegE, bezogen indes nur auf die objektiven Anforderungen, nicht auf vertragliche Vereinbarungen zwischen Unternehmer und Verbraucher.[71]

58 Begr. RegE, BT-Drs. 19/27653, 77.
59 *Spindler/Sein,* MMR 2019, 488 (493); *Möllnitz,* MMR 2021, 116 (120).
60 Zutr. *Möllnitz,* MMR 2021, 116 (120).
61 *EuGH* U. v. 13.7.2017 – C-133/16 – Ferenschild.
62 *Bitkom*, Stellungnahme RefE Umsetzung Digitale Inhalte Richtlinie v. 30.11. 2020, S. 5 abrufbar unter: https://www.bitkom.org/Bitkom/Publikationen/Referentenentwurf-zur-Umsetzung-der-Digitale-Inhalte-Richtlinie.
63 Begr. RegE, BT-Drs. 19/27653, 63.
64 Begr. RegE, BT-Drs. 19/27653, 62.
65 Begr. RegE, BT-Drs. 19/27653, 64 mit der Klarstellung, dass der relevante Zeitpunkt sich aus Art. 12 Abs. 5 S. 3 DI-RL ergebe.
66 Begr. RegE, BT-Drs. 19/27653, 64.
67 Auf diese Probleme weisen auch *Spindler/Sein,* MMR 2019, 488 (490) hin.
68 Begr. RegE, BT-Drs. 19/27653, 65; s. zu dieser Problematik bereits: *Spinder/Sein,* MMR 2019, 488 (490).
69 Begr. RegE, BT-Drs. 19/27653, 82.
70 S.a. Begr. RegE, BT-Drs. 19/27653, 81.
71 Begr. RegE, BT-Drs. 19/27653, 81.

§ 327u Abs. 2 BGB-RegE sieht als Frist für die Verjährung sechs Monate ab der Erfüllung der Ansprüche des Verbrauchers durch den Unternehmer vor, was gerade für Updates natürlich auf Grund des faktisch verlängerten Gewährleistungszeitraums weit über die sonst vorgesehenen zwei Jahre hinausgehen kann.[72] Ferner erklärt § 327u Abs. 3 BGB-RegE die Beweislastumkehrregeln der § 327k Abs. 1, 2 BGB-RegE für entsprechend anwendbar, allerdings naturgemäß auf Grund des fehlenden Kontakts mit dem Verbraucher nicht hinsichtlich der digitalen Umgebung des Verbrauchers.

Bemerkenswert ist ferner, dass nach § 327u Abs. 4 BGB-RegE die Regelungen zum Regress – anders als nach der DI-RL – nicht abdingbar sind, da der deutsche Gesetzgeber von einer strukturellen Unterlegenheit des Unternehmers gegenüber seinen Vertriebspartnern ausgeht.[73] Die an sich zwingende Geltung von § 327u BGB-RegE dürfte allerdings in der internationalen Lieferkette häufig unterlaufen werden: Denn ähnlich wie für § 478 BGB[74] greift Art. 9 Rom-I-VO als Ausnahmevorschrift für Eingriffsnormen hier nicht ein, sodass § 327u BGB-RegE international-privatrechtlich abbedungen werden kann.

Relativiert wird der zwingende Regress dadurch, dass § 377 HGB, mithin die Rügepflicht, unberührt bleiben soll, § 327u Abs. 5 BGB-RegE; mit anderen Worten verliert der Unternehmer seinen Regressanspruch gegenüber seinem Vertriebspartner, wenn er den bereitgestellten digitalen Inhalt nicht unverzüglich auf Mängel hin untersucht. Offen ist auch, wie mit Klauseln zu § 377 HGB im Verhältnis zu § 327u Abs. 4 BGB-RegE verfahren werden soll; da § 377 HGB unberührt bleiben soll, muss dies auch für entsprechende Klauseln, die sich auf § 377 HGB beziehen, gelten. Dieses Prinzip ist bereits aus dem Verbrauchsgüterkaufrecht mit § 445a Abs. 4 BGB bekannt.

VII. Folgeänderungen im BGB

Auf Grund der erforderlichen Verzahnung des neuen Titels im Schuldrecht Allgemeiner Teil wurden auch Änderungen im Besonderen Teil erforderlich, der die Verträge über digitale Produkte von den ansonsten einschlägigen Regelungen ausnimmt, etwa im neuen § 453 Abs. 1 BGB-RegE oder § 475a BGB-RegE, hier bereits in Verzahnung mit der noch umzusetzenden Warenkauf-RL im Hinblick auf Waren, deren Funktionalität von digitalen Produkten abhängt, § 475a Abs. 2 BGB-RegE.[75] Bemerkenswert ist ferner die Ausnahme der schenkungsrechtlichen Gewährleistungsansprüche: Hier verweist § 516a Abs. 1 BGB-RegE ohne jede Einschränkung vollumfänglich auf die Gewährleistungsansprüche für die digitalen Produkte, einschließlich der Schadensersatzansprüche. Die Gesetzesbegründung rekurriert hierfür vor allem auf Verträge, die kein preisliches Entgelt, sondern nur Daten als „Gegenleistung" vorsehen.[76] Die daraus entstehende Komplexität wird nicht zuletzt anhand von § 516a Abs. 2 BGB-RegE verdeutlicht, der für Sachen mit digitalen Produkten für die Sachen auf das Schenkungsrecht nach wie vor verweist, für die digitalen Produkte aber auf die §§ 327a ff. BGB-RegE.

Ebenfalls komplexe Probleme wirft die Differenzierung zwischen der Miete von Sachen und derjenigen von digitalen Produkten auf, wie sie in § 548a BGB-RegE aufgenommen wird. Der Gesetzgeber will etwa die Klärung der Frage, ob die Überlassung eines Servers an einen Mieter, der aber nur den Online-Zugang auf die Sache erhält, dem klassischen Mietrecht oder demjenigen der §§ 327a ff. BGB zu unterstellen ist, der Rechtsprechung und Wissenschaft überlassen.[77] § 578b BGB-RegE verweist dann wiederum auf die §§ 327a ff. BGB-RegE bzw. bedingt diejenigen Normen des Mietvertragsrechts ab, die von den §§ 327a ff. BGB-RegE verdrängt werden. Gleiches gilt entsprechend für das Dienstleistungsvertragsrecht (§ 620 Abs. 4 BGB-RegE) und das Werkvertragsrecht (§ 650 Abs. 2 bis 4 BGB-RegE). Im Gegensatz zur Schenkung regelt der BGB-RegE jedoch nichts zu seinem Pendant im Mietrecht, der Leihe.[78]

VIII. Zusammenfassung

Die Umsetzung der DI-RL hat den Gesetzgeber fast vor eine Herkules-Aufgabe gestellt, geht es doch um dem BGB sonst fremde, vertragstypenunabhängige Regelungen über Verträge mit digitalen Produkten. Dem Gesetzgeber ist jedoch zu bescheinigen, dass er – auch bedingt durch die vollharmonisierende Wirkung der DI-RL – die Richtlinie weitgehend getreu umgesetzt hat. Entscheidende Fragen werden aber der Klärung durch Rechtsprechung und Wissenschaft überlassen bleiben, wozu nach wie vor das Verhältnis von Datenschutzrecht zu Zivilrecht ebenso wie zum Urheberrecht gehören wird. Auch die Fragen, wie lange Updates geschuldet sind, wird der kasuistischen Klärung überlassen bleiben. Probleme wirft ferner das Verhältnis von AGB-Klauselkontrolle zu den von § 327h BGB möglichen individuellen Abweichungen von den Anforderungen zum Produktmangel auf.

Schnell gelesen ...

- Die Umsetzung der DI-RL hält an dem bewährten System der Rechtsbehelfe weitgehend fest, überlässt allerdings dem Unternehmer die Wahlfreiheit, ob er nacherfüllt oder nachbessert.
- Hinsichtlich des Schadensersatzes führt das Umsetzungsgesetz in § 327m BGB-RegE die bisherigen Voraussetzungen fort, indem der Schadensersatzanspruch verschuldensabhängig ausgestaltet wird.
- Für das Verhältnis zum Datenschutzrecht trennt § 327q BGB-RegE scharf zwischen schuld- und datenschutzrechtlicher Ebene. Eine Einordnung der Preisgabe von personenbezogenen Daten in das Synallagma nimmt auch das Umsetzungsgesetz nicht vor, sodass zahlreiche Fragen nach wie vor offenbleiben.
- Der Regress zwischen Unternehmern ist zwar als zwingendes Recht ausgestaltet, kann jedoch in internationalen Lieferketten abbedungen werden, da die Regelungen keine zwingenden Eingriffsnormen i.S.v. Art. 9 Rom-I-VO darstellen. Zudem schränkt § 377 HGB den Regress weiter ein.

Professor Dr. Gerald Spindler
ist Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Multimedia- und Telekommunikationsrecht an der Georg-August-Universität in Göttingen sowie Mitherausgeber der MMR.

72 Darauf weist zutr. Begr. RegE, BT-Drs. 19/27653, 81 hin.
73 Begr. RegE, BT-Drs. 19/27653, 81.
74 *Arnold*, in: BeckOGK, Stand: 15.1.2021, BGB § 478 Rn. 72; s.a. *Martiny*, in: MüKoBGB, 8. Aufl. 2021, Rom-I-VO Art. 9 Rn. 88.
75 Begr. RegE, BT-Drs. 19/27653, 83.
76 Begr. RegE, BT-Drs. 19/27653, 83 f.; krit. *Rosenkranz*, ZUM 2021, 195 (204).
77 Begr. RegE, BT-Drs. 19/27653, 84 unter Verweis auf *BGH* MMR 2007, 243.
78 S. *Bitkom* (o. Fußn. 62), S. 1 ff.; s.a. *Rosenkranz*, ZUM 2021, 195 (204).

ANDREAS HARTL / ANNA LUDIN

Recht der Datenzugänge

Was die Datenstrategien der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen

Datenpolitik

Die Auswertung von Daten verbessert Entscheidungen in Politik und Wirtschaft. Der steigenden politischen Relevanz haben EU-Kommission und Bundesregierung mit jeweiligen Datenstrategien Rechnung getragen. Auf beiden Ebenen werden die Strategien durch gesetzgeberische Maßnahmen umgesetzt. Ein Rechtsrahmen für den Zugang zu und die Nutzung von Daten entsteht derzeit. Dieser Beitrag soll einen Überblick über die einzelnen parallelen Gesetzesinitiativen geben. Dargestellt werden Regelungen auf europäischer und nationaler Ebene zunächst für öffentlich finanzierte Daten, schließlich für Datenzugang zwischen Privaten. Lesedauer: 21 Minuten

Unternehmerischer Erfolg ist im globalen Wettbewerb zunehmend von der Fähigkeit zur Datennutzung abhängig. Die Datennutzung beinhaltet zunächst, den Wert der relevanten Daten im Kontext zu verstehen und das Potenzial zur Wertschöpfung mit entsprechenden Verknüpfungen und Analysemethoden zu erschließen. Angesichts von Klimawandel und Pandemie ist auch die Erfüllung staatlicher Aufgaben offenkundig zunehmend durch evidenz- und damit datenbasierte Politik und Regierungsführung bestimmt. Die Politik reagiert auf diese Entwicklungen durch Datenstrategien, die Grundlage für zahlreiche Gesetzesinitiativen sind. Die *Bundesregierung* hat am 27.1.2021 eine Datenstrategie[1] beschlossen. Sie rückt dabei wie die *EU-Kommission* mit der Europäischen Datenstrategie v. 19.2.2020[2] die Datenpolitik in den Fokus ihrer digitalpolitischen Vorhaben.

Die im Wesentlichen übereinstimmende Zielsetzung beider Datenstrategien ist: Sowohl Unternehmen als auch der öffentliche Sektor können durch die Nutzung von Daten bessere Entscheidungen für soziales und wirtschaftliches Wohlergehen treffen. Um dieses Potenzial zu erschließen, braucht es eine Steigerung des Datenaustauschs, d.h. besseren Datenzugang und eine verantwortungsvolle Datennutzung.[3]

Seit Jahren debattieren Wissenschaft und Politik, ob Daten einer „eigentumsähnlichen" Zuordnung bedürfen. Die Datenstrategie macht deutlich, dass die *Bundesregierung* derzeit kein Erfordernis für Ausschließlichkeitsrechte an Daten sieht.[4] Hintergrund sind die besonderen Eigenschaften von Daten als nicht-rivale Wirtschaftsgüter. Ökonomische Allokationsfragen sind somit unter anderem Vorbedingungen zu beantworten als bei physischen Gütern. Nicht die ausschließliche Zuordnung zur Verarbeitung oder zum Verbrauch eines Rohstoffs steht im Mittelpunkt, sondern die Frage der Nutzbarkeit und damit Fragen des Zugangs und der Bereitstellung.

Der Rechtsrahmen für diese Datenwirtschaft wird insbesondere auf EU-Ebene gestaltet, flankiert durch einzelne bundesrechtliche Initiativen wie die 10. GWB-Novelle sowie die Open-Data-Gesetzgebung. Die fragmentierte Rechtsmaterie des Datenrechts verdichtet sich mehr und mehr mit neuen (europäischen) Legislativvorschlägen. Dieser Beitrag bietet einen Überblick zu laufenden und bevorstehenden Initiativen. Zunächst wird die staatliche Bereitstellung von Daten beleuchtet, daran anschließend werden privatrechtliche Gesetzgebungsinitiativen dargestellt.

I. Öffentlich finanzierte Daten: Vom Zugang zur Bereitstellung und Nutzung

Die Datenstrategie der *Bundesregierung* will den Staat im Umgang mit Daten zum Vorreiter machen. Dabei geht es nicht nur um eine Ausweitung der proaktiven Bereitstellung von offenen Verwaltungsdaten (Open Data), sondern auch um die Frage, wie die öffentliche Hand Daten nutzt. Dieser Beitrag konzentriert sich auf die Bereitstellung von Daten durch den öffentlichen Sektor und ihre Nutzung außerhalb der öffentlichen Aufgabenerfüllung.

1. Der europäische Rechtsrahmen

Der europäische Rechtsrahmen zu offenen Daten des öffentlichen Sektors regelt nicht die Bereitstellungsverpflichtung hinsichtlich bestimmter Daten. Welche (Verwaltungs-)Daten in den Mitgliedstaaten zugänglich sind, obliegt weiterhin den nationalen Gesetzgebern.[5] Dennoch bildet seit 2003 die PSI-RL[6] einen horizontalen Rahmen, der die Hürden der grenzüberschreitenden Nutzung dieser Daten für kommerzielle und nicht-kommerzielle Akteure zunehmend abbauen soll.

Zum Verständnis der Weiterentwicklung des europäischen Rechtsrahmens trägt folgende Dreiteilung bei: Der Datenzugang kann offen, eingeschränkt oder verschlossen sein.[7] Mit der RL (EU) 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Open-Data- und PSI-Richtlinie – OD-PSI-RL) werden die Bedingungen der Weiterverwendung oder Nachnutzung öffentlich finanzierter Daten angeglichen, also von uneingeschränkt zugänglichen Daten.

Ein Großteil potenziell wertvoller Daten ist damit bereits nicht im Anwendungsbereich der OD-PSI-RL. Um die darüberhinausgehende Praxis in Bezug auf die Nachnutzung von Daten des öffentlichen Sektors zu harmonisieren, hat die *EU-Kommission* i.R.d. Europäischen Datenstrategie einen ersten Legislativvorschlag vorgestellt. Für Daten des öffentlichen Sektors, die auf Grund von Rechten Dritter nicht offen bereitgestellt oder lediglich eingeschränkt zugänglich gemacht werden können, enthält ein am 25.11.2020 vorgelegter Vorschlag für ein Daten-Gover-

1 Datenstrategie der Bundesregierung – Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum v. 27.1.2021, abrufbar unter: https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632.

2 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, COM(2020) 66 final (EU-Datenstrategie).

3 EU-Datenstrategie (o. Fußn. 2), S. 5

4 S.o. Fußn. 1, S. 23.

5 Von diesem Grundsatz wird aus besonderen Erwägungen in bestimmten Bereichen abgewichen wie z.B. mit der INSPIRE-Richtlinie.

6 RL 2003/98/EG des Europäischen Parlaments und des Rates v. 17.11.2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (Public Sector Information – PSI).

7 Das *Open Data Institute* in London unterteilt das Datenspektrum in „Closed Data, Shared Data, Open Data", abrufbar unter: https://theodi.org/about-the-odi/the-data-spectrum/.

nance-Gesetz (engl. Data Governance Act – DGA)[8] in Kapitel II Regelungen für die Erleichterung der Weiterverwendung von geschützten Daten. Der DGA ergänzt somit die Regelungen der OD-PSI-RL mit Vorkehrungen für den Umgang mit geschützten Daten und zielt darauf ab, die Nutzung dieser Daten in sicheren Verarbeitungsumgebungen verstärkt zu ermöglichen.

Mit der OD-PSI-RL hat der europäische Gesetzgeber 2019 die PSI-RL neugefasst und an den Datennutzungsbedarf durch Schlüsseltechnologien wie Künstlicher Intelligenz angepasst. Die OD-PSI-RL verfolgt seit 2003 das Ziel, datenbasierte Geschäftsmodelle auf der Grundlage öffentlich finanzierter Daten zu befördern. Der Regelungsgehalt lässt sich im Kern in zwei Dimensionen einteilen: Zum einen dient die Richtlinie der Vermeidung von Wettbewerbsverzerrungen im Binnenmarkt durch die öffentliche Hand in Bezug auf Mehrwertdienste, die auf der Grundlage von Daten des öffentlichen Sektors entwickelt und angeboten werden (Nichtdiskriminierung, Verbot von Ausschließlichkeitsvereinbarungen). Zum anderen harmonisiert die Richtlinie Bedingungen der Weiterverwendung von zugänglichen Daten (Formate, Entgelte).

In der Neufassung hat der europäische Gesetzgeber den Anwendungsbereich über öffentliche Stellen hinaus auf öffentliche Unternehmen bestimmter Bereiche der Daseinsvorsorge erstreckt. Des Weiteren werden Forschungsdaten nunmehr erfasst. Die OD-PSI-RL verschärft die Grundsätze zur Entgeltdeckelung und führt besondere Anforderungen für dynamische Daten ein: Daten, die regelmäßig aktualisiert werden wie z.B. Sensordaten, sollen künftig in Echtzeit über Programmierschnittstellen (API) verfügbar sein. Die Pandemie zeigt exemplarisch, welche Auswirkungen die Aktualität einer Datenbasis für Maßnahmen der Politik haben kann, die wesentlich das gesellschaftliche und wirtschaftliche Zusammenleben bestimmen. Darüber hinaus werden sog. Hochwertige Datensätze eingeführt, die in bestimmten thematischen Kategorien (Anhang I der OD-PSI-RL) mit Durchführungsrechtsakten konkretisiert werden sollen (s. unter 4.). Die thematischen Kategorien können durch delegierte Rechtsakte geändert bzw. erweitert werden.

Neben der OD-PSI-RL als Rechtsrahmen für uneingeschränkt zugängliche Daten soll Kapitel II des DGA unionsweit Mechanismen unterstützen, unter denen verschlossene und z.T. brachliegende Daten zu eingeschränkt zugänglichen, also geteilten Daten werden können. Ausdrückliches Vorbild für den Vorschlag der *EU-Kommission* ist das in Deutschland bekannte und bewährte Beispiel der Forschungsdatenzentren, in denen Forschenden unter bestimmten Voraussetzungen Zugang zu Daten gewährt wird.[9] Die Schutzwürdigkeit der verschlossenen Daten kann folgen aus der geschäftlichen oder statistischen Geheimhaltungsbedürftigkeit sowie dem Schutz geistigen Eigentums oder personenbezogener Daten (Art. 3 Abs. 1 DGA).

Wie auch die OD-PSI-RL, begründet der DGA keine Bereitstellungspflichten. Wesentlicher Unterschied zur OD-PSI-RL ist, dass der DGA auch keine Verpflichtung für die Mitgliedstaaten auferlegt, die Weiterverwendung zu gestatten.[10] Kapitel II des DGA setzt voraus, dass Zugang und Weiterverwendung erlaubt sind, und harmonisiert den Regelungsrahmen für die bereits erlaubte Weiterverwendung. Hierzu werden wie bereits in der OD-PSI-RL Exklusivvereinbarungen grundsätzlich untersagt (Art. 4), Bedingungen für die Weiterverwendung und Modalitäten des bedingten Zugangs gesetzt (Art. 5) sowie Gebührenregelungen bestimmt (Art. 6).

2. Von der Informationsweiterverwendung zur Datennutzung

Die *Bundesregierung* hat im Februar 2021 einen Gesetzentwurf zur Umsetzung der OD-PSI-RL vorgelegt.[11] Mit dem Entwurf eines Gesetzes über die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz – DNG-E) soll das bisherige Informationsverwendungsgesetz abgelöst und grundlegend modernisiert werden. Im Wesentlichen schlägt die *Bundesregierung* eine 1:1-Umsetzung der OD-PSI-RL vor.

Der Anwendungsbereich des DNG-E ist in § 2 Abs. 1 erstmals positiv geregelt und stellt klar, dass die Anwendung des Gesetzes vom bestehenden Zugang zu Daten abhängt. Wie auch die OD-PSI-RL, schafft das DNG-E weder Erhebungspflichten noch Zugangsrechte oder Bereitstellungpflichten (§ 1 Abs. 2 DNG-E). Es greift erst dann, wenn ein anderes Gesetz einen Zugang (z.B. IFG) oder die Bereitstellung (z.B. Open-Data-Regelungen wie § 12a EGovG für den Bund) normiert oder die Bereitstellung auf sonstige Weise erfolgt.

Mit dem Wechsel der Bezeichnung „Informationsweiterverwendung" zu „Datennutzung" ist keine Änderung der Regelung intendiert.[12] Der Gesetzentwurf schlägt vor, die fragmentierte Sprache der OD-PSI-RL zu vereinheitlichen. Da die neugefasste OD-PSI-RL im Lichte jüngster Strategien zur Förderung neuer digitaler Technologien verabschiedet wurde, rückt der Gesetzentwurf als Grundanwendungsfall die Nutzung digitaler Daten in den Vordergrund, ohne dabei die herkömmlichen Aufzeichnungs- und Speicherungsarten auszuschließen. Ambition des Gesetzentwurfs ist es, die Nutzung maschinenlesbarer Datenformate stärker zu ermöglichen. Eine Umwandlungspflicht ist jedoch bei unverhältnismäßigem Aufwand gem. § 7 Abs. 3 S. 1 DNG-E weiterhin ausgeschlossen. In der Regel ist davon auszugehen, dass Behörden und betroffene Unternehmen heute bereits die meisten Papiervorgänge auch maschinenlesbar führen, sodass die Verpflichtung zur Herausgabe sämtlicher vorhandener Formate ohne zusätzlichen Aufwand möglich sein müsste.

3. „Zweites Open-Data-Gesetz" des Bundes

Mit dem DNG-E schlägt die *Bundesregierung* zugleich eine Änderung der bestehenden Open-Data-Regelung des Bundes vor, indem § 12a EGovG angepasst wird. Damit kommt die *Bundesregierung* nicht nur einer Vereinbarung aus dem Koalitionsvertrag für die 19. Wahlperiode[13] nach. Der verbundene Gesetzentwurf verdeutlicht auch die föderale Herausforderung, eine fragmentierte Datengesetzgebung zu vereinheitlichen, und die Bestrebung, beide Vorhaben (Open-Data-Gesetz und Datennutzungsgesetz) möglichst kohärent und ineinandergreifend zu gestalten.

Mit dem geänderten § 12a Abs. 1 EGovG soll nunmehr die Bundesverwaltung insgesamt verpflichtet sein, unbearbeitete Daten proaktiv bereitzustellen. Dafür wird grundsätzlich die mittelbare Bundesverwaltung, d.h. Körperschaften, Anstalten, Stiftungen des öffentlichen Rechts, erstmals einbezogen.

Darüber hinaus nimmt sich die Gesetzesänderung dem Umsetzungsdefizit[14] an und führt verpflichtende Open-Data-Koordinatorinnen und -Koordinatoren ein. Diese sollen innerhalb der

8 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance, COM(2020) 767 final.
9 Impact Assessment Report, SWD(2020) 295 final, S. 13.
10 Nach Art. 3 Abs. 1 OD-PSI-RL stellen Mitgliedstaaten sicher, dass die Dokumente für kommerzielle und nichtkommerzielle Zwecke weiterverwendet werden können.
11 BT-Drs. 19/27442.
12 BT-Drs. 19/27442, 38.
13 Koalitionsvertrag zwischen CDU, CSU und SPD der 19. Legislaturperiode, Rn. 2068 ff., abrufbar unter: https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1.
14 Vgl. Erster Bericht der Bundesregierung über die Fortschritte bei der Bereitstellung von Daten, BT-Drs. 19/14140, 29 ff.

Behörde Daten identifizieren, die sich für eine Veröffentlichung gem. § 12a EGovG eignen, sowie als Ansprechpartner fungieren und infolge eines Austauschs mit relevanten Stakeholdern die Veröffentlichungspraxis kontinuierlich an Bedarf und Nachfrage anpassen. Die Erfahrungen der Koordinatoren sind damit auch wesentlich für künftige gesetzgeberische Novellierungen im Bereich der Open-Data-Politik.

Weitere Änderungen des § 12a EGovG umfassen die Erstreckung auf Forschungsdaten (Streichung aus § 12a Abs. 2 Nr. 5 EGovG) sowie eine Verordnungsermächtigung in § 12a Abs. 12 EGovG insbesondere zur Konkretisierung des Bereitstellungsprozesses.

Die *Bundesregierung* bereitet als flankierende, nicht-legislative Maßnahme derzeit eine Open-Data-Strategie vor, die die Datenstrategie in Bezug auf den Umgang mit Open Government Data ergänzen und vertiefen wird.

4. Hochwertige Datensätze

Voraussichtlich noch Mitte 2021 wird die *EU-Kommission* mit einem Entwurf eines Durchführungsrechtsakts Regelungen zu Hochwertigen Datensätzen vorschlagen. Dieser Rechtsakt wird ein weiterer Schritt in der europäischen Open-Data-Politik sein, der mit der Europäischen Datenstrategie zunächst für das erste Quartal 2021 angekündigt wurde.

Grundlage für den nachgeordneten Rechtsakt ist die OD-PSI-RL. In Art. 13 ff. sieht die OD-PSI-RL vor, dass in sechs thematischen Kategorien (Georaum, Erdbeobachtung und Umwelt, Meteorologie, Statistik, Mobilität und Eigentümerschaft von Unternehmen) konkrete Datensätze festgelegt werden, die künftig kostenlos, maschinenlesbar und mit API sowie ggfs. mit Massendownload verfügbar sein müssen. Die Auswahl der Datensätze richtet sich nach dem sozio-ökonomischen und ökologischen Potenzial der Weiterverwendung dieser Datensätze. Mit diesem Vorhaben wird die unionsweite Bereitstellung bestimmter offener Datensätze weiter harmonisiert. Die Idee der hochwertigen Datensätze folgt u.a. aus der G8 Open Data Charter[15], in der bereits eine Grundlage geschaffen wurde, welche Datensätze der G8-Länder für ein rechtsstaatliches Mindestmaß an Verwaltungstransparenz nach den Open-Data-Prinzipien zu veröffentlichen sind.

Die unionsweite Bestimmung Hochwertiger Datensätze dient dem Ziel, die grenzüberschreitende Nutzung bestimmter Datensätze zu erleichtern, indem die Harmonisierung durch Standardsetzung erfolgt. Durchführungsrechtsakte sollen die einheitliche Durchführung europäischer Vorgaben verbessern. Deshalb ermöglicht Art. 14 Abs. 1 UAbs. 3 und UAbs. 4 OD-PSI-RL über die Festlegung der Datensätze hinaus auch die Regelung der Modalitäten ihrer Bereitstellung, einschließlich Vorgaben zu Daten- und Metadatenformaten. Von Bedeutung dürfte in diesem Rahmen auch die Standardisierung von APIs sein, um die Interoperabilität zu erleichtern.

Problematisch ist bei der Bestimmung Hochwertiger Datensätze, dass die Bereitstellung von Datensätzen als offene Daten nur für den Fall näher geregelt werden kann, dass die Daten in den Mitgliedstaaten bereits bereitgestellt werden bzw. uneingeschränkt zugänglich sind. Denn der Zugang bleibt i.R.d. OD-PSI-RL und damit auch in den nachgeordneten Rechtsakten den nationalen Gesetzgebern überlassen. Die Standardsetzung für Hochwertige Datensätze bedarf deshalb zunächst der gründlichen Untersuchung, welche Datensätze heute schon zu welchen Bedingungen unionsweit verfügbar sind.[16] Aber auch die Regelung lediglich von Bereitstellungsmodalitäten kann im Einzelfall Anlass zur Debatte geben: Nicht unerheblich können die Kosten von Bereitstellern sein, die die Veröffentlichung bestimmter umfangreichen Datensätze grundlegend umstellen müssten. Politisch brisant sind Datensätze, die teilweise noch mit Gebühren bereitgestellt werden, sodass die Festlegung als kostenfreier Hochwertiger Datensatz zu Einnahmeausfällen führen könnte. Die *EU-Kommission* plant deshalb, Förderprogramme zur Unterstützung des etwaigen Erfüllungsaufwands. Fest steht, dass die Umstellung auch den Bereitstellern selbst zugutekommt. Ein modernes Datenmanagement ermöglicht der jeweiligen Organisation ein besseres Verständnis ihrer eigenen Datenschätze.[17]

Die europäische und nationale Datenpolitik nimmt die Vorteile, die für die Verwaltung selbst durch Datenbereitstellung und -zugang entstehen, zunehmend in den Blick. In diesem Kontext könnte der Vorschlag eines Rechtsakts über Daten (Data Act), ankündigt für die zweite Jahreshälfte 2021, u.a. die Nutzung von Daten Privater für die öffentliche Aufgabenerfüllung in den Blick nehmen (sog. Business-to-Government Data Sharing).[18] Potenzielle Anwendungsfälle sind insbesondere Bereiche wie die Stadtentwicklung sowie die Pandemiebekämpfung.[19] Gestützt wird dieser Ansatz auf Bundesebene mit dem Ausbau von Kompetenzen zur behördlichen Datenanalyse.[20]

II. Der Datenzugang im Kontext Privater (B2B data sharing)

Zugang kann freiwillig eröffnet oder erzwungen werden. Die Motivation zum freiwilligen Datenteilen wird gerade im Business-to-Business-Umfeld auf ökonomischen Anreizen bestehen; es können aber auch altruistische Beweggründe zur „Datenspende" führen. Ökonomisch rational ist, dass Unternehmen zur Ertragssteigerung die Datennutzung anderen Unternehmen gegen Entgelt ermöglichen, sofern keine Geschäftsgeheimnisse oder andere rechtlich geschützten Interessen entgegenstehen. Diese theoretische Annahme wird empirisch selten Realität. Ein maßgeblicher Grund liegt darin, dass die Wert- und damit Preisermittlung mangels Transaktionsvolumen an Grenzen stößt.[21]

Der hoheitlich erzwungene Zugang zu Daten anderer Privater wird durch gesetzliche Zugangsansprüche umgesetzt. Diese Zugangseinräumung ist ein Eingriff in die grundrechtlich bewehrte Privatautonomie. Die Regelung des Zugangs bedarf daher einer angemessenen verfassungsrechtlichen Rechtfertigung, insbesondere eines legitimen Zwecks. Insbesondere bei privatrechtlichen Zugangsansprüchen wird es an der Erfüllung einer öffentlichen Aufgabe als Legitimation für den Zugang fehlen, sodass es a priori als schwierig erscheint, Zugangsansprüche außerhalb des Wettbewerbsrechts legitimieren zu können.

---

15 G8 Open Data Charter and Technical Annex v. 18.6.2013, abrufbar unter: https://www.gov.uk/government/publications/open-data-charter/g8-open-data-charter-and-technical-annex.

16 Zu möglichen Anpassungsbedarfen in Deutschland *Bruns/Demary/Goecke/Rusche/Scheufen/Horn*, Hochwertige Datensätze in Deutschland v. 10.2.2021, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/studie-hochwertige-datensaetze-in-deutschland.html.

17 Vgl. *Seibel*, Open Data in der Berliner Verwaltung, 2018, S. 40 f.; zu den Potenzialen für die Stadtentwicklung S. 21, abrufbar unter: https://www.technologiestiftung-berlin.de/fileadmin/user_upload/Open_Data_in-der-Verwaltung_WEB.pdf.

18 S.o. Fußn. 2, S. 15; *High-Level Expert Group on Business-to-Government Data Sharing*, Towards a European strategy on business-to-government data sharing for the public interest, 2020.

19 Zur Zusammenarbeit des *RKI* mit der *Deutschen Telekom*, FAZ v. 18.3.2020, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/digitec/rki-telekom-zusammenarbeit-handydaten-gegen-das-coronavirus-16685373.html.

20 S.o. Fußn. 1, S. 60.

21 Vgl. dazu das Forschungsprojekt „Future Data Assets – Intelligente Datenbilanzierung zur Ermittlung des unternehmerischen Datenkapitals", abrufbar unter: https://future-data-assets.de/.

Die *Bundesregierung* und die *EU-Kommission* verfolgen den Ansatz, das freiwillige Datenteilen zu stärken. Der Bedarf, den Zugang zu Daten zu regeln, besteht insbesondere bei Marktversagen.[22] Auf europäischer Ebene könnte mit dem bevorstehenden Data Act in bestimmten Bereichen Datenzugang geregelt werden, soweit die *Kommission* feststellt, dass der Wettbewerb auf nachgelagerten Märkten mangels Datenzugang anderweitig nicht gewährleistet werden kann (z.B. Fahrzeugdaten, Reparaturdienstleistungen für smarte Geräte).[23] Im Energiebereich ermöglicht der Rechtsrahmen zu intelligenten Messsystemen die perspektivische Anbindung zahlreicher Geschäftsmodelle der digitalen Energiewende, die auf den sicheren Zugang zu bestimmten Daten aufbauen.[24]

1. Rechtsrahmen für freiwilliges Datenteilen

Der DGA (s. unter I.1.) zielt darauf ab, die Verfügbarkeit von Daten zur Nutzung zu fördern, indem das Vertrauen in Datenmittler erhöht wird und Mechanismen zur gemeinsamen Datennutzung in der EU gestärkt werden. Zudem soll die Datenteilung zwischen Unternehmen verbessert sowie die Nutzung personenbezogener Daten mithilfe eines Datenmittlers ermöglicht und die altruistische Nutzung von Daten („Datenspende") unterstützt werden.[25]

In Kapitel III des DGA schlägt die *EU-Kommission* Anforderungen an Dienste für die gemeinsame Datennutzung vor. Für drei in Art. 9 Abs. 1 DGA abschließend aufgezählte Dienstarten wird ein Anmeldesystem eingeführt. Aus Art. 10 Abs. 4 und Abs. 5 DGA ist zu schließen, dass die *EU-Kommission* für Vermittlungsdienste ein Verbot mit Anmeldevorbehalt und Ex-post-Aufsicht vorschlägt. Nach Art. 10 Abs. 4 DGA kann der Anbieter die Tätigkeit nach der Anmeldung aufnehmen, und (erst) die Anmeldung berechtigt gem. Art. 10 Abs. 4 DGA zur Erbringung der Dienste in allen Mitgliedstaaten.

Weshalb drei Typen des Vermittlungsdienstes unterschieden werden, erschließt sich aus den materiellen Regelungen nicht. Lediglich in Art. 11 Nr. 10 DGA wird offensichtlich auf die Variante in Art. 9 Abs. 1 lit. b DGA (Vermittlungsdienste zwischen betroffenen Personen) abgestellt.

Auffällig ist die Diskrepanz zwischen der Formulierung in Erwägungsgrund 22 und dem Regelungsteil. Nach Erwägungsgrund 22 soll der DGA ausschließlich für Anbieter von Diensten für die gemeinsame Datennutzung gelten, „deren Hauptziel in der Herstellung einer geschäftlichen, rechtlichen und möglicherweise auch technischen Beziehung" zwischen den Dateninhabern einerseits und möglichen Nutzern andererseits besteht. Die Regelungen in Kapitel III DGA erfassen ohne qualitative Unterscheidung alle Anbieter, das Kriterium des „Hauptziels" wird nicht aufgestellt.

Rechtspolitisch im Fokus steht die Regelung in Art. 11 Nr. 1 DGA. Dort wird eine Zweckbegrenzung sowie die strukturelle Separierung des Anbieters als Bedingung für die Erbringung von Datenvermittlungsdiensten vorgeschrieben, um die Neutralität und Unabhängigkeit des Akteurs zu gewährleisten. Die *Bundesregierung* hat in ihrer Stellungnahme zum DGA die Frage aufgeworfen, ob die vorgeschlagenen Regelungen einen hinreichenden Anreiz zum Angebot und zur Inanspruchnahme der Dienste bieten. Ferner hat sie die ausdrücklich um Erläuterung der Rechtfertigung einer strukturellen Separierung sowie der Frage, wie die Vielzahl bestehender europäischer Geschäftsmodelle des Datenaustauschs im Industriebereich angemessen berücksichtigt wurden, gebeten.[26]

Das Zusammenspiel aus Verbot mit Anmeldevorbehalt, der undifferenzierten Erfassung auch von Vermittlungsdiensten als Nebenzweck sowie die Zweckbegrenzung und strukturelle Separierung ist für das Entstehen von neuen Angeboten recht unattraktiv; soweit in bestehende unternehmerische Tätigkeiten eingriffen wird, stellt sich die Frage der Verhältnismäßigkeit.

Die *Bundesregierung* hat in ihrer Datenstrategie sich zum Ziel gesetzt, Datentreuhänder im Datenökosystem zu etablieren, u.a. durch konkrete Anforderungen und Qualitätskriterien im DGA, die insbesondere die Neutralität und wirtschaftliche Unabhängigkeit von Datentreuhändern und deren Eignung gewährleisten.[27] Gleichzeitig hat sie sich für einen unbürokratischen Akkreditierungs- oder Zertifizierungsprozess von Datentreuhändern ausgesprochen.[28] Dieser Ansatz scheint zu Beginn der regulativen Auseinandersetzung mit der Idee von Treuhändern als neutrale Dritte angemessener, um die Auswirkungen auf den Markt zunächst weiter zu beobachten.

In Kapitel IV DGA wird – abweichend zum Verbot mit Anmeldevorbehalt in Kapitel III – ein freiwilliges Labelling-System vorgeschlagen. Bestimmte Organisationen können sich bei der zuständigen Behörde in eine Liste eintragen und dann gem. Art. 15 DGA die Bezeichnung „in der Union anerkannte datenaltruistische Organisation" verwenden. Die Eintragungsanforderungen sind in Art. 16 DGA geregelt, insbesondere muss die Organisation zur Verfolgung von Zielen von allgemeinem Interesse gegründet worden sein (Art. 16 lit. a) und muss ohne Erwerbszweck und unabhängig sein (Art. 16 lit. b). Die Eingrenzung dieses Kapitels auf Non-Profit-Organisationen ist nicht ohne Weiteres ersichtlich. Dem Kriterium liegt die Annahme zu Grunde, dass erwerbswirtschaftliche Akteure in der Verfolgung altruistischer Zwecke weniger vertrauenswürdig wären. Dieses Vertrauen soll jedoch gerade durch das aufzubauende Register und Label gestärkt werden. Um das altruistische Datensammeln zu erleichtern, soll gem. Art. 22 DGA ein Europäisches Einwilligungsformular für Datenaltruismus durch einen Durchführungsrechtsakt der *EU-Kommission* festgelegt werden.

2. Datenbereitstellung in der Daseinsvorsorge

Zur Erbringung von Diensten der Daseinsvorsorge greift der Staat auf privatwirtschaftlich verfasste Unternehmen zurück. Diese können sich anders als Behörden auf die grundrechtlich garantierte Privatautonomie berufen und damit grundsätzlich selbst entscheiden, ob und inwiefern sie Daten bereitstellen. Gleichzeitig kann die Gewährung des Datenzugangs und die Gestattung der Datennutzung durch öffentliche und private Unternehmen im Einklang mit der grundrechtlich geschützten Privatautonomie zulässig und geboten sein, wenn es sich um öffentlich finanzierte Daten in der Daseinsvorsorge handelt.

Mit der Neufassung der PSI-RL im Jahr 2019 wurde der Anwendungsbereich durch Art. 1 Abs. 1 lit. b OD-PSI-RL auf bestimmte öffentliche Unternehmen erstreckt. Insbesondere öffentliche Versorgungsunternehmen sollten in den Anwendungsbereich aufgenommen werden, da der Richtliniengeber feststellte, dass Dokumente, die i.R.d. Erbringung von Dienstleistungen im all-

22 S.o. Fußn. 2, S. 16, dort Fußn. 39.
23 Zu den EU-Vorschriften zur Typgenehmigung s.o. Fußn. 2, S. 32 f.
24 Vgl. o. Fußn. 2, S. 36; in Deutschland im Messstellenbetriebsgesetz geregelt.
25 Neben den im Beitrag dargestellten drei inhaltlichen Bausteinen (Weiterverwendung von geschützten Daten des öffentlichen Sektors, Datenmittler und Datenaltruismus) schlägt die *EU-Kommission* zudem die Einrichtung eines Europäischen Dateninnovationsrates (Kapitel VI) vor.
26 Vorläufige Stellungnahme der Bundesregierung zum DGA, S. 21 f., abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/S-T/stellungnahme-bundesrepublik-deutschland-zu-daten-governance-gesetz.pdf.
27 S.o. Fußn. 1, S. 36.
28 S.o. Fußn. 1, S. 35.

gemeinen Interesse erstellt werden, nur in unzureichendem Maße für die Weiterverwendung zur Verfügung stehen.[29]

Von der ausdrücklich in Erwägungsgrund 19 OD-PSI-RL angesprochenen Ausweitung auch auf private Unternehmen, hat die *Bundesregierung* beim Gesetzentwurf für das Datennutzungsgesetz keinen Gebrauch gemacht.[30]

Ein Beispiel für eine sektorspezifische Pflicht zur Bereitstellung von Daten eines Unternehmens findet sich im neuen Personenbeförderungsgesetz. Die bevorstehende Novelle des PBefG[31] zur Umsetzung der Delegierten Verordnung (EU) 2017/1926 schafft umfangreiche Datenbereitstellungpflichten. Konkret wird eine Pflicht für personenbefördernde und die Beförderungsleistung vermittelnde Unternehmer zur Bereitstellung von statischen und dynamischen Mobilitätsdaten eingeführt. Die in § 3a Abs. 1 PBefG-E aufgezählten Daten sind dem Nationalen Zugangspunkt bereitzustellen. Die Befugnis zur Datenverwendung ist in § 3b PBefG-E geregelt. Positiv hervorzuheben ist an dem Entwurf, dass die unionsrechtliche Möglichkeit ausgeschöpft wird, auch dynamische Daten mit zu erfassen.

3. Datenzugang im Wettbewerbsrecht und bei Torwächtern

Mit dem GWB-Digitalisierungsgesetz hat der Gesetzgeber in § 20 Abs. 1a GWB einen kartellrechtlichen Anspruch auf Datenzugang in bestimmten Konstellationen aufgenommen, in denen dem Zugang zu Daten aus wettbewerblicher Sicht eine besondere Bedeutung zukommt. Der Zugang zu wettbewerbsrelevanten Daten kann in der digitalen Ökonomie für die Wettbewerbschancen eines Unternehmens von entscheidender Bedeutung sein und letztlich wegen der Nutzbarmachung von Daten entlang der gesamten Wertschöpfungskette zu den wesentlichen Treibern der wirtschaftlichen Entwicklung gehören.[32] Nach Ansicht des Gesetzgebers wird der Datenzugang zumindest mitentscheidend für die Wettbewerbsfähigkeit einer Volkswirtschaft sein, weshalb die zuständige Wettbewerbsbehörde im Fall einer relativen Marktmacht den Datenzugang zu wettbewerbsrelevanten Daten anordnen kann.

Auf unionsrechtlicher Ebene wird derzeit der Kommissionsvorschlag für ein Gesetz über digitale Märkte (Digital Markets Act – DMA) beraten.[33] Unternehmen mit „Torwächter"-Stellung, deren Praktiken die Bestreitbarkeit beschränken und unlauter sind, können Datenzugangspflichten unterliegen: Zum einen gem. Art. 6 Abs. 1 lit. i DMA im Fall von Daten, die im Zusammenhang mit der Nutzung der relevanten zentralen Plattformdienste bereitgestellt oder generiert werden, zum anderen gem. Art. 6 Abs. 1 lit. j DMA im Fall von Ranking-, Such-, Klick- und Anzeigedaten in Bezug auf unbezahlte und bezahlte Suchergebnisse, die von Endnutzern in Online-Suchmaschinen des Gatekeepers generiert werden. Ergänzt werden die Zugangsrechte insbesondere mit der Gewährleistung der Portabilität (Art. 6 Abs. 1 lit. h DMA).

III. Fazit und Ausblick

Alle datenpolitischen Initiativen stehen unweigerlich in Beziehung zu der bisher das Datenrecht prägenden Kodifikation: die Datenschutz-Grundverordnung (DS-GVO). Eine strenge Datenschutzpraxis sowie die weiterhin existierende Zurückhaltung von Unternehmen, Daten zu teilen, hindern bislang Innovation und Wachstum. Insofern besteht zwischen DS-GVO und den aktuellen datenpolitischen Gesetzesinitiativen ein Spannungsverhältnis, denn die Bereitstellung von mehr Daten und stärkere Nutzung dieser Daten steht in einem Zielkonflikt mit den Grundsätzen der DS-GVO (insbesondere Datenminimierung). Das europäische Grundbekenntnis zum Schutz der informationellen Selbstbestimmung (Art. 8 GRCh) zwingt die EU zu einem eigenen Ansatz auf dem schmalen Grat zwischen Wahrung europäischer Werte und Aufrechterhaltung der Wettbewerbsfähigkeit.

Auf europäischer Ebene bahnt sich in Umsetzung der Europäischen Datenstrategie ein übergreifender Ansatz zum Umgang mit Daten an, nach dem die Erfahrungswerte aus bestimmten Sektoren auch auf andere Bereiche übertragen werden könnten. Nicht nur bleibt die datenschutzkonforme und sichere Ausgestaltung eine wiederkehrende Herausforderung in der grundrechtskonformen und verhältnismäßigen Regulierung von Datenzugängen; auch die Durchsetzung bestehender bewährter Konzepte der Interoperabilität und Portabilität bedarf künftig flankierender Maßnahmen, um den Datenaustausch in sämtlichen Bereichen zum Leben zu erwecken.

Schnell gelesen ...

- Die politische Relevanz der Datennutzung ist durch technologischen Fortschritt und stärkerem Bewusstsein für das Potenzial von Daten für bessere Entscheidungen gestiegen. Dies schlägt sich nun auch in vielen Gesetzgebungsvorhaben über Datenzugänge nieder.
- Neben der Open-Data-Gesetzgebung des Bundes (Änderung § 12a EGovG und Einführung eines Datennutzungsgesetzes) werden derzeit auf EU-Ebene die Rahmenbedingungen für eine stärkere Nutzung geschützter Daten durch das Daten-Governance-Gesetz (DGA) harmonisiert.
- Der DGA will eine stärkere Datennutzung durch Vertrauensinstrumente (Datenmittler und Datenaltruismus) bewirken. Die horizontale Regelung von Nutzungsrechten bleiben dem angekündigten EU-Rechtsakt über Daten vorbehalten, der ggf. durch sektorspezifische Regelungen zum Datenzugang ergänzt wird.
- Regelungen zum Zugang zu Daten von Torwächtern wird das EU-Gesetz über digitale Märkte enthalten. Bundesrechtlich wurde mit dem durch das GWB-Digitalisierungsgesetz eingeführten § 20 Abs. 1a GWB ein kartellrechtlicher Anspruch auf Datenzugang aufgenommen. Vertikale Bereitstellungspflichten werden derzeit etwa im Personenbeförderungsrecht diskutiert.

Andreas Hartl
ist Leiter des Referats KI1 „Künstliche Intelligenz, Datenökonomie, Blockchain" im Bundesministerium für Wirtschaft und Energie.

Anna Ludin
ist Referentin im Referat KI1 „Künstliche Intelligenz, Datenökonomie, Blockchain" im Bundesministerium für Wirtschaft und Energie.

Der Beitrag gibt ausschließlich die persönliche Meinung der Autoren wieder.

29 Erwägungsgrund 24 OD-PSI-RL
30 S.o. Fußn. 10, S. 3.
31 Entwurf eines Gesetzes zur Modernisierung des Personenbeförderungsrechts, BT-Drs. 19/26175.
32 BT-Drs. 19/23492, 80.
33 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte); COM(2020) 842 final.

CHRISTOF VÖLKLE

Ethereum 2.0

Grundbaustein der weiterentwickelten Digitalisierung des Rechts

Dezentrale Softwareapplikationen

Unsere Rechtswelt wird zunehmend digitaler. Über neue Softwareintegrationen bis hin zur Distributed-Ledger-Technology (DLT), umgangssprachlich auch Blockchain-Technologie genannt, wird sich in den kommenden Jahren vieles im juristischen Arbeitsalltag verändern. In der Welt der „Legal-Tech"-Themen werden sog. Smart Contracts, d.h. bei Eintritt vordefinierter Ereignisse selbstausführende „Verträge", eine wesentliche Rolle spielen. Ein fundiertes Wissen diesbezüglich ist zukunftsweisend und für angehende und bereits praktizierende Jurist*innen unerlässlich. Der folgende Beitrag soll dabei helfen Ethereum, eine elementare Plattform für DLT-basierte Smart Contracts, leicht verständlich zu machen.

Lesedauer: 20 Minuten

I. Kurze Einführung in die Welt der „Kryptowerte"

Dieser Artikel stellt in großen Teilen eine Transferleistung von dem aktuell vorhandenen Verständnis einer neuen Technologie auf deren juristisch relevante Anwendungsgebiete dar. Zuerst ist es sinnvoll einige grundlegende Begrifflichkeiten zu klären. Zur vereinfachten Darstellung werden die Begriffe Blockchain und DLT in diesem Beitrag synonym verwendet.[1]

Eine Blockchain kann als öffentliche Datenbank beschrieben werden, welche dezentral über viele beteiligte Computer in einem globalen Netzwerk ständig aktualisiert wird.[2]

Die in dieser Datenbank gespeicherten Daten werden in Blöcken („Block-") zusammengefasst. Diese Blöcke sind kryptografisch so miteinander verkettet („-chain"), dass jeder neue Block den vorherigen Block eindeutig referenziert. Die Daten in einem Block können somit nicht nachträglich abgeändert werden, ohne alle vorherigen Blöcke ebenfalls abzuändern. Hierfür bräuchte es den Konsens des gesamten Netzwerks (bzw. abhängig vom Konsensmechanismus > 50%), wodurch die gespeicherten Daten eine extrem hohe Validität aufweisen. Durch diesen Sicherheitsmechanismus kann keine einzelne zentrale Stelle Daten abändern, worauf das grundlegende Vertrauen aller beteiligten Akteure in die vorhandenen Daten basiert.

Jeder neue Block in der Kette muss von den Knotenpunkten im Netzwerk bestätigt werden, bevor er der Verkettung hinzugefügt wird. Dadurch hat immer jeder dieselben Daten vorliegen.

Um die Bestätigung eines neuen Blocks zu erreichen, muss sich das Netzwerk auf einen Konsensmechanismus einigen.

Der Bitcoin, wie auch bisher Ethereum, nutzt dafür das sog. „Proof of Work"(PoW)-Konzept. Jeder neue Block muss hierbei durch eine schwer zu lösende mathematische Gleichung validiert werden. Die notwendigen Rechenoperationen übernehmen dabei die sog. „Miner", welche die notwendige Rechenleistung in eigens dafür geschaffenen Rechenzentren bündeln. Dieser „Schürfprozess" (mining) wird wirtschaftlich entlohnt, indem die Rechenzentrumsbetreiber an dem Kryptowert beteiligt werden. Die neuen Blöcke werden anschließend an das Netzwerk kommuniziert, von diesem überprüft, verifiziert und in der aktuellen Version der bestehenden Verkettung hinzugefügt.

Ethereum selbst ist ein Blockchain-System, das seinen eigenen Kryptowert, namens Ether, besitzt. Es funktioniert als Plattform für zahlreiche andere Kryptowerte sowie für die Ausführung von dezentralen Smart Contracts.

Ethereums selbst erklärtes Ziel ist es, eine globale Plattform für dezentrale Anwendungen zu werden, die Benutzern aus aller Welt ermöglicht, Verträge zu schreiben und auszuführen, die gegen Zensur, Ausfallzeiten und Betrug vollumfänglich abgesichert sind.[3]

Was ist der Bitcoin bzw. der Ether, wenn er nicht Teil dieser Datenstruktur ist? Der Zweck des „Coins" ist grundsätzlich der wirtschaftliche Anreiz dem Netzwerk die Rechenleistung bereitzustellen. Der deutsche Gesetzgeber hat auch eine Legaldefinition in § 1 Abs. 11 S. 4 KWG bereitgestellt: „Kryptowerte im Sinne dieses Gesetzes sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann."

Der Coin ist die Währung, welcher an Krypto-Börsen gehandelt werden kann. Die wesentlich wertbestimmenden Faktoren hierbei sind sowohl der Angebot- und Nachfragemechanismus des Markts als auch die künstliche Angebotsverknappung des Coins (beim Bitcoin auf 21.000.000), welche so im Code hinterlegt wurde.

Im Mai 2021 beträgt die Marktkapitalisierung aller „Kryptowerte" beträchtliche 1,9 Bio. Euro.[4] Die summierte Marktkapitalisierung aller 30-DAX-Unternehmen wird hiervon bereits übertroffen. Zum Vergleich dazu ist *SAP* mit der im Jahr 2020 größten Marktkapitalisierung aller deutschen DAX-gelisteten Unternehmen gerade einmal 126 Mrd. Euro wert.[5][6] Durch diese beeindruckende Zahl allein sollte die tragende Rolle von Kryptowerten in der Zukunft deutlich werden. Sei es als reiner institutioneller Fiatgeld-Währungsersatz oder als funktionelle Token.[7]

Die bisher häufigste Nutzung der Ethereum-Plattform ist das „hosten" von anderen Token in Form anderer Kryptowerte, die auf dem Ethereum Kompatibilitätsmodus ERC-20 ausgeführt

1 Auf fundierte technische Ausführungen bzgl. der programmiertechnischen Prozesse wird bewusst zu Gunsten der leichteren Leserzugänglichkeit verzichtet. Interessierten Lesern empfehle ich als Primärquellen das Ethereum Whitepaper zu lesen und aktuelle Entwicklungen im GitHub-Repository zu verfolgen: https://github.com/ethereum

2 Vgl. *Ernst*, in: MüKoBGB, BGB Einleitung (Einl. SchuldR), 8. Aufl. 2019, Rn. 68.

3 https://ethereum.org/en/what-is-ethereum/.

4 https://coin360.com/, Stand: 6.5.2021.

5 https://de.statista.com/statistik/daten/studie/322374/umfrage/die-groessten-deutschen-dax-unternehmen-nach-marktkapitalisierung/, Stand: 22.3.21.

6 https://de.wikipedia.org/wiki/DAX#Kurse_und_Marktkapitalisierungen

7 *Wendehorst*, in MüKoBGB, 8. Aufl. 2021, EGBGB Art. 43 Rn. 309 ff.

werden. Mehrere Hunderttausend solcher ERC-20 basierten Token existieren bereits.

Für alle im Bereich des Kapitalmarkt- sowie Steuerrechts tätigen Jurist*innen ist die Verwendung als Währung und deren Einstufung als Finanzinstrument durch die *BaFin* bereits hochinteressant und praxisrelevant. Eine aktuelle Übersicht zu den gesetzgeberischen Bemühungen hinsichtlich der fünften Geldwäscherichtlinie mit einer genaueren Kategorisierung der Token-Arten findet sich im lesenswerten Aufsatz „Kryptowerte vs. Virtuelle Währungen".[8]

Die Blockchain-Technologie wird richtungsweisende Veränderungen für die (Dezentrale-)Finanzbranche bereitstellen. Diesbezüglich werden hier bereits viele Fragen aufgeworfen, die den Rahmen dieses Beitrags jedoch massiv sprengen würden und auch keinen Schwerpunkt bilden sollen.

II. Ethereum 2.0

Gemessen an der Marktkapitalisierung ist Ethereum der zweitgrößte Kryptowert. Einer der entscheidenden Unterschiede zu dem bekanntesten Kryptowert der Welt, dem Bitcoin, ist der Zweck von Ethereum. Dieser Beitrag fokussiert sich auf die praktischen Anwendungsfelder der Blockchain-Technologie selbst und nicht der Kryptowerte.

Ethereum (ETH) wurde nicht als reiner Währungs- oder Goldersatz geschaffen. Die wichtigste Innovation von Ethereum war die Entwicklung einer Plattform, welche es ermöglicht, Smart Contracts mittels der Blockchain auszuführen. Dies wird nun durch das anstehende Upgrade auf Ethereum 2.0 umso deutlicher, als dass der erklärte Proof-of-Work-Ansatz abgeschafft wird. Anstelle der Rechenaufgaben für die Miner zur Validierung neuer Blöcke tritt nun ein „Proof of Stake" (PoS)-Ansatz.

Hierbei werden neue Blöcke von den größten „Stakeholdern" also Anteilseignern verifiziert.[9] Der funktionelle Gedanke dahinter ist, dass die Parteien mit den größten Ethereum Anteilen, auch das größte Interesse an der Validität der hinzugefügten Informationen und der damit korrelierenden Werthaltigkeit des Ethereum-Netzwerks haben.[10] Ein weiterer Nebeneffekt ist die deutliche Verringerung der „Minerfees" oder „Gasfees". Dies war im bisher bewährten Validierungsansatz die wirtschaftliche Vergütung der Miner für ihre Arbeit. Mit Umstellung von PoW auf PoS fällt auch die Notwendigkeit des traditionell sehr stromintensiven minings weg. Dies wiederum macht den wirtschaftlichen Nutzen von Ethereum für den Rechtsverkehr umso interessanter, da nun bei der Abbildung von Verträgen auf der Blockchain keine horrend hohen und somit unwirtschaftlichen Gebühren mehr anfallen.

Die Miner werden nach wie vor vergütet, jedoch ändert sich das Vergütungssystem auf eine „Basefee" und einen Bonusbetrag, der an die Miner gezahlt wird. Dadurch werden die Transaktionskosten insgesamt gesenkt. Zusätzlich wird die Basefee durch das Netzwerk „verbrannt". Da die verbrannte Basefee die neu geschürften ETH des Bonusbetrags der Miner übersteigen sollte, wird insgesamt ETH mit jeder Transaktion wegfallen und eine deflationäre ETH Tendenz sollte eintreten.[11]

Ethereum 2.0 bringt noch viele weitere Upgrades, die die Skalierbarkeit, Sicherheit und Nachhaltigkeit von Ethereum verbessern werden.[12] Ethereum ist 2020 mit 1,6 Mrd. transferierten USD bereits zur größten werttransferierenden Blockchain aufgestiegen und hat Bitcoin in diesem Aspekt überholt.[13] Auch deshalb ist Ethereum und nicht der Bitcoin der zentrale Gegenstand dieses Aufsatzes. Das Ethereum-2.0-Upgrade ist mehrstufig strukturiert, hat bereits im Dezember 2020 begonnen und sollte 2022 abgeschlossen werden.[14]

III. Juristisch interessante Anwendungsfelder über Kryptowerte hinaus

Bei Legal Tech 2.0 Anwendung werden juristische Arbeitsschritte z.T. schon selbsttätig durch Informationstechnologie abgewickelt. Bei der noch komplexeren Variante Legal Tech 3.0 sollen Prozesse ganz ohne menschliches Zutun abgewickelt werden können. In diesen Bereich fallen auch blockchain-basierte Smart Contracts.[15] Smart Contracts sind Programme, die automatisch Prozesse ausführen, um eine Vereinbarung zwischen mehreren Parteien im Internet abzuschließen. Sie wurden u.a. entwickelt, um den Bedarf an vertrauenswürdigen Drittparteien zwischen Vertragspartnern zu verringern, dadurch Transaktionskosten zu senken und gleichzeitig die Zuverlässigkeit zu erhöhen.[16] Die Nachfrage nach automatisch ausführenden Verträgen ist heute bereits enorm groß.

1. Smart Contracts als Kontrakte

„Ether Smart Contracts" können mit einer eigens dafür entwickelten Programmiersprache, Solidity, geschrieben werden.[17] Ein darin codierter Kontrakt besteht aus einer Funktion und Zieldaten auf der Ethereum-Blockchain. Die Funktion enthält vordefinierte Aktionen, die bei Eintritt eines Ereignisses Daten in der Ethereum-Chain festschreibt.[18] Hierdurch können z.B. automatisch Ether versandt oder empfangen werden, ohne dass es zusätzlicher Buchführungskontrollen bedarf.

Juristisch betrachtet bedarf es zur Begründung eines Kontrakts zweier korrespondierender Willenserklärungen.[19] Die Mindestanforderungen an den kommunizierten Inhalt sind dabei die Funktion, d.h. was passieren soll und die beteiligten Parteien.[20] Der zweite Teil ist im bisherigen Wirtschaftsalltag meist bekannt. Smart Contracts adressieren jedoch nicht unmittelbar natürliche oder juristische Personen. Diese Transaktionen werden an anonymisierte (bzw. zumindest pseudonymisierte) öffentliche Adressen weitergeleitet. Auf die so hinterlegten Werte kann nur mit einem privaten geheimen Schlüssel zugegriffen werden. Dadurch sind auch Verträge zwischen sich komplett unbekannten Parteien denkbar.

Beim Abschluss von herkömmlichen verschriftlichten Verträgen steht die Identität der Vertragspartner hingegen meist bereits vorher fest. Von diesem Grundsatz gibt es zahlreiche Ausnahmen, wenn die Identität des Vertragspartners z.B. noch nicht bekannt ist oder es auf diese gerade nicht ankommt.

Das Konzept von sich im Vorhinein unbekannten Personen, die miteinander Verträge abschließen, ist dem Zivilrecht also nicht fremd und es sollte auch hierfür bereits Lösungen vorgesehen haben.

Darüber hinaus benutzt das Ethereum-Netzwerk einen kryptografischen Zeitstempelmodus. Wenn die öffentlichen Adressen

8 *Zöllner*, in: BKR 2020, 117.
9 https://eth.wiki/concepts/proof-of-stake-faqs.
10 https://vitalik.ca/general/2020/11/06/pos2020.html.
11 https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md.
12 https://vitalik.ca/general/2021/04/07/sharding.html.
13 https://www.statista.com/statistics/730818/average-number-of-ethereum-transactions/.
14 https://ethereum.org/en/eth2/. Auf technische Ausführungen hinsichtlich der ETH-2.0-Upgradereihe wird nachfolgend verzichtet und nur die juristisch relevanten Bereiche näher beleuchtet. Technisch versierten Leser*innen sei der Blog des Ethereum-Begründers *Vitalik Buterin* (vitalik.ca), die Webseite der *Ethereum Foundation* (ethereum.org) oder die jeweils lokale „Legal-Tech-Community" empfohlen.
15 *Gunnar Groh*, in: Creifelds kompakt, Rechtswörterbuch, Legal Tech.
16 https://coinmarketcap.com/de/currencies/ethereum/.
17 https://docs.soliditylang.org/.
18 https://docs.soliditylang.org/en/v0.8.3/introduction-to-smart-contracts.html.
19 *H.-W. Eckert*, in: BeckOK BGB, 57. Ed., Stand: 1.2.2021, § 145 Rn. 2.
20 *Busche*, in: MüKoBGB, 8. Aufl. 2018, BGB § 145 Rn. 6.

also eindeutig einer Person zugeordnet werden können, dann ist die digitale Signatur tatsächlich aussagekräftiger als die manuelle Unterschrift es jemals sein könnte. Eine Abänderung des Datums oder sonstiger Informationen ist im Ethereum-Netzwerk nicht möglich.[21]

Wirklich neu ist hingegen die Eigenschaft, dass ohne weiteres Zutun von Menschen wirksame Verträge begründet werden können. Diese Kontrakte können darüber hinaus bei Eintritt vordefinierter Konditionen selbstständig weitere Kontrakte begründen. Die Eigenschaft bei vordefinierten Ereignissen bestimmte Verträge im Interesse der beteiligten Parteien zu schließen kann vollständig automatisiert werden. Der zu Grunde liegende Kontrakt kann dabei als Rahmenvertrag angesehen werden, welcher die Begründung neuer Kontrakte vorgibt.[22] Dies wirft eine Reihe von komplexen Problemfällen hinsichtlich des Rechtsbindungswillens und der Stellvertretung auf. Solche Vertragsschlüsse durch automatisiert und autonom agierender Systeme, werden bereits seit längerem diskutiert.[23] Lösungsansätze reichen von erweiterten Anwendungsbereichen bestehender Normen bis hin zur Forderung der Anerkennung einer rechtsfähigen „E-Person".[24]

Der Smart Contract selbst kann dabei weiterhin auch als eine Art Anderkonto gesehen werden. Vorherig bestimmte Ether werden beim Ereigniseintritt automatisch transferiert oder im korrespondierenden Gegenbeispiel bei Transfer der Ether die im Vertrag bestimmten Leistungen automatisch vollzogen. Die Kryptowerte werden somit hinterlegt und keine der Parteien muss sich um die Leistung der Gegenseite sorgen oder deren Eingang nachträglich manuell überprüfen. Zahlungsziele oder Aufforderungen werden genau wie diesbezügliche Mahnungen obsolet.[25]

Zusammenfassend ist festzuhalten: Ein Smart Contract ist ein Programmcode, der rechtlich relevante Handlungen steuern und lückenlos dokumentieren kann.[26] Der Code wird dabei dezentral und nicht abänderbar auf der Blockchain gespeichert.

2. Smart Contracts als gesellschaftsrechtliche Organisationseinheit

Auch gesellschaftsrechtlich bieten Smart Contracts weitere interessante Möglichkeiten.

Decentralized Atononomous Organizations (DAO) sind Organisationen, deren Verwaltungsstrukturen durch einen Smart Contract festgelegt werden. Die dezentrale Lagerung macht konventionelle Entscheidungsgremien wie Vorstände oder Geschäftsführer überflüssig.

a) Frühes Fallbeispiel Slock.it

Ein Pilotprojekt bestand bereits überaus prominent mit Slock.it.[27] Dabei handelt es sich um ein automatisiertes Investmentunternehmen, in welches Teilnehmer*innen weltweit Ether einzahlen konnten, um dann später gebündelt per Mausklick entscheiden zu können was mit dem Geld passieren soll. Da das Investment nicht irreversible sein sollte, wurde auch eine Funktion eingebaut, die es erlaubt, das getätigte Investment wieder abzuziehen. Hierbei wurde jedoch eine Kontrollfunktion im Code vergessen, welche die Rückzahlung dokumentiert und mit dem ursprünglich getätigten Investment saldiert. Infolgedessen kam es zu mehrfachen Rückzahlungsaufforderungen, welche auch weit über den ursprünglich eingezahlten Betrag ausgeführt wurden.

Das „Scheitern" eines solches Investmentvehikels zeigt auch die Problemfelder der „Smart" Contracts. Der Vertrag führt nur das aus, was in seinem Code festgehalten wurde. Die Ausnutzung dieser Lücke ist jedoch keine Eigenheit der Smart Contracts und somit auch keine programmiertechnisch spezifische Schwäche. Die mehrfache Rückerstattung ähnelt dabei der Cum-Ex-Strategie, bei der mehrfach gezahlte Kapitalertragssteuern zurückerstattet wurden, ohne dass diese tatsächlich mehrfach bezahlt wurden. Dennoch wurde hierbei die Limitation von Smart Contracts offensichtlich, welche bei der grundlegenden Planung und Konstruktion des Codes vorlag. Der Smart Contract kann nachträglich keine Fehler heilen, die bei der Vertragsgestaltung begangen wurden.

Die gute Nachricht für Jurist*innen ist dabei, dass sie weiterhin einen festen Platz bei der Vertragsgestaltung einnehmen und ihre erworbene Expertise gebraucht wird. Es sollte jedoch jedem bewusst sein, dass sich die grafische Aufbereitung der Verträge verändern und eine Auseinandersetzung mit Programmiersprachen daher zunehmend an Bedeutung gewinnen wird.

Dieses Fallbeispiel soll hier zusätzlich bewusst gewählt sein, da es nach diesem Vorfall zu einer Abstimmung der beteiligten Parteien kam, welche mit einer Mehrheit für eine Abänderung der Blockchain gestimmt hat, um die Fehlbuchungen rückgängig zu machen. Dadurch kam es zu einer sog. „Hardfork" und Ethereum wurde aufgespalten in Ethereum Classic (ETC) und Ethereum (ETH).[28] Nur an Ethereum wird weiterhin von der *Ethereum Foundation* gearbeitet, da diese den ETH-Code unverändert weiterführen wollten, um nicht den Grundsätzen der Blockchain zu widersprechen und das Vertrauen in die Datenintegrität aufrechtzuerhalten. Insofern handelte es sich hierbei um ein historisches Ereignis für die Ethereum Blockchain aus dem vielerlei Lehren gezogen werden müssen.

b) Willensbildung in Gesellschaften

Weitere gesellschaftsrechtliche Anwendungsfälle sind die blockchain-basierten Abstimmungen in Gesellschafter- bzw. Aktionärsversammlungen. Hierzu bedarf es in Zukunft entsprechender Satzungsänderungen und ggf. der Mitwirkung des Gesetzgebers, um diese Möglichkeit zu implementieren. Ein Bedarf nach dezentralen Entscheidungsfindungen innerhalb von Gesellschaften hat sich nicht zuletzt auch durch die Restriktionen der Corona-Pandemie verdeutlicht. Hierbei werden die Stimmberechtigten eindeutig identifiziert und Ihre Stimmabgabe manipulationssicher und in Echtzeit dokumentiert. Erste Pilotprojekte wurden bereits erfolgreich im Ausland durchgeführt.[29] Vergleichbare Vorhaben wurden auch bereits bei politischen Wahlen durchgeführt, was die Skalierbarkeit der Anwendung unter Beweis stellt.[30]

3. Öffentlich einsehbare Register

Weitere Anwendungsfelder sind öffentlich einsehbare Register, die einen Vertrauensanschein begründen, wie das Handelsregister oder das Grundbuch. Auch hierbei spielt die Blockchain ihre Stärken aus, um die beteiligten Parteien eindeutig zu identifizieren und die Validität der Daten zu gewährleisten. Der o.g. Ersatz

21 https://www.btc-echo.de/news/wordproof-mit-ethereum-blockchain-gegen-fake-news-102420/.
22 *Busche* (o. Fußn. 20), vor § 145 Rn. 41.
23 *Paulus*, JuS 2019, 960.
24 *Specht/Herold*, MMR 2018, 40.
25 https://legal-tech-blog.de/smart-contracts-ethereum-future-of-contracting .
26 *Lehmann*, in: MükoBGB, Int. Wirtschaftsrecht, Teil 12. D., 8. Aufl. 2021, Rn. 549.
27 https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5.
28 https://blog.slock.it/options-in-the-hard-fork-90e467483c0#.olasqn6th.
29 https://www.broadridge.com/_assets/pdf/broadridge-next-generation-proxy-voting-strategies.pdf.
30 https://de.cointelegraph.com/news/ruling-russian-political-party-launches-blockchain-based-e-voting.

des Notar-Anderkonto könnte von besonderem Interesse in diesem Bereich sein.

Einige Modellprojekte wurden hier bereits im Ausland umgesetzt. Vielversprechend erscheint dabei z.B. das schwedische Projekt Chromaway, dass es ermöglicht Grundbucheintragungen auf der Blockchain zu vollziehen.[31] Auch Georgien benutzt bereits seit 2017 in der *Nationalen Agentur für das Öffentliche Register* die Blockchain-Technologie für die Registerführung und verzeichnet damit große Erfolge.

Einen Schritt weiter gedacht könnte die Blockchain hierbei die Stellung sämtlicher vertrauenswürdiger Dritter wie Banken und Notare einnehmen. Durch einen Smart Contract könnte somit der gesamte Prozess automatisiert und sowohl Zahlung als auch Eigentumsübergang durch die Grundbucheintragung im selben Moment vorgenommen werden. Sämtliche Ungewissheiten, die u.a. durch den wochenlangen Eintragungsprozess resultieren, würden somit der Vergangenheit angehören. Georgien arbeitet an einem entsprechenden Konzept namens „Trust Contracts".[32]

Weder Notare noch Banken werden dadurch in absehbarer Zeit obsolet werden. Jedoch gilt, wie bei jeder neuen Technologie, dass diejenigen die sich frühzeitig darauf einstellen und sich anpassen, auch früher von den Vorteilen profitieren.

Ein weiterer Vorreiter ist Estland, mit seinem E-Healthcare-Register, das auf der Blockchain-Technologie aufbaut.[33] Es handelt sich um ein gebündeltes, national-dezentral gelagertes Register, das nur für berechtigte Personen zugänglich ist. Auch in anderen Bereichen hat Estland bereits bemerkenswerte Fortschritte in der Digitalisierung der öffentlichen Verwaltung gemacht.

4. Streng vertrauliche Vertragstexte

Grundsätzlich sind die Vertragsinhalte von Smart Contracts öffentlich einsehbar und werden nicht bei den Vertragspartnern, sondern auf einem dezentralen globalen Computernetzwerk verwahrt. Was ist aber mit Vertragstexten, die gerade nicht öffentlich einsehbar sein sollen? Es gibt Verträge, wie z.B. die Absichtserklärung Vertragsbeziehungen einzugehen (Letter of Intent) oder auch Vertraulichkeitsvereinbarungen[34], deren Vertragsnatur gerade darin besteht, nur den jeweiligen Parteien zugänglich zu sein, und keiner Dritten unbeteiligten Partei offengelegt werden zu dürfen. Das Grundkonstrukt der ständigen öffentlichen Einsehbarkeit der Blockchain scheint dem Vertragszweck zuerst einmal zu widersprechen.

Auch hierfür haben sich jedoch inzwischen blockchainbasierte Lösungsansätze herausgebildet. Die öffentlich zugänglichen Informationen bescheinigen demnach nur noch einen pseudonymisierten Vertragsinhalt.[35] Gem. Art. 4 Nr. 5 DS-GVO ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Die auslösenden Ereignisse werden also weiterhin öffentlich dokumentiert, der genaue Inhalt der Aktion ist jedoch nur den beteiligten Parteien bekannt. Auf diese Weise können auch viele datenschutzrechtliche Problemfälle umgangen werden. Was als hinreichend pseudonymisiert gilt, wird die Rechtsprechung im Verlauf der Zeit herausarbeiten müssen.

5. Non-Fungible-Token (NFT)

Ein komplett neuer Markt wurde mit Non-Fungible-Tokens (NFT) erschlossen. Die Medienberichte über Rekordsummen bei Auktionen für digitale Kunstwerke häufen sich. An sich ist ein gezahlter Preis für ein Kunstwerk bei einer Auktion nichts neues, zumindest nicht in der physischen Welt. Ein echtes *Picasso*-Gemälde gibt es nur als Unikat und der Eigentümer kann dies exklusiv für sich nutzen und bewundern. Die hohe Nachfrage trifft hierbei auf das absolut begrenzte Angebot und bildet somit den Preis.

In der digitalen Welt verhält es sich jedoch anders. Eine Kopie einer Datei ist (meist) genau so gut wie das Original und kann unendlich oft repliziert werden. Auch bei einer hohen Nachfrage nach einer digitalen Kopie von einem Bild, kann dies einfach auf einer Kunstmuseums-Website beliebig oft aufgerufen und heruntergeladen werden. Niemand würde also auf die Idee kommen für eine digitale Version eines Picasso-Bildes Geld zu zahlen.

Der Gedanke hinter NFT steckt bereits im Namen. „Fungible" sind Güter, welche nach Maßeinheit, Zahl oder Gewicht bestimmbar und anhand dessen innerhalb derselben Gattung durch andere Stücke gleicher Art, Menge und Güte austauschbar sind.[36]

„Non-Fungible" bedeutet, dass es sich hierbei um nicht gleichwertig eintauschbare kryptografische Token handelt, welche eine eindeutige Identifikation des Kunstwerks als Metadaten enthalten. Zum Vergleich: Ein Bitcoin kann jederzeit gegen einen anderen Bitcoin eingetauscht werden und i.E. erhält man immer noch eine gleichwertige Sache. Bei Bitcoins handelt es sich daher um „fungible Token".[37]

NFT können somit digitale Anlageklassen bilden und Eigentümerschaft eindeutig nachweisen. Der Inhaber des NFT ist gleichsam Eigentümer. Alle anderen digitalen Versionen des Werks sind somit lediglich Kopien, an denen, so die Theorie, auch kein Eigentum entstehen kann.

Gleichsam können Künstler*innen neue Kunstwerke von Anfang an mit einer eindeutigen Blockchain-Signatur versehen, welche die Urheberschaft nachweist.

Die Verknüpfung der Eigentümerstellung samt Übertragungshistorie mit einem einzigartigen und eindeutig zu identifizierenden Token hält vielerlei Anwendungsbereiche, weit über den Kunstsammlermarkt hinaus, bereit. So wäre es vorstellbar andere Sachwerte gleichsam einer Person zuzuordnen, ohne dabei auf institutionelle dritte Parteien zurückfallen zu müssen. Dies könnte wiederum Nebenerwerbskosten, wie sie z.B. beim Grundstückserwerb anfallen, signifikant senken.

Während es bei Kryptowerten gerade um ihre äquivalente Austauschbarkeit und Akzeptanz als wertbildende Faktoren geht, spielen NFT ihre Stärken in ihrer Einzigartigkeit aus. Dies ist eine Eigenschaft, die im digitalen Bereich sehr selten ist, da Daten beliebig oft replizierbar sind. Ein weiterer Anwendungsfall wurde von *EY* bereits 2019 eingeführt. Hierbei wurde Wein mit Non-Fungible-Tokens gehandelt und somit ein einfaches Investmentvehikel begründet. Die sog. „Wine Asset Tokens" wurden auf die Ethereum Blockchain geschrieben, wo die Transaktionshistorie nachvollzogen werden kann.[38] Beim Handel des fertigen Weins kam es zu einer erheblichen Kosten- und Zeitersparnis. Dies ist wiederum auf die lückenlose Erzeugungs- und Transaktionshistorie zurückzuführen und den Fakt, dass zur Übertra-

31 https://govchain.world/sweden/.
32 https://legal-tech-verzeichnis.de/fachartikel/georgiens-grundbuch-auf-der-blockchain-funktionsweise-und-erste-erfahrungen/.
33 https://e-estonia.com/solutions/healthcare/e-health-record/.
34 S.a. *Hoeren/Münker*, MMR 2021, 523 – in diesem Heft.
35 https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf, S. 30 ff.
36 https://wirtschaftslexikon.gabler.de/definition/fungibilitaet-34994.
37 https://www.investopedia.com/non-fungible-tokens-nft-5115211.
38 https://www.ey.com/en_gl/news/2019/08/ey-helps-wiv-technology-accelerate-fine-wine-investing-with-blockchain.

gung lediglich der Token übertragen werden musste. Dies wiederum ermöglicht die einfache Implementierung eines breiten Spektrums an strukturierten Finanzprodukten. Die eindeutige Identifizierung von Gütern in der physischen, aber auch digitalen Welt wird erhebliche Auswirkungen auf den globalen Handel haben, und die Grundsteine dafür können wir jetzt gerade miterleben.

6. Aktueller Stand

Viele der angesprochenen Ideen wären bereits umsetzbar gewesen, wenn auch immer mit der Gefahr der nachträglichen Regulierung oder des Totalverbots. Praktikabel und wirtschaftlich sinnvoll werden die Umsetzungen jedoch erst jetzt. Die Technologie erreicht in den nächsten zwei Jahren das Stadium der Marktreife und viele regulatorische Rahmenbedingungen werden gerade festgelegt. Daher ist nun auch mit einem rapiden Aufschwung der Adaptierung der Blockchain und speziell der ethereum-basierten dezentralen Applikationen (dApps) zu rechnen. In den Jahren 2021 und 2022 sollte die Entwicklung dann zusätzlich an Schwung gewinnen, wenn die Upgrade-Phasen auf Ethereum 2.0 abgeschlossen werden. Am 15.4.2021 kam es mit dem Block 12.244.000 zu dem Berlin Upgrade in Form einer „Hardfork" und im Juli 2021 wird dann das London („Ethereum Improvement Proposals" – EIP 1559) Upgrade durchgeführt werden.[39] Eine Hardfork ist eine irreversible Änderung des Protokolls einer Blockchain. Diese wird jedoch nicht zur Bildung eines neuen Coins führen, wie es bei Ether und Ethereum Classic (ETC) im Jahr 2016 der Fall war.[40] Mit diesen Upgrade-Phasen werden auch die Grundsteine für verringerte Transaktionskosten eingeführt, was wiederum die Skalierbarkeit der Ethereum-Smart-Contracts erheblich verbessert.[41] Diese neue Architektur bietet eine verlässliche, globale Opensource-Blockchain, die speziell auf die Bedürfnisse von Smart Contracts ausgerichtet sein wird.

IV. Kurzer Ausblick

Mit der Vielzahl an Möglichkeiten kommen natürlich auch unzählige regulatorische Fragen auf. Der deutsche und auch der europäische Gesetzgeber wurde im Bereich der Finanzmärkte bereits tätig und hat mit der neuen Geldwäscherichtlinie und der „Markets in Crypto-Assets Regulation" (MiCA) u.a. versucht Auflagen an die Krypotverwahrungsstellen innerhalb der EU zu knüpfen.[42]

Im Bereich der Smart Contracts sind noch viele juristische Themenfelder unberührtes Neuland. So stellen sich vielfältige datenschutzrechtliche Fragen an die Publizität der Blockchain. Auch die Unveränderlichkeit und Unmöglichkeit der Löschung alter Blöcke stellen die Juristen und Programmierer in Zukunft vor schwere, aber lösbare Herausforderungen.

Die *Deutsche Börse*, die *Bundesbank* und die *Finanzagentur des Bundes* haben gemeinsam mit weiteren Marktteilnehmern eine Abwicklungsschnittstelle für elektronische Wertpapiere entwickelt und erfolgreich getestet. Die auf der Distributed-Ledger-Technologie basierenden Wertpapiere können mit Hilfe einer sog. Trigger-Lösung und eines Transaktionskoordinators in TARGET2, dem Zahlungsverkehrssystem des Eurosystems für Großbeträge, abgewickelt werden.[43] Hierbei ist vor allem anzumerken, dass dieses Projekt eine funktionsfähige Schnittstelle zwischen der DLT und einer bereits bestehenden Infrastruktur darstellt. In naher Zukunft werden sicherlich noch mehr solcher Synergieprojekte auf den Weg gebracht werden.

Die EU hat im Januar 2021 Ambitionen hinsichtlich eines „digitalen Euros", parallel zur bestehenden analogen Währung, geäußert, dessen Entwicklung sich jedoch noch auf nicht absehbare Zeit hinauszögern wird.[44]

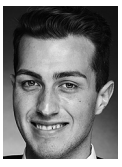
Ein interessantes Projekt ist die „Pan-European blockchain regulatory sandbox". Eine Art Testumgebung, die es ermöglichen soll, neue Technologien in gelockerten regulatorischen Umgebungsfeldern auszuprobieren, damit die beteiligten Parteien gemeinsam Erfahrungen sammeln können, anstatt Projekte wie bisher schlicht an den Regulatorien in ihrer Entstehung zu hindern.[45]

Die einzelnen Staaten werden daran interessiert sein, eigene Blockchains zu entwickeln, um ihre zentrale nationale Einflussnahmemöglichkeit nicht aufgeben zu müssen. Dennoch empfiehlt es sich Ethereum genauer zu studieren, da die große und überaus aktive Entwickler-Community sämtlichen staatlichen Projekten um viele Jahre voraus ist. Die zukunftsweisenden Erfahrungen werden heute bereits auf dieser Blockchain gesammelt und maßgeblich den Kurs zukünftiger Unternehmungen im Bereich dezentralisierter kryptografischer Verkettung bestimmen.

Technisch fundierten Interessenten rate ich, sich die überaus aktive Ethereum-Community einmal näher anzusehen. Die „Lernen Sektion" auf der Ethereum.org-Homepage bietet übersichtlich aufbereitetes Grundwissen zur Materie an. Ihre lokale Legal-Tech-Community ist ebenfalls eine gute Anlaufstelle zum Ausbau Ihres erworbenen Wissens und zur Vernetzung mit anderen technikaffinen Jurist*innen.

Schnell gelesen ...

- Die Ethereum-Blockchain-Entwickler arbeiten 2021 mit Hochdruck an der Verbesserung der Skalierbarkeit des Netzwerks.
- Nach der erfolgreichen Implementierung des ETH-2.0-Upgrades werden Smart Contracts dank sinkender Transaktionskosten endlich wirtschaftlich.
- Die Bemühungen um einen sicheren regulatorischen Rechtsrahmen in der EU befinden sich teilweise bereits in der Umsetzungsphase.
- Das Potenzial der dezentralen Applikationen geht weit über den bereits sehr aktiven dezentralen Finanzmarkt hinaus und wird in Zukunft eine Schlüsselrolle für viele juristische Arbeitsbereiche darstellen.



Christof Völkle, LL.B.,
ist Unternehmensjurist an der Universität Mannheim und Gründungsmitglied der legal tech community Mannheim e.V.

39 https://www.coindesk.com/ethereum-improvement-proposal-1559-london-hard-fork.
40 https://de.cointelegraph.com/news/ether-price-flirts-with-2-400-ath-as-irreversible-hard-fork-looms.
41 https://blog.ethereum.org/2021/01/20/the-state-of-eth2-january-2021/.
42 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.
43 https://www.bundesbank.de/de/presse/pressenotizen/abwicklung-von-dlt-basierten-wertpapieren-in-zentralbankgeld-erfolgreich-getestet-861438.
44 https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/210119-ec-ecb-joint-statement-digital-euro_en.pdf.
45 https://ec.europa.eu/digital-single-market/en/european-blockchain-partnership-0.

ANDREAS SESING

Cookie-Banner – Hilfe, das Internet ist kaputt!

Ansätze zur Verbesserung der Nutzererfahrung

Softwarebasierte Einwilligung

Internetnutzer*innen, die dieser Tage unbeschwert „surfen" möchten, haben es nicht leicht: Bei nahezu jedem Aufruf einer Internetseite erscheint ein Banner, mit dem Anbieter über die beabsichtigte Verwendung von Cookies (und anderen Tracking-Mechanismen) informieren und Nutzer*innen um die erforderliche Zustimmung ersuchen. Diese stehen dabei regelmäßig vor der Wahl, entweder durch einen einzigen Klick auf die zumeist auffälligste Schaltfläche ihre Zustimmung zu erteilen oder den oftmals deutlich müßigeren Weg zur Verweigerung der Einwilligung ausfindig zu machen. Insbesondere eilige Nutzer*innen dürften sich daher das Internet der Prä-Cookie-Banner-Ära zurückwünschen. Der Beitrag diskutiert, wie dieser Tendenz entgegengewirkt werden könnte.

Lesedauer: 22 Minuten

I. Einführung

„Cookie-Banner spalten Internet-Nutzer" – unter dieser Überschrift stellte der *Bitkom e.V.* im November 2020 eine von *Bitkom-Research* durchgeführte Befragung von knapp über 1.000 Internetnutzer*innen zu Cookies bzw. Cookie-Bannern vor.[1] Die Umfrageergebnisse zeichnen in der Tat ein gespaltenes Bild: Während Cookie-Banner für 46% der Befragten nach eigenem Empfinden nützliche Informationen bereitstellen, gaben 43% der Befragten zu Protokoll, dass sie von Cookie-Hinweisen „genervt" seien, ebenfalls 43% der Befragten bekannten sich dazu, Cookie-Banner nicht zu beachten. Das zweitgenannte Lager ist zwar gegenüber einer vergleichbaren Befragung von 2018 etwas geschrumpft;[2] es ist jedoch noch immer so groß, dass bei einem erheblichen Teil der Internetnutzer*innen eine gewisse Cookie-Einwilligungsmüdigkeit diagnostiziert werden kann, für die sich zwischenzeitlich das Bonmot der „Cookie-Fatigue"[3] etabliert hat. Die derzeitige Situation kann daher mit Fug und Recht als unbefriedigend bezeichnet werden.[4]

Abhilfe schaffen soll in diesem Zusammenhang das am 20.5.2021 verabschiedete Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG),[5] das jedoch nur punktuelle Neuerungen enthält und im Hinblick auf die Nutzerfreundlichkeit von Banner-Lösungen hinter den Anregungen und Vorschlägen aus der Stellungnahme des *Bundesrates* zurückbleibt.[6] Eine weitere Hoffnungsträgerin könnte daher die geplante ePrivacy-VO sein: Der jüngste Entwurf[7] adressiert – worauf zurückzukommen sein wird[8] – die Problematik der Einwilligungsmüdigkeit in Erwägungsgrund 20a ganz ausdrücklich und setzt insbesondere auf die Förderung softwarebasierter Lösungen.

Freilich ist nicht zu übersehen, dass die alleinige Fokussierung auf „Cookie-Banner" der Wirklichkeit nicht (mehr) vollumfänglich gerecht wird,[9] da die Aktivitätenverfolgung von Internetnutzer*innen – etwa mittels „device fingerprinting" – auch ohne Cookies möglich ist.[10] So hat etwa *Google*[11] angekündigt, die Nutzung von Cookies künftig einschränken zu wollen, auch *Apple* hat jüngst einen entsprechenden Vorstoß verkündet.[12] Dementsprechend sind die hiesigen Ausführungen – wenngleich sie terminologisch an den noch vorherrschenden Einsatz von Cookies angelehnt sind – auch auf Consent-Banner allgemein übertragbar, soweit diese der Einholung einer Einwilligung des Nutzers in die Verwendung von Tracking-Mechanismen dienen.[13]

Der Beitrag stellt zunächst Arten und Nutzen von Cookies (II.) sowie die rechtlichen Grundlagen von Cookie-Bannern (III.) dar. Sodann werden Regelungsoptionen diskutiert, die – alternativ oder kumulativ – dem Internet ein Stück seiner abhanden gekommenen Nutzerfreundlichkeit zurückgeben könnten (IV.).

II. Arten und Nutzen von Cookies

In technischer Hinsicht handelt es sich bei Cookies um Textdateien, die beim Aufruf einer Internetseite auf dem Computer eines Benutzers gespeichert und zu einem späteren Zeitpunkt – insbesondere beim erneuten Aufrufen der Seite – wieder abgerufen werden.[14]

Die Hinterlegung von Cookies auf dem Endgerät des Nutzers kann dabei unterschiedliche Zwecke verfolgen: Der *BGH* geht in seinem Planet49-Urteil etwa davon aus, dass Cookies dazu dienen können, „die Navigation im Internet oder Transaktionen zu erleichtern oder Informationen über das Nutzerverhalten zu sammeln".[15] In der Literatur wird zwischen bis zu vier unter-

1 Die Meldung des *Bitkom e.V.* ist abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Cookie-Banner-spalten-Internetnutzer.

2 Vgl. die Zusammenfassung des *Bitkom e.V.* zur Befragung v. 25.7.2018, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Cookie-Banner-stoeren-Internetnutzer.html.

3 Ursprünglich wohl *Engeler/Marosi*, CR 2019, 707 (712); übernommen von *Ettig/Herbrich*, K&R 2020, 719; *Hansen/Brechtel*, GRUR-Prax 2020, 385; *Rauer/Bibi*, 887 (890); *Rauer/Ettig*, ZD 2021, 18 (19).

4 So etwa *Haberer*, MMR 2020, 810 (814); vgl. auch *Baumann/Sesing*, jM 2020, 455 (458); *Heidrich/Koch*, MMR 2020, 581 (584).

5 Initial BT-Drs. 19/27441, die verabschiedete Fassung ist enthalten in Beschlussempfehlung und Bericht des *Ausschusses für Wirtschaft und Energie* (9. Ausschuss), BT-Drs. 19/29839; s. dazu *Hanloser*, ZD 2021, 121 ff.; *Jandt*, DSB 2021, 66 ff.; *Schwartmann/Benedikt/Reif*, MMR 2021, 99 ff.; speziell zum Tracking nach TTDSG-E *Benedikt*, DSB 2021, 76 ff.

6 S. die Stellungnahme des *Bundesrates* v. 26.3.2021, BR-Drs. 163/21 (Beschluss).

7 Der Entwurf datiert v. 10.2.2021 und ist abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

8 S. unter IV.4.

9 Krit. daher zum Begriff des „Cookie Consent Banner" im Hinblick auf die Ausblendung anderer Tracking-Technologien *Becker*, CR 2021, 87 (88).

10 Hierzu etwa *Dieterich*, ZD 2015, 199 ff.; *Funke*, DSRITB 2020, 179 ff.; *Karg/Kühn*, ZD 2014, 285 ff.

11 S. die Ankündigung „Charting a course towards a more privacy-first web" im Google-Blog v. 3.3.2021, abrufbar unter: https://www.blog.google/products/ads-commerce/a-more-privacy-first-web.

12 Vgl. die Berichterstattung mit weiterführenden Hinweisen auf heise.de v. 29.4.2021, abrufbar unter: https://heise.de/-6031264.

13 Zu den gesetzlichen Grundlagen entsprechender Banner s. unter III.1.

14 *Ernst*, WRP 2020, 962; *Hanloser*, ZD 2018, 213 f.; *Munz*, in: v. Westphalen/Thüsing, Vertragsrecht und AGB-Klauselwerke, 46. EL Oktober 2020, Teil „Klauselwerke", Datenschutzklauseln, Rn. 107; *Schwartmann/Benedikt/Reif*, MMR 2021, 99.

15 *BGH* MMR 2020, 609, Rn. 49 m. Anm. *Gierschmann* = ZD 2020, 467 m. Anm. *Eckhardt* – Cookie-Einwilligung II.

schiedlichen Arten von Cookies differenziert, namentlich zwischen technisch notwendigen Cookies, funktionalen Cookies, Performance-Cookies und Tracking- bzw. Marketing-Cookies,[16] wobei die Terminologie nicht einheitlich[17] und mitunter auch missverständlich[18] ist.

Von zentraler Bedeutung für die nachfolgend untersuchten Anforderungen an die Gestaltung von Cookie-Bannern ist zunächst die Unterscheidung zwischen technisch notwendigen Cookies einerseits und allen übrigen Cookies andererseits. Technisch notwendige (auch: „funktionale" oder „essential")[19] Cookies sind – in Anlehnung an die Vorschrift des Art. 5 Abs. 3 S. 2 ePrivacy-RL[20] i.d.F. der RL 2009/136/EG[21] – solche, deren Setzung unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Beispiele hierfür sind – unter anderem[22] – Cookies zur vorübergehenden Beibehaltung eines Logins auf einer passwortgeschützten Internetseite oder zur Ermöglichung einer Warenkorb-Funktion in einem Online-Shop.[23]

Von Relevanz ist – jedenfalls im Ausgangspunkt[24] – überdies, ob durch die Speicherung eines Cookies personenbezogene Daten verarbeitet werden. Insbesondere Cookies, die mit eindeutig identifizierbaren Gerätekennungen (sog. „unique identifier") operieren, können daher personenbezogene Daten enthalten[25] und werfen unklare Folgefragen hinsichtlich der maßgeblichen Rechtsgrundlagen auf.[26]

III. Die Gestaltung von Cookie-Bannern de lege lata

Wenngleich der geltende Rechtsrahmen für den Einsatz von Cookie-Bannern für die Praxis weitgehend klar abgesteckt ist (1.), zeigen sich jedoch spezifische Unklarheiten insbesondere mit Blick auf die Gestaltung von Cookie-Bannern (2.).

1. Gesetzliche Grundlagen

Der Einsatz von Cookie-Bannern geht maßgeblich auf die gesetzliche Anforderung zurück, dass Nutzer*innen grundsätzlich in die Speicherung von Cookies auf ihren Endgeräten einwilligen müssen.[27] Dieses Erfordernis folgt im Unionsrecht aus Art. 5 Abs. 3 S. 1 ePrivacy-RL, im deutschen Recht derzeit aus einer unionsrechtskonformen Auslegung des § 15 Abs. 3 S. 1 TMG[28] und künftig aus § 25 Abs. 1 S. 1 TTDSG.[29]

Eine Ausnahme vom Einwilligungserfordernis besteht gem. Art. 5 Abs. 3 S. 2 ePrivacy-RL einzig für technisch notwendige Cookies:[30] Für diese ist eine Einwilligung nach den Vorgaben der ePrivacy-RL nicht erforderlich,[31] § 25 Abs. 2 Nr. 2 TTDSG enthält eine entsprechende Ausnahme. Ob in diesem Fall gleichwohl ein Erlaubnistatbestand des Datenschutzrechts erfüllt sein muss, soweit durch das Speichern von Cookies personenbezogene Daten verarbeitet werden, ist unklar und hängt maßgeblich von der Interpretation des Art. 95 DS-GVO ab.[32] Soweit in Art. 5 Abs. 3 ePrivacy-RL eine gegenüber der DS-GVO speziellere Vorschrift erblickt wird,[33] dürfte eine gesonderte Rechtfertigung nicht erforderlich sein.[34] Wird hingegen der Schutzzweck des Art. 5 Abs. 3 ePrivacy-RL nicht im Schutz personenbezogener Daten erblickt, ist auch eine gesonderte datenschutzrechtliche Erlaubnis – die nicht zwingend aus einer Einwilligung folgen muss – erforderlich.[35]

Soweit technisch nicht notwendige Cookies genutzt werden, ist die Einholung einer Einwilligung durch den Nutzer unumgänglich. Wird hierzu ein Cookie-Banner verwendet, muss dieses so gestaltet sein, dass es die Anforderungen an eine wirksame Einwilligung nach Maßgabe der DS-GVO erfüllt, da diese insbesondere auch im Anwendungsbereich der ePrivacy-RL maßgeblich sind.[36] Dies wird auch in § 25 Abs. 1 S. 2 TTDSG klargestellt, der für die Information des Nutzers sowie für die Einwilligung insgesamt auf die Anforderungen der DS-GVO verweist. Die bei technisch nicht notwendigen Cookies ebenfalls diskutierte Frage des Verhältnisses von Art. 5 Abs. 3 ePrivacy-RL zu Art. 6 DS-GVO[37] ist von praktisch geringer Bedeutung, da eine wirksame Einwilligung nach den Grundsätzen der ePrivacy-RL zugleich auch die Anforderungen an eine wirksame Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO erfüllt.[38]

Beim Einsatz von anderen Tracking-Mechanismen als Cookies ist danach zu differenzieren, ob diese Verfahren auf Endgeräteinformationen zugreifen.[39] Dies kann etwa im Fall des „device fingerprinting" je nach konkreter Funktionsweise jedenfalls nicht stets ausgeschlossen werden,[40] sodass in diesen Fällen eine Ein-

---

16 Für diese Unterteilung etwa *Ernst*, WRP 2020, 962 (963).
17 *Steinrötter*, GPR 2020, 106 (107) setzt etwa „unbedingt erforderliche" und „funktionale" Cookies jedenfalls aus rechtlicher Sicht gleich.
18 Missverständlich ist insb. die Einordnung von Cookies zum Zweck der Bereitstellung virtueller Warenkörbe und zum Login-Management auf passwortgeschützten Internetseiten als Cookies zur Bereitstellung von „Komfortfunktionen" (*Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 36 Rn. 131), da beide Anwendungsfälle einen unstreitigen Fall „technisch notwendiger" Cookies darstellen (vgl. sogleich die Nachweise Fußn. 23).
19 Vgl. die Terminologie bei *Steinrötter*, GPR 2020, 106 (107).
20 RL 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG L 201, 37.
21 ABl. EG L 337, 11.
22 Ausf. zu weiteren Beispielen *Piltz/Kühner*, ZD 2021, 123 (127 f.); *Rauer/Ettig*, ZD 2021, 18 (21).
23 *Böhm/Halim*, MMR 2020, 651 (652); *Ernst*, WRP 2020, 962 (963); Anm. von *Moos/Rothkegel* zu *EuGH* MMR 2019, 732 (736) (737) – Planet49 = ZD 2019, 556 m. Anm. *Hanloser*; *Piltz/Kühner*, ZD 2021, 123 (127); *Rauer/Ettig*, ZD 2021, 18 (21); *Steinrötter*, GPR 2020, 106 (107).
24 I.E. bestimmt jedoch maßgeblich die vorstehende Unterscheidung zwischen „technisch notwendigen" und sonstigen Cookies darüber, ob vom Nutzer eine Einwilligung in das Setzen eines Cookies erforderlich ist.
25 *EuGH* MMR 2019, 732 m. Anm. *Moos/Rothkegel* = ZD 2019, 556 (558), dort Rn. 45 m. Anm. *Hanloser* – Planet49; *Haberer*, MMR 2020, 810 (811); *Hanloser*, ZD 2018, 213 (214); *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 66; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 4 Nr. 1 Rn. 36.
26 Dazu sogleich unter III.1.
27 Aus diesem Grund ist gelegentlich auch der Begriff der Consent-Banner anzutreffen, vgl. *Heidrich/Koch*, MMR 2020, 581 (584).
28 S. hierzu nur *BGH* MMR 2020, 609, Rn. 47 ff. m. Anm. *Gierschmann* = ZD 2020, 467 m. Anm. *Eckhardt* – Cookie-Einwilligung II.
29 § 25 Abs. 1 S. 1 TTDSG lautet: „Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat."
30 Zum Begriff s. unter II.
31 *Böhm/Halim*, MMR 2020, 651 (652); *Steinrötter*, GPR 2020, 106 (107).
32 S. dazu *BGH* MMR 2020, 609, Rn. 57 ff. m. Anm. *Gierschmann* = ZD 2020, 467 m. Anm. *Eckhardt* – Cookie-Einwilligung II.
33 Hierfür speziell im Hinblick auf Art. 5 Abs. 3 ePrivacy-RL *Golland*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 95 Rn. 11; wohl auch *Pauly*, in: Paal/Pauly, DS-GVO, 3. Aufl. 2021, Art. 95 Rn. 2 f.
34 *Golland* (o. Fußn. 33); wohl auch *Rauer/Ettig*, ZD 2021, 18 (20 f.); *Steinrötter*, GPR 2020, 106 (107); implizit auch *Böhm/Halim*, MMR 2020, 651 (652).
35 *Benedikt*, DSB 2021, 76 (79); *Haberer*, MMR 2020, 810 (812); *Rauer/Ettig*, ZD 2021, 18 (20); wohl auch *Baumgartner/Hansch*, ZD 2020, 435 (437); *Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 95 Rn. 6.
36 Vgl. Art. 2 lit. f ePrivacy-RL i.V.m. Art. 94 Abs. 2 DS-GVO; *EuGH* MMR 2019, 732 m. Anm. *Moos/Rothkegel* = ZD 2019, 556 (559), dort Rn. 50 m. Anm. *Hanloser* – Planet49; *BGH* MMR 2020, 609, Rn. 63 f. m. Anm. *Gierschmann* = ZD 2020, 467 m. Anm. *Eckhardt* – Cookie-Einwilligung II; a.A. offenbar *Haberer*, MMR 2020, 810 (814): Cookie-Einwilligung folge nicht dem Regime der DS-GVO.
37 Hierzu *Haberer*, MMR 2020, 810 (812); zum Verhältnis des geplanten TTDSG und DS-GVO auch *Benedikt*, DSB 2021, 76 (78 f.).
38 *Ettig/Herbrich*, K&R 2020, 719 (720); *Rauer/Ettig*, ZD 2021, 18 (20); für die Zulässigkeit der Verbindung beider Einwilligungen *Haberer*, MMR 2020, 810 (812 f.).
39 *Rauer/Ettig*, ZD 2021, 18 (21).
40 Mit überzeugender Differenzierung *Funke*, DSRITB 2020, 179 (186 f.); vgl. ferner *Conrad/Hausen* (o. Fußn. 18), Rn. 163; *Dieterich*, ZD 2015, 199 (201).

willigung bereits nach Art. 5 Abs. 3 ePrivacy-RL erforderlich sein wird;[41] i.Ü. kann auch bei der Verarbeitung personenbezogener Daten eine Einwilligung den maßgeblichen Erlaubnistatbestand darstellen.

2. Unklarheiten bei der Gestaltung von Cookie-Bannern

Durch die Maßgeblichkeit der Einwilligungsvoraussetzungen der DS-GVO bestehen prima facie klare Anforderungen an die Einholung einer Einwilligung in die Speicherung von Cookies auf dem Endgerät eines Nutzers. So besteht heute etwa Klarheit hinsichtlich der Frage, ob eine Einwilligung wirksam per voreingestelltem Ankreuzkästchen eingeholt werden kann: Der *EuGH* hat hierzu bekanntermaßen entschieden, dass entsprechende Opt-out-Gestaltungen nicht zu einer wirksamen Einwilligung i.S.v. DS-GVO und ePrivacy-RL führen.[42]

Jenseits dieser klaren Vorgabe ist aber etwa umstritten, ob die Nutzung einer Internetseite initial von einer Einwilligung in das Setzen von Cookies und anderer Trackingmechanismen mittels sog. „Paywalls" oder „Cookie-Walls" abhängig gemacht werden darf. Während dies insbesondere vom *Europäischen Datenschutzausschuss (EDSA)*,[43] von der deutschen *Datenschutzkonferenz (DSK)*[44] sowie von einem Teil der Literatur[45] verneint wird, geht die herrschende Literaturmeinung i.E. von einer grundsätzlichen Zulässigkeit dieser Praxis aus,[46] überwiegend allerdings unter der Bedingung, dass ein gleichwertiger Alternativzugang angeboten wird.[47] Die letztgenannte Ansicht liegt auch dem jüngsten Entwurf der ePrivacy-VO zu Grunde.[48]

Ebenfalls nicht eindeutig geklärt ist die – häufig mit den Schlagworten „dark patterns" oder „nudging" adressierte[49] – Frage, ob und ggf. in welchem Umfang es zulässig ist, den Nutzer bei der von ihm zu treffenden Entscheidung durch die gezielte Gestaltung des Cookie-Banners zu beeinflussen.[50] Im Einzelnen hängt hiervon etwa ab, ob der Weg zur Ablehnung aller Cookies umständlicher sein darf als der Weg zum Akzeptieren aller Cookies; dies wird von der wohl überwiegenden Ansicht in Rechtsprechung und Literatur verneint,[51] von der Gegenansicht hingegen bejaht.[52] Die Zulässigkeit der unterschiedlichen farblichen Gestaltung der Schaltflächen zur Auswahl der Nutzerentscheidung ist ein weiterer Teilaspekt dieser Fragestellung; eine unterschiedliche farbliche Hervorhebung wird dabei von der herrschenden Literaturauffassung grundsätzlich[53] als unschädlich für die Wirksamkeit der Einwilligung angesehen,[54] z.T. eine optisch unausgewogene Gestaltung aber auch für unzulässig erachtet.[55]

Die Analyse von Rechtsprechung, Literatur und Stellungnahmen der Aufsichtsbehörden zeigt, dass zahlreiche Einzelaspekte mit erheblicher Bedeutung für die Gestaltung von Cookie-Bannern unklar sind und nicht einheitlich gehandhabt werden.

IV. Ansätze zur Verbesserung der Nutzererfahrung de lege ferenda

Die vorstehende Darstellung legt – sowohl aus Perspektive der Nutzer als auch aus Perspektive der Betreiber von Internetseiten – nahe, dass im Hinblick auf die Gestaltung von Cookie-Bannern erheblicher Handlungsbedarf besteht. Der folgende Abschnitt beleuchtet einige Ansätze, mit denen die Regulierung von Cookies in nutzerfreundlichere und zugleich für Anbieter rechtssichere Bahnen gelenkt werden könnte.

1. Vereinheitlichung statt Wildwuchs

Ein erster Schritt zu mehr Nutzerfreundlichkeit könnte in der Schaffung vereinheitlichter Vorgaben für die Gestaltung von Cookie-Bannern bestehen. Klare Gestaltungsvorgaben hätten zudem für Anbieter den Vorteil größerer Rechtssicherheit.

Im Verbraucherschutzrecht etwa setzt der europäische Gesetzgeber bereits seit geraumer Zeit auf vereinheitlichte Gestaltung, wenn mit der Verbraucherrechte-RL[56] sowohl für die Erteilung einer Widerrufsbelehrung durch Unternehmer als auch für die Erklärung des Widerrufs durch Verbraucher vom Gesetzgeber verbindliche Muster bereitgestellt werden.[57]

Da die Erscheinungsformen von Tracking-Mechanismen im Allgemeinen und Cookies im Speziellen sehr vielfältig sind, erscheint die Schaffung einheitlicher Vorgaben zur Gestaltung durch den Gesetzgeber in hoher Granularität wenig zielführend. Denkbar wäre aber jedenfalls, zumindest den Schritt der ersten Konfrontation des Nutzers mit einem Cookie-Banner durch eine entsprechende Vorgabe einheitlich zu gestalten. Zugleich könnte – zum Schutz des Nutzers vor einer Überfrachtung mit Informationen[58] – verbindlich vorgegeben werden, welche Informationen in diesem ersten Schritt bereitzustellen sind (und welche nicht).

Eine derartige Vereinheitlichung hätte den unabweisbaren Vorteil, dass Nutzer*innen bei einer manuellen Entscheidung eine

---

41 S. die Analyse unterschiedlicher Anwendungsfälle auch die Stellungnahme der *Art. 29-Datenschutzgruppe*, Opinion 09/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, 9 ff., abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf.

42 *EuGH* MMR 2019, 732 m. Anm. *Moos/Rothkegel* = ZD 2019, 556 (558 f. Rn. 44 ff.) m. Anm. *Hanloser* – Planet49.

43 *EDSA*, Leitlinien 05/2020 zur Einwilligung gem. Verordnung 2016/679, Version 1.1, S. 13 Rn. 39, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

44 *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, März 2019, S. 10, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

45 *Baumgartner/Hansch*, ZD 2020, 435 (438); in diese Richtung auch *Hilgert/Hilgert*, jM 2020, 97 (100).

46 Für eine weitreichende Zulässigkeit *Haberer*, MMR 2020, 810 (813).

47 *Lang*, K&R 2019, 698 (701); *Rauer/Ettig*, ZD 2021, 18 (22); näher hierzu auch *Golland*, MMR 2018, 130 (134).

48 Vgl. Erwägungsgrund (20aaaa) ePrivacy-VO-E (o. Fußn. 7).

49 Mit „nudging" wird dabei z.T. eine vermeintlich schwächere Form der Suggestion beschrieben, während „dark patterns" gezielt darauf gerichtet sind, dass Nutzer*innen gegen die eigenen Interessen handeln, vgl. *Ettig/Herbrich*, K&R 2020, 719 (721); ausf. zum Begriff der „dark patterns" etwa *Weinzierl*, ZD-Aktuell 2020, 04419.

50 Während teilweise ein großer Gestaltungsspielraum der Anbieter befürwortet wird (*Haberer*, MMR 2020, 810 (814)), wird der Einsatz derartiger Manipulationstechniken von anderen Stimmen durchaus als kritisch angesehen (*Weinzierl*, NVwZ 2020, 1087 ff.; *ders.*, ZD-Aktuell 2020, 04419) oder gänzlich abgelehnt (*Hilgert/Hilgert*, jM 2020, 97 (99)).

51 *Baumgartner/Hansch*, ZD 2020, 435 (437); *Ettig/Herbrich*, K&R 2020, 719 (721); *Rauer/Ettig*, ZD 2021, 18 (22); *Wilfling*, DSRITB 2019, 301 (310).

52 *Haberer*, MMR 2020, 810 (813 f.); *Kollmar/Schirmbacher*, WRP 2020, 1015 (1017).

53 Die ausschließlich farbliche Gestaltung ohne jede Beschriftung der Auswahlmöglichkeiten soll indes unzulässig sein, s. etwa *Ettig/Herbrich*, K&R 2020, 719 (721).

54 *Baumgartner/Hansch*, ZD 2020, 435 (437); *Kollmar/Schirmbacher*, WRP 2020, 1015 (1016); wohl auch *Ettig/Herbrich*, K&R 2020, 719 (721).

55 *LG Rostock* ZD 2021, 166 (167), dort Rn. 53 f.; *Hilgert/Hilgert*, jM 2020, 97 (99).

56 RL 2011/83/EU über die Rechte der Verbraucher, ABl. EU L 304, 64 ff.

57 Vgl. Anhang I zur VRRL mit Abschnitt A. (Muster-Widerrufsbelehrung) und Abschnitt B. (Muster-Widerrufsformular).

58 Allg. zur Gefahr des „information overload" *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 12 Rn. 12; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 83; zu möglichen Lösungsansätzen *Strassemeyer*, DSRITB 2019, 31 ff.; krit. zur Erfüllung der Anforderungen an eine freiwillige und informierte Einwilligung bei komplexen Verarbeitungsvorgängen auch *Kollmar/El-Auwad*, K&R 2021, 73 (74 f.).

gewisse Routine entwickeln können und sich nicht auf jeder Internetseite neu zurechtfinden müssen.[59] Zugleich könnte eine Vereinheitlichung dazu beitragen, den nutzerseitigen Einsatz von Software zu fördern, die Cookie-Banner in einer vom Nutzer voreingestellten Art und Weise behandeln.[60]

2. Warnfunktion mittels „Button-Lösung"

Ein klassisches Instrument, um Nutzer*innen vor uninformierten und potenziell nachteiligen Entscheidungen zu schützen, stellt die Etablierung von Warnfunktionen dar. Traditionell erfüllen im Zivilrecht oftmals Formvorschriften eine derartige Warnfunktion;[61] mit Bezug zur Internetregulierung wird insbesondere der in Verbraucherrechte-Richtlinie und § 312j Abs. 4 BGB geregelten „Button-Lösung" eine derartige Warnfunktion zugeschrieben:[62] Durch weitgehend bindende Vorgaben zur Beschriftung einer Schaltfläche, mit deren Betätigung ein Verbraucher eine auf Abschluss eines entgeltlichen Vertrags gerichtete Willenserklärung abgibt, sollen Verbraucher*innen vor sog. Kostenfallen geschützt werden.[63]

Die Frage, ob „Daten als Gegenleistung" zum Vorliegen eines entgeltlichen Vertrags i.S.d. Verbraucherschutzrechts führen, wurde bereits in der Vergangenheit oftmals bejaht,[64] die Digitale Inhalte-Richtlinie[65] sieht dies nunmehr explizit vor.[66] Für Cookie-Banner hingegen folgt hieraus jedoch unmittelbar nichts, da das unionale Verbraucherschutzrecht auf dem Gebiet des Datenschutzrechts und dementsprechend auch für Cookies keine Regelungen trifft.[67]

Gleichwohl erscheint es lohnenswert, eine Button-Lösung für Cookie-Banner zu erwägen:[68] Insbesondere beim Einsatz von „Paywalls" könnte dem Nutzer klar vor Augen geführt werden, dass er für den Besuch einer Internetseite in jedem Fall – nämlich wahlweise mit seinen Daten oder mit seinem Ersparten – bezahlen muss.[69] Abseits von „Paywalls" könnte von einer Schaltfläche, die mit den Worten „Jetzt mit meinen Daten bezahlen!" oder „Jetzt einer Verfolgung meines Surfverhaltens zustimmen!" beschriftet ist, immerhin eine nachdrückliche Warnung ausgehen:[70] Der eine oder andere Internetnutzer wird möglicherweise davon abgehalten, den kürzesten und schnellsten Weg zum Ausblenden eines Cookie-Banners zu wählen, indem alle Cookies akzeptiert werden. Der *Bundesrat* hat in seiner Stellungnahme zum TTDSG-Entwurf eine entsprechende Regelung zwar angeregt,[71] diese hat jedoch in die verabschiedete Fassung keinen Eingang gefunden.

Allein ausreichend wäre eine solche Regelung jedoch in vielen Fällen womöglich nicht: Bliebe die Ablehnung von Cookies aus anderen Gründen zu umständlich, könnte eine entsprechende Warnung des Nutzers ihre Wirkung verfehlen.

3. Verankerung eines echten Äquivalenzgebots

Von entscheidender Bedeutung ist somit die Frage, ob dem Nutzer die Nichterteilung der Einwilligung genauso einfach möglich sein sollte wie deren Erteilung.[72] Für ein entsprechendes Gestaltungsgebot sprechen dabei gleich mehrere Gesichtspunkte.

Ein naheliegendes Argument lässt sich aus der „Planet49"-Entscheidung des *EuGH* ableiten: Wenn schon das erforderliche Deaktivieren einer Vorauswahl den Anforderungen an eine wirksame Einwilligung nicht genügt,[73] dann sollte a fortiori auch ein erforderlicher „Umweg" über eine Einstellungsseite keine wirksame Einwilligung darstellen. Auch die vom *BGH* in der nachfolgenden Entscheidung „Cookie-Einwilligung II" aufgestellten Grundsätze stützen dieses Verständnis:[74] Bei einer Gestaltung von Einwilligungserklärungen, die darauf angelegt ist, dass Verbraucher*innen von der Ausübung ihrer Wahlmöglichkeiten Abstand nehmen, soll keine wirksame Einwilligung vorliegen.[75] Als weiteres Argument kann auch der Rechtsgedanke aus Art. 7 Abs. 3 S. 4 DS-GVO angeführt werden:[76] Wenn hiernach der Widerruf einer Einwilligung so einfach wie deren Erteilung sein muss, dann liegt nahe, dass auch die schlichte Nicht-Erteilung einer Einwilligung so einfach wie deren Erteilung sein sollte.[77]

Bereits nach geltender Rechtslage erscheint es damit überzeugend, dass dem Nutzer bereits bei der ersten Konfrontation mit einem Cookie-Banner die Extreme der zur Auswahl stehenden Entscheidungsmöglichkeiten in gleichwertiger Weise zu offenbaren sind. Dies sollte nicht nur bedeuten, dass die wesentlichen Entscheidungen mit derselben Anzahl an Mausklicks ermöglicht werden müssen, sondern auch, dass die übrige optische Gestaltung die Gleichwertigkeit der angebotenen Auswahlmöglichkeiten nicht konterkarieren darf.[78] Eine gesetzgeberische Klarstellung, die ein derartig weit verstandenes Äquivalenzgebot ausdrücklich fixiert, wäre daher uneingeschränkt zu befürworten. Der Gesetzgeber des TTDSG hat sich auch hier – obwohl die Stellungnahme des *Bundesrats* eine überaus sinnvolle Ergänzung vorsah, wonach die Einwilligung und deren Ablehnung „graphisch gleichwertig dargestellt werden" sollten[79] – gegen eine derartige Klarstellung entschieden. Mit Blick darauf, dass dem deutschen Gesetzgeber für eine verbindliche gesetzliche Regelung zu den Voraussetzungen einer wirksamen Einwilligung nach DS-GVO die Kompetenz fehlt, ist diese Zurückhaltung jedoch nachvollziehbar.

59 Generell zur Gefahr der Überforderung des Betroffenen durch zu viele Einwilligungsanfragen *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 211.
60 Dazu noch unter IV.4.
61 Dies gilt insb. für die Schriftform, vgl. *Borges*, Verträge im elektronischen Geschäftsverkehr, Vertragsabschluss, Beweis, Form, Lokalisierung, anwendbares Recht, 2003, S. 596 ff.
62 Vgl. *Fervers*, NJW 2016, 2289 (2293).
63 Begr. RegE zu § 312g BGB a.F. (heute: § 312j BGB), BT-Drs. 17/7745, 6; *Benninghoff*, VuR 2013, 361; *Fervers*, NJW 2016, 2289; *Roth*, VuR 2012, 477 (478); *Schöttle*, in: Auer-Reinsdorff/Conrad (o. Fußn. 18), § 25 Rn. 258.
64 *Brönneke/Schmidt*, VuR 2014, 3; *Föhlisch*, in: BeckOK IT-Recht, 1. Ed., Stand: 1.9.2020, § 312 BGB Rn. 2; *Martens*, in: BeckOK BGB, 57. Ed., Stand: 1.2.2021, § 312 Rn. 10; beschränkt auf personenbezogene Daten etwa *Busch*, in: BeckOGK, Stand: 1.1.2021, § 312 BGB Rn. 11; *Czajkowski/Müller-ter Jung*, CR 2018, 157 (161); differenzierend *Buchmann*, K&R 2014, 369; abl. *Schirmbacher*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 312 Rn. 32.
65 RL (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. EU L 136, 1 ff.
66 Vgl. Art. 3 Abs. 1 UAbs. 2 Digitale Inhalte-RL.
67 Vgl. Art. 3 Abs. 8 UAbs. 2 Digitale Inhalte-RL.
68 Andeutungsweise bereits *Jandt*, ZD 2020, 551 (555).
69 Für eine Button-Lösung beim „Bezahlen mit Daten" allg. etwa *Benninghoff*, VuR 2013, 361; *Biesenbach*, jM 2018, 305 (306).
70 Eine fehlende Kenntnis über die Tragweite des Betätigens von Buttons in Cookie-Bannern bemängelt auch das *LG Rostock* ZD 2021, 166 (167), dort Rn. 53.
71 BR-Drs. 163/21 (Beschluss), S. 6.
72 Vgl. die Nachweise zu den Einzelfragen o. Fußn. 50-55.
73 *EuGH* MMR 2019, 732 m. Anm. *Moos/Rothkegel* = ZD 2019, 556 (558 f.), dort Rn. 44 ff. m. Anm. *Hanloser* – Planet49.
74 Offen zur Übertragbarkeit der *BGH*-Rspr. auf die Gestaltung von Cookie-Bannern *Böhm/Halim*, MMR 2020, 651 (655).
75 *BGH* MMR 2020, 609, Rn. 32 m. Anm. *Gierschmann* = ZD 2020, 467 m. Anm. *Eckhardt* – Cookie-Einwilligung II.
76 Art. 7 DS-GVO gilt dabei auch im Anwendungsbereich der ePrivacy-RL, vgl. *LG Rostock* ZD 2021, 166, Rn. 38; *Golland* (o. Fußn. 33), Rn. 11; *Kühling/Raab*, in: Kühling/Buchner (o. Fußn. 25), DS-GVO Art. 95 Rn. 7.
77 *Wilfling*, DSRITB 2019, 301 (310).
78 So hat das *LG Rostock* es etwa überzeugend als nicht ausreichend angesehen, wenn zwar mit einem Klick alle nicht-notwendigen Cookies abgelehnt werden können, der maßgebliche Button jedoch nicht klar als anklickbare Schaltfläche zu erkennen ist (*LG Rostock* ZD 2021, 166 (167), dort Rn. 54.
79 BR-Drs. 163/21 (Beschluss), S. 6.

4. Einbeziehung neuer Akteure

Ein letzter Aspekt schließlich betrifft die Einbeziehung neuer Akteure, die den Umgang mit Einwilligungsanfragen aus Nutzersicht maßgeblich erleichtern können.[80]

Zu nennen sind etwa schlichte Softwarelösungen, bei denen Nutzer*innen ihre Präferenzen voreinstellen können und das System Einwilligungsanfragen automatisch beantwortet.[81] Eine derartige Automatisierung bringt freilich die rechtliche Fragestellung mit sich, ob die resultierenden Einwilligungen noch als „für einen bestimmten Fall" i.S.v. Art. 4 Nr. 11 DS-GVO angesehen werden können.[82] Der letzte Stand des Entwurfs der ePrivacy-VO sieht eine derartige Möglichkeit zur Erteilung einer antizipierten Einwilligung auf Grund technischer Einstellungen immerhin explizit vor,[83] um der Einwilligungsmüdigkeit der Nutzer*innen entgegenzuwirken,[84] während der deutsche Gesetzgeber eine im ersten Entwurf des TTDSG noch enthaltene, dahingehende Klarstellung wieder gestrichen[85] und trotz der Befürwortung der Wiederaufnahme durch den *Bundesrat*[86] nicht ins Gesetz aufgenommen hat.

Eine weitergehende Frage ist, ob und ggf. mit welchen Mitteln etwa Browser-Hersteller dazu angehalten werden sollten, entsprechende Möglichkeiten zu implementieren.[87] Der Entwurf der ePrivacy-VO sieht zwar in Erwägungsgrund 20a die Schaffung entsprechender Anreize vor, wobei sich hierzu im verfügenden Teil des Entwurfs indes keinerlei materielle Entsprechungen finden.

Darüber hinaus wird kontrovers diskutiert, ob die Einführung von sog. Personal Information Management-Systemen (PIMS)[88] einen zielführenden Ansatz darstellen kann. Hierbei handelt es sich um Dienste, die als „Datentreuhänder" fungieren und die von Nutzer*innen geäußerten Interessen im Hinblick auf die Verwendung ihrer Daten gegenüber Diensteanbietern durchsetzen, die den Einsatz von Tracking-Mechanismen beabsichtigen.[89] Nachdem der erste Entwurf des TTDSG[90] in § 3 eine entsprechende Vorschrift enthielt, berücksichtigte ein späterer Entwurf dieses Modell zunächst nicht mehr.[91]

Mit einer abermaligen Kehrtwende hat der Gesetzgeber in § 26 TTDSG nunmehr doch eine entsprechende Vorschrift für anerkannte Dienste zur Einwilligungsverwaltung ins Gesetz aufgenommen: Anbieter, die nutzerfreundliche und wettbewerbskonforme Verfahren zur Einwilligungsverwaltung einsetzen (§ 26 Abs. 1 Nr. 1 TTDSG), können sich künftig – zur Stärkung des Vertrauens der Nutzer*innen in derartige Systeme – anerkennen lassen. Die mitunter geforderte Mindestanforderung an derartige Dienste, dass die unabhängig und ohne wirtschaftliche Verwertungsinteressen im Hinblick auf die von Nutzer*innen verarbeiteten Daten agieren,[92] ist künftig in § 26 Abs. 1 Nr. 2 TTDSG verankert.

Die Ausgestaltung der näheren Anforderungen an die Anerkennung der Anbieter sowie die von Browser-Herstellern zu ergreifenden Maßnahmen, damit Voreinstellungen befolgt und anerkannte Dienste unterstützt werden, soll durch Rechtsverordnung erfolgen (§ 26 Abs. 2 TTDSG).

Im Hinblick auf die Einbeziehung neuer Akteure ist allerdings die Nutzerperspektive im Blick zu behalten: Mit der bloß einmaligen Abfrage der Nutzerpräferenzen verlagert sich die Entscheidung in zeitlicher Hinsicht nach vorn und erleichtert dadurch die spätere Internetnutzung. Die zu treffende Entscheidung ist aber nicht minder komplex, zudem hat sie weitreichende, in die Zukunft gerichtete Folgen. Umso mehr ist auch hier daher darauf zu achten, dass die getroffene Entscheidung nicht durch die Gestaltung des Entscheidungsprozesses beeinflusst wird.

V. Fazit und Ausblick

Die (uneinheitliche) Gestaltung von Cookie-Bannern ist mit ihren derzeit zu beobachtenden Auswüchsen eine Zumutung für einen erheblichen Teil der Internetnutzer*innen. Auch für Anbieter ist die Einholung wirksamer Einwilligungen durch Nutzer*innen mittels Cookie-Bannern durchaus herausfordernd, da zahlreiche Einzelaspekte mit Bedeutung für die konkrete technische Umsetzung bereits aus rechtlicher Sicht nicht eindeutig sind.

Mit Blick darauf, dass die verbindliche Klärung von Einzelfragen durch die Rechtsprechung mitunter mehrere Jahre dauern kann[93] und Aufsichtsbehörden – selbst bei einer entsprechend klaren Positionierung – lediglich anfechtbare Entscheidungen treffen können, erscheint es geboten, dass der (europäische) Gesetzgeber die Anforderungen an eine wirksame Einwilligung zum Einsatz von Tracking-Mechanismen wie Cookies schärfer konturiert.

Der Beitrag hat hierzu unterschiedliche Ansätze aufgezeigt, die auf eine Vereinheitlichung der Entscheidungssituation für Nutzer*innen abzielen. Mittels einer „Button-Lösung" könnte das Nutzerbewusstsein für die Bedeutung der Einwilligungserteilung geschärft werden. Ein gesetzlich verankertes „Äquivalenzprinzip" könnte dazu beitragen, dass Nutzer*innen bei der Wahl zwischen dem Akzeptieren und dem Ablehnen von Tracking-Mechanismen (wieder) eine wirkliche Entscheidung treffen. Bei einer Einbeziehung neuer Akteure ist deren besondere Verantwortung zur integeren Durchsetzung der Nutzerinteressen zu berücksichtigen. Das TTDSG hält sich im Hinblick auf die hier vorgeschlagenen Maßnahmen weitgehend zurück. Ob und wie schnell Nutzer*innen von der Last von Einwilligungsanfragen mittels Cookie-Bannern befreit werden, bleibt daher abzuwarten – vorerst wird Vieles dabei von der Konkretisierung des § 26 TTDSG abhängen.

---

80 Im Überblick zu entsprechenden Datenmanagementsystemen etwa *Kelber*, ZD 2020, 73 (75).

81 Entsprechende Plugins für Internet-Browser sind bereits verfügbar, vgl. *Böhm/Halim*, MMR 2020, 651 (656); *Venzke-Caparese*, DuD 2017, 577 (581).

82 Krit. hierzu etwa *Jandt*, DSB 2021, 66 (68); vgl. in Bezug auf mehrere Einwilligungen mittels einer einzigen Schaltfläche bei Cookie-Bannern auch *Böhm/Halim*, MMR 2020, 651 (655); *Rauer/Ettig*, ZD 2021, 18 (22); *Wilfling*, DSRITB 2019, 301 (305).

83 Vgl. Art. 4a Abs. 2 ePrivacy-VO-E (o. Fußn. 7).

84 Erwägungsgrund 20a ePrivacy-VO-E (o. Fußn. 7).

85 Nach § 9 Abs. 4 des ersten TTDSG-Entwurfs sollte der Endnutzer eine Einwilligung auch erklären können, indem er „eine dafür vorgesehene Einstellung seines Browsers oder eine andere Anwendung auswählt"; der hier in Bezug genommene RefE v. 14.7.2020 ist abrufbar unter: https://cdn.netzpolitik.org/wp-upload/2020/08/20200731_RefE_TTDSG-clean.pdf.

86 BR-Drs. 163/21 (Beschluss), S. 4.

87 Gegen eine Verpflichtung der Browser-Hersteller *Jandt*, DSB 2021, 66 (68).

88 Krit. zum Begriff *Becker*, CR 2021, 87 (88) unter Verweis darauf, dass derartige Systeme nicht ausschließlich zum Management personenbezogener Daten (personal information) genutzt werden.

89 *Peitz/Schweitzer*, NJW 2018, 275 (278); *Schwartmann/Benedikt/Reif*, MMR 2021, 99 (101).

90 S.o. Fußn. 85.

91 Krit. zur Aufgabe des Ansatzes etwa *Schwartmann/Benedikt/Reif*, MMR 2021, 99 (101).

92 *Verbraucherzentrale Bundesverband e.V.*, Personal Information Management Systems (PIMS) – Chancen, Risiken und Anforderungen, Positionspapier v. 19.2.2020, S. 11, abrufbar unter: https://www.vzbv.de/publikationen/dateninterm ediaere-gesetzlich-regeln.

93 So hat etwa die Klärung der im „Planet49"-Verfahren entscheidenden Frage, ob eine Cookie-Einwilligung durch ein voreingestelltes Häkchen den Anforderungen des Unionsrechts entsprechend wirksam erteilt werden kann, von der erstinstanzlichen Entscheidung (*LG Frankfurt/M.* MMR 2015, 321 ff. m. Anm. *Laoutoumai*) bis zum Abschluss des Verfahrens durch den *Bundesgerichtshof* (*BGH* MMR 2020, 609 m. Anm. *Gierschmann* = ZD 2020, 467 m. Anm. *Eckhardt* – Cookie-Einwilligung II) knapp fünfeinhalb Jahre gedauert.

Schnell gelesen ...

- Bei der Gestaltung von sog. Cookie-Bannern besteht erheblicher Handlungsbedarf, da das Primat der freien und informierten Einwilligung durch die Cookie-Müdigkeit der Internetnutzer*innen in Gefahr ist.
- Es sollten vereinheitlichte Gestaltungsvorgaben für Cookie-Banner geschaffen werden, damit Nutzer*innen ihren Präferenzen entsprechend handeln und ggf. automatisierte Lösungen zur Umsetzung ihrer Präferenzen zum Einsatz bringen können.
- Für Cookie-Banner sollte eine „Button-Lösung" eingeführt werden, die eine klare und warnende Beschriftung von solchen Schaltflächen verbindlich vorschreibt, mit denen die Einwilligung in die Nutzung von Tracking-Mechanismen erteilt wird.
- Es sollte verbindlich vorgeschrieben werden, dass die Wege zur Erteilung der Einwilligung in die Nutzung von Tracking-Mechanismen und zu deren Ablehnung äquivalent auszugestalten sind.
- Neue Akteure können die Bearbeitung von Einwilligungsanfragen maßgeblich erleichtern. Bei deren Einbeziehung ist jedoch auf Nutzerfreundlichkeit besonderer Wert zu legen sowie die besondere Vertrauensstellung angemessen zu berücksichtigen.

Dr. Andreas Sesing
ist Geschäftsführer des Instituts für Rechtsinformatik und Wissenschaftlicher Mitarbeiter an der Universität des Saarlandes (Saarbrücken).

ÖOGH: Mehrere Personen als Geschäftsgeheimnisinhaber von Softwareprodukten

Softwarerechte

öUWG §§ 24, 26b Abs. 1 und Abs 2, 26c Abs. 2 Nr. 2, 26d Abs. 1, 26i Abs. 1; öUrhG §§ 40b; RL (EU) 2016/943 Art. 2 Nr. 1
Beschluss vom 10.12.2020 – 4 Ob 182/20y (OLG Wien, LG St. Pölten)

Leitsatz

Unter Verfügungsgewalt ist die tatsächliche Möglichkeit zu verstehen, den Zugriff auf das Geschäftsgeheimnis bestimmen, einschränken oder ausschließen zu können.

Anm. d. Red.: Vgl. ferner *OLG Karlsruhe* MMR 2020, 492 und *Hoeren/Münker*, MMR 2021, 523 – in diesem Heft.

Schlagworte: Geschäftsgeheimnis; Werknutzungsrecht; Quellcode-Übertragung; Offenlegung; Softwareentwicklung; Softwarerechte; Escrow-Hinterlegung

Sachverhalt

Die klägerische deutsche GmbH entwickelt und vertreibt in Österreich und in Deutschland Software für Ärzte, Krankenhäuser, Labore und sonstige medizinische oder gesundheitsbezogene Betriebe.

Der Bekl. hat ab 2001 die Software S entwickelt. Sein Know-how brachte er 2004 in eine von ihm mitbegründete GmbH (im Folgenden: SoftwareGmbH) ein, deren Geschäftsführer er bis Ende März 2019 war. Zur Produktfamilie S gehört auch die I-Software, die ab 2018 entwickelt wurde.

2017 schloss die SoftwareGmbH mit der Kl. einen Kooperationsvertrag (betreffend Marketing und Nutzung der Produktfamilie S) und eine sog. „Escrow"-Vereinbarung (betreffend die Hinterlegung der Quellcodes zu Gunsten der Kl. bei einem neutralen Dritten als Treuhänder). Unstrittig ist der Inhalt dieser Verträge: Festgehalten wird, dass die SoftwareGmbH die Software am europäischen Markt entwickelt, vertreibt und lizenziert (Präambel des Kooperationsvertrags). Der Kl. wird das exklusive Vertriebsrecht für Österreich und Deutschland sowie ein Vorkaufsrecht hinsichtlich der Geschäftsanteile der SoftwareGmbH eingeräumt. Für den Fall des Eintritts bestimmter Umstände (Insolvenz, Liquidation oder Einstellung des Geschäftsbetriebs der SoftwareGmbH) wird der Kl. das Recht eingeräumt, den Quellcode um einen bereits bestimmten und genannten Betrag ausgefolgt zu erhalten und danach die Vertragssoftware unwiderruflich und unbegrenzt in jeder Hinsicht selbst oder durch Weitergabe an Dritte zu verwerten und weiterzuentwickeln.

Nach der Auflösung seines Dienstverhältnisses zur SoftwareGmbH und dem Ausscheiden als deren Geschäftsführer Ende März 2019 teilte der Bekl. der Kl. mit, dass er an der SoftwareGmbH kein Interesse mehr habe und alle weiteren strategischen und die Partnerschaft zwischen Kl. und SoftwareGmbH betreffenden Gespräche künftig mit seiner Ex-Gattin zu führen seien. Diese ist nunmehr alleinige Gesellschafterin und mit Stichtag 15.3.2019 auch alleinige Geschäftsführerin der SoftwareGmbH. In der Folge hat die Kl. als Käuferin mit Kaufvertrag v. 15.10.2019 von der SoftwareGmbH als Verkäuferin alle von dieser entwickelten und hergestellten Produkte und Dienstleistungen der Produktfamilie S (zu der auch die I-Software gehört) erworben. Mit dem Kaufvertrag wurden der Kl. sämtliche IP-Rechte an dieser Softwareproduktfamilie übertragen. Die Verkäuferin garantiert darin der Käuferin, dass die S-Programme keine Open-Sources-, Public-Domain- und/oder Freeware-Programme oder Programmbestandteile haben.

Der Bekl. hatte sich den Quellcode zu den von ihm entwickelten Programmen auch nach seinem Ausscheiden aus der SoftwareGmbH behalten. Am 27.5.2020 verfasste er eine WhatsApp-Nachricht an seine Ex-Gattin, in der er ankündigte, als nächstes die Kl. „angehen zu wollen" und den Quellcode der Software I öffentlich und gratis ins Internet zu stellen und alle Kunden darüber zu informieren, dass sie die Dienstleistungen dazu von ihm sehr günstig bekommen würden.

Die Kl. beantragte im Sicherungsverfahren, dem Bekl. aufzutragen, es zu unterlassen, den Source-Code einer Software der Kl., insb. der Software I und/oder S ohne Einwilligung der Kl. zu verbreiten, unbefugt zu vervielfältigen und/oder unbefugt hergestellte oder unbefugt erworbene Kopien zu gebrauchen oder inhaltsgleiche Handlungen zu setzen, insb. es zu unterlassen, den Quellcode der Software I und/oder S in über das Internet abrufbaren Servern zu veröffentlichen oder anderen zugänglich zu machen.

Das *Erstgericht* erließ die beantragte einstweilige Verfügung. Der Kl. drohe auf Grund des bescheinigten Sachverhalts ein unmittelbarer Eingriff des Bekl. in ihre Rechte an den gegenständlichen Programmen, und zwar eine Verletzung ihres Geschäftsgeheimnisses daran. Das *Rekursgericht* wies den Sicherungsantrag ab. Der Bekl. sei Urheber der gegenständlichen Software.

Der Kl. seien mit der Kooperationsvereinbarung 2017 lediglich Vertriebsrechte eingeräumt worden, nicht aber ein Werknutzungsrecht. Gegen diese Entscheidung richtet sich der außerordentliche Revisionsrekurs der Kl. mit dem Antrag, die einstweilige Verfügung des *Erstgerichts* wiederherzustellen.

Aus den Gründen

13 Der Revisionsrekurs ist mangels höchstgerichtlicher Rspr. zu §§ 26a ff. öUWG zulässig; er ist auch berechtigt.

14 1. Die Kl. macht zunächst geltend, dass die SoftwareGmbH schon auf Grund von § 40b öUrhG ein unbeschränktes Werknutzungsrecht an der vom Bekl. entwickelten Software hatte und dieses daher wirksam der Kl. übertragen konnte.

15 1.1. § 40b öUrhG bestimmt, dass dem Dienstgeber an einem von einem Dienstnehmer in Erfüllung seiner dienstlichen Obliegenheiten geschaffenen Computerprogramm ein unbeschränktes Werknutzungsrecht zusteht, wenn er mit dem Urheber nichts anderes vereinbart hat.

16 1.2. § 40b öUrhG ist nur auf Dienstnehmer anzuwenden; Organe juristischer Personen sind keine Dienstnehmer im Sinne dieser Norm, wenn und weil sie keine abhängige und weisungsgebundene Tätigkeit entfalten (*Ciresa*, ZAS 2006, 15; *Grützmacher,* in: Wandtke/Bullinger, Urheberrecht, 5. Aufl., § 69b Rn. 3; vgl. RIS-Justiz RS0071234; offenlassend 8 ObA 86/12y). Nach den Feststellungen war der Bekl. von Beginn an [zu 50% beteiligter] Gesellschafter-Geschäftsführer der GmbH (vgl. RS0021243). § 40b UrhG ist auf ihn daher nicht anzuwenden.

17 2. Die Rechtsmittelwerberin macht weiters geltend, der Bekl. habe durch sein Verhalten als Geschäftsführer der SoftwareGmbH dieser dadurch (schlüssig) ein Werknutzungsrecht auf vertraglicher Grundlage eingeräumt, dass er den Kooperationsvertrag und die Escrow-Vereinbarung abgeschlossen und damit zum Ausdruck gebracht habe, die SoftwareGmbH sei befugt, ggü. Dritten über die Software und den Quellcode frei zu verfügen. Dies ist zutreffend.

18 2.1. Richtig ist, dass ein Werknutzungsrecht auch schlüssig eingeräumt werden kann (RS0106668). Die Befugnisse des Werknutzungsberechtigten aus einem solchen Werknutzungsvertrag reichen im Zweifel nicht weiter, als es für den praktischen Zweck der beabsichtigten Werknutzung erforderlich ist (RS0077726; RS0077666). Der *Senat* hat bereits wiederholt ein schlüssig eingeräumtes Werknutzungsrecht des Gesellschafter-Geschäftsführers an „seine" GmbH angenommen (4 Ob 100/20i; 4 Ob 23/15h).

19 2.2. Entgegen der Auffassung des *Rekursgerichts* kann unter Berücksichtigung des gesamten Verhaltens des Bekl. (vgl. RS0110838) kein vernünftiger Zweifel daran bestehen, dass er der SoftwareGmbH das Werknutzungsrecht an der von ihm entwickelten Software (einschließlich des Quellcodes) übertragen hat. Zutreffend verweist die Kl. auf den Abschluss des Kooperationsvertrags und der Escrow-Vereinbarung, die der Bekl. als damaliger Geschäftsführer der SoftwareGmbH unterfertigt hat. In diesen Vertragswerken wurde nicht nur festgehalten, dass die GmbH die Software am europäischen Markt „entwickelt, vertreibt und lizenziert", sondern der Kl. wurden exklusive Vertriebsrechte für Österreich und Deutschland sowie ein Vorkaufsrecht hinsichtlich der Geschäftsanteile der GmbH eingeräumt; weiters wurde die Hinterlegung des Quellcodes zu Gunsten der Kl. und eine Kaufoption der Kl. daran mit dem damit verbundenen Recht vereinbart, die Vertragssoftware unwiderruflich und unbegrenzt in jeder Hinsicht selbst oder durch Weitergabe an Dritte zu verwerten und weiterzuentwickeln.

20 Der Bekl. hat damit selbst an Verträgen mitgewirkt, die die Möglichkeit eines Übergangs aller Rechte an der Software auf die Kl. einschließlich der Herausgabe des Quellcodes an diese vorsehen (vgl. 4 Ob 304/97b). Ein solcher Übergang erfordert aber – entgegen der Ansicht des *Rekursgerichts* – ein unbeschränktes Werknutzungsrecht und nicht bloß eine Werknutzungsbewilligung. Werden sämtliche Verwertungsrechte übertragen, spricht dies für ein Werknutzungsrecht (vgl. 4 Ob 2093/96i), ebenso, wenn – wie hier durch das Anbot auf Überlassung des Quellcodes – das „Eigentum" an einem Werk übertragen werden soll (RS0077662). Hinzu kommt das Vorkaufsrecht, das bei wirtschaftlicher Betrachtungsweise nur dann Sinn ergibt, wenn die Kl. damit die exklusive Werknutzungsberechtigung erlangen hätte können. Schließlich hat der Bekl. – nachdem er als Geschäftsführer der SoftwareGmbH ausgeschieden war – die Kl. in einer E-Mail darauf hingewiesen, dass alle weiteren die strategische Partnerschaft der Unternehmen betreffenden Fragen mit der neuen Geschäftsführerin, seiner Frau, zu besprechen seien. Hätte er der SoftwareGmbH nur ein mit seinem Ausscheiden befristetes Recht eingeräumt, wäre dieser Hinweis unverständlich.

21 3. Zu beurteilen ist hier das Begehren auf Sicherung des Anspruchs auf Unterlassung der drohenden rechtswidrigen Verletzung eines Geschäftsgeheimnisses durch dessen Offenlegung (§ 26f Abs. 1 öUWG).

22 3.1. § 26b Abs 1 öUWG übernimmt die Definition des Geschäftsgeheimnisses aus Art. 2 Ziff. 1 RL EU 2016/943 v. 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (Geschäftsgeheimnis-RL) nahezu wörtlich, wonach Informationen dann ein Geschäftsgeheimnis sind, wenn drei Kriterien kumulativ erfüllt sind, nämlich dass sie a) geheim sind, b) einen kommerziellen Wert haben und c) durch angemessene Geheimhaltungsmaßnahmen geschützt werden.

23 3.2. Der Quellcode eines Computerprogramms kann grds. ein Geschäftsgeheimnis i.S.d. § 26b Abs. 1 öUWG sein (vgl. *Pollirer*, Dako 2019, 89). Dass der im Anlassfall umstrittene Quellcode unter den vorliegenden Umständen unter diesen gesetzlichen Tatbestand fällt, hat das *Rekursgericht* zutreffend erkannt und wird vom Bekl. auch nicht in Frage gestellt. Zu prüfen bleibt allerdings, ob die Kl. Inhaberin dieses Geschäftsgeheimnisses ist.

24 3.3. Inhaber eines Geschäftsgeheimnisses ist nach § 26b Abs. 2 UWG jede natürliche oder juristische Person, welche die rechtmäßige Verfügungsgewalt über ein Geschäftsgeheimnis besitzt. Die Bestimmung setzt Art. 2 Abs. 2 der Geschäftsgeheimnis-RL um, der von rechtmäßiger Kontrolle spricht.

25 3.4. Grds. können auch mehrere Personen Inhaber eines Geschäftsgeheimnisses sein (arg.: „jede [...] Person"). Die Inhaberschaft setzt sich aus zwei Tatbestandsmerkmalen zusammen, nämlich einerseits aus der Verfügungsgewalt und andererseits aus dem Merkmal rechtmäßig. Unter Verfügungsgewalt ist die tatsächliche Möglichkeit zu verstehen, den Zugriff auf das Geschäftsgeheimnis bestimmen, einschränken oder ausschließen zu können (*Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl., § 2 GeschGehG Rn. 98). Rechtmäßige Verfügungsgewalt erfordert darüber hinaus aber auch die rechtliche Legitimation der tatsächlich ausgeübten Kontrolle. Weder das öUWG noch die Geschäftsgeheimnis-RL geben dafür Kriterien an die Hand. Rechtmäßig ist die Verfügungsgewalt jedenfalls dann, wenn das Geschäftsgeheimnis originär im Unternehmen des Inhabers entwickelt wurde. Rechtmäßig ist sie aber auch dann, wenn die Berechtigung vertraglich vom bisherigen Inhaber abgeleitet wird (vgl. § 26d Abs. 1 öUWG; *Thiele,* in: Wiebe/Kodek, UWG, 2. Aufl., § 26b Rn. 36; *Alexander*, a.a.O., Rn. 102). Die abgeleitete Befugnis braucht nach zutreffender Ansicht keine ausschließliche zu sein (*Ohly*, GRUR 2019, 441 (446)).

26 3.5. Hier hat die Kl. von der SoftwareGmbH alle von dieser entwickelten und hergestellten Produkte und Dienstleistungen der Produktfamilie S (zu der auch die I-Software gehört) erworben. Mit dem Kaufvertrag wurden der Kl. sämtliche IP-Rechte an dieser Softwareproduktfamilie übertragen. Die Kl. kann somit ihre Berechtigung am Geschäftsgeheimnis vertraglich vom bisherigen Inhaber ableiten und besitzt damit die rechtmäßige Verfügungsgewalt daran.

27 4.1. Es bleibt zu prüfen, ob die Offenlegung des Quellcodes durch den Bekl. rechtswidrig wäre. Nach § 26c Abs. 2 Ziff. 2 öUWG ist die Offenlegung eines Geschäftsgeheimnisses rechtswidrig, wenn sie gegen eine Vertraulichkeitsvereinbarung oder eine vertragliche oder sonstige Verpflichtung, das Geschäftsgeheimnis nicht offenzulegen oder nur beschränkt zu nutzen, verstößt.

28 4.2. Oben wurde bereits klargestellt, dass der Bekl. durch sein Verhalten zum Ausdruck gebracht hat, dass die SoftwareGmbH befugt sei, ggü. Dritten über die Software und den Quellcode zu verfügen. Mit dieser Einräumung des Werknutzungsrechts ist die Verpflichtung des Bekl. verbunden, den Quellcode (als Geschäftsgeheimnis) nicht offenzulegen, würde doch die Offenlegung des Quellcodes den Vertragsgegenstand (Software) drastisch entwerten. Auf diese Verschwiegenheitspflicht kann sich auch die Kl. als nunmehrige Inhaberin des Geschäftsgeheimnisses berufen, zumal der Bekl. einverstanden war, dass die SoftwareGmbH ggü. Dritten über die Software inklusive Quellcode frei verfügen kann.

29 5. Damit hat die Kl. seinen zu sichernden Anspruch (drohende rechtswidrige Verletzung eines Geschäftsgeheimnisses durch dessen Offenlegung) bescheinigt. Entgegen der Ansicht des *Rekursgerichts* steht dem nicht entgegen, dass der Bekl. Urheber des Quellcodes ist. Der Dienstnehmer oder Geschäftsführer, der für ein Unternehmen ein Geschäftsgeheimnis entwickelt, ist nicht dessen Inhaber, wenn er dem Unternehmen die Rechte daran abgetreten hat oder sie ihm bereits auf Grund des Gesetzes zukommen (vgl. *Hofmarcher*, Das Geschäftsgeheimnis, 2020, Rn. 2.76). Einer Gefährdungsbescheinigung bedarf es nicht (§§ 26i Abs. 1 i.V.m. 24 öUWG).

30 Dem Revisionsrekurs der Kl. ist somit Folge zu geben und die einstweilige Verfügung des *Erstgerichts* wiederherzustellen. ...

BGH: beA – Kein Anspruch auf Verwendung einer anderen Verschlüsselungstechnik

Hardware Security Module

BRAO § 31a Abs. 1, Abs. 3 u. Abs. 6; RAVPV §§ 19 u. 20; ZPO §§ 130a Abs. 4 Nr. 2, 174 Abs. 3 S. 3 u. S. 4; GG Art. 12 Abs. 1; TKG § 113a
Urteil vom 22.3.2021 – AnwZ (Brfg) 2/20 (AGH Berlin)

Leitsätze der Redaktion

1. Der Bundesrechtsanwaltskammer steht ein Spielraum bei der technischen Ausgestaltung der Nachrichtenübermittlung mittels des besonderen elektronischen Anwaltspostfachs (beA) zu, sofern das gewählte System eine im Rechtssinne sichere Kommunikation gewährleistet.
2. Ein Anspruch von Rechtsanwälten gegen die Bundesrechtsanwaltskammer darauf, dass diese das besondere elektronische Anwaltspostfach mit einer Ende-zu-Ende-Verschlüsselung i.S.d. Europäischen Patentschrift EP 0 877 507 B1 versieht und betreibt, besteht nicht. Weder die gesetzlichen Vorgaben für die Errichtung und den Betrieb des besonderen elektronischen Anwaltspostfachs noch die Verfassung gebieten eine derartige Verschlüsselung.
3. Eine sichere Kommunikation im Rechtssinne setzt nicht eine Freiheit von jeglichen Risiken voraus. Das gewählte Übermittlungssystem muss einen Sicherheitsstandard erreichen, bei dem unter Berücksichtigung der Funktionalität nach dem Stand der Technik die Übermittlung voraussichtlich störungs- und gefahrfrei erfolgt und Risiken für die Vertraulichkeit möglichst weitgehend ausgeschlossen werden.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 9686. Die Leitsätze 1 und 2 sind amtliche Leitsätze; Leitsatz 3 ist ein redaktioneller Leitsatz. Vgl. ferner *BVerfG* MMR 2010, 456 und *BGH* MMR 2016, 485.

Schlagworte: Sichere Kommunikation; Ende-zu-Ende-Verschlüsselung; privater Schlüssel; Hardware Security Module; Client; HSM; verfassungskonforme Auslegung; OSCI-Standard; EGVP; besonderes elektronischen Anwaltspostfach

Sachverhalt

Die Kl. sind zugelassene Rechtsanwälte. Die Bekl. richtete auf Grundlage von § 31a Abs. 1 BRAO für sie ein besonderes elektronisches Anwaltspostfach (beA) ein. Die Kl. wenden sich gegen die technische Ausgestaltung des beA durch die Bekl. und streben an, dass dieses mit einer Ende-zu-Ende-Verschlüsselung betrieben wird, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden.

Kern des Streits ist die Verwendung eines sog. Hardware Security Module (im Folgenden: HSM), das bei der Ablage und dem Abruf von Nachrichten vereinfacht wie folgt zum Einsatz kommt: Die versandten, mit einem symmetrischen Nachrichtenschlüssel verschlüsselten Nachrichten werden in verschlüsselter Form im Postfach des Empfängers gespeichert. Symmetrische Verschlüsselung bedeutet hierbei, dass derselbe Schlüssel – hier der sog. Nachrichtenschlüssel – verwendet wird, um die Nachricht zu verschlüsseln und auch wieder zu entschlüsseln. Der Empfänger der Nachricht benötigt mithin den Nachrichtenschlüssel, um die Nachricht entschlüsseln zu können. Der Nachrichtenschlüssel ist seinerseits verschlüsselt mit dem öffentlichen Schlüssel des Empfängerpostfachs, der – ebenso wie der zugehörige private Schlüssel des Postfachs – beim Anlegen des Postfachs im HSM erzeugt wurde. Dieser verschlüsselte Nachrichtenschlüssel wird an das HSM übergeben und dort auf den symmetrischen Schlüssel des Postfachs umgeschlüsselt. Der mit dem symmetrischen Schlüssel des Postfachs verschlüsselte Nachrichtenschlüssel wird sodann im Postfach gespeichert. Nachdem derjenige, der die Nachricht abrufen möchte (im Folgenden: Client), seine Berechtigung durch die vorgesehene Authentifizierung nachgewiesen hat, wird der verschlüsselte Nachrichteninhalt ohne Veränderung aus dem Postfach an den Client übertragen. Der mit dem symmetrischen Postfachschlüssel verschlüsselte Nachrichtenschlüssel wird im HSM auf einen dem Client zugeordneten symmetrischen sog. Kommunikationsschlüssel umgeschlüsselt. Der auf diese Weise verschlüsselte Nachrichtenschlüssel wird sodann an den Client übertragen und kann dort mit Hilfe seines Kommunikationsschlüssels entschlüsselt werden. Mit dem entschlüsselten Nachrichtenschlüssel lässt sich die verschlüsselte Nachricht entschlüsseln.

Nachdem bei der Inbetriebnahme des beA technische Probleme aufgetreten waren, nahm die Bekl. das beA Ende 2017 vorübergehend außer Betrieb und beauftragte die S.-AG mit der Begutachtung der Sicherheit des beA. Deren Abschlussgutachten v. 18.6.2018 ist von beiden Parteien in den Prozess eingeführt worden (im Folgenden: S.-Gutachten).

Das S.-Gutachten bewertete das beA als grds. geeignetes System zur vertraulichen Kommunikation, stellte aber gleichzeitig

auch betriebsverhindernde, betriebsbehindernde und sonstige nicht behobene Schwachstellen fest, die behebbar seien. Das Gutachten empfahl, die betriebsverhindernden Schwachstellen vor Wiederaufnahme des beA zu beseitigen, die betriebsbehindernden baldmöglichst danach. Bei Beachtung der Vorgaben sei eine Wiederaufnahme des Betriebs aus sicherheitstechnischer Sicht möglich. Wegen der Einzelheiten wird auf das Gutachten Bezug genommen. Im Spätsommer 2018 nahm die Bekl. das beA wieder in Betrieb.

Die Kl. machen geltend, die Bekl. sei verpflichtet, die über das beA geleiteten Nachrichten mittels einer Ende-zu-Ende-Verschlüsselung zu verschlüsseln, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden. Eine Ende-zu-Ende-Verschlüsselung liege bei der derzeitigen Struktur insb. nicht vor, weil die privaten Schlüssel der beA-Postfachinhaber zentral im HSM erstellt und gespeichert würden und damit nicht – was Voraussetzung einer Ende-zu-Ende-Verschlüsselung sei – in der alleinigen Verfügungsgewalt der sie verwendenden Kommunikationspartner stünden.

Der *AGH* hat die Klage abgewiesen. Die Kl. hätten keinen gegen die Bekl. gerichteten Anspruch darauf, dass diese das beA in einer bestimmten Weise konzipiere und betreibe. Namentlich könnten die Kl. nicht verlangen, dass das beA ausschließlich mit einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne betrieben werde. Eine entsprechende gesetzgeberische Vorgabe ergebe sich nicht unmittelbar aus den einfachen Gesetzen wie § 31a Abs. 3 BRAO oder §§ 174 Abs. 3 S. 3 i.V.m. 130a Abs. 4 Nr. 2 ZPO. Aus §§ 19 u. 20 RAVPV sei insoweit nichts Anderes herzuleiten.

Gegen die Abweisung der Klage wenden sich zwei der ursprünglich sieben Kl. mit ihrer vom *AGH* zugelassenen Berufung.

Aus den Gründen

18 II. Die Berufung ist unbegründet. Der *AGH* hat die Klage zu Recht abgewiesen. Diese ist zwar zulässig, aber unbegründet.

19 1. Die Klage ist hinsichtlich beider Klageanträge als allgemeine Leistungsklage statthaft und auch i.Ü. zulässig. …

22 2. Die Klage ist unbegründet. Den Kl. steht weder ein Anspruch darauf zu, dass die Bekl. es unterlässt, das beA ohne die von ihnen geforderte Ende-zu-Ende-Verschlüsselung, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden, zu betreiben, noch ein Anspruch auf ein Betreiben mit genau einer solchen Verschlüsselung.

23 a) Der mit Klageantrag zu 1 geltend gemachte Unterlassungsanspruch besteht nicht.

24 Ein öffentlich-rechtlicher Abwehr- und Unterlassungsanspruch setzt voraus, dass durch eine hoheitliche Maßnahme rechtswidrig in ein subjektiv-öffentliches Recht eingegriffen wird oder zu werden droht, wobei sich das subjektive Recht aus den Grundrechten oder aus einfachem Recht ergeben kann (vgl. *Detterbeck/Windthorst/Sproll*, Staatshaftungsrecht, § 13 Rn. 12 u. 17; *Ossenbühl/Cornils*, Staatshaftungsrecht, 6. Aufl., S. 373 f.).

25 Diese Voraussetzungen liegen nicht vor. Zwar erfüllt das von der Bekl. eingerichtete System der Nachrichtenübermittlung nicht die Anforderungen an eine Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift EP 0 877 507 B1 (hierzu nachfolgend unter aa)) [= Rn. 26]. Darin liegt jedoch kein rechtswidriger Eingriff in ein subjektiv-öffentliches Recht der Kl. Denn weder steht den Kl. ein einfachgesetzlich normiertes Recht darauf zu, dass die über das beA übermittelten Nachrichten mit einer Ende-zu-Ende-Verschlüsselung in diesem Sinne gesichert werden, noch greift das Betreiben des beA ohne Ende-zu-Ende-Verschlüsselung in diesem Sinne rechtswidrig in Grundrechte der Kl., insb. in die von Art. 12 Abs. 1 GG geschützte Berufsausübungsfreiheit, ein (hierzu unter bb)).

26 aa) Das von der Bekl. verwendete Verschlüsselungssystem entspricht nicht einer Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift (EP 0 877 507 B 1, abrufbar unter: https://register.epo.org/application?number=EP98108118).

27 (a) Charakteristisch für eine Ende-zu-Ende-Verschlüsselung in diesem Sinne ist die Verschlüsselung der Informationen am Ort des Senders und die Entschlüsselung erst beim Empfänger einer Nachricht, wobei der dazwischenliegende Kommunikationskanal keinen Einfluss auf die Chiffrierung besitzt. Innerhalb der digitalen Übertragungskette existiert keine Möglichkeit zur Umwandlung der Nachricht in den ursprünglichen Klartext. Für die Verschlüsselung wird ein symmetrisches Verschlüsselungsverfahren angewendet und der dafür benötigte geheime Schlüssel wird mittels eines asymmetrischen Verschlüsselungsverfahrens zwischen den Kommunikationspartnern ausgetauscht. Einer der Teilnehmer generiert den geheimen Schlüssel, verschlüsselt diesen mit dem öffentlichen Teil eines privaten Schlüssels des anderen Teilnehmers und übergibt ihn über das Kommunikationssystem an den zweiten Teilnehmer. Dieser entschlüsselt die übergebene, verschlüsselte Größe mit dem geheimen Teil seines Schlüssels und erhält so den geheimen Schlüssel für die Ende-zu-Ende-Verschlüsselung. Die Schlüssel der Ende-zu-Ende-Verschlüsselung sollen dabei zu keiner Zeit außerhalb einer sicheren Umgebung im Klartext erscheinen. Als sichere Umgebung gelten dabei nur die sender- und empfängerseitigen Kommunikationseinrichtungen (Europäische Patentschrift, a.a.O., Rn. [0002], [0004] und [0005]). Die Entschlüsselung des die Nachricht verschlüsselnden Schlüssels erfolgt mithin hiernach bei dem Empfänger der Nachricht mit dessen privatem Schlüssel, der sich ausschließlich in seiner Verfügungsgewalt befindet.

28 (b) Diesen Erfordernissen entspricht der i.R.d. beA verwendete Übermittlungsweg nicht vollständig.

29 (1) Eingehalten ist allerdings – entgegen der Auffassung der Kl. – das Erfordernis, dass die übermittelten Inhalte durchgehend mit demselben Schlüssel verschlüsselt sind, während der gesamten Übertragung durchgängig verschlüsselt bleiben und nur beim Sender und Empfänger unverschlüsselt vorliegen. Weder werden die Nachrichten selbst im HSM umgeschlüsselt noch werden Nachrichten vor der Entschlüsselung durch den berechtigten Empfänger auf dem Übertragungsweg entschlüsselt.

30 Die Bekl. hat den Übermittlungsweg der Nachrichten und das Verschlüsselungssystem mittels des S.-Gutachtens sowie der von der technischen Entwicklerin des beA, der Firma A. GmbH (im Folgenden: A.) erstellten Schaubilder, vorgelegt … . Hieraus ergibt sich, dass eingehende Nachrichten in verschlüsseltem Zustand direkt an das Postfach des Empfängers und von dort an den jeweils berechtigten Leser weitergeleitet werden, ohne dass diese zu irgendeinem Zeitpunkt entschlüsselt werden. Umgeschlüsselt wird nur der Nachrichtenschlüssel, mit dem die Nachricht verschlüsselt ist.

31 Es bestehen keine Anhaltspunkte dafür, dass diese Grundstruktur der Übermittlung und Verschlüsselung von Nachrichten über das beA in dem S.-Gutachten sowie den von der Betreiberin erstellten Schaubildern unzutreffend dargestellt wäre. …

32 (1.1) Im Hinblick auf die dargelegte, im Grundsatz unstreitige Struktur der Nachrichtenübermittlung und -verschlüsselung bestehen keine Anhaltspunkte dafür, dass die Nachricht selbst auf

dem Übermittlungsweg vom Sender zum Empfänger der Nachricht umgeschlüsselt wird. Die Kl. haben dies zwar in erster Instanz behauptet. Konkrete Anhaltspunkte hierfür sind indes auch dem Klägervortrag nicht zu entnehmen. Im Berufungsverfahren haben die Kl. im Gegenteil selbst vorgetragen, dass im beA nicht die Nachricht, sondern der Verschlüsselungsschlüssel der Nachricht entschlüsselt und erneut verschlüsselt werde.

33 (1.2) Keine Anhaltspunkte bestehen auch dafür, dass die Nachrichten nicht durchgängig bis zur Entschlüsselung durch den berechtigten Empfänger verschlüsselt sind. Das S.-Gutachten bestätigt, dass Nachrichteninhalte unverschlüsselt nur bei den Kommunikationspartnern vorliegen … . Die Kl. bestreiten dies zwar. Der betreffende Vortrag ist indes nicht geeignet, die diesbezüglichen Ausführungen im S.-Gutachten in Frage zu stellen. Die Kl. stützen sich insoweit ausschließlich auf einen Beitrag von *Hanno Böck* v. 10.9.2018 auf golem.de, der sich mit einer im S.-Gutachten unter Punkt 5.4.1. benannten, als betriebsverhindernd kategorisierten A-Schwachstelle und einer Stellungnahme der Bekl. hierzu befasst. S. hatte insoweit beanstandet, dass die beA-Client-Security aus mehreren Teilen bestehe, von denen ein Teil als Javascript-Code vom beA-Server ausgeliefert werde, welcher im Browser des Nutzers ausgeführt werde. Dieser Teil steuere die beA-Client-Security, welche für Verschlüsselung, Entschlüsselung und Authentisierung zuständig sei. Ein Innentäter könne diesen Code in der Absicht modifizieren, Nachrichten beim Versenden unverschlüsselt in eine beliebige Richtung zu versenden …

34 Insoweit ging es mithin um eine Sicherheitslücke, die bei einem Angriff durch einen Innentäter dahingehend hätte ausgenutzt werden können, dass Nachrichten unverschlüsselt versendet werden. Unverschlüsselt wären solche Nachrichten mithin nur dann, wenn ein Innentäter das beA-System bewusst und gezielt angreifen würde. Dies ist indes kein geeigneter Maßstab für die Frage, ob das beA seiner Struktur nach eine Verschlüsselung vorsieht, die sicherstellt, dass Nachrichten beim Versender verschlüsselt und erst bei dem berechtigten Empfänger wieder entschlüsselt werden. Die betreffende Sicherheitslücke ändert nichts daran, dass die Nachrichten grds. und im Normalbetrieb verschlüsselt übertragen und auf dem Übertragungsweg nicht entschlüsselt werden. …

37 Auch das aus Sicht der Kl. entscheidende Sicherheitsrisiko, dass die maßgeblichen Schlüssel als verschlüsselte Datei auch außerhalb des HSM vorliegen und hiermit bei missbräuchlicher Verwendung seitens der Bekl. oder der Betreiberin alle Nachrichten entschlüsselt werden könnten, ist für die Beantwortung der Frage, ob die Nachrichten im vorgesehenen Regelbetrieb durchgehend verschlüsselt sind, ohne Bedeutung (s. zu dieser Schwachstelle unten unter 2 a bb (b) (2.2)) [= Rn. 72].

38 (2) Im Unterschied zu dem in der europäischen Patentschrift dargelegten Verfahren der Ende-zu-Ende-Verschlüsselung wird bei dem von der Bekl. errichteten System der die Nachricht verschlüsselnde Schlüssel allerdings nicht direkt an den Empfänger übermittelt und dort entschlüsselt. Vielmehr wird er mit dem in dem externen HSM hinterlegten privaten Postfachschlüssel des Empfängers entschlüsselt und dort i.E. auf den Schlüssel des oder der leseberechtigten Nutzer umgeschlüsselt. Durch diese Umschlüsselung des Schlüssels und die hierfür erforderliche Hinterlegung des privaten Postfachschlüssels im HSM ist die der patentierten Ende-zu-Ende-Verschlüsselung immanente Voraussetzung, dass sich die Schlüssel nur bei den Kommunikationspartnern befinden, nicht erfüllt.

39 bb) Den Kl. steht indes kein Anspruch darauf zu, dass die von der Bekl. gewählte Verschlüsselung unterlassen wird, weil sie keine Ende-zu-Ende-Verschlüsselung in o.g. Sinne darstellt. Denn die Bekl. war weder nach den einfachgesetzlich normierten Vorgaben noch von Verfassungs wegen verpflichtet, eine derartige Verschlüsselung vorzusehen, sodass durch deren Unterlassen nicht in ein subjektiv-öffentliches Recht der Kl. eingegriffen wird.

40 (a) Aus § 31a Abs. 1 oder Abs. 3 BRAO, §§ 130a Abs. 4 Nr. 2, 174 Abs. 3 S. 3 u. S. 4 ZPO ergeben sich keine detaillierten Vorgaben für die Bewerkstelligung der Sicherheit der Nachrichtenübermittlung, insb. keine Verpflichtung zur Nutzung einer Ende-zu-Ende-Verschlüsselung in o.g. Sinne. Denn diese Vorschriften enthalten keine Vorgaben zur technischen Ausgestaltung im Hinblick auf die Sicherheit der Nachrichtenübermittlung, sodass sie den Kl. auch keinen Anspruch auf eine bestimmte Verschlüsselung der zu versendenden Inhalte gewähren.

41 (1) Aus § 31a Abs. 1 S. 1 BRAO ergibt sich lediglich die Verpflichtung der Bekl. zur empfangsbereiten Einrichtung eines beA. Vorgaben für besondere technische Sicherheitsstandards ergeben sich hieraus dagegen nicht.

42 (2) Nach § 31a Abs. 3 S. 1 BRAO hat die Bekl. sicherzustellen, dass der Zugang zum beA nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln möglich ist. Die Norm regelt nur die Sicherheit des Zugangs zum Postfach, nicht jedoch die hier streitgegenständliche Sicherheit der Datenübermittlung.

43 (3) § 130a Abs. 4 Nr. 2 ZPO, wonach der Übermittlungsweg zwischen dem beA und der elektronischen Poststelle des Gerichts als sicher gilt, begründet eine gesetzliche Fallgruppe eines im verfahrensrechtlichen Sinne als sicher geltenden Übermittlungswegs und stellt damit klar, dass Anwälte, die das beA nutzen, den Verpflichtungen aus § 130a Abs. 3 ZPO zur Übermittlung über einen sicheren Übermittlungsweg sowie aus § 174 Abs. 3 S. 4 ZPO zur Eröffnung eines sicheren Übermittlungswegs nachkommen. Aussagen zur technischen Ausgestaltung des beA enthält die Vorschrift ebenso wenig, wie sie den Nutzern einen Anspruch auf eine bestimmte Struktur und Technik zuspricht.

44 (4) Nichts Anderes gilt für § 174 Abs. 3 S. 3 u. S. 4 ZPO. Hieraus ergibt sich – ohne Bezug zum beA und dessen Sicherheit – lediglich die Verpflichtung, dass eine Zustellung an einen Anwalt bzw. eine der weiteren in § 174 Abs. 1 ZPO genannten Personengruppen über einen sicheren Übermittlungsweg i.S.d. § 130a Abs. 4 ZPO zu erfolgen hat. Zugleich sind die in § 174 Abs. 1 ZPO genannten Personengruppen verpflichtet, einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen. Der Verweis u.a. auf das beA in § 130a Abs. 4 Nr. 2 ZPO stellt dabei klar, dass dieses nach der Auffassung des Gesetzgebers ein zulässiger sicherer Übermittlungsweg ist.

45 Entgegen der Auffassung der Kl. ist auch der Gesetzesbegründung zu § 174 Abs. 3 S. 3 ZPO nichts dafür zu entnehmen, dass der Gesetzgeber das elektronische Anwaltspostfach nur mit einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne zulassen wollte. § 174 Abs. 3 S. 3 ZPO regelt, dass eine elektronische Zustellung auf einem sicheren Übermittlungsweg i.S.v. § 130a Abs. 4 ZPO zu erfolgen hat. Diese Regelung wurde durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten v. 10.10.2013 (BGBl. I 3786) eingefügt. Der *Bundesrat* hatte in seiner Stellungnahme hierzu vorgeschlagen, dass die Bezugnahme in § 174 Abs. 3 S. 3 u. S. 4 ZPO-E auf „sichere Übermittlungswege i.S.d. § 130a Abs. 4 ZPO-E" entfallen solle, um eine Beschränkung auf die dort genannten Übermittlungswege zu verhindern (BT-Drs. 17/12634, 46).

46 In diesem Zusammenhang steht die von den Kl. in Bezug genommene Passage der Stellungnahme des *Bundesrats*, wonach die vorgeschlagene Streichung der Bezugnahme auf „sichere Übermittlungswege" i.S.d. § 130a Abs. 4 ZPO-E nicht etwa zur Zulassung unsicherer Übertragungswege führe, da die Anforderung, die Übermittlung „gegen unbefugte Kenntnisnahme Dritter zu schützen", bestehen bleibe und diese beim Einsatz der EGVP-Infrastruktur durch die automatisierte (Ende-zu-Ende-)Verschlüsselung der Daten über das sog. OSCI-Protokoll gewährleistet werde (BT-Drs. 17/12634, 46 f.). Abgesehen davon, dass sich die Stellungnahme des *Bundesrats* nicht auf die Übermittlung mittels des beA, sondern im Gegenteil gerade auf die Übermittlung ohne dessen Nutzung bezieht und sich zur technischen Ausgestaltung des beA nicht verhält, ist der Änderungsvorschlag des *Bundesrats* ohnehin nicht übernommen worden. Dessen Stellungnahme bezieht sich mithin auf einen nicht Gesetz gewordenen Regelungsvorschlag und kann schon deshalb zur Ermittlung des Willens des Gesetzgebers nicht herangezogen werden.

47 (b) Eine Verpflichtung zur Verschlüsselung der über beA übermittelten Inhalte durch eine Ende-zu-Ende-Verschlüsselung, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden und keine Umschlüsselung im HSM stattfindet, ist entgegen der Auffassung der Kl. auch der RAVPV nicht zu entnehmen. Diese Verordnung regelt auf Grundlage von § 31c Nr. 3 BRAO u.a. Einzelheiten der Einrichtung, der technischen Ausgestaltung, der Führung, der Zugangsberechtigung und der Nutzung der elektronischen Anwaltspostfächer.

48 Nach § 19 Abs. 1 RAVPV dient das beA insb. der elektronischen Kommunikation mit den Gerichten sowie der Nutzer untereinander auf einem sicheren Übermittlungsweg. Nach § 20 Abs. 1 RAVPV hat die *BRAK* die beA auf der Grundlage des Protokollstandards „Online Services Computer Interface – OSCI" oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu betreiben und fortlaufend zu gewährleisten, dass die in § 19 Abs. 1 RAVPV genannten Personen und Stellen miteinander sicher elektronisch kommunizieren können.

49 Eine Verpflichtung, i.R.d. beA eine Ende-zu-Ende-Verschlüsselung in o.g. Sinne vorzusehen, enthalten diese Vorschriften nicht. Dies ergibt sich weder aus dem Erfordernis einer sicheren Kommunikation noch aus dem Verweis auf die OSCI-Protokollstandards in § 20 Abs. 1 RAVPV.

50 (1) Die unbestimmten Rechtsbegriffe „sicherer Übermittlungsweg" und „sichere Kommunikation" sind weder in §§ 19 Abs. 1 u. 20 Abs. 1 RAVPV noch an anderer Stelle der RAVPV näher definiert. Sie sind jedenfalls nicht dahingehend auszulegen, dass damit ausschließlich eine Übermittlung mittels einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne gemeint ist.

51 (1.1) Der Wortlaut impliziert eine technische Offenheit. Ihm ist nicht zu entnehmen, dass nur eine bestimmte Verschlüsselungsart als sicherer Übermittlungsweg anzusehen ist, vielmehr wird neutral und ohne technische Vorgaben allein auf das ausfüllungsbedürftige Kriterium der Sicherheit abgestellt. Dies spricht dafür, dass für die technische Umsetzung im Detail ein Spielraum besteht, sofern das Kriterium der Sicherheit beachtet wird.

52 (1.2) Sinn und Zweck der Vorschrift bestätigen ebenfalls die technische Offenheit und sprechen gegen eine Festlegung auf eine bestimmte Verschlüsselungstechnik. Bezweckt ist mit diesen Regelungen, dass ein zuverlässiges und sicheres Kommunikationsmittel für den elektronischen Rechtsverkehr zwischen den Rechtsanwälten und Gerichten sowie zwischen den Rechtsanwälten untereinander zur Verfügung gestellt wird (Begründung zu § 19 RAVPV, BR-Drs. 417/16, 34). Dieser Vorgabe ist nicht zu entnehmen, dass zwingend eine Ende-zu-Ende-Verschlüsselung nach o.g. Kriterien gegeben sein muss. Die offen gefasste, lediglich auf den Begriff der Sicherheit abstellende Formulierung erlaubt der Bekl., durch ein technisches Gesamtkonzept den besonderen Erfordernissen der Kommunikation über beA in ihrer Gesamtheit Rechnung zu tragen. Wie aus §§ 20 Abs. 1 S. 1 Hs. 2 u. 20 Abs. 1 S. 2 RAVPV hervorgeht, steht der Bekl. hierbei ein Spielraum zur Anpassung an technische Neuerungen zu.

53 (1.3) Auch die Systematik spricht dafür, dass der Verordnungsgeber die konkrete Art der Verschlüsselung nicht abschließend zu Gunsten einer bestimmten technischen Lösung regeln, sondern der Bekl. hinsichtlich der technischen Umsetzung einen gewissen Spielraum belassen wollte, solange gemessen am aktuellen Stand der Technik eine sichere Kommunikation gewährleistet ist. Das von der Bekl. zu errichtende System hat nicht nur den Erfordernissen einer sicheren Kommunikation zwischen zwei Kommunikationspartnern zu genügen, sondern muss auch eine Nutzung durch Vertreter, Abwickler und Zustellungsbevollmächtigte ermöglichen (§ 31a Abs. 3 S. 2 BRAO, § 25 RAVPV) und den vom Postfachinhaber Dritten nach § 23 RAVPV gewährten Zugang zu seinem besonderen elektronischen Postfach sicher regeln. Die Verordnung bestimmt das technische Gesamtkonzept nicht in allen Details, sondern belässt der Bekl. einen Umsetzungsspielraum, wobei vorgegeben wird, durch wen und wozu das System nutzbar sein und welcher Mindeststandard eingehalten sein muss (vgl. für einen Spielraum z.B. §§ 22 Abs. 3, 23 Abs. 1 u. 24 Abs. 1 RAVPV). Zugleich hat der Verordnungsgeber an anderer Stelle teils sehr konkrete Vorgaben gemacht (vgl. z.B. § 25 Abs. 3 RAVPV). Dem ist zu entnehmen, dass der Verordnungsgeber bewusst teils sehr konkrete Vorgaben in den Verordnungstext aufgenommen hat, an anderer Stelle aber Spielraum für die technische Umsetzung unter Einhaltung der im Verordnungstext vorgesehenen Standards gewährt.

54 Die technische Nachrichtenübermittlung nach § 20 RAVPV zählt zu den Regelungen, bei denen der Verordnungsgeber erkennbar zwar einen bestimmten Rahmen gesteckt, innerhalb dieses Rahmens jedoch keine detaillierten technischen Vorgaben formuliert hat. Diese Offenheit auch für künftige Entwicklungen zeigt sich u.a. darin, dass in § 20 Abs. 1 RAVPV auf den OSCI-Standard oder einen künftig nach dem Stand der Technik an dessen Stelle tretenden Standard verwiesen wird. Eine Festlegung auf ein Detail des Gesamtprozesses – wie eine Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift EP 0 877 507 B 1 v. 26.9.2007 – widerspräche dem, zumal der Verordnungsgeber die von den Kl. befürwortete Nachrichtenverschlüsselung i.S.d. bei Erlass der Verordnung bereits über einen Zeitraum von neun Jahren bestehenden europäischen Patentschrift ohne Weiteres verbindlich in § 20 Abs. 1 RAVPV hätte vorgeben können, wenn er dies gewollt hätte. Auch dies spricht dafür, dass der Verordnungsgeber mit Rücksicht auf die technische Komplexität des Gesamtsystems sowie die fortlaufende Weiterentwicklung im Bereich der elektronischen Kommunikation eine technische Offenheit gewährleisten wollte, die es bewusst vermeidet, die Bekl. auf eine bestimmte technische Lösung festzulegen.

55 (1.4) Die historische Entwicklung der RAVPV zeigt, dass dem Verordnungsgeber bei deren Verabschiedung bereits das später in die Praxis umgesetzte System der beA bekannt war und dieses von ihm gebilligt und damit als sicherer Kommunikationsweg angesehen wurde. Die Bekl. hat unwidersprochen vorgetragen, dass im Zeitpunkt des Erlasses von §§ 19 u. 20 RAVPV die von

den Kl. kritisierte Architektur des beA einschließlich der Umschlüsselung des Schlüssels im HSM bereits feststand und sie diese immer wieder mit den zuständigen Referatsleitern des *BMJV* erörtert hat. Auch die Kl. gehen davon aus, dass sich das Ministerium über Jahre hinweg in einem stetigen Austausch mit der Bekl. befand. …

57 Die Kenntnis des Verordnungsgebers von der bereits erarbeiteten Grundstruktur des beA unter Einschluss des HSM vor Erlass der Verordnung spricht dafür, dass der Verordnungsgeber diese Struktur gebilligt hat und diese von seinem Willen umfasst ist. Dies gilt umso mehr, als er in keiner Weise i.R.d. Verordnung oder deren Begründung zum Ausdruck gebracht hat, dass gegen das damals bereits erarbeitete System bzgl. des vorgesehenen Übermittlungswegs von Nachrichten unter Umschlüsselung des zur Verschlüsselung der Inhalte verwendeten Schlüssels im HSM Bedenken bestehen. Hieraus folgt zugleich, dass der Verordnungsgeber durch die Verwendung der Begriffe „sichere Kommunikation" und „sicherer Übermittlungsweg" nicht ausschließlich eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne gemeint hat.

58 (1.5) Nichts Anderes ergibt sich aus den Gesetzesmaterialien.

59 Unstreitig ist zwischen den Parteien, dass die Bekl. bis Februar 2018 öffentlich davon sprach, dass das beA eine „Ende-zu-Ende-Verschlüsselung" der Nachrichten vorsehe, obgleich die gewählte Struktur wegen der Umschlüsselung der Schlüssel im HSM nicht der Definition einer Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patents entsprach (vgl. hierzu oben 2 a aa)). Anhaltspunkte dafür, dass die Bekl. diesen Begriff etwa zur Täuschung des *BMJV* als Verordnungsgeber, der Anwaltschaft oder der allgemeinen Öffentlichkeit über die Sicherheit des Systems bewusst unzutreffend eingesetzt hätte, wie dies die Kl. behaupten, bestehen nicht. … Im Hinblick darauf, dass ein wesentliches Kernelement der Ende-zu-Ende-Verschlüsselung eingehalten war und die Bekl. zugleich das vorgesehene Verschlüsselungssystem und die Verwendung eines HSM öffentlich bekannt gemacht und auf Kammerversammlungen und Veranstaltungen des *EDV-Gerichtstags* erläutert hat, hält der *Senat* eine bewusste Täuschung durch die Bekl. für fernliegend.

60 Vor diesem Hintergrund ist § 20 RAVPV eine Verpflichtung zur Ende-zu-Ende-Verschlüsselung ohne Verwendung des HSM auch nicht deshalb zu entnehmen, weil der Verordnungsgeber in seiner Begründung zu §§ 20 Abs. 1 sowie zu 19 Abs. 2 RAVPV die Ende-zu-Ende-Verschlüsselung erwähnt hat. So wird in der Begründung zu § 20 Abs. 1 RAVPV ausgeführt, dass der Betrieb der beA zur Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung auf der Grundlage des Protokollstandards OSCI oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu erfolgen hat (BR-Drs. 417/16, 35). In der Begründung zu § 19 Abs. 2 RAVPV heißt es zur künftigen Ermöglichung einer Kommunikation auch mit Dritten über beA, dass dies insb. die Kommunikationsmöglichkeiten erfassen könne, die bereits jetzt in der Struktur des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP), in die auch das beA eingebettet sei, vorgesehen seien. Soweit auch dabei stets die Beachtung der elementaren Grundelemente des beA (wie z.B. die Ende-zu-Ende-Verschlüsselung von Nachrichten) sichergestellt sein müsse, werde dies dadurch gewährleistet, dass auch für die Kommunikation mit anderen Stellen und Personen die Vorgaben des § 20 Abs. 1 RAVPV gelten würden.

61 Es ist indes nicht davon auszugehen, dass der Verordnungsgeber durch die Verwendung des Begriffs „Ende-zu-Ende-Verschlüsselung" das von der Bekl. erstellte, ihm bekannte Konzept für unzulässig erklären und die Einhaltung einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne vorschreiben wollte. Vielmehr spricht alles dafür, dass der Verordnungsgeber der öffentlich bis 2018 von der *BRAK* verwendeten, technisch ungenauen Begrifflichkeit einer „Ende-zu-Ende-Verschlüsselung" gefolgt ist und hiermit auch das bereits konzipierte Verfahren gemeint hat, bei dem die Nachrichten verschlüsselt übertragen und nur vom berechtigten Empfänger entschlüsselt werden können, während die Schlüssel im HSM umgeschlüsselt werden. Die gewählte Formulierung „Ende-zu-Ende-Verschlüsselung von Nachrichten" in der Begründung zu § 19 RAVPV bestätigt diesen Fokus auf die Verschlüsselung der Nachricht an sich, also des Inhalts.

62 Der *Senat* hält es für ausgeschlossen, dass der Verordnungsgeber allein durch eine nicht in den Verordnungstext aufgenommene Formulierung in der Begründung des Verordnungsentwurfs abweichend von dem ihm bekannten und veröffentlichten Verschlüsselungskonzept unter Einschluss des HSM eine Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift vorgeben wollte. Denn eine solche Vorgabe hätte zur Folge gehabt, dass das beA in der konzipierten Form nicht hätte in Betrieb genommen werden können und die Grundstruktur grundlegend hätte überarbeitet werden müssen. Es ist anzunehmen, dass der Verordnungsgeber derart gravierende Folgen ausdrücklich thematisiert und kommuniziert hätte, wären diese beabsichtigt gewesen.

63 (1.6) Eine verfassungskonforme Auslegung von §§ 19 u. 20 RAVPV dahingehend, dass zwingend eine Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift vorzusehen ist, ist nicht geboten. Es genügt den verfassungsrechtlichen Anforderungen, dass die einschlägigen Normen dem Grunde nach ein sicheres Übermittlungsverfahren vorschreiben. Hierdurch ist dem rechtlich geschützten Vertrauensverhältnis zwischen Rechtsanwalt und Mandant (vgl. hierzu BVerfGE 113, 29 (49); B. v. 29.1.2015 – 2 BvR 497/12, Rn. 18) in ausreichendem Maße Rechnung getragen. Es steht dem Gesetzgeber frei, die technische Konkretisierung des gesetzlich vorgegebenen Maßstabs der Bekl. als Körperschaft des öffentlichen Rechts anzuvertrauen (vgl. für Aufsichtsbehörden im Bereich der Telekommunikation: BVerfGE 125, 260 (327) [= MMR 2010, 356]).

64 Entgegen der Auffassung der Kl. ergibt sich auch aus dem Nichtannahmebeschluss des *BVerfG* v. 20.12.2017 – 1 BvR 2233/17 nicht, dass §§ 19 u. 20 RAVPV verfassungskonform dahingehend auszulegen wären, dass das beA eine Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift gewährleisten müsste. Zwar hat das *BVerfG* in diesem Beschluss entsprechend der damals von der Bekl. verwendeten, in der Begründung zu § 20 Abs. 1 RAVPV enthaltenen Terminologie von einer Ende-zu-Ende-Verschlüsselung gesprochen. So führt das *BVerfG* in diesem Beschluss unter Verweis auf § 20 Abs. 1 RAVPV aus, dass das beA zur sicheren Übermittlung eine sog. Ende-zu-Ende-Verschlüsselung verwende (*BVerfG*, a.a.O., Rn. 5). Weiter wird in der Begründung darauf abgestellt, dass es in der Beschwerdeschrift an einer Auseinandersetzung mit den konkret getroffenen Sicherheitsvorkehrungen wie etwa der Ende-zu-Ende-Verschlüsselung fehle (a.a.O., Rn. 14). Damit ist indes nicht gesagt, dass das *BVerfG* eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne für gegeben sowie für geboten erachtete. Mit den technischen Details der beA-Struktur hat sich das *BVerfG* in diesem Beschluss nicht auseinandergesetzt. Erst Recht hat das *BVerfG* weder – wie die Kl. meinen – § 20 Abs. 1 RAVPV dahingehend ausgelegt, dass die Bekl. eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne gewährleisten müsse noch hat es dies für verfassungsrechtlich geboten erklärt. Der Nichtannahmebeschluss, dem ohnehin als Prozessentscheidung keine Bindungswirkung i.S.v. § 31 Abs. 1 BVerfGG zukommt, befasst sich hiermit schon nicht.

65 (2) Die Bekl. war auch nicht deshalb gehalten, eine Ende-zu-Ende-Verschlüsselung in dem von den Kl geforderten Sinne unter Verzicht auf eine Umschlüsselung der Schlüssel im HSM vorzusehen, weil einzig hierdurch die von § 20 Abs. 1 RAVPV geforderte sichere Kommunikation gewährleistet werden könnte. Ein Erfolg der Klage unter dem Aspekt der Sicherheit der Kommunikation setzte dies indes voraus. Denn die Klage ist ausdrücklich nur darauf gerichtet, das weitere Betreiben des bestehenden Verschlüsselungssystems im Hinblick auf die fehlende Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne zu unterlassen sowie das beA mit einer derartigen Verschlüsselung zu betreiben. Kann jedoch auch ein anderes System eine hinreichende Sicherheit gewährleisten, besteht kein Anspruch auf die von den Kl. geforderte Verschlüsselungstechnik. Eine sicherheitsrelevante Schwachstelle des bestehenden Systems könnte den von den Kl. geltend gemachten Anspruch auf Nutzung einer bestimmten Verschlüsselungstechnik nur dann begründen, wenn diese nicht behebbar wäre und damit eine fortlaufende Gefahr für die Sicherheit der Kommunikation darstellte. Denn nur in diesem Fall könnte diese Schwachstelle dazu führen, dass das gewählte System seiner Struktur nach keine sichere Kommunikation gewährleisten könnte und die *BRAK* den ihr zustehenden Spielraum für die technische Gestaltung durch die gewählte Technik überschritten hätte. Der von den Kl. geltend gemachte Anspruch auf eine bestimmte Verschlüsselungstechnik könnte sich hieraus nur unter der weiteren Voraussetzung ergeben, dass nicht ein sonstiges hinreichend sicheres System existierte.

66 Es ist auf Grundlage des von beiden Parteien vorgelegen S.-Gutachtens sowie des Parteivorbringens davon auszugehen, dass – i.V.m. entsprechenden organisatorischen Sicherheitsvorkehrungen beim Betreiber des beA und der Bekl. – auch das von der Bekl. gewählte System in ausreichendem Maße die erforderliche sichere Kommunikation gewährleisten kann. Nicht behebbare Sicherheitsmängel ergeben sich weder aus dem Sachvortrag der Parteien noch sind sie sonst ersichtlich.

67 Sicherheit ist hierbei nicht i.S.e. absoluten Sicherheit zu verstehen, die jegliches Risiko ausschließt. Eine solche Sicherheit existiert im Bereich der elektronischen Kommunikation nicht. Zu Recht hat der *AGH* hierzu ausgeführt, dass Sicherheit nur ein relativer Zustand der Gefahrenfreiheit bedeutet, Beeinträchtigungen nicht vollständig ausgeschlossen werden können und stets ein Restrisiko eines Angriffs auf übermittelte Daten verbleibt.

68 Eine sichere Kommunikation im Rechtssinne setzt demnach nicht eine Freiheit von jeglichen Risiken voraus. Das gewählte Übermittlungssystem muss einen Sicherheitsstandard erreichen, bei dem unter Berücksichtigung der Funktionalität nach dem Stand der Technik die Übermittlung voraussichtlich störungs- und gefahrfrei erfolgt und Risiken für die Vertraulichkeit möglichst weitgehend ausgeschlossen werden. Dementsprechend hat der *AGH* darauf abgestellt, dass Sicherheit erfordere, dass ein Schadenseintritt hinreichend unwahrscheinlich sei und insgesamt ein Zustand als sicher gelten könne, der unter Berücksichtigung der Funktionalität und Standards frei von unvertretbaren Risiken sei.

69 Der *Senat* teilt auf Grundlage des Sach- und Streitstands die Auffassung des *AGH*, wonach die Übermittlung von Nachrichten unter Einsatz der beA eine Sicherheit in diesem Sinne gewährleisten kann, wobei zu berücksichtigen ist, dass die für die Sicherheitsbeurteilung erforderliche Risikoermittlung und -bewertung stets eine Prognose über mögliche künftige Bedrohungen und deren Eintrittswahrscheinlichkeit bedingt und somit auch insoweit Unsicherheiten beinhaltet. Diese sind indes nicht vermeidbar und deshalb hinzunehmen, sofern die Einschätzung auf Grundlage fachwissenschaftlicher Maßstäbe methodisch fachgerecht erfolgte (vgl. *BVerwG* NVwZ-RR 1991, 129 (131) für die Sicherheitsanforderungen beim Flughafenbau).

70 (2.1) Das S.-Gutachten kommt zu dem Ergebnis, dass das dem beA zu Grunde liegende Verschlüsselungskonzept geeignet ist, die Vertraulichkeit der Nachrichten während der Übertragung und Speicherung durch das beA zu gewährleisten, auch ggü. dem Betreiber des beA. Die Umverschlüsselung sei in einem HSM gekapselt und schütze daher dort vorübergehend entstehende Schlüsselinformationen in einer besonderen manipulations- und ausspähsicheren Umgebung (S.-Gutachten, S. 11).

71 Die i.R.d. gutachterlichen Prüfung aufgezeigten, als betriebsverhindernd eingestuften Schwachstellen sind nach dem Vortrag der Bekl. vor der Wiederinbetriebnahme des beA beseitigt worden, was von der S. nach erneuter Begutachtung bestätigt wurde. Der entsprechenden Feststellung des *AGH* sind die Kl. in der Berufungsinstanz nicht entgegengetreten.

72 (2.2) Umstände, die trotz dieser fachwissenschaftlichen Sicherheitsüberprüfung einer Einstufung als sicher im Rechtssinne entgegenstehen und für die Annahme eines nicht hinreichend sicheren Kommunikationswegs sprechen würden, sind nicht ersichtlich. Sie ergeben sich auch nicht aus dem Vorbringen der Kl. Diese halten es für das entscheidende Sicherheitsrisiko des beA, dass es möglich sei, mit einem einzigen Angriff anwaltliche und gerichtliche Korrespondenz heimlich auszuspähen. Die Kl. beziehen sich hierbei auf die im S.-Gutachten unter 5.5.3 dargelegte Schwachstelle. Dort wird bemängelt, dass die Arbeitsschlüssel, die das HSM zur verschlüsselten Ablage und zur Umverschlüsselung verwendet, sowie die diese Arbeitsschlüssel verschlüsselnden Key Encryption Keys (KEKs) auch außerhalb des HSM als verschlüsselte Datei vorliegen, da diese nach deren Erzeugung vom Betreiber des beA an die Bekl. als Auftraggeberin übergeben worden seien und dort verwahrt würden. Im S.-Gutachten heißt es hierzu, dass die Sicherheit der KEK durch Schlüsselteilung, physikalisch getrennte Verwahrung und physikalisch auf spezifische Mitarbeiter des Auftraggebers, die sog. Key Custodians, beschränkten Zugriff geschützt sei. Die beiden Teile des KEK, die nur zusammen die Entschlüsselung und das Einspielen der Master-Schlüssel in ein HSM erlaubten, seien auf Papier in versiegelten Briefumschlägen in Safes verwahrt (S.-Gutachten, S. 78). Wer sich allerdings in den Besitz des Schlüsselmaterials bringe, könne die im beA-System gespeicherten Nachrichten auch ohne HSM entschlüsseln. Der Missbrauch könne auf zwei Arten geschehen: Die Key Custodians der Bekl. und ein Helfer beim Betreiber des beA könnten den verschlüsselten Nachrichtenbestand und die Schlüssel zusammenbringen und dann die Nachrichten entschlüsseln. Die zweite Missbrauchsmöglichkeit sei gegeben, wenn beim Betreiber des beA nach der Erzeugung der Schlüssel und vor der Übergabe an den Auftraggeber an einer Stelle eine Kopie erstellt worden sei. Dann könne das Personal des Betreibers alleine die Nachrichten entschlüsseln …

73 S. hat diese Schwachstelle als betriebsbehindernd eingeordnet. Die Bedrohung der Vertraulichkeit werde als hoch eingeschätzt, weil ein Angriff die umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten erlaube. Die Ausnutzbarkeit werde dagegen als niedrig bewertet, weil der Angriff nur durch bestimmte Innentäter durchführbar sei, die dabei eine Vertrauensstellung haben müssten, die sie missbrauchten …

74 Bereits die von den Parteien nicht in Frage gestellte Schilderung der Manipulationsmöglichkeiten im S.-Gutachten zeigt, dass ein entsprechender Angriff zwar die Vertraulichkeit der Kommunikation in ganz erheblichem Maße verletzen würde, die Gefahr eines solchen Angriffs indes als gering einzustufen

ist. Zum einen bedürfte es hierfür des Missbrauchs durch Innentäter, die eine besondere Vertrauensstellung innehaben. Anhaltspunkte für einen bereits im Zuge der damaligen Schlüsselerstellung und -übermittlung erfolgten Missbrauch seitens der Betreiberfirma bestehen nicht. Vor einem zukünftigen Angriff unter Verwendung der externen Schlüsselinformationen schützen erhebliche Sicherheitsvorkehrungen: Die für den Angriff erforderlichen, außerhalb des HSM bei der Bekl. aufbewahrten KEKs sind in zwei Teile aufgeteilt und – mit getrenntem Zugriff auf jeden Teil durch einen Key Custodian – aufbewahrt, sodass ein Zugriff hierauf eines kollusiven Zusammenwirkens mehrerer Vertrauenspersonen bedürfte. Um sodann Zugriff auf die Nachrichten zu erhalten, müssten in weiterem kollusiven Zusammenwirken mit einem Mitarbeiter des Betreibers der verschlüsselte Nachrichtenbestand und die Schlüssel zusammengeführt werden.

75 Die Bekl. hat ergänzend eine Stellungnahme der Betreiberin A. vom Januar 2018 vorgelegt, in der die Schritte, die dafür erforderlich wären, damit sich ein Mitarbeiter der Bekl. oder ein Mitarbeiter der Betreiberin Kenntnis vom Inhalt von Nachrichten verschaffen kann, im Einzelnen dargelegt sind. Hiernach müsste sich ein solcher Täter zunächst den nach dem Prinzip des splitknowlege in zwei getrennten Teilen sicher bei der Bekl. verwahrten KEK beschaffen, hiermit den verschlüsselten Arbeitsschlüssel, sodann aus der verschlüsselten beA-Datenbank die SAFE-ID eines Anwalts, die mit dem Arbeitsschlüssel verschlüsselten Nachrichtenschlüssel und die Nachrichten für diesen Anwalt. Anschließend müsste er mit dem KEK den Arbeitsschlüssel, mit diesem die Nachrichtenschlüssel und mit den entschlüsselten Nachrichtenschlüsseln die Nachrichten selbst entschlüsseln. A. kommt hierbei zu dem Schluss, dass auf Grund der Vielzahl an notwendigen Schritten und Informationen jeder einzelne Schritt mit Blick auf die jeweiligen Sicherheitsmaßnahmen unwahrscheinlich, das Durchlaufen aller dieser Schritte abwegig und eine Bedrohung daher nicht gegeben sei. Die Kl. sind dem nicht entgegengetreten. Anhaltspunkte dafür, dass demgegenüber das von den Kl. befürchtete Ausspähen der Nachrichten mittels eines gezielten Angriffs auf einfacherem Wege möglich wäre, bestehen auch nach dem Vorbringen der Kl. nicht.

76 Jedenfalls führt diese Schwachstelle unabhängig davon, ob sie – wie die Bekl. im Berufungsverfahren geltend gemacht und zuletzt ausführlich beschrieben hat – zwischenzeitlich behoben ist, nicht dazu, dass die Nachrichtenübermittlung über das beA-System grds. als nicht sicher anzusehen und deshalb die von den Kl. geforderte Ende-zu-Ende-Verschlüsselung als einzig sichere Verschlüsselungstechnik erforderlich wäre. Denn ein auf den Aspekt der Sicherheit gestützter Anspruch der Kl. auf Unterlassung ohne und Betreiben mit der von ihnen geforderten Verschlüsselungstechnik scheidet trotz der genannten Schwachstelle schon deshalb aus, weil diese nach den unangegriffenen Ausführungen von S. einfach behoben werden kann. Hierzu schlägt S. vor, dass die HSMs die Arbeitsschlüssel selbst erzeugen sollen, diese nur in verschlüsselter Form zur Übertragung auf andere HSMs herausgegeben werden sollen und alle HSM-Schlüssel nur innerhalb speziell gesicherter Hardware (HSM, Chipkarte) gespeichert werden. Die Schwachstelle ist mithin behebbar, indem auf die Verfügbarkeit der Arbeitsschlüssel sowie der KEKs außerhalb des HSM verzichtet wird. Durch die Verwendung von neuem Schlüsselmaterial wäre auch eine Sicherheitsgefahr durch etwaige Schlüsselkopien, die bei Erzeugung der ursprünglichen Schlüssel missbräuchlich erstellt worden sein könnten, gebannt. Nicht überzeugend ist der Einwand der Kl. gegen diese Lösungsmöglichkeit, dass hierdurch immer noch keine Ende-zu-Ende-Verschlüsselung vorgesehen sei und das System deshalb weiter unsicher sei. Denn das nach Auffassung der Kl. maßgebliche und entscheidende Sicherheitsrisiko, das darin bestehe, dass durch die Aufbewahrung der Schlüssel auch außerhalb des HSM die Möglichkeit des Ausspähens der gesamten beA-Kommunikation durch einen einzigen erfolgreichen Angriff ohne weitere Manipulation des HSM geschaffen werde, wäre durch die von S. vorgeschlagene Lösung behoben, ohne dass es hierzu einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. gewünschten Sinn bedürfte.

77 Das im S.-Gutachten im Zusammenhang mit dieser Schwachstelle angesprochene mögliche Risiko, dass der Betreiber i.R.v. Beschlagnahmen von Postfächern gezwungen werden könne, Nachrichten offenzulegen, stellt – wie der *AGH* zutreffend ausführt – schon keine Beeinträchtigung der Sicherheit des Übermittlungswegs dar.

78 An dieser Beurteilung ändert sich nichts dadurch, dass in einer von Klägerseite vorgelegten Vorversion des S.-Gutachtens v. 30.5.2018 die betreffende Schwachstelle noch als betriebsverhindernd eingestuft und zur Beschreibung der Schwachstelle ein teilweise abweichender Wortlaut verwendet worden war.

79 Zum einen ist eine nicht endgültige Arbeitsversion, die im Zuge der Begutachtung erstellt wurde, nicht maßgeblich. I.R.d. Erarbeitung von Schriftstücken wie Schriftsätzen oder Gutachten existieren regelmäßig mehrere Vorversionen. Entscheidende Beurteilungsgrundlage ist nur die letzte, vom Ersteller als endgültig herausgegebene Version und nicht ein Vorentwurf. Während der noch nicht abgeschlossenen Bearbeitungsphase ergeben sich regelmäßig noch Änderungen. Dies gilt hier schon deshalb, weil S. nicht ein abgeschlossenes System begutachtet hat, sondern fortlaufend während der Begutachtung identifizierte Schwachstellen behoben wurden. Nur die letzte abschließende Version enthält die endgültige Einschätzung des Gutachters, für die dieser einsteht und ggf. haftet. ...

82 (2.3) Sonstige weder behobene noch behebbare Sicherheitsmängel, die die Übermittlung mittels des beA als nicht hinreichend sicher erscheinen lassen und die Verwendung der von den Kl. geforderten Verschlüsselungstechnik als einzig sichere Variante gebieten würden, sind nicht ersichtlich und von den Kl. auch nicht vorgetragen. ...

83 Dafür, dass nur die von den Kl. geforderte Ende-zu-Ende-Verschlüsselung dem Stand der Technik entspräche und diese deshalb von der Bekl. verwendet werden müsste, bestehen keine Anhaltspunkte. Zwar mag diese Ende-zu-Ende-Verschlüsselung weit verbreitet sein. Dies bedeutet indes nicht, dass nicht auch das von der Bekl. gewählte Modell dem Stand der Technik entspricht, wovon der *Senat* auf Grundlage des S.-Gutachtens ausgeht. Aus diesem Gutachten geht – von den Kl. unwidersprochen – hervor, dass ein HSM auch in weiteren sicherheitsrelevanten Bereichen üblich ist. Das S.-Gutachten hat insoweit darauf verwiesen, dass das von der Bekl. verwendete HSM auch im Bankenwesen Anwendung findet. In dem von den Kl. vorgelegten Schreiben der Bekl. v. 30.1.2018 an die Präsidenten der Rechtsanwaltskammern, in dem diese über den beAThon am 26.1.2018 berichtet, ist davon die Rede, dass eine große Mehrheit der anwesenden IT-Experten anerkannt hätten, dass das HSM Industriestandard darstelle und ein hohes Sicherheitsniveau gewährleiste, sofern es entsprechende Verhaltensregeln für den Betreiber der Infrastruktur des beA gebe. Anhaltspunkte dafür, dass dem widersprechend die Verwendung des HSM veraltet und nicht oder nicht mehr dem Stand der Technik entspräche, bestehen nicht.

84 Vor diesem Hintergrund teilt der *Senat* die Auffassung des *AGH*, dass die Einholung eines Sachverständigengutachtens zur Sicherheit des beA – auch unter Berücksichtigung des Amtsermittlungsgrundsatzes – nicht erforderlich ist. Mit dem S.-Gutachten liegt eine Begutachtung durch einen unabhängigen Ex-

perten vor, auf die sich i.Ü. beide Parteien i.R.d. Verfahrens mehrfach bezogen haben. Insb. haben auch die Kl. die Frage, unter welchen Voraussetzungen unbefugte Dritte Kenntnis zuzustellender Dokumente erlangen könnten, als durch das S.-Gutachten geklärt angesehen, und sich – ebenso wie die Bekl. – ausdrücklich gegen eine von dem *AGH* zunächst beabsichtigte Einholung eines weiteren Sachverständigengutachtens gewandt.

85 (3) Das Erfordernis einer Ende-zu-Ende-Verschlüsselung ohne Umschlüsselung der Schlüssel im HSM ergibt sich auch nicht daraus, dass § 20 Abs. 1 RAVPV die Bekl. verpflichtet, die beA auf der Grundlage des Protokollstandards OSCI oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu betreiben.

86 Die beA werden auf Grundlage des Protokollstandards OSCI i.S.d. Vorschrift betrieben. Eine Ende-zu-Ende-Verschlüsselung ohne Umschlüsselung der Schlüssel im HSM erfordert dies nicht.

87 (3.1) Der Verweis auf den Protokollstandard OSCI ist so zu verstehen, dass die für die Registrierung als Drittanwendung am OSCI gestützten elektronischen Rechtsverkehr erforderlichen Voraussetzungen einzuhalten sind.

88 In der Begründung zu § 20 Abs. 1 RAVPV wird ausgeführt, dass der Betrieb auf der Grundlage des OSCI-Standards zur Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung zu erfolgen hat. Etwaige technische Änderungen seitens der Justiz, auf Grund derer eine sichere elektronische Kommunikation der Inhaber beA mit der Justiz nicht mehr jederzeit und vollumfänglich gewährleistet sei, habe die BRAK nachzuvollziehen (BR-Drs. 417/16, 35 f.). Auf diese sichere elektronische Kommunikation mit der Justiz bezieht sich auch der Verweis auf den OSCI-Standard. Denn hierfür bedarf es einer Einbindung des elektronischen Anwaltspostfachs in die Infrastruktur des EGVP. Das EGVP ist eine elektronische Kommunikationsinfrastruktur für die verschlüsselte Übertragung von Dokumenten und Akten zwischen authentifizierten Teilnehmern. Dem EGVP liegt der OSCI-Standard zu Grunde. Drittprodukte wie das beA, die Sende- und Empfangskomponenten für die Teilnahme an der EGVP-Infrastruktur bereitstellen, müssen für die Teilnahme am OSCI gestützten elektronischen Rechtsverkehr registriert werden. Dies setzt voraus, dass die für die Teilnahme von Drittanwendern am OSCI gestützten elektronischen Rechtsverkehr erforderlichen Anforderungen, wie sie von der Arbeitsgruppe „IT-Standards in der Justiz" erstellt wurden (abrufbar unter: https://egvp.justiz.de/Drittprodukte/index.php), eingehalten werden. Dort heißt es unter 3.2. zu den Grundlagen des Protokollstandards OSCI, dass OSCI-Transport-Nachrichten einen zweistufigen „Sicherheitscontainer" hätten. Hierdurch sei es möglich, Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptografisch unterschiedlich zu behandeln. Inhaltsdaten würden vom sog. Autor einer OSCI-Nachricht so verschlüsselt, dass nur der berechtigte Leser sie dechiffrieren könne. Es werde hier oft von dem „Prinzip des doppelten Umschlags" gesprochen: Die verschlüsselten Inhaltsdaten seien wiederum in einen verschlüsselten Container eingebettet. Als entscheidendes und für die Registrierung als Drittanwender unabdingbares Sicherheitsmerkmal wird demnach ein zweistufiger Sicherheitscontainer angesehen unter Trennung von Inhalts- und Nutzerdaten sowie ein durchgehender kryptografischer Schutz der Inhaltsdaten. Eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne wird hierbei nicht vorgegeben.

89 Der Verweis in § 20 Abs. 1 RAVPV auf die Grundlagen des OSCI-Standards ist vor diesem Hintergrund als Verweis auf die in dem Anforderungsprofil für die Registrierung als Drittprodukt genannten Grundlagen zu sehen, insb. auch auf das als wesentliches Sicherheitsmerkmal angesehene „ContainerModell". Er ist damit so zu verstehen, dass das beA die Anforderungen einhalten muss, um seiner vorgesehenen Verwendung entsprechend als Drittanwendung am OSCI gestützten Rechtsverkehr registriert werden zu können, ohne das[s] es darauf ankommt, ob darüber hinaus jede für die Registrierung nicht geforderte technische Einzelheit der OSCI-Standards eingehalten ist.

90 Dieses Verständnis des Verweises auf den OSCI-Standard bestätigt auch der jüngste Regierungsentwurf eines Gesetzes zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer prozessrechtlicher Vorschriften v. 12.2.2021 (BR-Drs. 145/21). Dort wird für das zur Einführung vorgesehene besondere elektronische Bürger- und Organisationspostfach bestimmt, dass dieses auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht (§ 10 Abs. 1 Nr. 1 ERVV-E). In der Begründung hierzu wird erläutert, dass OSCI-Transport-Nachrichten einen zweistufigen „Sicherheitscontainer" hätten. Hierdurch seien Vertraulichkeit, Integrität und Authentizität der Nachrichten gewährleistet. Eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne wird dagegen nicht für erforderlich erklärt.

91 Dieses Ergebnis wird dadurch bestätigt, dass – wie oben ausgeführt – die Struktur des beA vor Erlass der RAVPV bekannt war und der Verordnungsgeber die Verordnung in Kenntnis und Billigung dieser Struktur erlassen hat. Deshalb ist nicht davon auszugehen, dass der Verordnungsgeber mit dem Verweis auf die Grundlagen des Protokollstandards OSCI weitergehende oder anderslautende Anforderungen an die Verschlüsselung stellen wollte als das ihm bekannte Konzept, das planmäßig auf die Einhaltung der Anforderungen für die bestimmungsgemäße Registrierung als Drittanwendung ausgerichtet war, dies vorsah.

92 Der o.g. Regierungsentwurf bestätigt dies: Ausdrücklich wird dort in der Begründung zu § 10 ERVV-E unter Verweis auf § 20 Abs. 1 S. 1 RAVPV ausgeführt, dass auch die Anwaltschaft derzeit auf Grundlage des OSCI Protokollstandards kommuniziere (BR-Drs. 145/21, 43). Dem ist zu entnehmen, dass der Verordnungsgeber trotz der in Fachkreisen bekannten Diskussion zur fehlenden Ende-zu-Ende-Verschlüsselung des beA auf Grund der Verwendung des HSM auch weiterhin keine Bedenken gegen die Einhaltung der normierten Vorgaben durch das seitens der Bekl. errichtete System hat und dieses als auf Grundlage der OSCI-Standards errichtet ansieht.

93 (3.2) Wie die erfolgreiche Registrierung der beA-Webanwendung als registriertes Drittprodukt am OSCI-gestützten elektronischen Rechtsverkehr zeigt, erfüllt das beA die hierfür erforderlichen Voraussetzungen und wird damit zugleich auf der Grundlage des OSCI-Standards i.S.v. § 20 Abs. 1 RAVPV betrieben.

94 (3.3) Nur ergänzend ist darauf hinzuweisen, dass der OSCI-Standard eine Verschlüsselung ohnehin nicht grds. vorschreibt, sondern nur als Option ermöglicht (vgl. OSCI-Transport 1.2 – Entwurfsprinzipien, Sicherheitsziele und -mechanismen – der OSCI-Leitstelle, v. 6.6.2002, S. 6 unter 1.: „Das Signieren und Verschlüsseln der Inhaltsdaten erfolgt damit bei OSCI optional"; S. 18 unter 5.1.1: „OSCI stellt eine Verschlüsselung der Inhaltsdaten vom Absender zum Empfänger zur Verfügung …"). Auch deshalb besagt der Verweis auf die Grundlagen des Protokollstandards OSCI in § 20 Abs. 1 RAVPV nicht, dass der Bekl. eine bestimmte Verschlüsselungsart zwingend vorgeschrieben wäre.

95 Der Vortrag der Kl. dazu, weshalb die Vorgaben des OSCI-Standards nicht eingehalten seien, überzeugt überdies auch aus anderen Gründen nicht. Die Kl. verweisen auf Passagen der Entwurfsprinzipien, worin zum Thema Vertraulichkeit ausgeführt

wird, dass die Verschlüsselung die Vertraulichkeit der Inhaltsdaten während der Übertragung sowie ggü. dem Intermediär garantieren könne und durch die Trennung von Inhalts- und Nutzungsdaten auch der Intermediär keine Kenntnis von den Inhaltsdaten erhalte und nicht in der Lage sei, diese zu entschlüsseln und somit zu lesen. Diese Voraussetzungen werden grds. auch bei einer Übermittlung mittels der beA-Anwendung eingehalten, denn es bleiben – wie oben ausgeführt – entgegen dem Vorbringen der Kl. die Inhaltsdaten durchgehend verschlüsselt und es findet eine Umschlüsselung der Inhaltsdaten im HSM nicht statt. Soweit die Kl. darauf verweisen, dass nach dem S.-Gutachten nicht ausgeschlossen sei, dass ein Innentäter, der sich in den Besitz des gesamten Schlüsselmaterials bringe, Nachrichten entschlüsseln könne (S.-Gutachten, B-Schwachstelle Nr. 5.5.3, S. 86), ändert dies an der Erfüllung der von den Kl. genannten Voraussetzungen des OSCI-Standards nichts. Auch insoweit gilt, dass Maßstab für eine Vereinbarkeit der beA-Anwendung mit dem OSCI-Protokoll der Regelbetrieb und nicht ein missbräuchlicher und rechtswidriger Angriff auf das System ist.

96 (c) Ohne Erfolg bleibt auch der Verweis der Kl. darauf, dass die Ende-zu-Ende-Verschlüsselung i.S.d. europäischen Patentschrift aus datenschutzrechtlicher Sicht ein Mindeststandard sei. Es ist weder ersichtlich noch dargetan, dass datenschutzrechtliche Vorschriften für den Bereich der Kommunikation über das beA überhaupt eine Verschlüsselung, geschweige denn eine bestimmte Verschlüsselungstechnik vorschreiben.

97 (d) Eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne ist auch nicht aus verfassungsrechtlichen Gründen geboten.

98 Wie ausgeführt ist § 20 RAVPV nicht verfassungskonform dahingehend auszulegen, dass eine solche Verschlüsselung vorzusehen ist (hierzu oben unter 2 a bb (b) (1.6)). Es verstößt auch nicht gegen die Verfassung, dass die gesetzlichen Regelungen über die Einrichtung der beA einen Nutzungszwang vorsehen, ohne die genaue Art der Verschlüsselung vorzugeben. Die Bekl. ist zudem nicht verpflichtet, aus verfassungsrechtlichen Gründen auch ohne einfachgesetzliche Verpflichtung hierzu das beA nur mit einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne zu betreiben.

99 (1) Die Regelungen über die Einrichtung und Nutzung des besonderen elektronischen Rechtsverkehrs stellen bloße Berufsausübungsregeln dar (vgl. *BVerfG*, a.a.O., Rn. 10). Dies gilt insb. auch für die in § 31a BRAO geregelte Pflicht für Rechtsanwälte, die für die Nutzung des beA erforderlichen technischen Einrichtungen vorzuhalten sowie Zustellungen und den Zugang von Mitteilungen über das beA zur Kenntnis zu nehmen (sog. passive Nutzungspflicht). Regelungen, die lediglich die Berufsausübung betreffen, sind mit Art. 12 Abs. 1 GG vereinbar, soweit vernünftige Erwägungen des Gemeinwohls sie als zweckmäßig erscheinen lassen und das Grundrecht nicht unverhältnismäßig eingeschränkt wird (vgl. *BVerfG*, a.a.O., Rn. 11). Gemessen hieran bestehen gegen die Verfassungsmäßigkeit der Normen, die die Einführung sowie die Nutzungspflicht des beA betreffen, keine Bedenken (vgl. hierzu bereits *Senat* U. v. 11.1.2016 – AnwZ (Brfg) 33/15 [= MMR 2016, 485], Rn. 16; B. v. 28.6.2018 – AnwZ (Brfg) 5/18, Rn. 4, 10). Insb. ist durch die normierte Verpflichtung der Bekl., eine sichere Kommunikation zu gewährleisten, dem rechtlich geschützten Vertrauensverhältnis zwischen Rechtsanwalt und Mandant (vgl. hierzu BVerfGE 113, 29 (49); B. v. 29.1.2015 – 2 BvR 497/12, Rn. 18) in ausreichendem Maße Rechnung getragen. Die Vorgaben an die *BRAK* sind insoweit hinreichend bestimmt. Ein aus der Verfassung ableitbarer Anspruch darauf, dass normativ ein bestimmtes Verschlüsselungssystem vorgegeben wird, besteht nicht. Vielmehr steht es dem Gesetzgeber frei, die technische Konkretisierung des gesetzlich vorgegebenen Maßstabs der Bekl. als Körperschaft des öffentlichen Rechts anzuvertrauen (vgl. für Aufsichtsbehörden im Bereich der Telekommunikation: BVerfGE 125, 260 (327)).

100 (2) Die technische Ausgestaltung des beA in Bezug auf die Verschlüsselung unter Einsatz des HSM verstößt entgegen der Auffassung der Kl. nicht gegen die Grundrechte, insb. nicht gegen Art. 12 Abs. 1 GG. Eine verfassungskonforme Anwendung der Regelungen, die die Bekl. zur Einrichtung des beA verpflichten, gebietet die Verwendung einer Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne nicht.

101 Die Einrichtung des beA unter Verwendung des HSM entspricht – wie ausgeführt – den verfassungsmäßigen gesetzlichen Vorgaben. Soweit die Kl. geltend machen, dass die von der Bekl. vorgenommene Einrichtung des beA ohne Ende-zu-Ende-Verschlüsselung einen ungerechtfertigten Eingriff in die Berufsausübungsfreiheit darstelle, weil sie gegen die bestehenden gesetzlichen Vorgaben zur technischen Ausgestaltung des beA verstießen, ist dies schon deshalb unzutreffend, weil – wie oben ausgeführt – die normativen Vorgaben die Bekl. nicht dazu verpflichten, eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne vorzusehen. Dementsprechend stellt das Betreiben ohne die verlangte Ende-zu-Ende-Verschlüsselung entgegen der Auffassung der Kl. auch keinen Eingriff in den Anspruch auf Rechtmäßigkeit staatlichen Handelns dar.

102 Die Einrichtung als solche ist ein technischer Vorgang zur Umsetzung der die Bekl. hierzu verpflichtenden Normen. Sie stellt einen Zwischenschritt dar, der erforderlich ist, damit die gesetzlich normierte passive Nutzungspflicht des § 31a Abs. 6 BRAO eingreifen und das beA überdies aktiv als Übermittlungsweg i.R.d. elektronischen Kommunikation genutzt werden kann. Weder verpflichtet die bloße Einrichtung des beA als reiner Realakt diejenigen, für die ein beA eingerichtet wurde, zu dessen Nutzung noch schränkt diese die Nutzer ein. Für sich genommen hat die gesetzeskonforme technische Errichtung des beA mithin keinen Eingriffscharakter. Dieser ergibt sich grds. erst durch die gesetzlich normierte Nutzungspflicht, gegen deren Verfassungsmäßigkeit – wie ausgeführt – keine Bedenken bestehen.

103 Soweit die normierten Vorgaben für die Einrichtung des beA der Bekl. Spielraum lassen, bedarf dessen Ausfüllung durch die Bekl. zwar der Berücksichtigung der – mittelbaren – Beeinträchtigung der beruflichen Tätigkeit der Nutzer, die sich aus der passiven Nutzungspflicht des konkret von der Bekl. errichteten Systems ergeben kann. Dem ist die Bekl. indes in ausreichendem Maße nachgekommen. Eine Verletzung der Grundrechte der Kl., insb. der Berufsausübungsfreiheit nach Art. 12 Abs. 1 GG, liegt nicht deshalb vor, weil die Bekl. den ihr zustehenden Spielraum nicht dahingehend genutzt hat, um eine Ende-zu-Ende-Verschlüsselung in dem von den Kl. geforderten Sinne zu verwenden.

104 (2.1) Hierbei ist zunächst zu berücksichtigen, dass der Spielraum der Bekl. sich nur auf die Details der technischen Umsetzung bezog. Die berufsbezogenen Auswirkungen der reinen Ausführung betreffen deshalb nur einen sehr eingeschränkten Bereich des durch die Nutzungspflicht gesetzlich bewirkten Eingriffs in die Berufsausübungsfreiheit. Die mit der Nutzungspflicht an sich verbundenen Einschränkungen der freien Berufsausübung sind mithin für die Beurteilung der Umsetzung nicht relevant, da diese unabhängig von der gewählten technischen Ausführung entstehen.

105 (2.2) Eine Grundrechtsbeeinträchtigung durch die gewählte Verschlüsselungsstruktur ergibt sich auch weder im Hinblick auf die voraussichtlichen Kosten der verpflichtenden Nutzung

für die einzelnen Nutzer noch bzgl. der möglicherweise erforderlichen Anpassungen der kanzleiinternen oder organisatorischen Abläufe. Denn auch diese Beeinträchtigungen werden von der gewählten Verschlüsselungsstruktur nicht beeinflusst.

106 (2.3) Die Wahl der Verschlüsselungsmethode betrifft allein die Vertraulichkeit der Kommunikation und damit mittelbar das anwaltliche Vertrauensverhältnis zum Mandanten. Zwar ist auch dieser Bereich grundrechtlich geschützt. Indes beeinträchtigt die Wahl einer Verschlüsselungsmethode diese Vertraulichkeit nicht, wenn die gewählte Methode nach obigen Kriterien als sicher anzusehen ist. Vor diesem Hintergrund kann auch dahingestellt bleiben, ob die Behauptung der Kl. zutrifft, dass die von ihnen geforderte Ende-zu-Ende-Verschlüsselung sicherer sei als das von der Bekl. gewählte Modell und dennoch alle Anforderungen an das beA eingehalten werden könnten. Eine Beeinträchtigung der Berufsausübungsfreiheit durch das gewählte System ergibt sich nicht daraus, dass die Bekl. nicht andere mögliche technische Systeme gewählt hat. Die Verfassung gibt nicht detailgenau vor, welche Sicherungsmaßnahmen im Einzelnen geboten sind (vgl. zu § 113a TKG: BVerfGE 125, 260 (326)). Entscheidend ist vielmehr, ob das gewählte System zu einer (nicht gerechtfertigten) Beeinträchtigung führt, was bezogen auf die technische Gestaltung der Kommunikationsübermittlung bei der Wahl eines sicheren Übermittlungswegs nicht der Fall ist. Dementsprechend scheidet auch ein auf die Verfassung gestützter Anspruch der Kl. auf Unterlassung des Betreibens ohne die von ihnen geforderte Verschlüsselungsmethode und auf deren Verwendung aus, weil diese nicht die einzige Verschlüsselungsmethode darstellt, die die erforderliche Sicherheit gewährleisten kann. Denn wie ausgeführt ist auf Grundlage des Parteivorbringens sowie des S.-Gutachtens davon auszugehen, dass auch die gewählte Methode hierzu in der Lage ist.

107 Ein Eingriff durch die gewählte Art der Verschlüsselung ergibt sich auch nicht im Hinblick auf die von den Kl. geäußerte Befürchtung, sie könnten bei Nutzung des beA Mandanten verlieren, weil sie eine Vielzahl von Mandanten vertreten würden, die ein besonders gesteigertes Interesse an der Wahrung der Mandatsgeheimnisse hätten. Diese Gefahr sieht der *Senat* nicht. Denn zum einen sind alle Anwälte zur – passiven – Nutzung des beA verpflichtet, sodass der Wechsel des Anwalts für die Mandanten insoweit keinen Nutzen brächte. Zum anderen besteht eine Nutzungspflicht im Verhältnis zwischen Mandant und Anwalt nicht, sodass vertrauliche Kommunikation, die in diesem Verhältnis ausgetauscht werden soll, nicht über das beA-System erfolgen muss. Über das beA werden Inhalte ausgetauscht, die bestimmungsgemäß das interne Mandatsverhältnis verlassen und – bei der derzeit allein verpflichtenden passiven Nutzung – vom Gericht oder dem gegnerischen Anwalt stammen sowie – bei aktiver Nutzung – für das Gericht oder den gegnerischen Anwalt bzw. über diesen für die Gegenseite gedacht sind. Die Übermittlung mittels des beA ersetzt somit – ebenso wie die anderen in § 130a Abs. 4 ZPO als sicher anerkannten elektronischen Übermittlungswege – den bisherigen Postweg. Ebenso wie bei dem herkömmlichen Postversand die in den Schriftsätzen enthaltenen sensiblen Daten den Verfügungsbereich des Anwalts verlassen und der Mandant sich auf die Sicherheit der Postübermittlung verlassen muss, muss er dies bei der elektronischen Übermittlung, wobei hierfür indes – wie ausgeführt – mit dem beA ein sicherer Übermittlungsweg zur Verfügung steht, bei dem die Inhaltsdaten – anders als bei der postalischen Übermittlung – durchgängig verschlüsselt sind.

108 Etwas anderes ergibt sich auch nicht aus der von den Kl. vorgelegten Stellungnahme der Bekl. zu einem Entwurf eines Beschlusses des *Rats der EU* v. 3.11.2020, wonach Regelungen für einen Zugriff auch auf verschlüsselte Daten geschaffen werden sollen. Die Bekl. wendet sich im Hinblick auf den Schutz der Vertraulichkeit der anwaltlichen Kommunikation in ihrer Stellungnahme v. 23.11.2020 gegen das von ihr deshalb befürchtete Verbot von Verschlüsselungen. Für die vom *Senat* zu entscheidenden Frage, welche Verschlüsselungstechnik das beA-System vorsehen muss und ob das gewählte System den gesetzlichen und verfassungsrechtlichen Anforderungen genügt, ist diese Stellungnahme nicht erheblich. Gleiches gilt für die von den Kl. vorgelegte Stellungnahme der Bekl. vom März 2021 zu dem Entwurf einer Richtlinie des *Europäischen Parlaments und des Rates* über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, in der die Bekl. eine sichere verschlüsselte Online-Kommunikation als unabdingbare Grundvoraussetzung für die Gewährleistung des Mandatsgeheimnisses im digitalen Zeitalter ansieht und sich gegen die Beeinträchtigung der Wirksamkeit einer Ende-zu-Ende-Verschlüsselung wendet. Für die Anforderungen an die Verschlüsselungstechnik des beA ist diese Stellungnahme nicht von Relevanz.

109 b) Die Klage ist auch hinsichtlich des Klageantrags zu 2 unbegründet. Den Kl. steht kein Anspruch darauf zu, dass das beA mit einer Ende-zu-Ende-Verschlüsselung betrieben wird. Weder ergibt sich dieser aus den einfachen Gesetzen noch aus der Verfassung. Denn es verpflichten – wie ausgeführt – weder die Regelungen über die Einrichtung des beA noch die Verfassung die Bekl. dazu, das beA mit der von den Kl. geforderten Ende-zu-Ende-Verschlüsselung zu betreiben. …

BGH: Internationale Zuständigkeit bei Online-Flugbuchung

Elektronisches Ticket

Brüssel-Ia-VO Art. 7 Nr. 5, 17 Abs. 1 lit. c u. Abs. 3; TMG § 5 Abs. 1; RL 2000/31/EG Art. 5 Abs. 1 lit. a u. lit. b
Urteil vom 16.3.2021 – X ZR 9/20 (OLG Frankfurt/M., LG Frankfurt/M.)

Leitsatz

Die Angabe einer vom Hauptsitz abweichenden Betriebsstätte im Impressum einer Website darf ein Kunde, der über diese Website ein Vertragsangebot abgibt, in der Regel dahin verstehen, dass die angegebene Stelle im Namen des Stammhauses die Leistungen anbietet, Vertragsangebote entgegennimmt und ggf. deren Annahme erklärt.

Anm. d. Red.: Die Vorinstanz *OLG Frankfurt/M.* ist abgedruckt in MMR 2020, 712.

Schlagworte: Website; Impressum; elektronisches Ticket; unselbstständige Betriebsstätte; Zweigniederlassung; Erklärungsirrtum; offener Kalkulationsirrtum; IATA-Nummer

Sachverhalt

Der Kl. begehrt von der Bekl. Schadensersatz wegen der Stornierung eines Vertrags über eine Luftbeförderung. Der Kl. buchte am 19.12.2017 über die Website „a .de" bei der Bekl. für den 21.8.2018 ein Flugticket von San Francisco nach Paris in der First Class und einen Anschlussflug von Paris nach London in der Business Class für insg. 582,97 EUR.

Im Impressum der genannten Website heißt es unter der Überschrift „A. in Deutschland:
Unter der Überschrift „Firmen Hauptsitz" ist angegeben:
A., Aktiengesellschaft nach französischem Recht mit einem Grundkapital von … Euro."

Nach Überweisung des Flugpreises erhielt der Kl. ein elektronisches Ticket. Darin ist in den Spalten für Ausstellungsdatum und Ausstellungsort angegeben:

„19 Dec 2017 DIR – WEB Allemagne, F. IATA: 23494774".

Am 20.12.2017 teilte die Bekl. mit, das Ticket sei wegen eines Systemfehlers storniert worden und der gezahlte Betrag werde erstattet. Der Kl. hält den Vertrag weiterhin für wirksam und verlangt Schadensersatz wegen Nichterfüllung, den er anhand des am 31.1.2018 geltenden regulären Preises von 10.578,86 EUR berechnet. In erster Instanz hat er auf Zahlung dieses Betrags geklagt, in zweiter Instanz auf Zahlung der Differenz zu dem von ihm gezahlten Betrag. Die Bekl. hat die fehlende internationale Zuständigkeit gerügt und in der Sache geltend gemacht, sie habe den Vertrag wegen eines Erklärungsirrtums, zumindest aber wegen eines offenen Kalkulationsirrtums wirksam angefochten.

Das *LG* hat die Klage als unzulässig abgewiesen. Die Berufung des Kl. ist ohne Erfolg geblieben (*OLG Frankfurt/M.* MMR 2020, 712). Mit der Revision verfolgt der Kl. sein Begehren weiter.

Aus den Gründen

10 Die ... Revision hat Erfolg und führt zur Zurückverweisung der Sache an das *LG*.

11 I. Das *Berufungsgericht* [= MMR 2020, 712] hat seine Entscheidung im Wesentlichen wie folgt begründet:

12 Die internationale Zuständigkeit des *LG* ergebe sich nicht aus Art. 7 Nr. 5 Brüssel-Ia-VO. Unter der im Impressum der Website angegebenen Adresse in F. befinde sich zwar die Angabe eines Geschäftsführers der Bekl. für deren Marketingabteilung für Deutschland. Jedoch betreffe der Rechtsstreit nicht eine Streitigkeit aus dem Betrieb dieser Niederlassung. ...

14 II. Diese Beurteilung hält der rechtlichen Überprüfung in einem entscheidenden Punkt nicht stand.

15 1. Zu Recht und insoweit nicht angegriffen hat das *Berufungsgericht* eine internationale Zuständigkeit deutscher Gerichte auf Grund von Art. 33 des Montrealer Übereinkommens im Streitfall verneint.

16 2. Entgegen der Auffassung des *Berufungsgerichts* sind die deutschen Gerichte für den Rechtsstreit nach Art. 7 Nr. 5 Brüssel-Ia-VO zuständig.

17 a) Entgegen der Auffassung der Revisionserwiderung unterhält die Bekl. in F. eine Zweigniederlassung i.S.v. Art. 7 Nr. 5 Brüssel-Ia-VO.

18 Eine Zweigniederlassung in diesem Sinne setzt nach der st. Rspr. des *Gerichtshofs* einen Mittelpunkt geschäftlicher Tätigkeit voraus, der auf Dauer als Außenstelle des Stammhauses hervortritt, eine Geschäftsführung hat und sachlich so ausgestattet ist, dass sich Dritte zum Betreiben von Geschäften nicht unmittelbar an das Stammhaus zu wenden brauchen (vgl. nur *EuGH* U. v. 11.4.2019 – C-464/18, Rn. 33 – Ryanair; U. v. 25.2.2021 – C-804/19, Rn. 47 – Markt24).

19 Aus dem insoweit unstreitigen Vorbringen der Parteien ergibt sich, dass diese Voraussetzung im Streitfall erfüllt ist.

20 aa) Die Bekl. stellt nicht in Abrede, dass in der betreffenden Betriebsstätte u.a. Mitarbeiter tätig sind, die spezielle Angebote für in Deutschland ansässige Reisebüros und Firmenkunden erstellen. Damit liegt eine Tätigkeit vor, die es den angesprochenen Kunden ermöglicht, Geschäfte mit der Bekl. zu betreiben, ohne sich unmittelbar an das Stammhaus zu wenden.

21 bb) Nach dem Vorbringen der Bekl. befindet sich in der Betriebsstätte ferner der Sitz des Geschäftsführers für Deutschland. Damit ist eine Geschäftsführung vorhanden.

22 cc) Entgegen der Ansicht der Bekl. kann auf dieser Grundlage nicht davon ausgegangen werden, dass es sich nur um eine unselbstständige Betriebstätte handelt, die in jeder Hinsicht vom Hauptsitz abhängig ist.

23 Dabei kann dahingestellt bleiben, inwieweit die Mitarbeiter der Betriebsstätte für den Abschluss von Geschäften intern der Zustimmung durch Bedienstete des Hauptsitzes bedürfen. Ausschlaggebend sind nicht die geschäftsinternen Abläufe, sondern die Art und Weise, in der die Niederlassung ggü. Dritten im Geschäftsverkehr auftritt (*EuGH* U. v. 9.12.1987 – Rs. 218/86, Rn. 14 f. – Schotte).

24 b) Entgegen der Auffassung des *Berufungsgerichts* weist der Rechtsstreit den nach Art. 7 Nr. 5 Brüssel-Ia-VO erforderlichen Bezug zum Betrieb der Zweigniederlassung auf.

25 Der *Gerichtshof* hat hierzu ausgeführt, dass ein solcher Bezug vorliegt, wenn der Rechtsstreit Handlungen betrifft, die sich auf den Betrieb der Zweigniederlassung beziehen, oder eine Verpflichtung, die die Zweigniederlassung im Namen des Stammhauses eingegangen und die in dem Vertragsstaat zu erfüllen ist, in dem sich die Zweigniederlassung befindet (vgl. *EuGH* U. v. 22.11.1978 – Rs. 33/78, Rn. 13 – Somafer; ebenso: U. v. 19.7.2012 – C-154/11, Rn. 48 – Mahamdia; U. v. 5.7.2018 – C-27/17, Rn. 59 – Lithuanian Airlines; a.a.O., Rn. 33 – Ryanair; a.a.O., Rn. 48 – Markt24). Hinsichtlich der zweiten Alternative hat der *Gerichtshof* klargestellt, dass ein Erfüllungsort im Vertragsstaat der Zweigniederlassung nicht erforderlich ist (*EuGH* U. v. 6.4.1995 – C-439/93, Rn. 22 – Lloyds).

26 Im Streitfall ist ein Bezug des Rechtsstreits zur Zweigniederlassung durch das Eingehen einer Verpflichtung im Namen des Stammhauses gegeben.

27 aa) Nach der Rspr. des *Gerichtshofs* zu der mit Art. 7 Abs. 5 Brüssel-Ia-VO wortgleichen Regelung in Art. 5 Nr. 5 EuGVÜ muss sich eine rechtlich selbstständige Gesellschaft, die Geschäfte so abschließt, dass sie als Außenstelle einer anderen Gesellschaft auftritt, an dem so erweckten Anschein festhalten lassen, selbst wenn beide Gesellschaften gesellschaftsrechtlich voneinander unabhängig sind (*EuGH*, a.a.O. – Schotte; U. v. 18.5.2017 – C-617/15, Rn. 38 – Nike).

28 bb) Im Streitfall ist die Zweigniederlassung der Bekl. ggü. Kunden, die Buchungen über die Website „a .de" vorgenommen haben, als diejenige Stelle aufgetreten, die die Buchungen anbietet, das in der Vornahme einer Buchung liegende Vertragsangebot entgegennimmt und ggf. dessen Annahme erklärt. Dies ergibt sich aus dem Umstand, dass die Zweigniederlassung im Impressum der Website als „A. in Deutschland" bezeichnet wird.

29 (1) Angaben im Impressum einer Website dienen der Erfüllung der Informationspflichten aus § 5 TMG.

30 § 5 Abs. 1 TMG, der der Umsetzung von Art. 5 Abs. 1 lit. a u. lit. b RL 2000/31/EG des Europäischen Parlaments und des Rates v. 8.6.2000 über den elektronischen Geschäftsverkehr dient, schreibt u.a. vor, dass die Anbieter von Telemediendiensten für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien bestimmte Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar halten. Zu diesen Angaben gehören nach § 5 Abs. 1 Nr. 1 TMG insb. der Name des Diensteanbieters und die Anschrift, unter der er niedergelassen ist.

31 Eine entsprechende Informationspflicht war schon in § 6 TDG vorgesehen. Der Gesetzgeber hat diese Regelung unverändert übernommen (BT-Dr. 16/3078, 14 re. Sp.). Sie dient dem Zweck, für den Nutzer ein Mindestmaß an Transparenz und Information über die Person oder Personengruppe sicherzustellen, die ihm einen Teledienst anbietet; auf diese Weise soll insb.

im Konfliktfall auch ein Anknüpfungspunkt für eine Rechtsverfolgung bestehen (BT-Dr. 13/7385, 21 li. Sp.).

32 (2) Angesichts dieser Zwecksetzung ist die im Impressum angegebene Stelle im Geschäftsverkehr grds. als diejenige Stelle anzusehen, die die beworbene Dienstleistung anbietet und die maßgeblichen Vertragserklärungen abgibt oder entgegennimmt.

33 Die Angaben zum Anbieter können ihren Zweck nur dann erfüllen, wenn der angesprochene Nutzer sich darauf verlassen kann, dass ihm die angegebene Stelle als Anbieter und Vertragspartner gegenübertritt.

34 (3) Im Streitfall ist die Zweigniederlassung der Bekl. als Anbieter in diesem Sinne aufgetreten.

35 Die Verwendung der Top-Level-Domain „.de" und der deutschen Sprache deutet aus Sicht des Kunden darauf hin, dass sich das Angebot auf der genannten Website an Interessenten in Deutschland richtet. Wenn vor diesem Hintergrund eine vorhandene Betriebsstätte als „A. in Deutschland" bezeichnet wird, darf ein Kunde dies dahin verstehen, dass diese Betriebsstätte die Stelle ist, die die Buchungen anbietet.

36 (4) Der Umstand, dass im Impressum auch der Hauptsitz angegeben ist, führt vor diesem Hintergrund nicht zu einer abweichenden Beurteilung.

37 Diese Angabe war schon deshalb folgerichtig, weil der Diensteanbieter nach § 5 Abs. 1 Nr. 1 TMG auch Angaben über Rechtsform und Stammkapital machen muss und die Niederlassung weder über eigene Rechtspersönlichkeit noch über eigenes Stammkapital verfügt. In ihrer Gesamtheit sind die Angaben aus Kundensicht folglich dahin zu verstehen, dass die als „A. in Deutschland" bezeichnete Betriebsstätte den deutschen Kunden im Namen des Stammhauses gegenübertritt.

38 (5) In dieselbe Richtung deutete im Streitfall aus Kundensicht der Umstand, dass im elektronischen Ticket als Ausstellungsort ebenfalls F. angegeben ist.

39 Die Buchungsmöglichkeiten auf der Website stellen aus vertragsrechtlicher Sicht lediglich Aufforderungen zur Abgabe eines Angebots dar. Deshalb kann der Annahme eines solchen Angebots Bedeutung für die Frage zukommen, wer als Vertragspartner des Kunden auftritt.

40 Im Streitfall bestätigen die Angaben im elektronischen Ticket den bereits durch das Impressum erweckten Eindruck, weil der Ausstellungsort mit dem im Impressum angegebenen Sitz der Niederlassung übereinstimmt und weil die darin angegebene IATA-Nummer nach dem unbestrittenen Vorbringen des Kl. ebenfalls dieser Betriebsstätte zugeordnet ist.

41 (6) Dass die Mitarbeiter der Zweigniederlassung weder an der inhaltlichen Gestaltung und dem Betrieb der Website noch an der Bestätigung und Abwicklung der darüber getätigten Buchungen beteiligt waren, ist entgegen der Auffassung der Revisionserwiderung unerheblich.

42 Wie bereits oben dargelegt wurde, kommt einzelnen Details der betriebsinternen Abläufe keine ausschlaggebende Bedeutung zu, sofern eine – tatsächlich vorhandene – Betriebsstätte ggü. Interessenten und Kunden als diejenige Stelle auftritt, die im Namen des Stammhauses Angebote unterbreitet und Annahmeerklärungen abgibt oder Erklärungen des Kunden entgegennimmt. Diese Voraussetzung ist im Streitfall aus den o.g. Gründen erfüllt.

43 (7) Ebenfalls nicht zu einer abweichenden Beurteilung führt der Umstand, dass die angegebenen E-Mail-Adressen abweichend von der Website die Top-Level-Domain „.fr" aufweisen.

44 Dieser Umstand gab aus Kundensicht keinen hinreichend deutlichen Hinweis darauf, dass die für den Vertragsschluss maßgeblichen Personen in Frankreich ansässig sind. Er ist ohne Weiteres damit zu erklären, dass alle Mitarbeiter der Bekl. über eine nach gleichem Muster zusammengesetzte E-Mail-Adresse verfügen.

45 cc) An dem durch diese Erklärungen begründeten Anschein, dass die Buchungen durch die – tatsächlich vorhandene – Zweigniederlassung in F. angeboten und bestätigt werden, muss sich die Bekl. nach der aufgezeigten Rspr. des *Gerichtshofs* festhalten lassen.

46 Nach dieser Rspr. besteht eine Bindungswirkung selbst dann, wenn nicht eine Zweigniederlassung, sondern eine rechtlich selbstständige Gesellschaft tätig geworden ist. Eine entsprechende Bindungswirkung muss erst recht bestehen, wenn eine tatsächlich vorhandene Zweigniederlassung auf den Vertragsschluss bezogene Erklärungen ggü. den Kunden abgibt.

47 3. Ob sich eine Zuständigkeit im Streitfall zudem aus Art. 17 Abs. 1 lit. c u. Abs. 3 Brüssel-Ia-VO ergibt, kann angesichts all dessen offenbleiben. ...

BGH: Gerichtsstand bei Klagen gegen vermeintlich marktbeherrschende Stellung – Wikingerhof/Booking.com

Buchungsportal

Brüssel-Ia-VO Art. 7 Nr. 1 u. Nr. 2, Art. 25; GWB §§ 19, 33 Abs. 2; AEUV Art. 102; VO (EU) 1215/2012 Art. 25 Abs. 1 S. 2
Urteil vom 10.2.2021 – KZR 66/17 (OLG Schleswig, LG Kiel)

Leitsätze

1. Macht der Kläger einen Anspruch wegen Missbrauchs einer marktbeherrschenden Stellung durch das bekl. Unternehmen geltend, ist der unionsrechtliche Gerichtsstand der unerlaubten Handlung auch dann eröffnet, wenn in Betracht kommt, dass das als missbräuchlich beanstandete Verhalten den Bestimmungen eines zwischen den Parteien bestehenden Vertrags (hier: über die plattformgebundene Vermittlung von Hoteldienstleistungen) entspricht.

2. Ob die Parteien eine Gerichtsstandsvereinbarung getroffen haben, richtet sich nach Unionsrecht. Die Annahme einer entsprechenden Willensübereinstimmung erfordert die Feststellung, dass die nach den Allgemeinen Geschäftsbedingungen einer Partei die Zuständigkeit begründende Klausel tatsächlich Gegenstand einer klar und deutlich zum Ausdruck kommenden Einigung der Parteien war.

3. Eine in den Allgemeinen Geschäftsbedingungen des Plattformbetreibers enthaltene Gerichtsstandsklausel, nach der für aus dem Vertrag entstehende Streitigkeiten das Gericht seines Geschäftssitzes zuständig ist, erfasst Ansprüche wegen Missbrauchs einer marktbeherrschenden Stellung nur dann, wenn deutliche Anhaltspunkte dafür bestehen, dass die Vertragsparteien die sachliche Reichweite der Gerichtsstandsvereinbarung auch auf solche vom Vertrag unabhängigen Ansprüche erstrecken wollten.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 10819. Das Vorabentscheidungsersuchen des *BGH* in dieser Sache ist im Leitsatz abgedruckt in MMR 2019, 208. Die Entscheidung des *EuGH* hierzu ist abgedruckt in MMR 2021, 35 – Wikingerhof; vgl. ferner *BGH* MMR 2017, 825 – Kabelkanalanlagen und *EuGH* MMR 2015, 515 – Majdoub/CarsOnTheWeb.Deutschland GmbH.

Schlagworte: Gerichtsstandsvereinbarung; Missbrauch einer marktbeherrschenden Stellung; Internetplattform; Buchungsportal; Willenseinigung; Extranet; geänderte AGB; Einbeziehung

Sachverhalt

Die Kl. betreibt in Schleswig-Holstein ein Hotel. Die Bekl., die ihren Sitz in den Niederlanden hat, betreibt die Hotelbuchungsplattform booking.com. Die Kl. vermarktet ihr Hotel (auch) über diese Plattform. Sie sieht in bestimmten Verhaltensweisen der Bekl. bei der Vermittlung von Hotelbuchungen eine unbillige Behinderung durch ein marktbeherrschendes Unternehmen und nimmt die Bekl. deshalb auf Unterlassung in Anspruch.

Die Parteien schlossen 2009 einen Vertrag, der auf einem von der Bekl. vorgelegten Vertragsformular beruht, in dem auf eine bestimmte Version der AGB der Bekl. verwiesen wird, die auf der Plattform online verfügbar seien. Diese AGB (im Folgenden: AGB 2008) sehen u.a. vor, dass ausschließlich niederländisches Recht gelte und Gerichtsstand für alle aus dem Vertrag entstehenden Streitigkeiten mit Ausnahme von Zahlungs- und Rechnungsstreitigkeiten, für die als Gerichtsstand auch der Sitz des Hotels in Frage komme, Amsterdam sei. Die Bekl. änderte ihre AGB in der Folge mehrfach. Die Kl. widersprach der Einbeziehung einer Version der AGB, die die Bekl. ihren Vertragspartnern per E-Mail v. 25.6.2015 bekannt machte (im Folgenden: AGB 2015 neu). Die AGB 2015, die die Bekl. vor der Änderungsmitteilung verwendete (AGB 2015 alt), sehen ebenso wie die AGB 2015 neu vor, dass – sofern nichts anderes in dem Vertrag festgelegt ist – die aus oder in Verbindung mit dem Vertrag entstehenden Streitigkeiten ausschließlich vor die zuständigen Gerichte in den Niederlanden gebracht und dort verhandelt werden.

Das *LG* hat die Klage wegen fehlender örtlicher und internationaler Zuständigkeit abgewiesen. Die Berufung der Kl. ist erfolglos geblieben. Hiergegen wendet sich die Kl. mit der vom *Senat* zugelassenen Revision, deren Zurückweisung die Bekl. beantragt.

Auf ein Vorabentscheidungsersuchen des *Senats* v. 11.12.2018 (*BGH* MMR 2019, 208 (Ls.)) hat der *EuGH* mit U. v. 24.11.2020 (MMR 2021, 35 – Wikingerhof) entschieden, dass Art. 7 Nr. 2 Brüssel-Ia-VO dahin auszulegen ist, dass er für eine Klage gilt, die auf die Unterlassung bestimmter Verhaltensweisen i.R.e. Vertragsbeziehung zwischen dem Kl. und dem Bekl. gerichtet ist und die darauf gestützt wird, dass der Bekl. unter Verstoß gegen das Wettbewerbsrecht seine marktbeherrschende Stellung missbräuchlich ausnutze.

Aus den Gründen

5 I. Das *Berufungsgericht* hat zur Begründung seiner Entscheidung im Wesentlichen ausgeführt:

6 Für die Klage sei die örtliche und internationale Zuständigkeit des angerufenen Gerichts nicht gegeben. Weder sei der Gerichtsstand des Erfüllungsorts (Art. 7 Nr. 1 Brüssel-Ia-VO) noch der Gerichtsstand der unerlaubten Handlung (Art. 7 Nr. 2 Brüssel-Ia-VO) gegeben. Auf die Frage, ob eine wirksame Gerichtsstandsvereinbarung getroffen worden sei, komme es daher nicht an.

7 II. Die gegen diese Beurteilung gerichtete Revision hat Erfolg. Sie führt zur Aufhebung des Berufungsurteils und zur Zurückverweisung der Sache an das *Berufungsgericht* zur sachlichen Prüfung des Klagebegehrens. Seine Annahme, das angerufene *LG* sei örtlich und international unzuständig, hält der revisionsrechtlichen Nachprüfung nicht stand.

8 1. Zu Unrecht hat das *Berufungsgericht* den Gerichtsstand der unerlaubten Handlung nach Art. 7 Nr. 2 Brüssel-Ia-VO verneint. Für die Prüfung des Klagebegehrens ist ein im Bezirk des angerufenen *LG* belegener Gerichtsstand am Sitz der Kl. als demjenigen Ort eröffnet, an dem sich der mit der Klage geltend gemachte Missbrauch einer marktbeherrschenden Stellung ggü. der Kl. ausgewirkt hat (vgl. *EuGH* U. v. 21.5.2015 – C-352/13 – CDC Hydrogene Peroxide).

9 a) Mit der Klage begehrt die Kl. die Unterlassung des Missbrauchs einer marktbeherrschenden Stellung durch die Bekl. als Betreiberin der Hotelbuchungsplattform booking.com bei der Vermittlung von Beherbergungsverträgen an Hotelgäste und sonstige Kunden, die auf der Plattform nach Angeboten suchen. Als missbräuchlich beanstandet sie die Bewerbung von rabattierten Preisen ohne ihre Mitwirkung, eine Beschränkung der Kontaktmöglichkeiten zwischen den Vertragspartnern des über die Plattform abgeschlossenen Beherbergungsvertrags sowie eine von der Höhe der an die Bekl. gezahlten Provision abhängige Platzierung des Hotels in der Reihenfolge der auf der Plattform angezeigten Angebote.

10 b) Damit macht sie auf eine unerlaubte Handlung i.S.d. Art. 7 Nr. 2 Brüssel-Ia-VO gestützte Ansprüche geltend.

11 aa) Entgegen der Auffassung des *Berufungsgerichts* schließt das Bestehen einer Vertragsbeziehung zwischen den Parteien die Qualifikation des Klagebegehrens als deliktischer Anspruch nicht aus. Entscheidend für die Abgrenzung des besonderen Gerichtsstands des Art. 7 Nr. 2 Brüssel-Ia-VO von dem besonderen Gerichtsstand des Art. 7 Nr. 1 Brüssel-Ia-VO ist vielmehr, ob ein gesetzlicher Anspruch geltend gemacht wird, der unabhängig von einem Vertragsverhältnis zwischen den Parteien besteht (*EuGH* WuW 2021, 31 [= MMR 2021, 35], Rn. 33 – Wikingerhof). Dies ist dann der Fall, wenn die Rechtmäßigkeit oder Rechtswidrigkeit der mit der Klage beanstandeten Handlung des Anspruchsgegners nicht vom Inhalt der beiderseitigen vertraglichen Rechte und Pflichten abhängt, sondern hiervon unabhängig nach Deliktsrecht zu beurteilen ist (*EuGH*, a.a.O., Rn. 32 – Wikingerhof).

12 bb) So verhält es sich im Streitfall. Die Kartellrechtswidrigkeit der beanstandeten Handlungen hängt allein davon ab, ob der Bekl. nach § 18 GWB eine marktbeherrschende Stellung zukommt und sie diese missbräuchlich ausgenutzt hat (§ 19 GWB, Art. 102 AEUV). Auf den Inhalt des Vertrags kommt es hierfür nicht an. Es ist deshalb i.S.d. Abgrenzungsformel des *EuGH* zur Beurteilung der Begründetheit der Klage auch nicht unerlässlich, den Vertrag zwischen den Parteien auszulegen. Eine solche Auslegung ist allenfalls erforderlich, um das Vorliegen der beanstandeten Handlungsweisen festzustellen (*EuGH*, a.a.O., Rn. 35; Schlussanträge des GA *Saugmansgaard Øe* – C-59/19, Rn. 103). So kann etwa eine (Erst-)Begehungsgefahr nach § 33 Abs. 2 GWB für die mit der Klage als kartellrechtswidrig beanstandeten Verhaltensweisen daraus abgeleitet werden, dass die Bekl. sich vertraglich ausbedungen hat, in der angegriffenen Weise handeln zu dürfen.

13 cc) Allerdings erfordert die nach § 19 Abs. 1 u. Abs. 2 Nr. 2 GWB stets gebotene Interessenabwägung im Einzelfall (vgl. *BGH* U. v. 7.6.2016 – KZR 6/15, Rn. 48 – Pechstein/International Skating Union) bei einer Vertragsbeziehung der Parteien auch eine Betrachtung der vertragstypischen Rechte und Pflichten und der zwischen den Parteien getroffenen Regelungen (vgl. *BGH* U. v. 24.1.2017 – KZR 2/15 [= MMR 2017, 825], Rn. 31 – Kabelkanalanlagen). Für die Qualifikation des Klageanspruchs als deliktischen Anspruch ist dies jedoch ohne Belang, zumal dabei Interessen nicht berücksichtigt werden dürfen, deren Durchsetzung insb. nach den kartellrechtlichen Wertungen rechtlich missbilligt werden (*BGH*, a.a.O., Rn. 30 – Kabelkanalanlagen).

14 dd) Fehl geht auch die Erwägung des *Berufungsgerichts*, die Kl. verlange nicht nur Unterlassung, sondern erstrebe letztlich eine Abänderung des Vertrags. Die Kl. macht – sachlich richtig – einen Unterlassungsanspruch nach § 33 Abs. 1 GWB geltend. Dass die Bekl. einem entsprechenden gerichtlichen Verbot – außer durch eine Einstellung ihrer Vermittlungstätigkeit – ggf. nur durch eine andere Vertragsgestaltung nachkommen könnte,

ändert nichts daran, dass weder die Grundlage der Klage noch das Klagebegehren selbst vertraglicher Natur sind.

15 2. Die nach Art. 7 Nr. 2 Brüssel-Ia-VO begründete internationale Zuständigkeit deutscher Gerichte ist nicht auf Grund einer zwischen den Parteien geschlossenen Gerichtsstandsvereinbarung ausgeschlossen.

16 a) Eine wirksame Zuständigkeitsvereinbarung begründet allerdings nach Art. 25 Abs. 1 S. 2 VO (EU) 1215/2012 eine ausschließliche Zuständigkeit, sofern die Parteien nichts anderes vereinbart haben (vgl. *EuGH* U. v. 21.5.2015 – C-322/14 [= MMR 2015, 515], Rn. 24 – Majdoub/CarsOnTheWeb.-Deutschland GmbH).

17 b) Das *Berufungsgericht* hat – von seinem Standpunkt folgerichtig – nicht geprüft, ob der niederländische Gerichtsstand, welcher in den AGB der Bekl. vorgesehen war, auf die das von der Kl. unterzeichnete Vertragsformular Bezug nimmt (AGB 2008), zwischen den Parteien wirksam vereinbart worden ist. Dies kann auch weiterhin dahinstehen.

18 aa) Die Anwendung der Gerichtsstandsklausel auf die nach § 33 Abs. 1 GWB geltend gemachten Ansprüche ist allerdings nicht schon gem. Art. 25 Abs. 1 S. 1 Brüssel-Ia-VO ausgeschlossen. Danach kann eine Vereinbarung über die internationale Zuständigkeit nur eine bereits entstandene Rechtsstreitigkeit oder eine künftige aus einem bestimmten Rechtsverhältnis entspringende Rechtsstreitigkeit betreffen, was ihre Geltung auf Rechtsstreitigkeiten einschränkt, die ihren Ursprung in dem Rechtsverhältnis haben, anlässlich dessen die Vereinbarung geschlossen wurde. ... Da sich der hier geltend gemachte Missbrauch einer marktbeherrschenden Stellung in den vertraglichen Beziehungen und in den Vertragsbedingungen manifestieren kann, ist eine Erstreckung einer Gerichtsstandsvereinbarung auf darauf gestützte Klagen auch dann nicht überraschend, wenn sie sich nicht ausdrücklich auf Streitigkeiten im Zusammenhang mit einem Verstoß gegen das Wettbewerbsrecht bezieht ...

19 bb) Die Klausel erfasst die mit der Klage geltend gemachten Ansprüche jedoch nicht.

20 (1) Die sachliche Reichweite einer Gerichtsstandsvereinbarung ist durch Auslegung zu ermitteln (*BGH* U. v. 6.12.2018 – IX ZR 22/18, Rn. 25). ... Sie richtet sich, wenn sie – wie hier – Teil einer umfassenderen Vereinbarung ist, regelmäßig nach dem für den Vertrag geltenden Recht, soweit Art. 25 Brüssel-Ia-VO keine Maßstäbe und Vorgaben enthält (*BGH*, a.a.O.).

21 (2) Mithin unterliegt die Auslegung der Gerichtsstandsvereinbarung im Falle der wirksamen Einbeziehung der in den AGB enthalten Rechtswahlklausel niederländischem Recht. Da das *Berufungsgericht* – von seinem Standpunkt folgerichtig – das ausländische Recht nicht ermittelt und gewürdigt hat, kann der *Senat* dieses selbst ermitteln und seiner Entscheidung zu Grunde legen (vgl. *BGH* U. v. 12.11.2009 – Xa ZR 76/07, Rn. 21). Nach der grundlegenden Entscheidung „Haviltex" des *Hoge Raad der Nederlanden* ist bei der Auslegung nicht nur auf den Wortlaut der Vertragsbestimmung abzustellen. Vielmehr sind auch die Bedeutung und die Erwartung in Betracht zu ziehen, die die Parteien unter den gegebenen Umständen vernünftigerweise der Vertragsbestimmung beimessen ...

22 Damit unterscheidet sich das niederländische Recht im Wesentlich nicht von den im deutschen Recht maßgeblichen Auslegungsgrundsätzen. ...

23 (3) Die Auslegung kann der *Senat* selbst vornehmen, da keine weiteren Feststellungen zu erwarten sind (vgl. *BGH* U. v. 6.12.2018, a.a.O., Rn. 27).

24 (a) Die Gerichtsstandsklausel der AGB 2008 betrifft alle aus dem Vertrag entstehenden Streitigkeiten mit Ausnahme von Zahlungs- und Rechnungsstreitigkeiten. Dieser Wortlaut bietet keinen hinreichenden Anhalt dafür, dass mit ihr deliktische Ansprüche eines Vertragspartners der Bekl. wegen eines Missbrauchs einer marktbeherrschenden Stellung erfasst werden sollten. ...

25 (b) Auch die Interessenlage der Vertragsparteien, die Rückschlüsse auf den Parteiwillen zulässt, spricht gegen die Einbeziehung kartellrechtlicher Ansprüche in die Gerichtsstandsklausel. Durch die Klausel wird die Bekl. als Verwenderin begünstigt. Zuwiderhandlungen gegen das kartellrechtliche Missbrauchsverbot sind dem Vertragspartner im Zeitpunkt des Vertragsschlusses regelmäßig nicht bekannt, noch muss er damit rechnen (vgl. für den Verstoß gegen das Kartellverbot: *EuGH*, a.a.O., Rn. 70 – CDC Hydrogen Peroxide). Da ein entsprechender Regelungswille damit nicht unterstellt werden kann (vgl. *Mankowski*, in: Rauscher, Europäisches Zivilprozess- und Kollisionsrecht, 5. Aufl., Art. 25 Brüssel-Ia-VO Rn. 358) darf jedenfalls nicht ohne – im Streitfall fehlende – deutliche Anhaltspunkte hierfür angenommen werden, mit einer für aus dem Vertrag entstehende Streitigkeiten vereinbarten Gerichtsstandsvereinbarung unterwerfe sich der Vertragspartner des Marktbeherrschers dem Vertragsgerichtsstand auch für die Prüfung von Ansprüchen wegen Missbrauchs einer marktbeherrschenden Stellung.

26 Ob solche deutlichen Anhaltspunkte auch deshalb erforderlich sind, weil Bestehen und Reichweite solcher Ansprüche ... grds. der vertraglichen Regelung nicht zugänglich sind, oder ob der Berücksichtigung dieses Umstands bei der Interessenbewertung entgegensteht, dass im Anwendungsbereich der europäischen Gerichtsstands- und Vollstreckungsverordnungen nationale Beschränkungen der prozessualen Parteiautonomie vollständig verdrängt werden (*Wurmnest*, in: FS Magnus, 2014, S. 567 (570) mwN), kann vor diesem Hintergrund offenbleiben.

27 c) Ob die in den AGB 2015 alt enthaltene Klausel, die die internationale Zuständigkeit niederländischer Gerichte für aus oder in Verbindung mit dem Vertrag entstehende Streitigkeiten vorsieht, auch die hier geltend gemachten Ansprüche erfasst (dafür *Mankowski*, a.a.O., Rn. 91; *Weller*, in: Wieczorek/Schütze, ZPO, 4. Aufl., Art. 25 Brüssel-Ia-VO Rn. 17), kann dahinstehen. Denn es fehlt insoweit an einer Gerichtsstandsvereinbarung nach Art. 25 Abs. 1 S. 2 Brüssel-Ia-VO.

28 aa) Das Verständnis des Begriffs der Gerichtsstandsvereinbarung richtet sich nicht nach dem innerstaatlichen Recht eines beteiligten Staats. Es handelt sich vielmehr um einen autonomen Begriff des Unionsrechts (*EuGH* U. v. 18. 11.2020 – C-519/19, Rn. 38 – Ryanair DAC/DelayFix; vgl. *EuGH* U. v. 7.7.2016 – C-222/15, 635, Rn. 29 – Hőszig/Alstom Power Thermal Services). ...

29 bb) Eine Gerichtsstandsvereinbarung muss nach Art. 25 Abs. 1 S. 2 Brüssel-Ia-VO entweder schriftlich oder mündlich mit schriftlicher Betätigung („halbe Schriftlichkeit", *BGH* U. v. 25.1.2017 – VIII ZR 257/15, Rn. 17) oder in einer Form geschlossen werden, die den zwischen den Parteien entstandenen Gepflogenheiten oder im internationalen Handel einem Handelsbrauch entspricht. Der Schriftform gleichgestellt ist die elektronische Übermittlung, die eine dauerhafte Aufzeichnung der Vereinbarung ermöglicht (Art. 25 Abs. 2 Brüssel-Ia-VO). Damit soll verhindert werden, dass einseitig in den Vertrag eingefügte Gerichtsstandsklauseln unbemerkt bleiben (vgl. *EuGH* U. v. 20.4.2016 – C-366/13, Rn. 39 – Profit Investment SIM SpA/Ossi; *BGH* ZIP 2017, 2324, Rn. 25), und sichergestellt werden, dass eine Willenseinigung der Parteien tatsächlich vorliegt (vgl. *EuGH*, a.a.O., Rn. 36 f. – Hőszig/Alstom Power Thermal Servi-

ces; a.a.O., Rn. 30 – Majdoub/CarsOnTheWeb.Deutschland GmbH). Es bedarf deshalb der Feststellung, dass die die Zuständigkeit begründende Klausel tatsächlich Gegenstand einer klar und deutlich zum Ausdruck kommenden Einigung der Parteien war (*EuGH* U. v. 8.3.2018 – C-64/17, Rn. 25 – Saey Home & Garden; a.a.O., Rn. 38 – Ryanair DAC/DelayFix; vgl. auch U. v. 14.12.1976 – Rs. 24/76 – Colzani/Rüwa; a.a.O., Rn. 36 f. – Hőszig/Alstom Power Thermal Services).

30 cc) Da es sich bei der internationalen Zuständigkeit um eine von Amts wegen zu prüfende Prozessvoraussetzung handelt, kann der *Senat* das Vorliegen einer Gerichtsstandsvereinbarung in tatsächlicher und rechtlicher Hinsicht ohne Bindung an die Feststellungen des *Berufungsgerichts* prüfen und würdigen (vgl. *BGH* U. v. 14.12.1959 – V ZR 197/58 und v. 24.9.2009 – IX ZR 149/08, Rn. 9).

31 dd) Es kann nicht festgestellt werden und aus dem Parteivortrag ergeben sich auch keine hinreichenden Anhaltspunkte dafür, dass die in den AGB 2015 alt enthaltene Gerichtsstandsklausel tatsächlich Gegenstand einer Willenseinigung zwischen den Parteien war, die klar und deutlich zum Ausdruck gekommen ist (vgl. Rn. 29).

32 Zwar sieht Nummer 17 der AGB 2008 der Bekl. vor, dass diese berechtigt sein soll, die AGB zu ändern. Änderungen soll die Bekl. nach der Klausel auf ihren als Extranet bezeichneten Internetseiten bekannt geben, und sie sollen einen Monat nach Bekanntgabe in Kraft treten. Für den Fall, dass das Hotel zu den Änderungen nicht Stellung nimmt, sollen sie durch die weitere Inanspruchnahme „des Services" der Bekl. als vom Hotel angenommen gelten. Es kann dahinstehen, ob bei einer Veröffentlichung der Änderungen im „Extranet" von einer entsprechenden Willenseinigung auszugehen wäre. Denn es kann bereits nicht angenommen werden, dass eine Veröffentlichung der AGB 2015 alt im „Extranet" erfolgt ist. Damit können weder die Voraussetzungen für das Inkrafttreten der geänderten AGB gemäß der Änderungsvorbehaltsklausel in den AGB 2015 alt noch für eine Willenseinigung festgestellt werden. Denn ohne Kenntnis der Gerichtsstandsklausel oder zumindest die Möglichkeit der Kenntnisnahme bei normaler Sorgfalt konnte sich eine Einigung der Parteien nicht auf die Gerichtsstandsklausel erstrecken (vgl. *EuGH*, a.a.O. – Colzani/Rüwa; a.a.O., Rn. 40 – Hőszig/Alstom Power Thermal Services; *BGH* U. v. 28.3.1996 – III ZR 95/95).

33 Die Kl. hat behauptet, diese Version der AGB sei im „Extranet" nicht abrufbar gewesen ... und sie habe von ihr auch nicht auf andere Weise Kenntnis erlangt ... . Diesem Vortrag ist die Bekl. nicht mit Substanz entgegengetreten. Sie hat sich vielmehr dem unzutreffenden Standpunkt des *LG* angeschlossen, die Kl. habe diese Version in der Klage zitiert und zum Gegenstand ihrer Beanstandung gemacht, weshalb von einer wirksamen Einigung auszugehen sei ...

34 ee) Auf die Frage, ob der von der Bekl. behauptete internationale Handelsbrauch hinsichtlich der Einbeziehung geänderter AGB besteht, kommt es danach nicht an. Die Willenseinigung der Vertragsparteien über die Gerichtsstandsklausel wird zwar vermutet, wenn sie in einer Weise in die Geschäftsbeziehung eingeführt wird, die einem solchen Handelsbrauch entspricht, wenn dieser den Parteien bekannt ist oder als ihnen bekannt angesehen werden muss (vgl. *EuGH* U. v. 20.2.1997 – C-106/95, Rn. 25 – MSG; a.a.O, Rn. 50 – Profit Investment SIM/Ossi; vgl. *BGH* U. v. 26.4.2018 – VII ZR 139/17, Rn. 23). Da von einer Veröffentlichung der AGB 2015 alt nicht ausgegangen werden kann, fehlt es jedoch an einer Einführung in die Geschäftsbeziehung.

35 ff) Auch die vom *LG* angenommenen Gepflogenheiten i.S.v. Art. 25 Abs. 1 S. 3 lit. b Brüssel-Ia-VO können lediglich die ansonsten erforderliche Schriftform ersetzen, nicht jedoch die Einigung der Vertragsparteien (*BGH* U. v. 25.2.2004 – VIII ZR 119/03 und v. 6.7.2004 – X ZR 171/02; WuW 2019, 143 [= MMR 2019, 208 (Ls.)], Rn. 16), und damit auch nicht die unverzichtbare Einbeziehung der Gerichtsstandsklausel durch deren Kenntnisnahme oder zumindest die Möglichkeit der Kenntnisnahme.

36 d) Ohne Erfolg beruft sich die Bekl. auf die identische Gerichtsstandsklausel in den AGB 2015 neu. Die Kl. hat von der Änderung zwar durch die E-Mail v. 25.5.2015 Kenntnis erlangt. Da die geänderten Bedingungen auf der verlinkten Internetseite veröffentlicht waren, hatte sie auch die Möglichkeit, die hier interessierende Gerichtsstandsklausel bei normaler Sorgfalt zur Kenntnis zu nehmen. Die Gerichtsstandsklausel ist jedoch nicht Gegenstand einer Willenseinigung der Parteien geworden. Denn die Kl. hat mit der Geltung der geänderten AGB nicht ihr Einverständnis erklärt (vgl. *BGH* U. v. 25.3.2015 – VIII ZR 125/14, Rn. 30). Die Kl. hat ihrer Einbeziehung ausdrücklich widersprochen. Ohne Erfolg macht die Bekl. geltend, die Zustimmung ergebe sich nach niederländischem Recht daraus, dass die Bekl. den Vertrag durchgeführt habe. Wie ausgeführt (Rn. 28) richtet sich das Verständnis des Begriffs der Gerichtsstandsvereinbarung nicht nach dem niederländischen Recht. Es handelt sich vielmehr um einen autonomen Begriff des Unionsrechts. In der bloßen Vertragsdurchführung kann danach jedenfalls wegen des ausdrücklichen Widerspruchs der Kl. keine Zustimmung zu der Geltung einer erweiterten Gerichtsstandsklausel gesehen werden (vgl. *Mankowski*, a.a.O., Rn. 217). ...

BGH: Bereithalten einer Verdachtsberichterstattung in Online-Archiv

Presse-Archive

BGB §§ 823 Abs. 1, 1004; GG Art. 1 Abs. 1, 2 Abs. 1, 5
Urteil vom 26.1.2021 – VI ZR 437/19 (OLG Schleswig, LG Itzehoe)

Leitsätze der Redaktion

1. Soweit nicht die ursprüngliche oder eine neuerliche Berichterstattung, sondern das öffentlich zugängliche Vorhalten eines Berichts, insbesondere in Presse-Archiven, in Rede steht, ist dessen Zulässigkeit anhand einer neuerlichen Abwägung der im Zeitpunkt des jeweiligen Löschungsbegehrens bestehenden gegenläufigen grundrechtlich geschützten Interessen zu beurteilen.

2. Dabei ist die ursprüngliche Zulässigkeit eines Berichts allerdings ein wesentlicher Faktor, der ein gesteigertes berechtigtes Interesse von Presseorganen begründet, diese Berichterstattung ohne erneute Prüfung oder Änderung der Öffentlichkeit dauerhaft verfügbar zu halten.

3. Zumutbar sind einschränkende Maßnahmen ggü. der unbehinderten und unveränderten Bereitstellung von ursprünglich zulässigen Presseberichten in Online-Archiven nur, wenn deren Folgen für die Betroffenen besonders gravierend sind.

Anm. d. Red.: Vgl. ferner *BVerfG* MMR 2020, 99 m. Anm. *Hoeren* = ZD 2020, 100 m. Anm. *Petri*; *BVerfG* MMR 2020, 793 (Ls.) = ZD 2020, 631; *BVerfG* MMR 2020, 458; *BGH* MMR 2021, 43 und *BGH* MMR 2019, 824.

Schlagworte: Allgemeines Persönlichkeitsrecht; Verdachtsberichterstattung; Online-Archiv; ursprünglich zulässige Berichterstattung; Presse-Archive

Sachverhalt

Der Kl. verlangt von der Bekl., die Veröffentlichung von Presseberichterstattungen und deren Bereithalten zum Abruf im Inter-

net zu unterlassen. Der Kl. ist Propst eines Kirchenkreises. Am 1. u. 2.3.2017 veröffentlichte die Bekl. jeweils einen Artikel, in dem auch über den Kl. berichtet wird. Der Kl. wendet sich sowohl gegen die Wiedergabe verschiedener Äußerungen Dritter in den Artikeln als auch gegen deren Online-Archivierung und verlangt Unterlassung.

Das *LG* hat die Bekl. entsprechend verurteilt. Das *OLG* hat die Berufung der Bekl. im Wesentlichen zurückgewiesen.

Aus den Gründen

7 A. Nach Auffassung des *Berufungsgerichts* steht dem Kl. gegen die Bekl. wegen eines rechtswidrigen Eingriffs in sein allgemeines Persönlichkeitsrecht der Unterlassungsanspruch zu. Selbst wenn die Erstveröffentlichung unter dem Gesichtspunkt der Verdachtsberichterstattung zulässig gewesen sei, sei die Bekl. zum maßgeblichen Zeitpunkt des Schlusses der mündlichen Verhandlung nicht befugt, die Verdachtsberichterstattung im Online-Archiv zum jederzeitigen Abruf bereitzuhalten und damit die streitigen Äußerungen weiter zu verbreiten. …

8 B. Die Revision der Bekl. ist begründet und führt zur Abweisung der Klage.

9 I. Dem Kl. steht der geltend gemachte Anspruch aus §§ 823 Abs. 1, 1004 BGB nicht zu.

10 1. Das *Berufungsgericht* ist teilweise von einem unzutreffenden Aussagegehalt der von der Bekl. wiedergegebenen Äußerungen des J. F. und der S. R. ausgegangen.

11 a) Die zutreffende Sinndeutung einer Äußerung ist unabdingbare Voraussetzung für die richtige rechtliche Würdigung ihres Aussagegehalts. Sie unterliegt in vollem Umfang der Nachprüfung durch das *Revisionsgericht*. …

12 b) Die Bekl. berichtet in ihren Artikeln über Spannungen und Vorwürfe innerhalb einer Kirchengemeinde und gibt in diesem Zusammenhang auch Äußerungen des J. F. und der S. R. wieder. Diese Äußerungen macht sich die Bekl. nicht zu eigen, da sie sich mit ihnen nicht identifiziert, sie nicht in eigene Gedankengänge einfügt und die betroffenen Vorgänge selbst nicht bewertet. …

28 4. Die Beurteilung des *Berufungsgerichts*, die Bekl. dürfe die ursprünglich rechtmäßig veröffentlichten Berichterstattungen nicht weiterhin zum Abruf in ihrem Online-Archiv bereithalten, ist unzutreffend.

29 a) Soweit nicht die ursprüngliche oder eine neuerliche Berichterstattung, sondern das öffentlich zugängliche Vorhalten eines Berichts, insb. in Presse-Archiven, in Rede steht, ist dessen Zulässigkeit anhand einer neuerlichen Abwägung der im Zeitpunkt des jeweiligen Löschungsbegehrens bestehenden gegenläufigen grundrechtlich geschützten Interessen zu beurteilen. Dabei ist die ursprüngliche Zulässigkeit eines Berichts allerdings ein wesentlicher Faktor, der ein gesteigertes berechtigtes Interesse von Presseorganen begründet, diese Berichterstattung ohne erneute Prüfung oder Änderung der Öffentlichkeit dauerhaft verfügbar zu halten. Denn in diesem Fall hat die Presse bei der ursprünglichen Veröffentlichung bereits die für sie geltenden Maßgaben beachtet und kann daher im Grundsatz verlangen, sich nicht erneut mit dem Bericht und seinem Gegenstand befassen zu müssen (vgl. BVerfGE 152, 152 [= MMR 2020, 99 m. Anm. *Hoeren* = ZD 2020, 100 m. Anm. *Petri*], Rn. 112 f., 115, 127, 130; *BVerfG* AfP 2020, 302 [= MMR 2020, 793 (Ls.) = ZD 2020, 631], Rn. 10; NJW 2020, 1793 [= MMR 2020, 458], Rn. 10; *Senat* U. v. 22.9.2020 – VI ZR 476/19 [= MMR 2021, 43], Rn. 10).

30 Die Interessen des Betroffenen sind mit den Interessen der Presse und der Allgemeinheit an der dauerhaften Zugänglichkeit einer ursprünglich zulässigen Berichterstattung in Hinblick auf die veränderten Umstände angemessen in Ausgleich zu bringen. Insoweit haben die Gerichte insb. die Schwere der aus der trotz der verstrichenen Zeit andauernden Verfügbarkeit der Information drohenden Persönlichkeitsbeeinträchtigung, den Zeitablauf seit dem archivierten Bericht, das zwischenzeitliche Verhalten des Betroffenen einschließlich möglicher Reaktualisierungen, die fortdauernde oder verblassende konkrete Breitenwirkung der beanstandeten Presseveröffentlichung, die Priorität, mit der die Information bei einer Namenssuche im Internet kommuniziert wird, das generelle Interesse der Allgemeinheit an einer dauerhaften Verfügbarkeit einmal zulässig veröffentlichter Informationen und das grundrechtliche Interesse von Inhalteanbietern an einer grds. unveränderten Archivierung und Zurverfügungstellung ihrer Inhalte angemessen zu berücksichtigen. Zumutbar sind einschränkende Maßnahmen ggü. der unbehinderten und unveränderten Bereitstellung von ursprünglich zulässigen Presseberichten in Online-Archiven nur, wenn deren Folgen für die Betroffenen besonders gravierend sind und sie damit eine solche Bereitstellung über Einzelfälle hinaus nicht schon grds. in Frage stellen (vgl. BVerfGE 152, 152 [= MMR 2020, 99 m. Anm. *Hoeren* = ZD 2020, 100 m. Anm. *Petri*], Rn. 101 ff., 107, 112 f., 114, 121 ff., 125, 130, 153; *BVerfG* AfP 2020, 302 [= MMR 2020, 793 (Ls.) = ZD 2020, 631], Rn. 11; NJW 2020, 1793 [= MMR 2020, 458], Rn. 11; *Senat* U. v. 22.9.2020 – VI ZR 476/19 [= MMR 2021, 43], Rn. 11; v. 18.12.2018 – VI ZR 439/17 [= MMR 2019, 824], Rn. 16, 24 f.).

31 b) Danach überwiegen auch insoweit die rechtlich geschützten Interessen des Klägers nicht diejenigen der Bekl. Es sind keine Umstände festgestellt oder sonst ersichtlich, aus denen sich ergibt, dass das weitere Bereithalten der ursprünglich rechtmäßigen Presseberichte zum Abruf im Archiv der Bekl. zu besonders gravierenden Folgen für den Kl. führt. …

OLG Dresden: Sperrung nach Änderung der YouTube-Nutzungsbedingungen wegen COVID-19-Pandemie

Änderungsklausel

BGB §§ 241 Abs. 1 S. 2 u. Abs. 2, 280, 305 Abs. 2, 307
Urteil vom 30.4.2021 – 4 W 118/21 (LG Chemnitz); rechtskräftig

Leitsätze

1. Wendet sich der Nutzer eines sozialen Netzwerks gegen die Sperrung eines Beitrags, ist auf die zum Zeitpunkt der letzten mündlichen Verhandlung geltenden vertraglichen Regelungen abzustellen.

2. Die Änderung der Nutzungsbedingungen eines sozialen Netzwerks ist nur wirksam, wenn sich der Anbieter entweder wirksam eine einseitige Änderung vorbehält oder mit dem Nutzer einen Änderungsvertrag abschließt.

Anm. d. Red.: Vgl. ferner *OLG Stuttgart* MMR 2020, 415; *OLG Dresden* MMR 2021, 575 – in diesem Heft; *OLG Nürnberg* MMR 2020, 873 (Ls.); *OLG Dresden* MMR 2020, 626 und *BGH* MMR 2018, 230 m. Anm. *Kiparski*.

Schlagworte: Internetplattform; Registrierung; Nutzungsbedingungen; Änderung der Nutzungsbedingungen; Fehlinformationen über COVID-19; Änderungsklausel

Sachverhalt

Der Verfügungskläger (nachfolgend: Kl.) begehrt im Wege des einstweiligen Verfügungsverfahrens, es der Verfügungsbeklagten (nachfolgend: Bekl.) zu untersagen, ein von ihm auf der Plattform der Bekl. hochgeladenes Video zu entfernen und ihn

wegen des Hochladens des Videos mit einer Verwarnung zu versehen. Der Kl. betreibt auf der Plattform der Bekl. einen eigenen Kanal namens „... .tv", der zum Zeitpunkt der Einreichung des Antrags auf Erlass der einstweiligen Verfügung knapp 100.000 Abonnenten hatte. Die Bekl. bietet Nutzern die Möglichkeit, eigene Videoinhalte auf der von ihr betriebenen Plattform zum Abruf für Dritte einzustellen. Nutzer, die – wie der Kl. – sich auf der Plattform der Bekl. registrieren und eigene Inhalte einstellen, erklären sich einverstanden, die vertraglichen Bestimmungen, insb. Nutzungsbedingungen einzuhalten. Im Mai 2020 machte die Bekl. zudem die „Richtlinie zu medizinischen Fehlinformationen über COVID-19" zum Gegenstand des Nutzungsverhältnisses. Am 29.1.2021 veröffentlichte der Kl. auf der Plattform der Bekl. ein Video. In dem ca. 25-minütigen Video werden anlässlich einer Demonstration gegen „Corona-Maßnahmen" verschiedene Personen interviewt. Am 31.1.2021 war das Video auf Veranlassung der Bekl. nicht mehr abrufbar. Gleichzeitig verwarnte diese den Kl. Eine dagegen seitens des Kl. persönlich erhobene Beschwerde wies die Bekl. mit Mail v. 1.2.2021 zurück.

Das *LG Chemnitz* hat den Antrag auf Erlass einer einstweiligen Verfügung zurückgewiesen.

Aus den Gründen

8 II. ... Die sofortige Beschwerde hat ... Erfolg. ...

11 3. Dem Kl. steht der geltend gemachte Verfügungsanspruch zu.

12 Der vom Kl. geltend gemachte Anspruch folgt aus § 241 Abs. 1 S. 2 u. Abs. 2 BGB i.V.m. dem Nutzungsvertrag bzw. § 280 BGB, wobei sein Begehren ggü. der Bekl. dahin geht, dass der Leistungserbringung entgegenstehende Verhalten, nämlich das streitgegenständliche Video zu sperren und ihn diesbezüglich zu verwarnen, zu unterlassen. Selbst wenn man diesbezüglich – wie beim gesetzlichen Unterlassungsanspruch – eine Erstbegehungs- bzw. eine Wiederholungsgefahr voraussetzen würde (vgl. dazu *OLG Stuttgart* U. v. 23.1.2019 – 4 U 214/18 [= MMR 2020, 415]; offen gelassen durch *Senat* U. v. 12.1.2021 – 4 U 1600/20 [= MMR 2021, 575 – in diesem Heft]), wäre diese hier auf Grund der bereits stattgefundenen Sperrung/Verwarnung zu bejahen.

13 a) Zwischen den Parteien besteht ein vertragliches Schuldverhältnis, durch welches sich die Bekl. verpflichtet hat, dem Kl. die Nutzung des von ihr zur Verfügung gestellten Portals zu ermöglichen (vgl. dazu nur *Senat*, a.a.O.; *OLG Nürnberg* U. v. 4.8.2020 – 3 U 3641/19 [= MMR 2020, 873 (Ls.)]).

14 b) Unstreitig ist zwischen den Parteien, dass der Kl. sich auf der Plattform der Bekl. registriert hat und die Nutzungsbedingungen sowie die „Richtlinie zu medizinischen Fehlinformationen über COVID-19" Gegenstand des Vertrags geworden sind. Bei der vorgenannten Richtlinie und den Nutzungsbedingungen handelt es sich auf Grund der einseitigen Vorgabe durch die Bekl. um AGB i.S.v. § 305 BGB. Mit den darin enthaltenen Verhaltensregeln definiert der Plattformbetreiber zugleich seine eigenen Rechte, Rechtsgüter und Interessen, auf die der Nutzer gem. § 241 Abs. 2 BGB bei der Inanspruchnahme der bereitgestellten Leistungen seinerseits Rücksicht zu nehmen hat (vgl. *Senat* B. v. 7.4.2020 – 4 U 2805/19 [= MMR 2020, 626]).

15 c) Die Bekl. war jedoch weder zum Zeitpunkt der (erstmaligen) Verhängung der Sanktionen Ende Januar 2021 noch ist sie jetzt nach den zwischen den Parteien geltenden vertraglichen Regelungen berechtigt, die Sanktionen ggü. dem Kl. auf Grund des streitgegenständlichen Videos zu verhängen. Da der vom Kl. geltend gemachte Anspruch (auch) in die Zukunft gerichtet ist, ist maßgeblich, inwieweit die Bekl. nach den zum Zeitpunkt der letzten mündlichen Verhandlung geltenden vertraglichen Regelungen berechtigt ist, die streitgegenständlichen Sanktionen zu ergreifen (vgl. *BGH* U. v. 11.10.2020 – VI ZR 62/17; *BGH* U. v. 11.10.2017 – ZR 210/16 [= MMR 2018, 230 m. Anm. *Kiparski*]).

16 Dahingestellt bleiben kann dabei, ob die Nutzungsbedingungen bzw. die „Richtlinie zur medizinischen Fehlinformation über COVID-19" einer AGB-rechtlichen Kontrolle standhalten, insb., ob sie dem Transparenzgebot genügen bzw. den Nutzer nicht unangemessen benachteiligen (§ 307 BGB). Denn die Inhalte des streitgegenständlichen Videos verstoßen bereits nicht gegen die Ende Januar 2021 gültige „Richtlinie zu medizinischen Fehlinformationen über COVID-19" (aa). Bzgl. der Neufassung der vorgenannten Richtlinie hat die Bekl. dagegen nicht glaubhaft gemacht, dass diese wirksam in den Vertrag einbezogen ist (bb).

17 aa) Die „Richtlinie zu medizinischen Fehlinformationen über COVID-19" in der damals gültigen Fassung ... enthält folgende Regelungen:
„Auf YouTube sind keine Inhalte in Bezug auf Covid-19 erlaubt, die ein ernsthaftes Risiko erheblicher Gefährdung mit sich bringen. Auf YouTube sind keine Inhalte erlaubt, die medizinische Fehlinformationen zu Covid-19 verbreiten, die im Widerspruch zu medizinischen Informationen der WHO oder lokaler Gesundheitsbehörden stehen. Dies beschränkt sich auf Inhalte, die den Informationen der WHO oder lokaler Gesundheitsbehörden zu folgenden Themen widersprechen: ...
Die folgenden Inhalte dürfen auf YouTube nicht veröffentlicht werden:
Fehlinformationen zur Behandlung: Inhalte, in denen Nutzern von einer medizinischen Behandlung abgeraten wird. ... Fehlinformationen zur Prävention: Inhalte, die Präventionsmethoden propagieren, die im Widerspruch zu Informationen der WHO oder lokaler Gesundheitsbehörden stehen. ..."

19 Unter Berücksichtigung der einzelnen Regelungen in der Richtlinie, die das Verbot von Inhalten ausdrücklich auf bestimmte Themen „beschränkt", wobei die Inhalte unter „Fehlinformationen zur Behandlung", „Fehlinformationen zur Prävention", „Fehlinformationen zur Diagnose" und „Fehlinformationen zur Übertragung" im Einzelnen angeführt werden, die nach der Richtlinie nicht erlaubt sein sollen und bei denen es sich damit um einen abschließenden Regelungskatalog und nicht nur um Beispiele für nicht erlaubte Inhalte handelt, da letztere am Ende der Richtlinie gesondert aufgeführt sind, enthält das Video keine Inhalte die gegen die Richtlinie in der Ende Januar 2021 gültigen Fassung verstoßen. Dies gilt insb. auch, soweit die Bekl. ... konkrete Äußerungen moniert, indem „die Infektiösität bzw. Sterblichkeit durch eine Corona-Erkrankung ... wiederholt mit der saisonalen Grippe verglichen werde" bzw. behauptet werde, die „WHO habe gesagt, COVID-19 sei nicht gefährlicher als eine normale Grippe" oder erklärt werde," dass eine Eindämmung des Virus durch ganz normale Hygienemaßnahmen möglich sei". ... Der beanstandete Vergleich in den Äußerungen zwischen einer Corona-Erkrankung und der saisonalen Grippe war dagegen von vornherein nicht Gegenstand des Regelungskatalogs nach der damals gültigen Fassung der Richtlinie.

20 bb) Soweit die Bekl. sich auf die ... „Richtlinie zu medizinischen Fehlinformationen über COVID-19" in der aktuellen, jedoch – im Vergleich zur alten Fassung – erheblich geänderten sowie erweiterten Fassung der Richtlinie bezieht, die nunmehr unter dem Punkt „Inhalte, in denen die Existenz von COVID-19 geleugnet wird" ausdrücklich Inhalte anführt, die den Vergleich von COVID-19 mit einer saisonalen Grippe zum Gegenstand haben, hat sie im Verfahren nicht glaubhaft gemacht, diese Fassung wirksam in den Vertrag einbezogen zu haben (vgl. dazu *Senat*, a.a.O.; *OLG Nürnberg* B. v. 6.4.2020 – 3 U 4566/19). Mit der Neufassung der Richtlinie hat die Bekl. die AGB geändert. Zwar kann der Verwender von AGB – z.B. bei einer Änderung der Marktlage oder der gesetzlichen Bedingungen – auch bei

Dauerschuldverhältnissen vor die Notwendigkeit gestellt sein, seine AGB während der Laufzeit bestehender Verträge ganz oder teilweise neu zu fassen. Dazu bedarf es jedoch grds. eines Änderungsvertrags, wenn er sich nicht wirksam das Recht vorbehalten hat, die AGB einseitig zu ändern (vgl. *Senat*, a.a.O.; MüKoBGB, 8. Aufl., § 305 Rn. 88 mwN). Zwar hat die Bekl. in der Richtlinie auf die Möglichkeit der Anpassung der Richtlinie hingewiesen, mit dem bloßen Hinweis in den Richtlinien, dass diese sich ändern können, wenn sich die zu Grunde liegenden Informationen der weltweiten oder lokalen Gesundheitsbehörden zum Virus ändern, liegt jedoch keine Änderungsklausel vor, mit welcher sich der Verwender ein Änderungsrecht der Bedingungen einräumt. Aber selbst wenn man darin eine Änderungsklausel sehen würde, wäre diese ersichtlich nicht wirksam (vgl. wegen der Einzelheiten: *Senat*, a.a.O.; MüKoBGB, a.a.O., Rn. 90). Liegt daher – wie hier – eine wirksame Änderungsklausel nicht vor, müssen die geänderten AGB unter Beachtung der Voraussetzungen des § 305 Abs. 2 BGB einbezogen werden, d.h. der Verwender muss den anderen Teil ausdrücklich auf die Neufassung hinweisen und ihm den geänderten Text zugänglich machen. Erst wenn dieser sich dann nach einem entsprechenden Hinweis mit den geänderten AGB – z.B. durch Anklicken eines Links oder (konkludent) durch ein Fortsetzen der Nutzung – einverstanden erklärt, kommt ein entsprechender Änderungsvertrag zu Stande (vgl. *Senat*, a.a.O., *OLG Nürnberg*, a.a.O.). Dabei wird der Verwender seinen Hinweispflichten (§ 305 Abs. 2 Nr. 1 BGB) im Allgemeinen aber nur gerecht, wenn er die Neufassung drucktechnisch hervorhebt oder dem Vertragspartner erläutert (vgl. MüKoBGB, a.a.O., Rn. 88 ff.). Der Kl. hat jedoch in der mündlichen Verhandlung erklärt, was von der Bekl. auch nicht durch entsprechende Glaubhaftmachung, einen (ausreichenden) Hinweis erteilt zu haben, widerlegt worden ist, bereits einen derartigen Hinweis auf die Neufassung der Richtlinie seitens der Bekl. nicht erhalten zu haben, sodass eine wirksame Einbeziehung der geänderten Richtlinie nicht festgestellt werden kann. ...

OLG Koblenz: Voraussetzungen des Medienprivilegs bei Online-Journalismus

Gegendarstellung

MStV § 20 Abs. 1, Abs. 3; RStV § 56; GG Art. 5 Abs. 1 S. 2
Beschluss vom 12.4.2021 – 4 W 108/21 (LG Koblenz)

Leitsätze der Redaktion

1. Eine kumulativ zur redaktionellen Gestaltung erforderliche journalistische Gestaltung setzt jedenfalls voraus, dass die Auswahl und Strukturierung der Inhalte gewissen Kriterien genügt, zu denen zumindest auch eine erkennbar publizistische Zielsetzung des Angebots gehört.

2. Nicht alle redaktionell gestalteten Angebote gehören auch zum Online-Journalismus. Es muss die Absicht einer Berichterstattung i.S.d. Art. 5 Abs. 1 S. 2 GG gegeben sein, denn nur die Tätigkeiten, die der Erfüllung der Aufgaben einer funktional verstandenen Presse bzw. des Rundfunks dienen, werden vom Medienprivileg erfasst.

3. Davon ausgehend wird kommerzielle Kommunikation grds. nicht als journalistisch-redaktionell gestaltetes Angebot angesehen, da sie nicht an Kriterien gesellschaftlicher Relevanz ausgerichtet ist, sondern an den verfolgten wirtschaftlichen Interessen.

Anm. d. Red.: Vgl. ferner *VGH München* ZD 2017, 348; *OVG Bautzen* ZD 2016, 200 (Ls.); *KG* ZD 2017, 139 und *OLG Bremen* MMR 2011, 337.

Schlagworte: Gegendarstellung; journalistisch-redaktionell gestaltetes Angebot; kommerzielle Kommunikation

Aus den Gründen

1 Die ... sofortige Beschwerde des Ast. ist unbegründet.

2 Zu Recht ist das *LG* davon ausgegangen, dass es an der hinreichenden Erfolgsaussicht der Rechtsverfolgung i.S.d. § 114 ZPO mangelt, weil kein Verfügungsanspruch besteht. Der Ast. hat keinen Anspruch gegen den Ag. auf Veröffentlichung der begehrten Gegendarstellung gem. § 20 Abs. 1 u. Abs. 3 MStV (entspricht § 56 RStV), weil kein journalistisch-redaktionell gestaltetes Angebot i.S.d. § 20 Abs. 1 MStV durch den Ag. vorliegt.

3 1. Welche Angebote als journalistisch-redaktionell anzusehen sind, ist im MStV nicht definiert und die Frage, unter welchen Voraussetzungen im Einzelnen ein Angebot i.S.d. § 20 MStV „journalistisch-redaktionell" gestaltet ist, ist bisher nicht in jeder Hinsicht abschließend geklärt. Insb. gilt dies betreffend die Abgrenzungsschwierigkeiten gerade in Fallkonstellationen, in denen Angebote nicht von klassischen Redaktionen mit speziell ausgebildeten Journalisten nach tradierten Berufsregeln erstellt werden (vgl. ausf. *Held*, in: Binder/Vesting, Rundfunkrecht, 4. Aufl., § 54 RStV Rn. 38 ff.). Dieser Umstand steht indessen einer Versagung der Prozesskostenhilfe nicht etwa deshalb entgegen, weil sich einer Klärung im Hauptsachverfahren vorbehaltene Rechtsfragen stellen würden.

4 Denn eine kumulativ zur redaktionellen Gestaltung erforderliche journalistische Gestaltung setzt jedenfalls voraus, dass die Auswahl und Strukturierung der Inhalte gewissen Kriterien genügt, zu denen zumindest auch eine erkennbar publizistische Zielsetzung des Angebots gehört. Daran fehlt es hier. Dafür ist nämlich erforderlich, dass die Informationen – für den Nutzer erkennbar – nach ihrer gesellschaftlichen Relevanz und mit dem Ziel des Anbieters, zur öffentlichen Kommunikation beizutragen, ausgewählt werden (vgl. *Held*, a.a.O., Rn. 51; ebenso *OLG Bremen* U. v. 14.1.2011 – 2 U 115/10 [= MMR 2011, 337], Rn. 44 zu § 56 RStV; *OVG Berlin-Brandenburg* B. v. 13.8.2014 – OVG 11 S 15.14, Rn. 24; *VGH Baden-Württemberg* U. v. 9.5.2017 – 1 S 1530/16, Rn. 105; *BayVGH* B. v. 27.1.2017 – 7 CE 16.1994 [= ZD 2017, 348], Rn. 20; *OVG Bautzen* B. v. 10.7.2015 – 3 B 96/15 [= ZD 2016, 200 (Ls.)], Rn. 10). Nicht alle redaktionell gestalteten Angebote gehören daher auch zum Online-Journalismus (*VGH Baden-Württemberg*, a.a.O.). Es muss die Absicht einer Berichterstattung i.S.d. Art. 5 Abs. 1 S. 2 GG gegeben sein, denn nur die Tätigkeiten, die der Erfüllung der Aufgaben einer funktional verstandenen Presse bzw. des Rundfunks dienen, werden vom Medienprivileg erfasst (*BGH* U. v. 22.2.2011 – VI ZR 115/09, Rn. 26 zu § 57 Abs. 1 RStV; *OVG Berlin-Brandenburg*, a.a.O.).

5 Davon ausgehend wird u.a. kommerzielle Kommunikation grds. nicht als journalistisch-redaktionell gestaltetes Angebot angesehen, da sie nicht an Kriterien gesellschaftlicher Relevanz ausgerichtet ist, sondern an den verfolgten wirtschaftlichen Interessen (*Held*, a.a.O., Rn 59; *OVG Berlin-Brandenburg*, a.a.O.; *VGH Baden-Württemberg*, a.a.O.).

6 Aus dem vom Ast. zitierten Beschluss des *KG* v. 28.11.2016 – 10 W 173/16 [= ZD 2017, 139] ergibt sich nichts Anderes.

7 2. Vorliegend fehlt es erkennbar an der erforderlichen publizistischen Zielsetzung sowohl der Homepage des Ag. selbst, als auch des Blogs, über den der beanstandete Artikel aufgerufen werden kann, als auch des Artikels selbst. Zu weit geht es jedenfalls, in die Betrachtung, ob ein journalistisch-redaktionell gestaltetes Angebot vorliegt, andere Websites und Internetplattformen, auf denen der Ag. Veröffentlichungen vornehmen mag, einzubeziehen.

8 Auf seiner Homepage gibt der Ag. als Tätigkeitsfelder seiner Kanzlei die Rechtsbereiche Abmahnung, Wettbewerbsrecht, Ur-

heberrecht, Arbeitsrecht, Rufschädigung und IT-Recht an und stellt sich und seine Kanzlei vor. ...

11 In dem vom Ast. beanstandeten Artikel berichtet der Ag. – zu seinem Tätigkeitsfeld passend ... – über diverse Rechtsverletzungen durch den Ast. auf seinem YouTube-Kanal, vorrangig durch die Verletzung fremder Marken und Inhalte und stellt ihn als gewinnerzielungsorientierten Wettbewerber dar, der sich nicht auf journalistische Freiheitsrechte berufen könne. Die Frage, ob und inwieweit die Inhalte rechtlich und tatsächlich zutreffen, sowie der Umstand, dass Stil, Hauptüberschrift und Einleitung eher dazu dienen, die Aufmerksamkeit des Lesers zu erregen und sein Interesse am Weiterlesen zu fördern, sind für die Frage, ob es sich um ein journalistisch-redaktionell gestaltetes Angebot handelt, irrelevant. Maßgebend ist allein, dass der Artikel nach Standort und Inhalt von einer ersichtlich kommerziellen Zielsetzung des Ag. geprägt ist, nämlich der Mandantenwerbung aus einem vom Ast. potenziell geschädigten Personenkreis.

12 Der Sachverhalt ist nicht [mit] dem vergleichbar, der der Entscheidung des *OLG Bremen*, a.a.O., zu Grunde lag. Dort gab der Anwalt unter einer Rubrik „Medien" laufend Pressemitteilungen heraus, unterhielt ein „Pressearchiv" und betrieb – auch nach der Selbstdarstellung – aktive „Medienarbeit" mit dem erklärten Ziel der Aufklärung von Anlegern und dem Kampf gegen den verbreiteten Lobbyismus von Banken und Finanzdienstleistern. Das geht über ein Kanzleimarketing hinaus. ...

OLG Köln: Unlautere Behinderung auf einem Marketplace

Herkunftshinweis

MarkenG §§ 4, 14 Abs. 1, Abs. 2 Nr. 1, Abs. 5, 23 Nr. 2, 140 Abs. 3; BGB § 242; UWG §§ 3, 4 Nr. 4, 5 Abs. 1 S. 2
Urteil vom 26.3.2021 – 6 U 11/21 (LG Köln)

Leitsätze

1. Ein unterhalb der Artikelbezeichnung auf dem Portal Amazon.de als „Marke" eingetragenes Zeichen wird in der Regel als Herkunftshinweis des Produkts wahrgenommen.

2. Es ist rechtsmissbräuchlich, wenn ein Anbieter auf dem Amazon-Marketplace, der als erster ein Angebot erstellt und so eine ASIN generiert, als „Marke" eine Marke einträgt, die entgegen den Richtlinien des Marketplace-Betreibers nicht auf dem Produkt oder dessen Verpackung abgedruckt ist, und sodann gegen Verkäufer vorgeht, die sich diesem Angebot anschließen.

Anm. d. Red.: Vgl. ferner *BGH* MMR 2012, 694 m. Anm. *Albrecht* – pjur/pure; *BGH* MMR 2008, 777 (Ls.) – EROS; *OLG Frankfurt/M.* MMR 2012, 183; *LG Düsseldorf* MMR 2014, 613; *LG Düsseldorf* MMR-Aktuell 2014, 358272 (Ls.); *Spindler/Seins*, MMR 2013, 415; *BGH* MMR 2018, 230 m. Anm. *Kiparski* – Portierungs-Auftrag und *BGH* MMR 2002, 605 – Vanity-Nummer.

Schlagworte: Marke; Artikelbezeichnung; Herkunftshinweis; ASIN; Rechtsmissbrauch; Behinderung; Amazon-Marketplace

Sachverhalt

Die Parteien streiten über die Frage, ob die Ag. eine Marke der Ast. i.R.e. Angebots auf dem Amazon-Marketplace unbefugt genutzt und Verbraucher in die Irre geführt hat.

Die Ast. betreibt einen Handel mit Lebensmitteln und Getränken vorwiegend aus dem US-Import. Ihr Angebot richtet sich an Verbraucher und Gewerbetreibende. Die Ast. ist Inhaberin der Wortmarke „Marke1", die u.a. für die Waren „Chips, Erdnussbutter, Bonbons, Cerealien, Kaugummi, Nudeln und Schokolade" geschützt ist. Für die Ware „Bier" genießt die Marke keinen Schutz. Am 1.9.2020 stellte die Ast. fest, dass die Ag. auf dem Internetverkaufsportal Amazon Bonbons und alkoholische Getränke unter Verwendung des Zeichens „Marke1" anbot. Die „Marke" des jeweiligen Produkts wird durch den ersten Anbieter, der das Produkt über die Plattform Amazon.de anbieten möchte, angegeben. Nach den von *Amazon* vorgegebenen Grundsätzen darf an der entsprechenden Stelle lediglich eine Marke eingetragen werden, die entweder auf dem Produkt selbst oder auf dessen Verpackung zu finden ist.

Die Ast. hat in dem Angebot der Ag. von Süßigkeiten eine Markenverletzung gesehen. Das Angebot sei darüber hinaus – wie auch das Angebot von Bier – irreführend, weil eine Täuschung über die betriebliche Herkunft i.S.d. § 5 Abs. 1 S. 2 UWG erfolge. Die Ast. hat eine e.V. des *LG* erwirkt. Es könne dahinstehen, ob die Angebote der Firma „V2" der Ast. „zuzurechnen" seien und diese die Angebote als erste eingestellt hätte. Dies unterstellt, liege eine Markenverletzung vor, weil die Nutzung der Bezeichnung „Marke1" durch die Ag. die Rechte der Ast. an der Wortmarke der Ast. verletze, sodass diese Unterlassung verlangen könne, §§ 4, 14 Abs. 1, Abs. 2 Nr. 1 MarkenG.

Die Ag. habe sich das Angebot insgesamt zu eigen gemacht. Das Zeichen werde als Marke genutzt und die Marke genieße Schutz für die angebotenen Produkte. Es bestehe Zeichen- und Warenidentität und die Nutzung sei nicht nach § 23 Nr. 2 MarkenG zulässig. Die Ast. handele nicht rechtsmissbräuchlich. Soweit das „Anhängen" an identische Produkte auf der Plattform Amazon.de vorgesehen sei, entbinde dies die Ag. nicht von der Verpflichtung, ein Angebot zu prüfen, bevor sie sich an ein solches anhänge. Wenn eine Markenverletzung festgestellt werde, müsse ein eigenes Angebot erstellt werden.

Aus den Gründen

23 II. Die ... Berufung der Ag. hat ... Erfolg. Zwar besteht im Ausgangspunkt ein Unterlassungsanspruch nach § 14 MarkenG. Entgegen der Ansicht der Ast. ist die Geltendmachung des Unterlassungsanspruchs durch die Ast. aber rechtsmissbräuchlich, sodass die Ast. den an sich bestehenden Anspruch nicht durchsetzen kann. Im Einzelnen:

24 1. Das *LG* hat mit Recht ... angenommen, dass sich ein Unterlassungsanspruch der Ast. gegen die Ag. aus § 14 Abs. 1, Abs. 2 S. 1 Nr. 1, Abs. 5 S. 1 MarkenG ergibt.

25 a) Die Ast. ist als Inhaberin der Antragsmarke befugt, den Unterlassungsanspruch geltend zu machen.

26 b) Die sich gegenüberstehenden Zeichen sind identisch i.S.d. § 14 Abs. 2 S. 1 Nr. 1 MarkenG.

27 c) Die Ag. hat die Klagemarke der Ast. benutzt. Eine markenmäßige Benutzung oder – was dem entspricht – eine Verwendung als Marke setzt voraus, dass die Bezeichnung i.R.d. Produkt- oder Leistungsabsatzes jedenfalls auch der Unterscheidung der Waren oder Dienstleistungen eines Unternehmens von denen anderer dient (vgl. *BGH* [= MMR 2012, 694 m. Anm. *Albrecht*] – pjur/pure, mwN). ...

28 Vorliegend ist der Verkehr daran gewöhnt, dass als „Marke" unterhalb der eigentlichen Artikelbezeichnung im oberen Bereich der Darstellung des jeweiligen Produktangebots auf der Plattform Amazon.de die Marke des Produkts benannt wird. Dies stelle regelmäßig eine Wiederholung der bereits in der Überschrift genannten Produktmarke dar.

29 Dass die Produktmarke auf der Plattform Amazon.de regelmäßig an der genannten Stelle angegeben wird, sodass der Verkehr sich an eine entsprechende Bezeichnung gewöhnt hat, ergibt sich auch aus den Verkäuferbedingungen für ein Angebot

auf dem Amazon-Marketplace. Denn in den Bedingungen ist festgelegt, dass eine Marke „kein anderer Name sein (darf), der nicht auf den Markenprodukten oder -verpackungen angegeben ist". Da sich die große Mehrheit der Händler auf dem Amazon-Marketplace an diese Vorgabe hält, ist auf Grund der entsprechenden Bedingungen ein Rückschluss auf die entsprechenden Gewohnheiten und damit auch auf die Verkehrsauffassung möglich. ...

31 Wie das *LG* mit Recht angenommen hat, führt § 23 MarkenG nicht zu einer Berechtigung der Ag., die Marke zu nutzen. Die entsprechende Annahme des *LG* hat die Ag. auch nicht angegriffen.

32 2. Es besteht auch ein Anordnungsgrund. Dieser wird gem. § 140 Abs. 3 MarkenG vermutet. ...

33 3. Der Geltendmachung der Ansprüche aus § 14 MarkenG steht aber der Einwand des Rechtsmissbrauchs i.S.v. § 242 BGB entgegen, weil die Geltendmachung der Ansprüche unlauter gem. §§ 3, 4 Nr. 4 UWG ist.

34 a) Den aus einer Marke hergeleiteten Ansprüchen kann einredeweise entgegen gehalten werden, dass auf Seiten des Markeninhabers Umstände vorliegen, die die Geltendmachung des markenrechtlichen Schutzes als eine wettbewerbswidrige Behinderung i.S.v. § 4 Nr. 4 UWG erscheinen lassen (vgl. *BGH* U. v. 15.10.2015 – I ZB 69/14 – GLÜCKSPILZ; U. v. 26.6.2008 – I ZR 190/05 [= MMR 2008, 777 (Ls.)] – EROS; U. v. 12.7.2007 – I ZR 148/04 – CORDARONE; *Hacker*, in: Ströbele/Hacker/Thiering, MarkenG, 13. Aufl., § 14 Rn. 55). Das wettbewerbsrechtlich Unlautere kann darin liegen, dass ein Zeichenanmelder die mit der Eintragung des Zeichens kraft Zeichenrechts entstehende und wettbewerbsrechtlich an sich unbedenkliche Sperrwirkung zweckfremd als Mittel des Wettbewerbskampfs einsetzt (vgl. *BGH* U. v. 3.2.2005 – I ZR 45/03 – Russisches Schaumgebäck; *OLG Frankfurt/M.* U. v. 27.10.2011 – 6 U 179/10 [= MMR 2012, 183]). Der *BGH* hat ausdrücklich angenommen, dass bei einer böswillig angemeldeten Marke dem Unterlassungsanspruch der Einwand des § 4 Nr. 4 UWG entgegengehalten werden kann, auch wenn Löschungsansprüche nicht bestehen (vgl. *BGH* U. v. 15.10.2015 – I ZB 44/14 – LIQUIDROM).

35 b) Nach diesen Grundsätzen stellt die Geltendmachung der markenrechtlichen Ansprüche eine unlautere Behinderung der Ag. gem. § 4 Nr. 4 UWG dar.

36 aa) Eine Behinderung liegt vor, wenn die wettbewerbliche Entfaltungsmöglichkeit des Mitbewerbers beeinträchtigt wird. Das setzt eine Beeinträchtigung der wettbewerblichen Entfaltungsmöglichkeiten der Mitbewerber voraus, die über die mit jedem Wettbewerb verbundene Beeinträchtigung hinausgeht und bestimmte Unlauterkeitsmerkmale aufweist. Unlauter ist die Beeinträchtigung im Allgemeinen, wenn gezielt der Zweck verfolgt wird, Mitbewerber an ihrer Entfaltung zu hindern und sie dadurch zu verdrängen oder wenn die Behinderung dazu führt, dass die beeinträchtigten Mitbewerber ihre Leistung am Markt durch eigene Anstrengung nicht mehr in angemessener Weise zur Geltung bringen können. Ob diese Voraussetzungen erfüllt sind, lässt sich nur auf Grund einer Gesamtwürdigung der relevanten Umstände des Einzelfalls unter Berücksichtigung der Interessen der Mitbewerber, Verbraucher oder sonstiger Marktteilnehmer sowie der Allgemeinheit beurteilen (vgl. *BGH* U. v. 11.10.2017 – I ZR 210/16 [= MMR 2018, 230 m. Anm. *Kiparski*] – Portierungs-Auftrag; U. v. 21.2.2002 – I ZR 281/99 [= MMR 2002, 605] – Vanity-Nummer). Hierzu zählen alle Wettbewerbsparameter, wie der Absatz, wobei die Eignung zur Behinderung ausreicht, auch wenn diese noch nicht eingetreten ist (vgl. *BGH*, a.a.O. – Portierungs-Auftrag; *Köhler*, in: Köhler/Bornkamm/Feddersen, UWG, 39. Aufl., § 4 Nr. 4 Rn. 4.6). ...

38 bb) Nach diesen Grundsätzen liegt eine gezielte Behinderung vor. Die Ag. wird daran gehindert, die mit der jeweiligen Marke gekennzeichneten Produkte über den Amazon-Marketplace anzubieten.

39 Die Ag. hat durch die Vorlage der „Richtlinie zur ASIN-Erstellung" des Amazon-Marketplace glaubhaft gemacht, dass ein Produkt nur einmal unter einer sog. „ASIN" angeboten werden darf. Dies hat zur Folge, dass der erste Anbieter eines bestimmten Produkts ein Angebot erstellen muss, an das sich weitere Anbieter „anhängen" können, aber auch dürfen und müssen. Den weiteren Anbietern ist es – was die Ag. glaubhaft gemacht hat – untersagt, für dasselbe Produkt ein neues Angebot unter einer neuen „ASIN" zu erstellen. In der RL ist ausdrücklich Folgendes festgeschrieben:

40 Die Erstellung einer neuen ASIN für ein Produkt, das bereits im Amazon-Katalog vorhanden ist, ist nicht gestattet und kann dazu führen, dass Ihnen die Verkaufsberechtigung oder die Berechtigung für die Erstellung von ASINs vorübergehend oder dauerhaft entzogen wird.

41 Vor diesem Hintergrund läuft ein Anbieter, der entgegen der Regelungen durch den Amazon-Marketplace neue Angebote erstellt und sich nicht an bestehende Angebote anhängt, Gefahr, keine Angebote mehr für den Amazon-Marketplace erstellen zu dürfen oder von der Nutzung der Plattform ausgeschlossen zu werden.

42 Dies hat zur Folge, dass der erste Anbieter eines bestimmten Produkts durch die Gestaltung des ersten Angebots, mit dem die sog. „ASIN" angelegt wird, zahlreiche Vorgaben machen kann. Wie die Ag. glaubhaft gemacht hat, ist es etwa möglich, eine „Marke" einzutragen, die in der dargestellten Form unterhalb des Produkts wiedergegeben wird. Diese Angaben sind zwar grds. durch die RL des Amazon-Marketplace begrenzt, weil in diesem Feld – wie dargelegt – lediglich die Angabe der Bezeichnung zulässig ist, mit der das Produkt oder dessen Verpackung gekennzeichnet sind. Diese Vorgabe ist allerdings im vorliegenden Fall umgangen worden, weil die Bezeichnung „Marke1" eingetragen wurde, obwohl weder das Produkt, noch die Verpackung diese Kennzeichnung aufweisen.

43 Die Eintragung der Bezeichnung „Marke1" in dem Feld Marke hat sodann zur Folge, dass sich weitere Verkäufer, die das dort angebotene Produkt, das tatsächlich von der Marke „Mike And Ike" stammt und auch so gekennzeichnet ist, lediglich diesem Angebot „anschließen" können und daher die Marke „Marke1" zwangsläufig – wie dargestellt – als Marke in unzulässiger Weise nutzen. Ein Verkäufer hat lediglich die Wahl, das konkrete Produkt nicht über den Amazon-Marketplace anzubieten oder – entgegen den Vorgaben für die Nutzung des Amazon-Marketplace – eine weitere ASIN für ein vermeintlich neues Produkt zu erstellen. Faktisch wird damit jeder Dritte daran gehindert, dasselbe Produkt anzubieten.

44 Es ist auch zu berücksichtigen, dass der angesprochene Verkehr es gewohnt ist, dass der Verkäufer von Produkten bei Amazon.de in einem gesonderten Bereich genannt wird, weil eine Vielzahl der Produkte über Amazon.de von zahlreichen Verkäufern, aber unter einer einheitlichen Präsentation angeboten werden. Daher kann die Bezeichnung des Anbieters in dem Feld „Marke" im konkreten Fall eine Irreführung der angesprochenen Verkehrskreise darstellen (vgl. *OLG Hamm* U. v. 22.11.2018 – 4 U 73/18). ...

46 Insgesamt ist die Eintragung der Marke „Marke1" in dem konkret zum Gegenstand des Unterlassungsantrags gemachten Angebot vor diesem Hintergrund als gezielte Behinderung i.S.d. § 4 Nr. 4 UWG anzusehen. ...

Anmerkung

RA Dr. Ruben A. Hofmann, HEUKING KÜHN LÜER WOJTEK, Köln

Amazon ist unbestreitbar einer der wichtigsten Online-Marktplätze der Welt geworden. Dementsprechend überrascht es nicht, dass immer wieder findige Händler versuchen, Produktangebote über die sog. Amazon Standard Identification Number (ASIN) für sich zu monopolisieren. Denn i.R.d. Ansatzes maximaler (End-)Kundenfreundlichkeit und Preistransparenz ist Amazon darauf erpicht, dass nach Möglichkeit alle Anbieter eines Produkts gemeinschaftlich bei diesem Produkt bzw. der entsprechenden ASIN angegeben werden, damit die Kunden so die Preise auf einen Blick vergleichen können. So hat sich der Ausdruck des „Anhängens" an eine ASIN entwickelt, wenn mehrere Anbieter das gleiche Produkt anbieten und dies jeweils unter Nutzung der ursprünglich für dieses Produkt angelegten ASIN.

Bei einer Vielzahl von ASIN zeigt Amazon seit geraumer Zeit unmittelbar unterhalb der Artikelbezeichnung ein Zeichen als „Marke" an, das in der Regel als Herkunftshinweis des Produkts wahrgenommen wird. Oft handelt es sich dabei nicht um eine eingetragene Marke, sondern um den Verkäufernamen. Dies erkennt man daran, dass wenn man auf die Informationen zur „Marke" unterhalb der Artikelbeschreibung klickt, eine Auflistung der Angebote eines bestimmten Verkäufers angezeigt werden. Eine eigene Marke bei Amazon ist allerdings insoweit von Vorteil, da der Anbieter so die ASIN exklusiv nutzen kann und andere Anbieter von der Nutzung ausgeschlossen werden. So auf jeden Fall die bisherige Rechtslage.

Die aktuelle Entscheidung des *OLG Köln* zeigt aber, dass die Anforderungen für eine exklusive Nutzung nun gestiegen sind und das Anmelden einer Marke allein, die sich in der ASIN findet, nun nicht mehr ausreichend sein kann.

1. Ausgangslage

Die Ast. ist Inhaberin der Wortmarke „lifestyledrinkz" und vertreibt über Amazon eine Vielzahl von Lebensmittel, insb. aus dem US-Import. Sie stellte fest, dass die Ag. auf Amazon Bonbons und alkoholische Getränke unter Verwendung dieser Wortmarke anbot. Unter der Artikelüberschrift war die Marke der Ast. angegeben worden – die Ag. hatte sich an die ASIN angehangen. Darin sah die Ast. eine Markenrechtsverletzung und Irreführung. Sie erwirkte eine einstweilige Verfügung des *LG Köln*, die durch Urteil bestätigt wurde. Auf Grund dessen wurde die Ag. zunächst dazu verpflichtet, den Verkauf der entsprechenden Produkte unter Angabe der Marke zu unterlassen.

Dagegen wandte sich die Ag. im Wege der Berufung vor dem *OLG Köln*. Mit dieser machte sie geltend, die Ast. handle rechtsmissbräuchlich, indem sie die Kennzeichnung der Angebote mit „lifestyledrinkz" bewusst nutze, um andere Wettbewerber vom Vertrieb der Originalwaren amerikanischer Hersteller auszuschließen und sie so in ihrem Tätigwerden am Markt zu behindern.

2. Rechtsumfeld der ASIN

Im Bereich „Marketplace" auf der Internetverkaufsplattform Amazon können Händler ihre Angebote einstellen. Zur eindeutigen Identifizierung von Produkten implementierte Amazon die ASIN. Eine solche besteht aus 10 Buchstaben und/oder Ziffern anhand derer Artikel bei Amazon eindeutig identifiziert werden können und wird nur einmal pro Produkt vergeben, welches auf Amazon zum Verkauf angeboten wird. Für jedes Produkt gibt es daher (nur) eine individuelle ASIN. In der „Richtlinie zur ASIN-Erstellung" von Amazon (abrufbar unter: https://sellercentral.amazon.de/gp/help/external/G201844590?language=de_DE) heißt es:

„Richtlinie zur Erstellung doppelter ASIN: Die Erstellung einer neuen ASIN für ein Produkt, das bereits im Amazon-Katalog vorhanden ist, ist nicht gestattet und kann dazu führen, dass Ihnen die Verkaufsberechtigung oder die Berechtigung für die Erstellung von ASINs vorübergehend oder dauerhaft entzogen wird."

Die Angabe einer Marke ist nach den von Amazon vorgegebenen Grundsätzen nur zulässig, wenn das Produkt oder dessen Verpackung mit der Marke gekennzeichnet ist, die Marke also im rechtlichen Sinne (§ 26 MarkenG) auch benutzt wird. Dies führt dazu, dass der Erstanbieter eines bestimmten Produkts ein Angebot erstellen muss, an das sich anderen Anbieter „anhängen" können. Dies mag zwar für den preisvergleichenden Kunden praktisch sein. Erstanbieter eines bestimmten Produkts können aber durch die Gestaltung des ersten Angebots, mit dem die ASIN angelegt wird, zahlreiche Vorgaben machen. Dabei kann es für die Händler zu Verletzungen von Markenrechten kommen oder gegen das Wettbewerbsrecht verstoßen werden.

3. Urteil des OLG Köln

Warum das Anhängen weiterer Anbieter an den Erstanbieter u.U. wettbewerbswidrig und sogar rechtsmissbräuchlich sein kann, entschied das *OLG Köln* nun im vorliegenden Urteil.

Grds. nimmt das *OLG Köln* das Vorliegen einer Markenrechtsverletzung zwar an. Der Verkehr sei daran gewöhnt, dass auf Amazon als „Marke" unterhalb der eigentlichem Artikelbezeichnung im oberen Bereich der Darstellung des jeweiligen Produktangebots die Marke des Produkts benannt wird. Dies ergebe sich auch aus den Verkäuferbedingungen des Online-Marktplatzes. In diesen wird festgelegt, dass eine Marke „kein anderer Name sein (darf), der nicht auf den Markenprodukten oder -verpackungen angegeben ist". Hier trugen die betroffenen Produkte der Ag. zwar den Namen „Mike And Ike Mega Mix Candy", als Marke wurde darunter aber „lifestyledrinkz" angegeben. Teile des Verkehrs, welchen die Marke „Mike And Ike" fremd ist, nähmen an, das Produkt stamme eben vom Inhaber dieser Marke, d.h. die Marke würde somit als Herkunftsnachweis genutzt.

So entschied in der Vergangenheit schon das *OLG Hamm* (U. v. 19.7.2011 – I-4 U 22/11), dass das Anhängen an eine fremde ASIN regelmäßig eine Markenrechtsverletzung sein kann, sofern eine fremde eingetragene Marke für das eigene Angebot mit einem anderen Produkt verwendet wird oder unzulässig ein fremdes Unternehmenskennzeichen wie z.B. eine Firma des Konkurrenten im eigenen Angebot benutzt wird.

Ebenso entschied das *LG Düsseldorf* (MMR 2014, 613), dass das Anhängen eines eigenen Produkts an eine fremde ASIN eine irreführende Angabe über die betriebliche Herkunft der Ware darstelle und die Nutzung einer fremden ASIN folglich als Markenrechtsverletzung gewertet werden kann. Durch die Täuschung über die betriebliche Herkunft der angebotenen Produkte werde der Eindruck erweckt, die Produkte des Konkurrenten stammten aus dem Betrieb der Markeninhaberin. In einem weiteren Urteil entschied das *LG Düsseldorf* (MMR-Aktuell 2014, 358272 (Ls.)), dass ein Konkurrent ein identisch beschafftes Produkt nicht als Ware aus dem Betrieb des Ersterstellers anbieten kann, wenn er es von einem Dritten beziehen kann.

In Bezug auf die Nutzung von Bildrechten auf Grund des Anhängens durch andere Händler hatte das *OLG Frankfurt/M.* in einer Entscheidung (MMR 2012, 183) die Geltendmachung von Unterlassungsansprüchen als rechtsmissbräuchlich betrachtet, sofern die Produkte zumindest kurzfristig erst mit entsprechenden gebrandeten Bildern versehen wurden (hier-

zu *Spindler/Seins*, MMR 2013, 415 ff.). Somit war es in der Vergangenheit für Händler unter Beachtung der Nutzungsbedingungen von Amazon der einzige Weg, eine ASIN für sich zu monopolisieren, indem eine Marke in die Artikelbeschreibung innerhalb der ASIN eingebettet wurde. Dieser Weg ist nun an höhere Anforderungen geknüpft.

Nach der Ansicht des *OLG Köln* ist der gegebene Unterlassungsanspruch nicht durchsetzbar, da im vorliegenden Fall ein Rechtsmissbrauch in Form eines Behinderungswettbewerbs gegeben ist. Die Ast. habe die Eintragung der Marke in unlauterer Weise vorgenommen. Andere Händler würden daran gehindert werden, die mit der jeweiligen Marke gekennzeichneten Produkte bei Amazon anzubieten. Die Folge der „Richtlinie ASIN-Erstellung" von Amazon ist, dass ein Produkt nur einmal unter einer ASIN angeboten werden darf. Dies führt dazu, dass der Ersteller der ASIN diese so gestalten muss, dass auch weitere Anbieter sich daran anhängen können, dürfen und müssen. Das Anlegen einer weiteren ASIN auf Grund der unzulässigen Monopolisierung einer ASIN kann sogar zum Ausschluss von der Nutzung der Amazon-Plattform führen.

Problematisch ist hier, dass eine Marke zwar eingetragen und unterhalb der Artikelüberschrift angezeigt wurde, die Produkte selbst aber nicht mit dieser gekennzeichnet waren. Nach den von Amazon vorgegebenen Grundsätzen darf an der entsprechenden Stelle nur eine Marke eingetragen werden, die entweder auf dem Produkt selbst oder auf dessen Verpackung zu finden ist. Die einzige Alternative für einen Verkäufer, der das Produkt ebenfalls anbieten möchte, ist dieses nicht mehr über Amazon zu verkaufen oder eine weitere ASIN für ein vermeintlich neues Produkt zu erstellen (was nach den Amazon-Nutzungsbedingungen wohl unzulässig wäre). Hier differenziert das *OLG Köln* klar zwischen solchen Markenprodukten, auf denen die Marke abgedruckt ist und solchen bei denen dies nicht der Fall ist. Dies dürfte für die Zukunft die entscheidende Weichenstellung sein.

Weiter geht das *OLG Köln* davon aus, dass einem Verkäufer bei Amazon die Bedingungen für die Nutzung der Plattform bekannt sind. Diese Annahme ist sicher zutreffend, muss der Händler doch eben diese Bedingungen vor der Aufnahme von Geschäftsaktivitäten auf Amazon akzeptieren. Die Eintragung einer eigenen Marke entgegen den Bedingungen von Amazon könne nur den Zweck haben, Dritte daran zu hindern, das Produkt über Amazon anzubieten und so den Wettbewerb Dritter zu behindern. Auch die für den Kunden bedeutsame Möglichkeit, den Verkäufer mit dem günstigsten Verkaufspreis auszuwählen, kann so verhindert werden. Dem hat das *OLG Köln* nun einen Riegel vorgeschoben.

4. Fazit

Eine vom Händler exklusiv genutzte ASIN kann auf dem Marketplace von Amazon einen relevanten Wettbewerbsvorteil begründen. Daher machen Amazon-Verkäufer immer häufiger von (nun wohl: unlauteren) Mitteln Gebrauch, um eigene Angebote zu monopolisieren und so andere Wettbewerbsteilnehmer bei der Nutzung zu behindern oder sogar davon auszuschließen. Grds. hat die Einrede des Rechtsmissbrauchs hohe Anforderungen.

Es ist zu begrüßen, dass das *OLG Köln* in seinem Urteil klare Worte findet und erkennt, dass es bei der Frage, ob eine Abmahnung gegen das Anhängen an eine Marken-ASIN einen Rechtsmissbrauch darstellt, von Belang ist, ob auf dem Markenprodukt die Marke nicht abgedruckt ist. Nach der Ansicht des *OLG Köln* handelt es sich bei einer Abmahnung gegen das Anhängen an Marken-ASIN um einen Rechtsmissbrauch, solange auf dem Markenprodukt die Marke nicht abgedruckt ist.

Insgesamt stellt sich die Frage, ob es möglich sein soll, dass einzelne Händler Marken-ASIN auf dem Marketplace von Amazon für sich monopolisieren können. Dies wird maßgeblich durch die Amazon-Richtlinien vorgegeben. Auf Grund der erheblichen Marktmacht von Amazon muss daher die Frage gestellt werden, ob hier nun sogar ein weiteres, gesetzgeberisches (?) Eingreifen erforderlich ist. Das *OLG Köln* hat in jedem Fall hier einen wunden Punkt des ASIN-Systems beleuchtet.

OLG Rostock: Dringender Tatverdacht wegen Verwendung eines Krypto-Handys

Verschlüsseltes Nachrichtensystem

StPO §§ 112 ff.
Beschluss vom 23.3.2021 – 20 Ws 70/21 (LG Rostock, AG Rostock)

Leitsätze der Redaktion

1. Schon die Verwendung eines Krypto-Handys der Fa. EncroChat deutet auf ein konspiratives Verhalten zur Begehung und Verdeckung von Straftaten hin.

2. Die EncroChat-Erkenntnisse und die darauf aufbauenden Beweisergebnisse sind im Strafprozessrecht verwertbar.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 6824.

Schlagworte: EncroChat; verschlüsseltes Nachrichtensystem; Verwertung von Beweismitteln; konspiratives Verhalten; kriminelles Milieu

Sachverhalt

Die *StA Rostock* führt gegen den Beschuldigten das verfahrensgegenständliche Ermittlungsverfahren wegen unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge.

Am 2.12.2020 erließ das *AG Rostock* gegen den Beschuldigten einen Haftbefehl wegen des dringenden Tatverdachts des unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge in vier Fällen. Der dringende Tatverdacht stützte sich hiernach auf die Auswertungen der von den französischen Ermittlungsbehörden in einem dortigen Verfahren erlangten und sodann im Rechtshilfeweg an die deutschen Ermittlungsbehörden übermittelten EncroChat-Nachrichten.

Aus den Gründen

10 II. Die … weitere Beschwerde … ist unbegründet. Die Voraussetzungen für den Fortbestand des Haftbefehls des *AG Rostock* … liegen vor.

11 1. Der dringende Tatverdacht (§ 112 Abs. 1 StPO) folgt aus den bislang gewonnenen, verwertbaren Beweismitteln. Schon die Verwendung eines Krypto-Handys der Fa. *EncroChat* deutet auf ein konspiratives Verhalten zur Begehung und Verdeckung von Straftaten hin (*OLG Bremen* B. v. 18.12.2020 – 1 Ws 166/20). Soweit der Beschuldigte die Ansicht vertreten lässt, die EncroChat-Erkenntnisse und die darauf aufbauenden Beweisergebnisse seinen prozessrechtlich nicht verwertbar, teilt der *Senat* diese Auffassung nicht. Zur Vermeidung von Wiederholungen wird auf die Beschlussgründe des *OLG Bremen* (a.a.O.) und des *OLG Hamburg* v. 29.1.2021 – 1 Ws 2/21 – Bezug genommen. Den dort vertretenen Auffassungen schließt sich der *Senat* an. Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden (EncroChat) vgl. zudem *Pauli*, NStZ 2021, 146 mwN …

OLG Köln: Auskunftsanspruch nach § 14 TMG bei internem Beschwerdesystem

Handelsplattform

TMG §§ 2 Nr. 1, 14 Abs. 3 u. Abs. 4; EuGVVO Art. 7 Nr. 2; NetzDG § 1 Abs. 3; StGB § 186
Beschluss vom 11.3.2021 – 15 W 10/21 (LG Köln)

Leitsätze der Redaktion

1. Der Betreiber einer Handelsplattform ist als Diensteanbieter zur Auskunft über Bestandsdaten verpflichtet, wenn Beschwerden über ein Unternehmen unwahre ehrenrührige Tatsachenbehauptungen enthalten. Unter Bestandsdaten fallen nicht nur die zur Feststellung der Identität der Kunden erforderlichen Informationen, sondern auch die – dem Unternehmen bislang nicht bekannten – Inhalte der Kundenbeschwerden unter Angabe deren vollständigen Wortlauts.

2. Kapitalgesellschaften kommt der Schutz der §§ 185-187 StGB zu, wenn sie eine rechtlich anerkannte soziale Funktion erfüllen und einen einheitlichen Willen bilden können.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 7395. Vgl. ferner *OLG Celle* ZD 2021, 211; *BGH* ZD 2020, 152 und *BGH* MMR 2021, 322.

Schlagworte: Handelsplattform; Bestandsdaten; Kundenbeschwerden; Marketplace; Gestattungsverfahren

Sachverhalt

Die Ast. begehrt vorliegend eine gerichtliche Anordnung über die Zulässigkeit einer Auskunftserteilung nach § 14 Abs. 4 TMG. Dabei begehrt sie i.E. von der Beteiligten Auskunft betreffend in ihren Anträgen näher bezeichneter (Bestands-)Daten im Zusammenhang mit auf der Plattform Internetadresse 1 von registrierten Nutzern über Online-Formulare in den Kundenkonten zu einzelnen, über die sog. A (A) im Antrag konkretisierten Angeboten der Ast. eingereichte Beschwerden als Kunden der Ast.

Die Beteiligte verantwortet den „Betrieb" des sog. „Marketplace" auf Internetadresse 1, über den Online-Händler Produkte bundesweit über das Internet vertreiben können. Händler können ihre Waren dabei unter Verwendung eigener Produktbilder und -beschreibungen einstellen, wobei neu eingestellten Angeboten jeweils eine A zugewiesen wird, über die das Produkt im System eindeutig identifiziert und aufgefunden werden kann. Für die Erstellung von Angeboten durch ihre Kunden (= Onlinehändler) hat die Beteiligte Richtlinien aufgestellt. Die Ast. ist Kundin der Beteiligten und bietet so als Online-Händlerin unter dem Namen „Träumegut" Neuwaren – keine Gebrauchtwaren – aus dem Bereich Matratzen/Matratzentopper an.

Kunden, welche über Internetadresse 1 Bestellungen bei den dort agierenden Online-Händlern getätigt haben, können über ihr Kundenkonto im System eigene Bestellungen einsehen, Waren retournieren und (intern) über bereitgestellte Onlineformulare auch etwaige Probleme mit einer Bestellung (wie z.B. Abweichungen zwischen Zustand und Beschreibung) der Beteiligten melden. Der Fortbestand der Verkaufsberechtigung der Online-Händler auf dem „Marketplace" der Beteiligten ist dabei auch von der sog. „Verkäuferleistung" abhängig, die sich anhand verschiedener Kriterien bestimmt, u.a. von veröffentlichten Kundenbewertungen, aber auch von Beschwerden von Kunden ggü. der Beteiligten über das zur Verfügung gestellte Online-System abhängig ist. Die „Verkäuferleistung" kann in dem im Verkäuferkonto eines jeden Online-Händlers integrierten sog. „Kennzahlenmonitor" eingesehen werden. Hinsichtlich der Einhaltung der „Produktrichtlinien" der Beteiligten als Kriterium sollen nach deren Vorgaben „0 Beschwerden oder Verstöße" erreicht werden, um nicht die Verkaufsberechtigung auf dem „Marketplace" zu gefährden. Die einzelnen Beschwerden werden in dem System dabei für die Internethändler wiederum nicht sichtbar hinterlegt; diese erhalten von der Beteiligten auch keine Angaben zur Identität der Bf.

Die Ast. verlangte ergebnislos eine Entfernung der Beschwerden aus dem Verkäuferkonto bzw. die Nichtberücksichtigung bei der Ermittlung der „Verkäufer-Performance" und zudem auch Auskunftserteilung über die Einzelheiten zum Zwecke der eigenen Inanspruchnahme der jeweiligen Bf. wegen Falschbehauptungen. Die Ast. hat daraufhin einen „Antrag auf Erlass einer einstweiligen Anordnung gem. § 14 Abs. 3-5 TMG" gestellt, mit der der Beteiligten eine entsprechende Auskunftserteilung „gestattet" werden sollte.

Das *LG* hat den Antrag zurückgewiesen. Es hat dies im Wesentlichen darauf gestützt, dass die internationale Zuständigkeit fehle. Der Antrag sei i.Ü. aber auch unbegründet: Zwar sei die Beteiligte als Diensteanbieter gem. § 2 Nr. 1 TMG anzusehen, aber es fehle an „Inhalten" i.S.v. § 14 Abs. 3 TMG mangels öffentlicher Äußerung/Veröffentlichung/Einsehbarkeit der hier nur intern gebliebenen und nicht öffentlich einsehbaren Kundenbeschwerden (anders als bei veröffentlichten Kundenbewertungen); diese Konstellation werde von § 14 TMG nicht erfasst.

Aus den Gründen

14 II. Die ... Beschwerde ... hat ... in der Sache keinen Erfolg.

15 1. Es fehlt ... an der internationalen Zuständigkeit der deutschen Gerichte für den hier gestellten Antrag nach § 14 Abs. 4 TMG. ...

34 2. Hat der hier gestellte Antrag schon allein deswegen ohne Erfolg zu bleiben, stellt der *Senat* jedoch vorsorglich klar, dass i.Ü. hinsichtlich des Antrags ... Bedenken an der Lesart des *LG* bestehen ...

35 a) Der *Senat* geht mit dem *VI. Zivilsenat des BGH* davon aus, dass § 14 TMG nicht nur auf Betreiber sog. sozialer Netzwerke, sondern richtigerweise auf alle Diensteanbieter i.S.d. § 2 Nr. 1 TMG Anwendung findet (*BGH* B. v. 24.9.2019 – VI ZB 39/18 [= ZD 2020, 152], Rn. 46-54). Die Beteiligte ist hier aber „Diensteanbieter", mag auch der rein technische Betrieb der Website ... als solches durch eine andere juristische Person (AEC) erfolgen und die Beteiligte daran anknüpfend nur den „Marketplace" verantworten. ...

36 Bei dem in die Nutzerkonten der Kunden der Onlinehändler fest integrierten Beschwerde- und Kommunikationssystem mit einer festen Einbindung gerade auch in die automatisierte und dort abrufbare Auswertung der „Verkäufer-Performance" handelt es sich um elektronische Informations- und Kommunikationsdienste, die nicht nur reine TK-Dienste i.S.d. § 3 Nr. 24 TKG – mit Diensten die ganz oder überwiegend in der Übertragung von Signalen über TK-Netz bestehen – sind oder die den anderen Ausnahmen in § 1 Abs. 1 S. 1 TMG unterfallen. ... Dass Angebote der Individualkommunikation über Handelsplattformen im Grundsatz vom TMG erfasst werden, ist auch anerkannt (*Spindler*, in: Spindler/Schmitz, TMG, 2. Aufl. 2018, § 1 Rn. 75); im Gegenzug ist zweifelhaft, ob auf der Plattform der Beteiligten der einzelne Online-Händler selbst noch Diensteanbieter ist (*Spindler*, a.a.O., § 2 Rn. 14). ...

40 e) Die Auskunft beträfe in dem nach dieser Auslegung beantragtem Umfang dann auch „Bestandsdaten" (nachfolgend: aa)). Entgegen der Auffassung des *LG* würden dabei auch Fälle

wie der vorliegende (zugegeben spezielle) Sonderfall erfasst, in denen es nicht um öffentlich gemachte und deswegen allen Beteiligten bereits bekannte „Inhalte" im Internet geht (die vom Gericht im Gestattungsverfahren dann nur inhaltlich zu würdigen wären), sondern um „sonstige" Persönlichkeitsrechtsverletzungen im Internet (nachfolgend: bb)). Die begehrte Auskunft wäre ... auch „zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte auf Grund rechtswidriger Inhalte, die von ... § 1 Abs. 3 NetzDG erfasst werden, erforderlich." § 1 Abs. 3 NetzDG verweist u.a. auf § 186 StGB, der hier – wie sogleich zu zeigen ist (nachfolgend: cc)) – einschlägig ist. Auch bestünde – was im Gestattungsverfahren gleichsam von Amts wegen zu prüfen ist (*BGH*, a.a.O., Rn. 58; *OLG Celle* B. v. 7.12.2020 – 13 W 80/20 [= ZD 2021, 211], Rn. 27), von § 14 Abs. 4 TMG bewusst nicht geregelt und insgesamt der Rspr. zur Klärung überlassen bleibt (BT-Drs. 18/13013, 23) – hier richtigerweise wohl auch ein materieller Auskunftsanspruch der Ast., ohne dass die Einzelheiten des luxemburgischen Sachrechts zu klären sind ...

41 aa) Die hier verlangte Auskunft erfasst „Bestandsdaten" i.S.d. § 14 Abs. 1 TMG, sodass es auf den ergänzend für Nutzungsdaten flankierend eingreifenden § 15 Abs. 5 S. 4 TMG nicht mehr ankommen würde. Soweit teilweise im Zusammenhang mit Online-Shops generell ausgetauschte „inhaltsbezogene" Daten ausgeklammert werden, wenn die Telemedien nur als Kommunikationsmittel der Vertragsparteien genutzt werden (so wohl *Hullen/Roggenkamp*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, § 14 TMG Rn. 3, 5, weiter u.U. Rn. 18 zu den Inhalten bei Auktionsplattformen wegen der Speicherung für die vermittelten Vertragsschlüsse mit Dritten), wäre das zwar möglicherweise auf den vorliegenden Fall zu übertragen, in dem der Endkunde – der ebenfalls in die Nutzung der Plattform eingewilligt hat und insofern vertraglich an die Beteiligte gebunden ist – der Beteiligten ggü. eine Mitteilung zu einem mit der Ast. geschlossenen Vertrag macht (und dies wiederum Folgen für diese haben kann). Diese enge Lesart überzeugt richtigerweise aber so nicht (*Schmitz*, in: Spindler/Schmitz, a.a.O., § 14 Rn. 13), weil der Telemediendienst eben hier auch und gerade in der Bereitstellung des Marketplace mit seinen verschiedenen Interaktions- und Beschwerdemöglichkeiten liegt, dort Persönlichkeitsrechtsverletzungen wegen der dabei mitgeteilten Inhalte drohen und die datenschutzrechtliche Ausgangslage letztlich noch dem Regelungszweck des § 14 TMG entspricht. Der *Senat* verkennt dabei ausdrücklich nicht, dass im Regelfall des § 14 Abs. 4 TMG die rechtsverletzende Handlung als solche offen zu Tage getreten ist (wie bei einer Internetveröffentlichung etwa in sozialen Netzwerken) oder dem Betroffenen zumindest als solche bekannt ist (wie bei rechtsverletzenden Mitteilungen über einen Messenger-Dienst an Bekannte des Betroffenen im Fall *BGH*, a.a.O.). Die richterlich zu gestattende Auskunft betrifft in einem solchen Regelfall sicher nur die Bestandsdaten, die zur Feststellung der Identität des Verletzten bekannt sind. Auch ist § 14 Abs. 4 TMG bewusst der Regelung in § 101 Abs. 9 UrhG nachgebildet, wo die Rechtsverletzung mit Blick auf § 109 Abs. 2 UrhG regelmäßig als solche „offensichtlich" und auch nach außen hin (etwa über illegale Filesharing-Dienste) erkennbar geworden ist und es ebenfalls allein um die Aufdeckung der Identität geht. Das spricht nach Auffassung des *Senats* in einem Sonderfall wie dem vorliegenden aber dennoch nicht dagegen, als Bestandsdaten auch den „Inhalt der Kundenbeschwerden unter Angabe des vollständigen Wortlauts" zu erfassen, zumal auch diese nach § 14 Abs. 1 TMG als personenbezogene Daten zur „inhaltlichen Ausgestaltung" der wechselseitigen Nutzerbeziehungen i.R.d. Telemediendienstes der Beteiligten erhoben, verwendet und gespeichert werden. ...

42 Soweit der Auskunftsanspruch aus § 103 Nr. 1 UrhG jedenfalls E-Mail-Adressen nicht erfasst (*BGH* U. v. 10.12.2020 – I ZR 153/17 [= MMR 2021, 322]) ist das dem dortigen enger gefassten Wortlaut und Art. 8 RL 2004/48/EG geschuldet und daher auch nicht nach hier zu übertragen.

43 bb) § 14 Abs. 4 S. 1 TMG verweist auf § 14 Abs. 3 TMG und dieser wiederum auf „rechtswidrige Inhalte", die von § 1 Abs. 3 NetzDG erfasst werden. Diese Regelung nennt wiederum „Inhalte im Sinne des Absatzes 1", welche zugleich den Tatbestand einer der in Bezug genommenen strafrechtlichen Regelungen im konkreten Fall erfüllen. § 1 Abs. 1 NetzDG erläutert den Begriff der „Inhalte" weiter, sodass es um „Plattformen" geht, die dazu bestimmt sind, dass Nutzer „beliebige Inhalte" entweder „mit anderen Nutzern teilen" oder aber „der Öffentlichkeit zugänglich machen"; aus dem so definierten Begriff der „soziale(n) Netzwerke" werden dann in Abs. 1 S. 2 u. S. 3 NetzDG bestimmte Fälle ausgenommen. Spricht schon der erste Satzteil von Absatz 1 S. 1 eher dagegen, nur allgemein im Internet der Öffentlichkeit zugänglich gemachte Inhalte (wie etwa Tatsachenbehauptungen in Kundenbewertungen) zu erfassen (sondern zumindest bei sozialen Netzwerken eben auch direkt übermittelte Nachrichten z.B. im Messengerdienst), hat jedenfalls der *BGH* die richterliche Gestattung aus § 14 Abs. 4 TMG – vorbehaltlich fehlender Feststellungen zur Einordnung als Telemedium im damaligen Fall – ausdrücklich von dem engen Begriff der „sozialen Netzwerke" und dem NetzDG losgelöst und ganz allgemein so etwa auch auf Fälle erstreckt, in denen private Nachrichten mit ehrverletzenden Inhalten an einzelne Nutzer verschickt worden sind, weil richtigerweise hier alle Rechtsverletzungen im Internet im Zusammenhang mit der Nutzung von Telemedien zu erfassen seien (*BGH* B. v. 24.9.2019, a.a.O., Rn. 53). Das ist überzeugend. Der Gedanke greift dann aber auch hier durch, weil es – durchaus vergleichbar – um ehrverletzende Tatsachenbehauptungen in bilateral bleibenden Beschwerden/Nachrichten (nur) der Beteiligten ggü. geht; auch darin liegen „Persönlichkeitsrechtsverletzungen im Internet", die § 14 Abs. 4 TMG eigentlich bei gebotener Schwere umfassend ahnden helfen soll. Dass der Gesetzgeber Sonderfälle wie den vorliegenden dabei sicher nicht vor Augen gehabt haben mag, trägt allein keine einschränkende Auslegung der Norm.

44 cc) Wie eingangs bereits betont, ginge es hinsichtlich des Antrags ... dann auch um eine tatbestandliche Erfüllung der in § 1 Abs. 3 NetzDG genannten Strafvorschriften, hier konkret des § 186 StGB. Das Gericht ist in Verfahren nach § 14 Abs. 4 TMG gehalten, sicherzustellen, dass es nicht „vorschnell" zur Herausgabe der Daten kommen kann, weswegen etwa eine bloße Behauptung, ein Nutzer habe eine verletzende Nachricht verschickt, nicht genügen kann, sodass das Gericht in solchen Fällen etwa von Amts wegen zu ermitteln (§§ 26 ff. FamFG) und sich davon zu überzeugen hat (§ 37 FamFG), ob, wann und mit welchem Inhalt zu den streitgegenständlichen A von Kunden Beschwerden mit rechtswidrigen Inhalten i.S.d. § 1 Abs. 3 NetzDG versandt worden sind (*BGH*, a.a.O., Rn. 57). Im hier vorliegenden Fall tritt insofern aber die oben bereits beim Begriff der „Bestandsdaten" angesprochene Problematik hinzu, dass – anders als im Regelfall des § 14 Abs. 4 TMG – die genauen Inhalte der persönlichkeitsrechtsverletzenden Äußerung bisher der Ast. gar nicht bekannt und als solche erst Gegenstand des Auskunftsverlangens sind, doch würde dies im vorliegenden Fall die Gestattung nicht hindern.

45 (1) Denn dass es insofern tatsächlich entsprechende Nachrichten (Beschwerden) der (vermeintlichen) Kunden der Ast. zu den genauen ASIN über die Systeme der Plattform der Beteiligten ggü. gegeben hat und deswegen durch diese auch die Entfernung der Produkte erfolgt ist, ist unstreitig. Ebenso ist unstreitig, dass alle Beschwerden inhaltlich stets die angebliche Zusendung von gebrauchter Ware statt der vertraglich zugesagten

Neuware rügten. Dass dies wiederum nicht den Tatsachen entsprach und mithin mit der Behauptung unwahre Tatsachenbehauptungen aufgestellt worden ist, hat die Ast. aber mittels eidesstattlicher Versicherung glaubhaft gemacht und dafür streitet auch deutlich die im i.Ü. wiederum unstreitige Tatsache, dass sie erheblichen Angriffen durch missbräuchlich agierende Wettbewerber ausgesetzt war, sie allein durch den Verkauf von Neuware auf der Plattform der Beteiligten erhebliche Umsätze generiert und retournierte Ware gerade nicht erneut veräußert. Dass eine derartige unwahre Tatsachenbehauptung jedenfalls für einen Onlinehändler im Bereich der aus Kundensicht ganz besonderen Hygieneanforderungen unterliegenden Matratzenwelt ehrenrührig i.S.d. § 186 StGB ist, steht außer Frage. Soweit *OLG Celle*, a.a.O., Rn. 12 juristischen Personen offenbar generell den Schutz des § 186 StGB abgesprochen hat, folgt das nicht aus der a.a.O. zitierten Entscheidung des *BGH* U. v. 8.1.1954 – 1 StR 260/53, Rn. 19 (sondern im Gegenteil), die zitierte Literaturstimme von *Kett-Straub*, ZStW 120 (2008), 759 (776 ff.) ist auch eine Minderauffassung. Es entspricht – zu Recht – der seit langem herrschenden Auffassung im Strafrecht, dass Kapitalgesellschaften gleichsam der Schutz der §§ 185-187 StGB zukommt, wenn sie – wie die Ast. – eine rechtlich anerkannte soziale Funktion erfüllen und einen einheitlichen Willen bilden können (vgl. etwa *OLG Köln* U. v. 20.2.1979 – 1 Ss 69/79; BeckOK StGB/*Valerius*, 48. Ed., § 185 Rn. 11 ff.; Schönke/Schröder/*Eisele/Schittenhelm*, 30. Aufl. 2019, Vorbem zu den §§ 185 ff. Rn. 3; *Schneider*, in: Dölling u.a., Gesamtes Strafrecht, 4. Aufl. 2017, § 185 Rn. 10). ...

OLG Dresden: Posten eines Bilds mit Symbolen einer „Hassorganisation"

Soziales Netzwerk

BGB §§ 129, 241 Abs. 1 S. 2, 242, 256, 305 ff.; ZPO §§ 256, 531 Abs. 1; DS-GVO Art. 82
Urteil vom 12.1.2021 – 4 U 1600/20 (LG Chemnitz); rechtskräftig

Leitsätze

1. Die nach den Nutzungsbedingungen eines sozialen Netzwerks unzulässige Unterstützung von Hassorganisationen liegt nicht bereits im kommentarlosen Posten eines Bilds, das Symbole einer solchen Hassorganisation zeigt.

2. Die Auslegung von Posts in einem sozialen Netzwerk hat unter Berücksichtigung anderer, im zeitlichen und räumlichen Zusammenhang der Seite stehender Äußerungen zu erfolgen.

3. Ein Klageantrag auf Feststellung, dass die Sperrung oder Löschung einzelner Posts auf einem sozialen Netzwerk rechtswidrig war, ist unzulässig.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 879. Vgl. hierzu ferner *OLG Dresden* ZD 2021, 93; *OLG Dresden* ZD 2020, 308; *OLG Dresden* MMR 2020, 407; *OLG Dresden* ZD 2020, 413; *OLG Dresden* MMR 2021, 58; *OLG Dresden* MMR 2012, 542; *OLG Dresden* MMR 2020, 418 und *OLG Dresden* ZD 2019, 567.

Schlagworte: Soziales Netzwerk; Fotografie; Wiederherstellungsanspruch; Unmöglichkeit; Feststellungsinteresse; Persönlichkeitsrecht; Read-only-Modus; Auskunft; Verschwörungstheorien

Sachverhalt

Der Kl., der bei der Bekl. ein privates Nutzerkonto unterhält, macht Ansprüche im Zusammenhang mit der Entfernung einer von ihm geposteten Fotografie geltend.

Aus den Gründen

5 II. ... Der Kl. hat gegen die Bekl. einen Anspruch auf Unterlassung der Sperrung und Datenberichtigung auf der Grundlage des § 241 Abs. 1 S. 2 BGB i.V.m. dem zwischen den Parteien geschlossenen Nutzungsvertrag. Die geltend gemachten Sekundäransprüche auf Feststellung, Auskunftserteilung und Schadensersatz stehen ihm hingegen nicht zu.

6 1. Indem der Kl. bei der Bekl. ein privates Nutzerkonto eingerichtet hat, ist zwischen den Parteien ein Vertrag zu Stande gekommen, nach dessen Inhalt die Bekl. im Rahmen ihrer seit April 2018 geltenden Nutzungsbedingungen verpflichtet ist, dem Kl. eine Plattform für seine Äußerungen zur Verfügung zu stellen. Diesen Bedingungen hat der Kl. am 30.4.2018 durch Anklicken des entsprechenden Buttons auf der Benutzeroberfläche zugestimmt. Der *Senat* hat bereits mehrfach entschieden, dass durch Anklicken der „Ich-stimme-zu"-Schaltfläche wirksam in die Änderung der Nutzungsbedingungen des sozialen Netzwerks der Bekl. eingewilligt werden kann und dass die geänderten Nutzungsbedingungen sich i.R.d. §§ 305 ff. BGB halten (U. v. 20.8.2020 – 4 U 784/20 [= ZD 2021, 93]; B. v. 13.11.2019 – 4 U 1471/19 [= ZD 2020, 308]; B. v. 6.12.2019 – 4 U 2198/19 [= MMR 2020, 407]; B. v. 11.12.2019 – 4 U 1680/19 [= ZD 2020, 413]). Dies gilt auch für das in Nr. 2 der Gemeinschaftsstandards enthaltene Verbot der Unterstützung von „Hassorganisationen".

7 2. ... Das vom Kl. gepostete Foto stellt keinen Verstoß gegen die Nutzungsbedingungen und Gemeinschaftsstandards dar. Auf die vom *LG* bejahte Frage, ob die „Identitäre Bewegung" (IB), deren Flagge u.a. auf diesem Bild zu sehen ist, eine „Hassorganisation" i.S.v. Ziff. 2 der Gemeinschaftsstandards ist, kommt es insofern nicht an.

8 Entgegen der Auffassung des Kl. in der Berufungsbegründung wird der verständige Betrachter des im Tenor aufgenommenen Fotos allerdings nicht davon ausgehen, dass die dort zu sehende Flagge der IB lediglich zufälliges „Beiwerk" ist, das in der dort ebenfalls zu sehenden Menschenmenge mehr oder weniger untergeht und das Bild daher nicht zu prägen vermöchte. Tatsächlich dokumentiert das Foto mit der Flagge der IB i.V.m. den übrigen auf dem Bild erkennbaren Flaggen und Spruchbänder wie dem unschwer auszumachenden Transparent mit dem Slogan „Merkel muss weg" und der sog. Wirmer-Flagge die typische Symbolik, die sich auf Demonstrationen von Anhängern der Rechten Szene ... seit etwa 2015 eingebürgert hat. ...

9 Die bloße Einstellung dieses Fotos ... stellt jedoch noch keine Unterstützungshandlung i.S.v. Nr. 2 der Gemeinschaftsstandards dar. Der durchschnittliche Nutzer, der sich die Gemeinschaftsstandards aufmerksam durchliest, wird diesen Begriff ebenso verstehen, wie er auch im Strafrecht Verwendung findet (vgl. *Senat* U. v. 16.6.2020 – 4 U 2890/19 [= MMR 2021, 58]). Danach ist als Unterstützungshandlung jedwedes Tätigwerden zu verstehen, das die innere Organisation und den Zusammenhalt einer Hassorganisation unmittelbar fördert oder sich sonst auf die Aktionsmöglichkeiten und Zwecksetzung der Vereinigung in irgendeiner Weise positiv auswirkt (*BGH* NJW 2009, 3448; *Fischer*, StGB, 64. Aufl., § 129 Rn. 30). Auch wenn die Bekl. bereits die Präsenz von Hassorganisationen als solche in ihrem Netzwerk nicht dulden will (Abschnitt I. Ziff. 2 der Gemeinschaftsstandards), kann gleichwohl nicht jede Abbildung, die Symbole dieser Organisationen oder deren Verantwortliche zeigt, als Unterstützung einer Hassorganisation eingestuft werden. Anderenfalls wäre etwa auch die journalistische Berichterstattung über derartige Organisationen nicht möglich, zumindest aber in auch verfassungsrechtlich erheblicher Weise eingeschränkt. Auch die kommentarlose Abbildung dieser Symbole wird als Unterstützung in der Regel nicht ausreichend. Entschei-

dend ist vielmehr, ob sich aus dem Zusammenhang, in den eine Fotografie gestellt ist und den sie begleitenden Posts ergibt, dass sich der Nutzer mit den abgebildeten Positionen identifiziert oder diese zumindest befürwortet und sie sich in diesem Sinne „zu eigen macht" (vgl. *Senat* U. v. 7.2.2017 – 4 U 1419/16 [= MMR 2017, 542]). Da es auf die Eignung eines Posts ankommt, Ziele und Handlungen der IB zu fördern, muss ein Foto in einen Kontext eingebettet sein, der beim durchschnittlichen Nutzer den Eindruck eines Unterstützens oder Befürwortens hervorruft. Der durchschnittliche Betrachter ... wird nämlich in aller Regel ein Foto nicht nur isoliert zur Kenntnis nehmen, sondern vielmehr die Timeline der Seite auf der Suche nach weiteren Bildern oder Äußerungen durchscrollen, die einen zuverlässigen Rückschluss auf das Meinungsbild des Verfassers erlauben. ... Die Löschung des Posts erfolgte daher gemessen an den eigenen Nutzungsbedingungen der Bekl. zu Unrecht.

10 3. Hieraus folgt ein Anspruch des Kl. auf die begehrte Unterlassung einer weiteren Sperrung § 241 Abs. 1 S. 2 BGB. Ob es für diesen auf eine Hauptleistungspflicht bezogenen Unterlassungsanspruch überhaupt einer Wiederholungsgefahr bedarf (vgl. *OLG Stuttgart* U. v. 23.1.2019 – 4 U 214/18 [= MMR 2020, 415], Rn. 120), kann dahinstehen, weil diese jedenfalls auf Grund der zurückliegenden Löschung des Fotos und der Sperrung des Accounts des Kl. gegeben ist.

11 4. Mit seinem Wiederherstellungsanspruch dringt der Kl. dennoch nicht durch. Die Bekl. hat bereits mit der Klageerwiderung substanziiert die objektive Unmöglichkeit nach § 275 Abs. 1 BGB behauptet. Sie könne die Wiederherstellung wegen zwischenzeitlich kompletter Löschung und Vernichtung nicht mehr leisten. Diesen Einwand hat die Klägerseite erstmals mit der Berufungsbegründung bestritten; gem. § 531 Abs. 1 ZPO ist sie in der Berufungsinstanz mit diesem Vorbringen ausgeschlossen.

12 5. Einen Feststellungsanspruch hat der Kl. neben dem Unterlassungsanspruch nicht. In der vorliegenden Konstellation ist ein Feststellungsbegehren unzulässig.

13 Nach § 256 Abs. 1 ZPO kann Gegenstand einer Feststellungsklage nur die Feststellung des Bestehens oder Nichtbestehens eines gegenwärtigen Rechtsverhältnisses sein (vgl. *BGH* U. v. 7.6.2001 – I ZR 21/99, Rn. 150, 151 mwN). Dagegen ist eine Klage auf Feststellung einzelner Elemente eines Rechtsverhältnisses wie hier der Rechtswidrigkeit eines bestimmten, in der Vergangenheit erfolgten Verhaltens der Bekl., unzulässig (vgl. *BGH*, a.a.O.). ...

14 6. Der Kl. hat auch keinen Anspruch auf Schadensersatz. Für einen Geldentschädigungsanspruch würde es bereits an einem schwerwiegenden Persönlichkeitsrechtseingriff mangeln, der allein eine solche Geldentschädigung rechtfertigt. Die Löschung des Posts und die 30-tägige Versetzung in den „Read-only-Modus" berührt den Kl. nur in seiner Sozialsphäre, sie wird nicht öffentlich mitgeteilt, zeitigt also keine „Prangerwirkung" und auch sonst ist eine erhebliche Beeinträchtigung des Kl. nicht ersichtlich (vgl. *Senat* B. v. 11.6.2019 – 4 U 760/19 [= ZD 2019, 567], Rn. 8). Ebenso scheitert mangels konkreter Darlegungen zu einem entstandenen Schaden die Annahme einer fiktiven Lizenzgebühr wie auch etwaige Ansprüche auf der Grundlage von Art. 82 DS-GVO (*Senat*, a.a.O., Rn. 9 bis 13).

15 7. Der Kl. hat auch trotz rechtswidriger Löschung weder einen Anspruch auf Auskunftserteilung über die mögliche Beteiligung eines beauftragten Unternehmens, noch bzgl. möglicher Weisungen von Seiten der *Bundesregierung*.

16 Ersterer kommt mangels einer spezialgesetzlichen Grundlage nur nach § 242 BGB in Betracht. Dies setzt voraus, dass der Anspruchsberechtigte über das Bestehen oder den Umfang seines Rechts im Ungewissen ist und der Verpflichtete unschwer in der Lage ist, die zur Beseitigung dieser Ungewissheit erforderliche Auskunft zu erteilen (*BGH* U. v. 17.7.2002 – VIII ZR 64/01). Seinerseits wird dieser allgemeine Auskunftsanspruch aber ebenfalls durch § 242 BGB begrenzt. Seine Geltendmachung ist rechtsmissbräuchlich, wenn die Auskunft für den in Frage stehenden Anspruch unter keinem Aspekt relevant ist oder wenn der Gläubiger sie zu „sachwidrigen Zwecken begehrt" (Palandt/*Grüneberg*, BGB, 80. Aufl., § 259 Rn. 9). So liegt es hier, denn selbst – wofür keine Anhaltspunkte bestehen und wofür der Kl. auch keinen Beweis angetreten hat – die Löschungen durch einen von der Bekl. beauftragten Dienstleister vorgenommen werden sollten, kämen Direktansprüche gegen diesen nicht in Betracht. Zudem ist nicht ersichtlich, welchen Schaden er hierdurch überhaupt erlitten haben sollte. Das Auskunftsbegehren ist daher unbegründet (*Senat*, a.a.O.). Ebenso scheitert ein Auskunftsanspruch des Kl. bzgl. möglicher Weisungen von Seiten der *Bundesregierung*. Die durch das NetzDG ausgelösten Handlungsaufforderungen für Betreiber sozialer Netzwerke lassen sich bereits ohne Weiteres dem Gesetzestext entnehmen, für eine weitergehende Einflussnahme im konkreten Einzelfall hat der Kl. keine durchgreifenden Indiztatsachen behauptet. Die Annahme, die *Bundesregierung* oder eine nachgeordnete Stelle der öffentlichen Verwaltung habe im vorliegenden Fall auf die Bekl. eingewirkt, um den Post des Kl. zu sperren, liegt ersichtlich fern und knüpft eher an in einschlägigen Kreisen über das Internet verbreitete Verschwörungstheorien an (so bereits *Senat*, a.a.O.). Die Geltendmachung eines Auskunftsanspruchs mit dem eine Aussage des in Anspruch genommenen über durch nichts belegte Behauptungen erzwungen werden soll, ist als Fall des Rechtsmissbrauchs unzulässig (*Senat*, a.a.O.). ...

OLG Frankfurt/M.: Streitwert für wettbewerbsrechtlichen Unterlassungsantrag

Verbraucherinteresse

GKG § 51 Abs. 2; LMIV Art. 9 Abs. 1 lit. h, 14 Abs. 1 lit. a; UWG §§ 8 Abs. 3 Nr. 3, 13a Abs. 3; UKlaG § 4
Beschluss vom 7.1.2021 – 6 W 131/20 (LG Hanau)

Leitsatz

Für einen einzelnen Verstoß gegen die Informationspflichten nach Art. 9 Abs. 1 lit. h, 14 Abs. 1 lit. a LMIV (hier: fehlende Angaben auf einem im Internet angebotenen Brotaufstrich) kann u.U. ein Gebührenstreitwert von 3.000,– EUR ausreichend sein.

Anm. d. Red.: Vgl. zu den Informationspflichten nach LMIV *LG Mannheim* MMR 2018, 256 und *KG* MMR 2018, 694.

Schlagworte: Informationspflichten; Fernabsatz; fehlende Angaben; Gebührenstreitwert; Verbraucherinteresse

Aus den Gründen

2 1. Nach § 51 Abs. 2 GKG ist der Streitwert entsprechend der sich aus dem Antrag des Kl. ergebenden Bedeutung der Sache zu bestimmen. Entscheidend ist bei Unterlassungsanträgen das Interesse an der Unterbindung weiterer gleichartiger Verstöße, das maßgeblich durch die Art des Verstoßes, insb. seine Gefährlichkeit und Schädlichkeit für die Träger der maßgeblichen Interessen bestimmt wird (*BGH* GRUR 2017, 21 – Finanzsanierung).

3 2. Gegenstand des Unterlassungsantrags ist ein Verstoß gegen Art. 9 Abs. 1 lit. h, 14 Abs. 1 lit. a LMIV. Danach sind im Fernab-

satz verpflichtende Informationen über Name bzw. Firma und Anschrift des Lebensmittelunternehmers vorzusehen. Nach dem Vortrag der Kl. hat die Bekl. im Internet einen Brotaufstrich angeboten, der diesen Anforderungen nicht genügte. Das *LG* hat den Streitwert entsprechend der Anregung des Kl. auf 10.000,– EUR festgesetzt. Dies erscheint übersetzt.

4 a) Das *LG* hat zu Recht angenommen, dass bei Verbänden nach § 8 Abs. 3 Nr. 3 UWG, § 4 UKlaG für die Streitwertfestsetzung auf das satzungsgemäß wahrgenommene Interesse der Verbraucher abzustellen ist. Dieses Interesse kann erheblich höher liegen als das eines einzelnen Mitbewerbers (vgl. *OLG Frankfurt/M.* B. v. 15.1.2020 – 6 W 119/19, mwN). Für ein nicht unerhebliches Verbraucherinteresse spricht im Streitfall, dass die verletzte Informationspflicht die Lebensmittelsicherheit betrifft. Verbraucher sollen wissen, an wen sie sich wenden können, um z.B. Inhaltsstoffe und Lebensmittelunverträglichkeiten abzuklären. Nach Ansicht des *Senats* wiegt der Verstoß jedoch deshalb nicht schwer, weil aus dem Internetauftritt zumindest das Unternehmensschlagwort des Lebensmittelunternehmers hervorging. Auf der in dem beanstandeten Angebot fotografisch abgebildeten Produktverpackung ist der Name „A" deutlich erkennbar. Interessierte Verbraucher konnten anhand dieser Angabe den Lebensmittelunternehmer nebst Adresse mit geringem Aufwand selbst ermitteln. Auch handelt es sich nur um einen einzelnen Verstoß. Ein systematisches Missachten der Informationspflichten der LMIV wird der Bekl. nicht vorgeworfen. Die Gefährlichkeit der zu unterbindenden Handlung war daher gering.

5 b) Eine weitergehende Reduzierung auf 1.000,– EUR kam unter Berücksichtigung der dargelegten Umstände nicht in Betracht. Die Bestimmung des § 13a Abs. 3 UWG n.F. kommt entgegen der Auffassung der Bekl. nicht zur Anwendung. Die Abmahnung wurde noch vor Inkrafttreten des Gesetzes zur Stärkung des fairen Wettbewerbs ausgesprochen. Außerdem betrifft die genannte Bestimmung nicht den Streitwert, sondern die Höhe der Vertragsstrafe. ...

OLG Hamm: Anzeige gesetzeswidriger Angebote beim Plattformbetreiber durch einen Mitbewerber

Aggressive geschäftliche Handlung

UWG §§ 3 Abs. 1, 3a, 4, 4a, 8 Abs. 1 S. 1; VO (EU) Nr. 874/2012 Art. 4 Abs. 2 lit. d, Anhang VIII
Urteil vom 8.10.2020 – 4 U 7/20 (LG Bochum); rechtskräftig

Leitsatz der Redaktion

Wählt ein Konkurrent statt einer Abmahnung zunächst den Weg der Beschwerde an den Plattformbetreiber und spricht nicht sofort eine ggf. Kostenerstattungsansprüche auslösende Abmahnung aus, spricht dies dafür, dass sein Vorgehen dem Interesse an einem lauteren, gesetzeskonformen Wettbewerb entspricht.

Anm. d. Red.: Vgl. hierzu ferner *OLG Frankfurt/M.* MMR 2020, 243 m. Anm. *Albrecht*.

Schlagworte: Anschwärzung beim Plattformbetreiber; Behinderung; aggressive geschäftliche Handlung; Beschwerde; Internetplattform; Nötigung

Sachverhalt

Die Kl. vertreibt Lampen und Leuchten auf dem deutschen Markt. Die Bekl. zu 1), eine Gesellschaft bürgerlichen Rechts, vertreibt ebenfalls Lampen und Leuchten auf dem deutschen Markt, die Bekl. zu 2) und 3) sind die Gesellschafter der Bekl. zu 1).

Anfang Juni 2019 unterhielt die Bekl. zu 1) auf der Internetplattform „B" u.a. das Produktangebot „LED Einbaustrahler schwenkbar flach 3000K warmweiß 230V dimmbar Deckenstrahler Einbauleuchte Einbauspot, Farbe: Weiß, Einheit: 1 Stück [Energieklasse A+++]" und das Produktangebot „LED Einbaustrahler schwenkbar flach 3000K warmweiß 230V dimmbar Deckenstrahler Einbauleuchte Einbauspot, Farbe: Weiß, Einheit: 6 Stück [Energieklasse A+++]".

Die Kl. erhielt spätestens am 3.6.2019 Kenntnis von den beiden vorbezeichneten Produktangeboten. Am 3.6.2019 wandte sich die Kl. an den Betreiber der Internetplattform „B" (im Folgenden: Plattformbetreiber) und äußerte, (zumindest) diese beiden Produktangebote entsprächen nicht den Vorgaben der „Delegierten Verordnung (EU) Nr. 874/2012 der Kommission v. 12.7.2012 zur Ergänzung der RL 2010/30/EU des Europäischen Parlaments und des Rates im Hinblick auf die Energieverbrauchskennzeichnung von elektrischen Lampen und Leuchten" (im Folgenden: VO (EU) Nr. 874/2012). Der Plattformbetreiber entfernte daraufhin die beiden o.g. Produktangebote sowie zehn weitere Produktangebote der Bekl. zu 1) von der Internetplattform „B" und informierte die Bekl. zu 1) hierüber mit E-Mail v. 11.6.2019. Die Entfernung der Produktangebote begründete der Plattformbetreiber in dieser E-Mail wie folgt:
„(...) Das Energieeffizienzlabel wird bei den Angeboten nicht ordnungsgemäß dargestellt (Anhang VIII VO EU 874/2012). Das Label wird weder unmittelbar neben dem Preis noch mittels einer geschachtelten Anzeige dargestellt. (...)"

Mit anwaltlichem Schriftsatz v. 4.7.2019 mahnte die Bekl. zu 1) die Kl. ab. Die „Beschwerde" der Kl. bei dem Plattformbetreiber sei unlauter gewesen. Sie stelle eine aggressive geschäftliche Handlung i.S.d. § 4a UWG, eine „Anschwärzung" i.S.d. § 4 Nr. 2 UWG und eine gezielte Behinderung i.S.d. § 4 Nr. 4 UWG dar. Ihr, der Bekl. zu 1), stehe daher ein Unterlassungsanspruch gegen die Kl. zu. Die Kl. sei darüber hinaus zur Auskunftserteilung über den Umfang ihres unlauteren Verhaltens und zur Leistung von Schadensersatz verpflichtet; sie, die Bekl. zu 1), schätze den entstandenen Schaden überschlägig auf einen Betrag von ca. 191.000,– EUR. Schließlich sei die Kl. verpflichtet, die ihr, der Bekl. zu 1), entstandenen Abmahnkosten i.H.v. 3.652,71 EUR (Rechtsanwaltsvergütung, berechnet nach einem Gegenstandswert von 60.000,– EUR) zu erstatten.

Die Kl. mahnte ihrerseits mit anwaltlichem Schriftsatz v. 20.7.2019 die Bekl. zu 1) ab. Die von der Bekl. zu 1) auf der Internetplattform „B" unterhaltenen Produktangebote für Leuchten hätten den sich aus Anhang VIII VO (EU) Nr. 874/2012 ergebenden unionsrechtlichen Anforderungen an die Information über die Energieeffizienzklasse nicht genügt.

Mit E-Mail v. 26.7.2019 informierte der Plattformbetreiber die Bekl. zu 1) darüber, dass er weitere 29 Produktangebote der Bekl. zu 1) von der Internetplattform „B" entfernt habe.

Die Kl. hat die Auffassung vertreten, die von der Bekl. zu 1) in ihrer Abmahnung v. 4.7.2019 genannten Ansprüche bestünden nicht. Gegenstand ihrer, der Kl., Eingabe an den Plattformbetreiber v. 3.6.2019 seien lediglich das Produktangebot gewesen. Sie, die Kl., sei berechtigt gewesen, dem Plattformbetreiber diese beiden Angebote zu melden, weil sie den Vorgaben der VO (EU) Nr. 874/2012 nicht entsprochen hätten. Der Plattformbetreiber stelle sogar ein besonderes Software-„Tool" zur Verfügung, das es den Anbietern ermögliche, ihre Produktangebote rechtskonform zu gestalten. Dieses „Tool" ermögliche auch eine sog. „geschachtelte Anzeige" i.S.d. VO (EU) Nr. 874/2012

und stehe allen Anbietern auf der Internetplattform „B" – unabhängig von ihrer Größe – zur Verfügung. Mit den negativen Feststellungsanträgen zu 1) bis 4) wendet sie, die Kl., sich gegen die von der Bekl. zu 1) in ihrer Abmahnung v. 4.7.2019 geltend gemachten Ansprüche.

Mit dem angefochtenen Urteil hat die *13. Zivilkammer – Kammer für Handelssachen* – des *LG Bochum* der Klage in vollem Umfang stattgegeben.

Aus den Gründen

22 Die Berufung ist ... [im Wesentlichen] unbegründet.

23 a) Die Klage ist mit diesem negativen Feststellungsantrag zulässig. ...

26 b) Die Klage ist ... auch begründet. Der Bekl. zu 1) steht der mit der Abmahnung v. 4.7.2019 geltend gemachte Unterlassungsanspruch unter keinem denkbaren rechtlichen Gesichtspunkt zu.

27 Als Grundlage für den geltend gemachten Unterlassungsanspruch kommt allenfalls die Regelung in §§ 8 Abs. 1 S. 1, 3 Abs. 1 UWG in Betracht. Die „Beschwerde" der Kl. bei dem Plattformbetreiber v. 3.6.2019 – nur diese ist Gegenstand der Abmahnung der Bekl. zu 1) v. 4.7.2019 – stellt indes keine unlautere geschäftliche Handlung dar.

28 aa) Es handelt sich um keine „aggressive geschäftliche Handlung" i.S.d. § 4a UWG. Eine solche geschäftliche Handlung setzt nach § 4a Abs. 1 S. 2 UWG eine Belästigung, eine Nötigung oder eine unzulässige Beeinflussung voraus. Dass die Kl. den „B"-Plattformbetreiber mit ihrer Beschwerde belästigt oder genötigt hat, ist nicht ersichtlich. Auch eine unzulässige Beeinflussung liegt nicht vor. Nach § 4a Abs. 1 S. 3 UWG liegt eine unzulässige Beeinflussung vor, wenn der Unternehmer eine Machtposition ggü. dem Verbraucher oder sonstigen Marktteilnehmer zur Ausübung von Druck, auch ohne Anwendung oder Androhung von körperlicher Gewalt, in einer Weise ausnutzt, die die Fähigkeit des Verbrauchers oder sonstigen Marktteilnehmers zu einer informierten Entscheidung wesentlich einschränkt. Hierfür fehlt jeglicher Anhaltspunkt.

29 bb) Die Beschwerde v. 3.6.2019 beinhaltete auch keine „Anschwärzung" i.S.d. § 4 Nr. 2 UWG. Eine solche Anschwärzung setzt nach dem Wortlaut der vorbezeichneten Vorschrift die Behauptung oder Verbreitung falscher oder nicht erweislich wahrer Tatsachen voraus.

30 (1) Es liegt kein Anhaltspunkt dafür vor, dass die Kl. – sei es nun in der Beschwerde v. 3.6.2019 und/oder in einer etwaigen weiteren Beschwerde – dem Plattformbetreiber über das Produktangebot ... hinaus weitere Produktangebote der Bekl. zu 1) gemeldet hat. Die Bekl. haben insofern letztlich nur Vermutungen geäußert. Dass die Bekl. – die Bekl. zu 1) verfügt immerhin über eine eigene vertragliche Beziehung zu dem Plattformbetreiber – nicht in der Lage gewesen wären zu eruieren, wie häufig und mit welchem jeweiligen konkreten Inhalt die Kl. sich über die Bekl. zu 1) bei dem Plattformbetreiber beschwert hat, und hierzu im vorliegenden Rechtsstreit konkret vorzutragen, ist nicht erkennbar. Der Umstand, dass der Plattformbetreiber sowohl in seiner E-Mail v. 11.6.2019 als auch in seiner E-Mail v. 26.7.2019 auf eine „Beschwerde" der Kl. Bezug genommen hat, ist ohne Aussagekraft, weil die – einzige und auf die beiden ... Produktangebote beschränkte – Eingabe der Kl. als Auslöser für eigene Überprüfungen des Plattformbetreibers gedient haben kann und nur aus diesem Grunde in den E-Mails Erwähnung gefunden haben mag.

31 (2) Dass die Kl. über die beiden ... Produktangebote falsche oder nicht erweislich wahre Tatsachen behauptet hat, ist nicht ersichtlich. Es wäre ohnehin unsinnig, ggü. dem „B"-Plattformbetreiber unrichtige Tatsachen über den Wortlaut oder die sonstige Gestaltung von Produktangeboten auf seiner eigenen Internetplattform zu behaupten.

32 cc) Die Beschwerde der Kl. v. 3.6.2019 enthielt auch keine Herabsetzung oder Verunglimpfung der Bekl. zu 1) i.S.d. § 4 Nr. 1 UWG. Die in dieser Beschwerde von der Kl. geäußerte Rechtsauffassung, die beiden Produktangebote, die Gegenstand der Beschwerde waren und die hier auch nur in Rede stehen, entsprächen nicht den Vorgaben der VO (EU) Nr. 874/2012, war vielmehr zutreffend.

33 Gegenstand des Produktangebots ... waren jeweils Leuchten mit fest eingebauten LED-Modulen. Art. 4 Abs. 2 lit. d VO (EU) Nr. 874/2012 in der bis zum 24.12.2019 geltenden Fassung verpflichtete Händler von Leuchten, die an Endnutzer vermarktet wurden, dafür zu sorgen, dass jedes Modell, das im Internet zum Verkauf, zur Vermietung oder zum Ratenkauf angeboten wurde und für das vom Leuchtenlieferanten ein elektronisches Etikett bereitgestellt wurde, mit diesem Etikett gemäß dem Anhang VIII der VO versehen war.

34 Die beiden hier in Rede stehenden „B"-Produktangebote der Bekl. zu 1) richteten sich – jedenfalls auch – an Endnutzer. Dass der Lieferant der Leuchten für diese Produkte kein elektronisches Etikett bereitstellte, haben die Bekl. nicht vorgetragen. Die beiden Produktangebote genügten den Vorgaben des Anhangs VIII VO (EU) Nr. 874/2012 indes nicht. Nach Anhang VIII Nr. 2 S. 1 und S. 2 VO (EU) Nr. 874/2012 musste das Etikett gut sichtbar und leserlich in der Nähe des Produktpreises dargestellt werden; hilfsweise erlaubte Anhang VIII Nr. 2 S. 3 und S. 4 VO (EU) Nr. 874/2012 die Anzeige des Etiketts mit Hilfe einer sog. „geschachtelten Anzeige" (Legaldefinition in Anhang VIII Nr. 1 lit. b VO (EU) Nr. 874/2012). Nach Anhang VIII Nr. 3 lit. a VO (EU) Nr. 874/2012 musste das als „Link" für den Zugang zum Etikett genutzte Bild bei einer geschachtelten Anzeige ein Pfeil in der Farbe der Energieeffizienzklasse des Produkts auf dem Etikett sein; Anhang VIII Nr. 3 lit. b und lit. c VO (EU) Nr. 874/2012 enthielten weitere Vorgaben für die Gestaltung dieses Pfeils. Dieser Pfeil musste wiederum nach Anhang VIII Nr. 4 lit. a VO (EU) Nr. 874/2012 in der Nähe des Produktpreises dargestellt werden. Die beiden hier in Rede stehenden Produktangebote der Bekl. zu 1) enthielten in der Nähe des jeweiligen Produktpreises weder ein den Vorgaben des Anhangs I VO (EU) Nr. 874/2012 entsprechendes Etikett noch einen den o.g. Vorgaben entsprechenden „Link" für eine „geschachtelte Anzeige" des Etiketts.

35 dd) Die Beschwerde der Kl. v. 3.6.2019 ist schließlich auch nicht als gezielte Behinderung der Bekl. zu 1) i.S.d. § 4 Nr. 4 UWG zu werten.

36 Nicht jede Behinderung eines Wettbewerbers unterfällt der Regelung des § 4 Nr. 4 UWG. Es müssen vielmehr besondere, die Unlauterkeit der Behinderung des Wettbewerbers begründende Umstände hinzutreten (vgl. *Köhler/Bornkamm/Feddersen*, UWG, 38. Aufl. 2020, § 4 Rn. 4.7 mwN). Derartige besondere Umstände sind hier nicht ersichtlich.

37 (1) Dass die beiden hier in Rede stehenden Produktangebote den für sie geltenden gesetzlichen Anforderungen nicht genügten und dementsprechend die von der Kl. ggü. dem „B"-Plattformbetreiber geäußerte Rechtsauffassung zutreffend war, hat der *Senat* oben bereits ausgeführt.

38 (2) Dass die Kl. ihre Beschwerde an den Plattformbetreiber aus sachfremden – wettbewerbsfremden – Interessen abgesetzt hat, ist nicht ersichtlich. Dass die Kl. zunächst den Weg der Beschwerde an den Plattformbetreiber gewählt hat, der überdies schnell und effizient zu einer Entfernung der nicht gesetzeskonformen Produktangebote aus dem Internet geführt hat, und

nicht sofort eine ggf. Kostenerstattungsansprüche auslösende Abmahnung ausgesprochen hat, spricht im Gegenteil dafür, dass ihr Vorgehen dem Interesse an einem lauteren, gesetzeskonformen Wettbewerb entsprang.

39 (3) Dass die Kl. das sog. „Infringement"-Verfahren des „B"-Plattformbetreibers missbraucht hat, ist ebenfalls nicht ersichtlich. Die Kl. hat vorgetragen, sie habe dieses Verfahren nicht genutzt, sondern sich vielmehr direkt an die Rechtsabteilung des Plattformbetreibers gewandt. Hierfür spricht auch der Wortlaut der beiden E-Mails …, in denen von einer Verletzung gewerblicher Schutzrechte nicht die Rede ist, sondern ausdrücklich auf eine Zuwiderhandlung gegen Anhang VIII VO (EU) Nr. 874/2012 abgestellt wird. Das Vorbringen der Bekl. zu einem angeblichen Missbrauch des „Infringement"-Verfahrens ist vor diesem Hintergrund substanzlos und geht über bloße Vermutungen nicht hinaus.

40 (4) Eine gezielte Behinderung könnte allenfalls dann vorliegen, falls der Kl. im unmittelbaren Rechtsverhältnis zwischen ihr und der Bekl. zu 1) keine (lauterkeitsrechtlichen) Ansprüche gegen die Bekl. zu 1) wegen der Zuwiderhandlung gegen Anhang VIII VO (EU) Nr. 874/2012 zustehen, z.B. weil diese Zuwiderhandlungen nicht spürbar i.S.d. § 3a UWG sind. Die von der Kl. beim Plattformbetreiber erhobene Beschwerde wäre dann mit dem Fall einer unberechtigten „externen" Abmahnung ggü. einem für den (vermeintlichen) Wettbewerbsverstoß „Mitverantwortlichen" vergleichbar (vgl. zu dieser Fallgruppe: *Köhler/Bornkamm/Feddersen*, a.a.O., Rn. 4.167). Abgesehen davon, dass das *LG Frankfurt/M.* in den beiden dort anhängigen Verfahren jeweils lauterkeitsrechtliche Ansprüche der Kl. gegen die Bekl. zu 1) bejaht hat, wäre eine „gezielte Behinderung" der Bekl. zu 1) durch die Beschwerde der Kl. bei dem Plattformbetreiber nur dann anzunehmen, wenn die Kl. Kenntnis vom Fehlen (unmittelbarer) lauterkeitsrechtlicher Ansprüche gegen die Bekl. zu 1) gehabt hätte oder sich dieser Kenntnis bewusst verschlossen hätte (vgl. *Köhler/Bornkamm/Feddersen*, a.a.O., Rn. 4.167). Hierfür fehlt jeglicher Anhaltspunkt. …

LG München I: AGB zu pauschalem Schadensersatz bei Verlust eines Routers

TK-Anbieter

BGB §§ 280 Abs. 1 u. Abs. 3, 281 Abs. 1 u. Abs. 2, 286 Abs. 2 Nr. 2, 307 Abs. 2 Nr. 1 u. Nr. 2, 309 Nr. 4 u. Nr. 5 lit. a, 439 Abs. 1, 602, 604 Abs. 1
Urteil vom 25.3.2021 – 12 O 7213/20; nicht rechtskräftig

Leitsatz der Redaktion

Die Klausel in AGB eines TK-Anbieters, wonach bei Überlassung eines Geräts zur Nutzung der Kunde dieses bei Vertragsbeendigung zurückzugeben hat und bei beschädigten, funktionsuntüchtigen oder nicht zurückgegebenen Geräten eine Pauschale zu zahlen hat, ist unwirksam, wenn als Pauschale letztlich der Neupreis zu Grunde liegt.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 7929. Die Berufung ist beim *OLG München* anhängig.

Schlagworte: Vodafone; Router; Verlust; pauschaler Schadensersatz; AGB; TK-Anbieter

Sachverhalt

Die Parteien streiten im Verbandsklageverfahren um einen Unterlassungsanspruch. Der Kl. ist ein eingetragener Verein, der beim *Bundesamt für Justiz* in der Liste qualifizierter Einrichtungen gem. § 4 Abs. 2 UKlaG geführt wird. Die Bekl. bietet TK-Dienstleistungen an. Ihr Angebot umfasst u.a. Internetzugänge für Verbraucher über Breitbandkabel.

Beim Abschluss ihrer Verträge mit Verbrauchern verwendete die Bekl. eine „Preisliste und Leistungsbeschreibung". Diese enthält unter der Überschrift „Endgeräte zur Nutzung" folgende Regelung: „Pauschalen gem. AGB für Ersatzgerät (bei durch Kunden verursachten Verlust/Defekt), einmalig: … HomeBox Fritz!Box 6490 EUR 160,00 …"

In den weiter verwendeten AGB „Internet und Telefon" findet sich folgende Regelung:
„4. Pflichten und Obliegenheiten des Kunden
4.1 Der Kunde ist verpflichtet: …
4.1.14 Nach Beendigung des Vertragsverhältnisses ihm zur Nutzung überlassene Geräte unverzüglich auf seine Kosten und seine Gefahr zurückzugeben. Andernfalls ist Vodafone berechtigt, für ein beschädigtes, funktionsuntüchtiges oder nicht zurückgegebenes Gerät eine jeweils mit dem Kunden vereinbarte Pauschale zu berechnen, es sei denn der Kunde ist nachweislich für die vorgenannten Fälle nicht verantwortlich. Dem Kunden ist der Nachweis unbenommen, dass kein oder ein wesentlich geringerer Schaden als die Pauschale entstanden ist."

Die AGB enthalten ferner unter Ziffer 3.2.2 folgende Regelung: „Kauft der Kunde Endgeräte, verbleiben diese bis zur vollständigen Bezahlung durch den Kunden im Eigentum von Vodafone. …"

Der Kl. mahnte die Bekl. ab und forderte sie zur Abgabe einer entsprechenden Unterlassungserklärung sowie zur Zahlung von Abmahnkosten i.H.v. 260,– EUR auf. Die Bekl. wies die Ansprüche zurück. Der Kl. verlangt von der Bekl. die Unterlassung der Verwendung der streitgegenständlichen Klauseln und ein Berufen auf dieselben. Er vertritt die Auffassung, die Klauseln seien unwirksam.

Aus den Gründen

28 II. Die Klage ist begründet. Der Kl. hat ggü. der Bekl. Anspruch auf Unterlassung der Verwendung der streitgegenständlichen Klauseln sowie auf Zahlung der Abmahnpauschale.

29 1. Die Klauseln der „Preisliste und Leistungsbeschreibung" zur Schadensersatzpauschale für Kabelrouter – 100,– EUR und HomeBox Fritz!Box 6490 – 160,– EUR verstoßen gegen § 309 Nr. 5 lit. a BGB und sind deswegen unwirksam.

30 a) Nach § 309 Nr. 5 lit. a BGB besteht ein Klauselverbot ohne Wertungsmöglichkeit für die Vereinbarung eines pauschalierten Anspruchs des Verwerters auf Schadensersatz oder Ersatz einer Wertminderung, wenn die Pauschale den in den geregelten Fällen nach dem gewöhnlichen Lauf der Dinge zu erwartenden Schaden oder die gewöhnlich eintretende Wertminderung übersteigt.

31 b) Dies ist vorliegend nach den eigenen Ausführungen der Bekl. der Fall: Die Bekl. hat zur Rechtfertigung ihrer Pauschale und zur Darlegung des ihr entstehenden Schadens ausgeführt, dass im Fall der Nichtrückgabe eines Geräts von der Bekl. für einen von ihr unterhaltenen sog. „Gerätepool" ein neues Gerät angeschafft und diesem Pool zugeführt werde. Dabei handle es sich um ein Neugerät und um das neuere, auf dem Markt noch erhältliche Modell. Die Bekl. hat weiter ausgeführt, dass die Pauschale für die Lieferung eines Ersatzgeräts berechnet werde.

32 Daraus ergibt sich, dass die Bekl. als Pauschale letztlich den Neupreis der Geräte zu Grunde legt und in der Pauschale allenfalls noch Verwaltungskosten für den Gerätepool enthalten sind. Dies entspricht jedoch nicht dem tatsächlich zu erwarten-

den Schaden bei Nichtrückgabe eines Geräts der streitgegenständlichen Art durch den Kunden.

33 Die Bekl. überlässt den Kunden die Endgeräte ausweislich ihrer AGB für die Dauer der Vertragslaufzeit kostenlos im Wege der Leihe. Einem solchen Leihvertrag ist immanent, dass der Verleiher den Wertverlust zu tragen hat, der in Folge des Zeitablaufs entsteht, § 602 BGB. Der Leihvertrag verpflichtet nur zur Rückgabe des entliehenen Geräts, nicht jedoch zum Ersatz in Form eines Neugeräts. Dementsprechend bemisst sich der Schadensersatz, den die Bekl. von einem Kunden im Fall der Zerstörung oder nicht Rückgabe eines Geräts verlangen könnte, am Zeitwert eines Gebrauchtgeräts im Zeitpunkt der Rückgabepflicht. Diese entsteht nach Ablauf der Vertragslaufzeit, die ausweislich der AGB der Bekl. mind. 24 Monate beträgt. Dass ein zwei Jahre oder noch älteres elektronisches Gerät in Form eines Routers den Neuwert nicht mehr ansatzweise erreicht, ist offensichtlich und allgemein bekannt.

34 Bereits die Ausführungen der Bekl. lassen danach den Schluss zu, dass die Klausel und die mit ihr festgelegte Höhe der Pauschalen auf der irrigen Rechtsmeinung der Bekl. beruhen, als pauschalen Schadensersatz einen Betrag verlangen zu können, der dem Neupreis eines Routers – ggf. nach Abzug eines Verwaltungskostenanteils – entspricht.

35 Damit verkennt sie den Maßstab des § 309 Nr. 5 lit. a BGB. Wie dargelegt erreichen zwei Jahre alte oder ältere Elektrogeräte ihren Neuwert bei weitem nicht mehr. Maßgeblich ist i.Ü. der Marktwert eines solchen Gebrauchtgeräts, nicht jedoch irgendwelche von der Bekl. angestellten Erwägungen dahingehend, dass die Geräte auf Grund ihrer Gerätepool-Lösung „nicht wertlos" seien. Auch von der Bekl. berechnete Rechtsverfolgungskosten für die Rückholung gebrauchter Geräte sind nicht zu berücksichtigen: Die Bekl. hat ausdrücklich vorgetragen, sie ersetze nicht zurückgegebene Geräte in ihrem Pool durch Neuanschaffung. Dazu ist eine Rechteverfolgung jedoch nicht erforderlich, weshalb solche Kosten nicht bei dem zu erwartenden Schaden zu berücksichtigen sind.

36 Die von der Bekl. angesetzten Pauschalwerte übersteigen den in den geregelten Fällen nach dem gewöhnlichen Lauf der Dinge zu erwartenden Schaden oder die gewöhnlich eintretende Wertminderung erheblich.

37 Vertragsgemäßheit genügt (vgl. *Westermann*, in: MüKo-BGB, 8. Aufl., § 439 Rn. 14).

38 c) Weil es sich bei der Nacherfüllung um eine Entsprechung des ursprünglichen Erfüllungsanspruchs handelt, reicht beim Verkauf eines Neugeräts für die Nacherfüllung durch Lieferung einer mangelfreien Sache i.S.d. § 439 Abs. 1 BGB die Lieferung einer gebrauchten Sache nicht aus. Dies gilt auch dann, wenn ein solches generalüberholtes Gebrauchtgerät voll funktionsfähig ist. Es kommt bei der Nacherfüllung gerade nicht nur darauf an, dass die nachgelieferte Sache keine Mängel i.S.e. Funktionseinschränkung aufweist, sondern darauf, dass die nachgelieferte Sache der ursprünglich geschuldeten Sache vollständig i.S.e. Gattungsschuld entspricht.

39 Dementsprechend gilt, dass die Bekl. weder bei der ursprünglichen Erfüllung des Kaufvertrags, noch bei der Nacherfüllung ein wiederaufbereitetes Gerät liefern darf, wenn sie ein Neugerät verkauft hat. Eine entsprechende Regelung in den AGB, wie sie die Bekl. im vorliegenden Fall vorgenommen hat, widerspricht dem Grundgedanken des § 439 Abs. 1 BGB, weil durch die Klausel der Kaufgegenstand ausgetauscht wird. Es wird statt der ursprünglich geschuldeten Neuware ein Gebrauchtgerät geliefert. Ein gebrauchtes Gerät wird auch durch eine vom Hersteller vorgenommene Aufbereitung rechtlich betrachtet nicht zu einer neuen Sache.

40 d) Die streitgegenständliche Klausel weicht dadurch vom Grundgedanken der gesetzlichen Regelung des § 439 Abs. 1 BGB erheblich ab. Mit der Klausel wird der ursprüngliche Anspruch des Verbrauchers auf Lieferung einer neuen Sache auf ein Gebrauchtgerät beschränkt und damit so eingeschränkt, dass die Erreichung des ursprünglichen Vertragszwecks in Form der Hauptleistungspflicht zur Lieferung einer neuen Sache gefährdet ist. Die Klausel ist nach § 307 Abs. 2 Nr. 1 u. Nr. 2 BGB unwirksam, weil sie den Verbraucher unangemessen benachteiligt.

41 Eine solche Klausel, mit der der Vertragsgegenstand ausgetauscht wird, ist zudem überraschend und auch deswegen unwirksam. Der durchschnittliche Verbraucher muss mit einem solchen über die AGB bewirkten Austausch des vertraglich vereinbarten Leistungsgegenstands nicht rechnen.

42 3. Auch hinsichtlich der Klausel 4.1.14 der AGB der Bekl. besteht ein Unterlassungsanspruch des Kl. Die Klausel verstößt gegen § 309 Nr. 4 BGB. Sie ist unwirksam.

43 a) Nach § 309 Nr. 4 BGB ist eine Bestimmung in AGB unwirksam, durch die der Verwender von der gesetzlichen Obliegenheit freigestellt wird, den anderen Vertragsteil zu mahnen oder ihm eine Frist für die Leistung oder Nacherfüllung zu setzen.

44 b) Die streitgegenständliche Klausel regelt die Berechtigung der Bekl., für den Fall, dass der Kunde nach Beendigung des Vertragsverhältnisses ihm zur Nutzung überlasse Geräte nicht unverzüglich auf seine Kosten und seine Gefahr zurückgibt, für ein beschädigtes, funktionsuntüchtiges oder nicht zurückgegebenes Gerät eine jeweils mit dem Kunden vereinbarte Pauschale zu berechnen.

45 c) Zwar muss die Bekl. einen Kunden, der ihm überlassene Geräte nicht unverzüglich nach Vertragsende zurückgibt, nicht mahnen, damit Verzug eintritt. Die Überlassung der Geräte erfolgt ausweislich der AGB der Bekl. im Wege der Leihe. Nach § 604 Abs. 1 BGB ist der Entleiher verpflichtet, die geliehene Sache nach dem Ablauf der für die Leihe bestimmten Zeit zurückzugeben. Die Geräte werden dem Kunden nach den AGB für die Vertragslaufzeit überlassen. Endet der Vertrag, besteht automatisch eine Rückgabepflicht, ohne dass es dazu einer Mahnung der Bekl. bedurfte.

46 Die Nichtrückgabe eines Geräts ist eine Pflichtverletzung i.S.d. § 280 Abs. 1 BGB. Die Mahnung ist gem. § 286 Abs. 2 Nr. 2 BGB entbehrlich. Durch die Nichtrückgabe nach Vertragsende tritt daher Verzug ein.

47 d) Ein pauschalierter Schadensersatz für ein nicht zurückgegebenes Gerät stellt jedoch keinen Verzögerungsschaden, sondern Schadensersatz statt der Leistung nach §§ 280 Abs. 1 u. Abs. 3, 281 BGB dar. § 281 Abs. 1 BGB verlangt neben den Voraussetzungen des § 280 die erfolglose Bestimmung einer angemessenen Frist zur Nacherfüllung. Diese ist vorliegend auch nicht entbehrlich.

48 Nach der von der Bekl. verwendeten Klausel entsteht der Schadensersatzanspruch automatisch durch die Nichtrückgabe des Geräts oder die Rückgabe eines beschädigten Geräts nach Vertragsende. Eine Fristsetzung sieht die Klausel nicht vor.

49 Hinsichtlich der tatsächlich erfolgten Rückgabe eines beschädigten Geräts mag dies deswegen unproblematisch sein, weil dann regelmäßig die Fristsetzung entbehrlich und die sofortige Geltendmachung des Schadensersatzanspruchs gerechtfertigt sein dürfte. Das gilt jedoch keinesfalls im Fall der Nichtrückgabe eines Geräts. In diesem Fall muss die Bekl. eine Nachfrist gem. § 281 Abs. 1 BGB setzen. Eine entsprechende Pflicht sieht die streitgegenständliche Klausel nicht vor.

50 Die Nachfristsetzung ist auch nicht entbehrlich. In der bloßen Unterlassung der Rückgabe eines Geräts liegt noch keine ernsthaft und endgültige Leistungsverweigerung i.S.d. § 281 Abs. 2 BGB. Auch besondere Umstände, die unter Abwägung der beiderseitigen Interessen die sofortige Geltendmachung des Schadensersatzanspruchs rechtfertigen könnten, liegen in einer solchen Situation regelmäßig nicht vor. Es ist der Bekl. ohne Weiteres zumutbar, den Kunden auf die Pflicht zur Rückgabe hinzuweisen und ihm eine Frist zu setzen.

51 Die angegriffene Klausel sieht dies jedoch nicht vor, sondern bestimmt vielmehr die automatische Entstehung eines Schadensersatzanspruchs. Die Klausel verstößt damit gegen § 309 Nr. 4 BGB. Sie ist unwirksam.

52 e) Soweit die Bekl. eine von dem genannten Inhalt der Klausel abweichende Anwendungspraxis in der tatsächlichen Abwicklung von Verbraucherverträgen geltend machen möchte, verfängt dies nicht. Im Verbandsklageverfahren gilt ein abstrakter Prüfungsmaßstab.

53 4. Die angegriffenen Klauseln wurden von der Bekl. unstreitig verwendet. Eine Unterlassungserklärung gab sie nicht ab. Wiederholungsgefahr besteht damit. ...

LG Kempten: Keine Geschäftsgeheimnisverletzung eines Versicherungsvermittlers

Datenhandel

GeschGehG §§ 2, 4, 6; BGB §§ 823, 1004; StGB § 203; BDSG § 34; DS-GVO Art. 15
Urteil vom 30.12.2020 – 1 HK O 503/20; rechtskräftig

Leitsatz der Redaktion

Auch wenn Versicherungsgesellschaften ein hohes Interesse daran haben, dass die Daten ihrer Versicherungsnehmer nicht an Dritte gelangen, kann aus dieser Interessenlage nicht der Rückschluss gezogen werden, dass die versicherungsspezifischen Datensätze der Versicherungsnehmer auf dem freien Markt nicht verfügbar wären bzw. nur verfügbar wären, wenn dem ein rechtwidriges Handeln vorangegangen ist.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2020, 45020.

Schlagworte: Krankenversicherung; Tarifoptimierung; Abwerbung; Lead; Datenhandel

Sachverhalt

Die Parteien streiten um einen Unterlassungsanspruch, gestützt auf die Verletzung von Geschäfts- und Betriebsgeheimnissen der Kl. durch die Bekl.

Die Kl. ist eine private Krankenversicherungsgesellschaft. Die Bekl. ist eine Versicherungsvermittlung und bietet u.a. Dienstleistungen als sog. „Tarifoptimierungen" an. Versicherungsnehmer der Kl. ist der Zeuge S1. Die kundenspezifischen Daten des Versicherungsnehmers S1, die bei ihr vorlagen, gab die Kl. an keinen unberechtigten Dritten, insb. nicht an die Firma A., Frau B. oder die Bekl., heraus.

Am 24.4.2019 erhielt der Zeuge S1 einen Anruf des Geschäftsführers der Bekl. Er bot an, dessen Krankenversicherungsvertrag gegen Honorar zu optimieren. Auf Bitten des Zeugen S1 gab der Geschäftsführer der Bekl. diesem für einen Rückruf seine Telefonnummer, da der Zeuge S1 zunächst Rücksprache mit der Rechtsabteilung der Kl. halten wollte.

Nach Absprache mit der Kl. ging der Zeuge S1 zum Schein auf das Angebot der Bekl. zur Tarifoptimierung ein und rief diese zurück. Der Zeuge S1 trat seine etwaigen Ansprüche an die Kl. ab. Die Kl. ist der Ansicht, dass die Bekl. Daten verwendet habe, zu deren Besitz sie nicht berechtigt gewesen sei. Bei den Daten, so dem Namen, Geburtsdatum, der Anschrift und den Kontaktdaten des Zeugen S1, die Versicherungsdauer, die Beitragshöhe und der Umstand, dass sein Kind zusatzversichert sei, würden dem Schutz des § 203 Abs. 1 Nr. 7 StGB, des § 34 BDSG, Art. 15 DS-GVO und des § 2 GeschGehG unterfallen.

Aus den Gründen

29 I. Die Klage ist ... unbegründet.

30 Die Kl. hat gegen die Bekl. weder Anspruch auf Abgabe einer Unterlassungserklärung, noch Erstattung vorgerichtlicher Rechtsanwaltskosten im Wege des Schadensersatzes.

31 Ein Unterlassungsanspruch ergibt sich nicht aus § 6 GeschGehG. ...

38 Das *Gericht* konnte nicht feststellen, dass die Bekl. eine Rechtsverletzung i.S.d. §§ 2 Nr. 3 i.V.m. 4 GeschGehG begangen hat. ...

42 (2) Die durchgeführte Beweisaufnahme hat den Beklagtenvortrag bestätigt, wonach die Bekl. ... einen Lead ... von der Fa. A. käuflich erworben hat. Dieser Lead war Grundlage für die Kontaktaufnahme des Geschäftsführers der Bekl. zum Zeugen S1 ...

53 Auch eine mittelbare Verletzungshandlung nach § 4 Abs. 3 GeschGehG ist der Bekl. nicht vorzuwerfen.

54 Eine mittelbare Verletzungshandlung nach § 4 Abs. 3 GeschGehG würde voraussetzen, dass die Bekl. das Geschäftsgeheimnis über eine andere Person erlangt hätte und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung wusste oder hätte wissen müssen, dass diese das Geschäftsgeheimnis entgegen § 4 Abs. 2 GeschGehG genutzt oder offengelegt hätte.

55 Die Kl. hat nicht bewiesen, dass die Bekl. Kenntnis oder fahrlässige Unkenntnis von einer Rechtsverletzung hatte.

56 Der Verletzungstatbestand fordert ein subjektives Element in der Person des Handelnden. Sie muss das Geschäftsgeheimnis erlangt haben, obwohl sie wusste oder hätte wissen müssen, dass die andere Person das Geschäftsgeheimnis entgegen § 4 Abs. 2 GeschGehG genutzt oder offengelegt hat. ... Ein Wissen liegt vor, wenn die handelnde Person Kenntnis davon hatte, dass der Dritte einen Tatbestand gem. § 4 Abs. 2 GeschGehG verwirklicht hat. Dies entspricht den Anforderungen an ein vorsätzliches Verhalten. Demgegenüber ist davon auszugehen, dass eine Person von der Rechtsverletzung „wissen müsste", wenn die Unkenntnis auf Fahrlässigkeit beruht, also bei Anlegung der im Verkehr erforderlichen Sorgfalt die Rechtsverletzung hätte erkannt werden können und müssen. Von einem Wissenmüssen ist insb. auch dann auszugehen, wenn sich die handelnde Person der Einsicht verschließt, dass das erlangte Geschäftsgeheimnis auf ein unerlaubtes Nutzen oder Offenlegen zurückzuführen ist (*Köhler/Bornkamm/Feddersen*, 39. Aufl. 2021, GeschGehG § 4 Rn. 69, 70).

57 Der Kl. ist zuzustimmen, dass die Versicherungsgesellschaften hohes Interesse daran haben, dass die Daten ihrer Versicherungsnehmer nicht an Dritte gelangen. Diese Dritte haben ein eigenes finanzielles Interesse daran, die Versicherungsnehmer zu einem Wechsel zu einer anderen Versicherungsgesellschaft zu bewegen oder zu einem günstigeren Tarif. Demgegenüber steht das Interesse der Versicherungsgesellschaften die Kunden zu halten.

58 Gleichwohl kann aus dieser Interessenlage der Versicherungsgesellschaften nicht der Rückschluss gezogen werden, so wie es die Kl. gerne vornehmen möchte, dass die versicherungsspezifischen Datensätze ihrer Versicherungsnehmer auf dem freien Markt nicht verfügbar wären bzw. nur verfügbar wären, wenn dem ein rechtwidriges Handeln vorangegangen ist.

59 So ist zu sehen, dass dem Interesse der Versicherungsgesellschaften das Interesse der Versicherungsnehmer gegenübersteht, zu optimalen Konditionen versichert zu sein. Abhängig von dem jeweiligen Versicherungsnehmer kann dies darin bestehen, zu einem günstigeren Tarif oder zu besseren Versicherungsbedingungen versichert zu sein. Aus diesem Interesse heraus erklären viele Versicherungsnehmer ihr Einverständnis, z.B. bei bestimmten Internetportalen, ihnen Angebote zukommen zu lassen bzw. mit einer Kontaktaufnahme, um Weiteres abzuklären.

60 Aus diesem Grund durfte die Bekl. von einem rechtmäßigen Angebot des Datensatzes ausgehen und davon, dass die Daten durch den Versicherungsnehmer erlangt worden waren und dieser seine Einwilligung mit einer Kontaktaufnahme durch die Bekl. erteilt hatte. Umstände, welche dafürsprachen, dass der streitgegenständliche Datensatz nicht rechtmäßig erlangt worden wäre, wurden von der Kl. nicht dargelegt. Auch oblag es der Bekl. bzw. einem Käufer von Datensätzen nicht im Einzelfall zu prüfen, ob die Datensätze rechtmäßig erlangt worden sind.

61 ... Der Erwerb von Leads ist ein üblicher Geschäftsvorgang. Auch liegen keine Anhaltspunkte vor, dass die Bekl., z.B. auf Grund anderer Vorgänge, mit falschen Angaben der Verkäuferin hätte rechnen müssen. ...

63 Maßgeblicher Zeitpunkt für die Kenntnis bzw. das Kennenmüssen, bildet der Zeitpunkt bzw. Zeitraum der Verletzungshandlung, also des Erlangten, Nutzens oder Offenlegens der Geschäftsgeheimnisse. Erhält eine handelnde Person später von der vorausgegangenen Rechtsverletzung des Dritten Kenntnis, dann begründet dies allein keine mittelbare Rechtsverletzung (*Köhler/Bornkamm/Feddersen*, a.a.O., Rn. 73).

64 Ein Unterlassungsanspruch nach § 6 GeschGehG ist bereits mangels Rechtsverletzung der Bekl. i.S.d. §§ 2 Nr. 3, 4 GeschGehG nicht gegeben. ...

67 2. Der Unterlassungsanspruch kann nicht auf §§ 823, 1004 BGB, ggf. i.V.m. § 34 BDSG oder Art. 15 DS-GVO, gestützt werden.

68 Auch insoweit fehlt es an einem dargelegten und bewiesenen Verschulden der Bekl. § 823 Abs. 1 BGB greift nur dann ein, wenn der Schädiger vorsätzlich oder fahrlässig gehandelt hat. ...

LG Frankfurt/M.: Haftung des Host-Providers bei der Verbreitung von Gerüchten

Internationale Zuständigkeit

BGB §§ 823, 1004; EuGVVO Art. 7; GG Art. 1 Abs. 1, 2 Abs. 2; TMG § 3 ZPO; §§ 293, 294, 286
Beschluss vom 23.12.2020 – 2-03 O 418/20

Leitsätze

1. In der Entscheidung „Svensk AB" [ZD 2018, 115] hat der EuGH nicht entschieden, dass die Mosaiktheorie auf die nationale örtliche Zuständigkeit nach Art. 7 Nr. 2 EuGVVO zu übertragen ist.

2. Wird der Host-Provider darauf aufmerksam gemacht, dass auf seiner Plattform ein Gerücht verbreitet wird, für das es keine tatsächliche Grundlage gibt und hat der ursprüngliche Verbreiter des Gerüchts dies bereits eingeräumt, treffen den Host-Provider Prüfungs- und Überwachungspflichten. Rügt der Antragsteller die Verbreitung einer unwahren Tatsachenbehauptung und prüft der Host-Provider daraufhin lediglich das Vorliegen einer „Beleidigung", kann darin eine Verletzung der entsprechenden Pflichten bestehen.

Anm. d. Red.: Vgl. hierzu ferner *EuGH* ZD 2018, 115; *BGH* MMR 2010, 441; *BGH* MMR 2013, 535 m. Anm. *Engels*; *BGH* MMR 2012, 703; *BGH* MMR 2020, 387; *BGH* MMR 2007, 518; *BGH* MMR 2012, 623; *BGH* MMR 2012, 124 m. Anm. *Hoeren*; *BGH* MMR 2016, 418 m. Anm. *Paal* = ZD 2016, 281 m. Anm. *Palzer* sowie *LG Hamburg* MMR 2018, 407.

Schlagworte: Internationale Zuständigkeit; Verbreitung eines unwahren Gerüchts; Herkunftslandprinzip; einstweiliger Rechtsschutz

Sachverhalt

Der Ast. begehrt den Erlass einer einstweiligen Verfügung gerichtet auf die Unterlassung einer Äußerung. Auf dem Video-Portal der Ag. wurde ein Video veröffentlicht, das die angegriffene Äußerung enthält. Das Video stammt von A. Der Ast. wandte sich zunächst an die A. Diese gab eine Unterlassungserklärung ab.

Der Ast. wies die Ag. mit Schreiben v. 12.11.2020 unter Nennung der entsprechenden URLs auf die Äußerung hin. Die Ag. erwiderte, dass sie keine Beleidigung erkennen könne. Mit anwaltlichem Schreiben v. 25.11.2020 ließ der Ast. die Ag. unter Angabe der URL abmahnen. Die Ag. erwiderte wiederum, dass sie keine Beleidigung erkennen könne. Die *Kammer* hat die Ag. angehört. Die Ag. trägt in ihrer Stellungnahme vor, dass sie das beanstandete Video am 17.12.2020 für das auf Deutschland ausgerichtete Länderangebot ihres Dienstes vorsorglich gesperrt habe.

Aus den Gründen

6 II. Der Antrag ist zulässig.

7 Die internationale Zuständigkeit für die auf persönlichkeitsrechtliche Ansprüche gestützten Anträge auf Unterlassung der Vervielfältigung und Verbreitung bzw. deren Ermöglichung ist nach Art. 7 Nr. 2 EuGVVO gegeben (vgl. *EuGH* GRUR 2018, 108 [= ZD 2018, 115] – Svensk AB; vgl. auch *BGH* NJW 2010, 1752 [= MMR 2010, 441], Rn. 20 mwN – New York Times).

8 Das *LG Frankfurt/M.* ist auch national örtlich zuständig nach Art. 7 Nr. 2 EuGVVO bzw. § 32 ZPO. Entgegen der Auffassung der Ag. steht dem die Rspr. des *EuGH* in Sachen „Svensk AB" (*EuGH*, a.a.O., Rn. 35, 48 – Svensk AB) nicht entgegen, da der *EuGH* insoweit eine Übertragung der Mosaiktheorie auf die nationale örtliche Zuständigkeit nicht entschieden hat. ...

10 Der Antrag ist begründet.

11 1. Der Ast. hat aus den §§ 823, 1004 BGB i.V.m. Art. 1 Abs. 1 bzw. Art. 2 Abs. 1 GG einen Verfügungsanspruch auf Unterlassung der angegriffenen Äußerung „Inzwischen kursieren Gerüchte, dass es bei dem Clankrieg um [Antragsteller] geht. Anscheinend soll er neue Beschützer suchen und von dem ...-Clan zu ... wechseln wollen."

12 a. Auf die vorliegende Veröffentlichung ist deutsches Recht anwendbar (vgl. *BGH* NJW 2013, 2348 [= MMR 2013, 535 m. Anm. *Engels*]; *BGH* NJW 2012, 2197 [= MMR 2012, 703], Rn. 31; *BGH* GRUR 2020, 435 [= MMR 2020, 287], Rn. 17 ff. – Yelp).

13 b. Die angegriffene Äußerung greift unzulässig in das Persönlichkeitsrecht des Ast. ein.

14 Die Ag. verbreitet vorliegend ein Gerücht. Die Quelle dieses Gerüchts, die A, hat eingeräumt, dass es keine tatsächliche Grundlage für das Gerücht gibt und hat – wie der Ag. i.R.d. Anhörung mitgeteilt worden ist – eine entsprechende Unterlassungserklärung abgegeben. ...

15 c. Die Ag. haftet insoweit als Störerin. ...

17 Mittelbarer Störer kann auch der Betreiber eines Internetportals oder ein Host-Provider sein, wenn er später positive Kenntnis von einer Rechtsgutsverletzung durch einen von einem Dritten eingestellten Inhalt erlangt (*BGH* NJW 2007, 2558 [= MMR 2007, 518]). Zwar trifft den Betreiber keine Verpflichtung, die bei ihm eingestellten Inhalte auf eine Verletzung von Persönlichkeitsrechten Betroffener zu überprüfen (*BGH* NJW 2012, 2345 [= MMR 2012, 623] – RSS-Feeds; *BGH* NJW 2012, 148 [= MMR 2012, 124 m. Anm. *Hoeren*]). Wird ihm die Rechtsverletzung jedoch bekannt, so ist er ex nunc zur Unterlassung verpflichtet. In dem Unterlassen, einen als unzulässig erkannten Beitrag zu entfernen, liegt nämlich eine Perpetuierung der Verletzung des Persönlichkeitsrechts des Betroffenen. Der Betreiber eines Internetforums ist „Herr des Angebots" und verfügt deshalb vorrangig über den rechtlichen und tatsächlichen Zugriff. Auch wenn von ihm keine Prüfpflichten verletzt werden, so ist er doch nach allgemeinem Zivilrecht zur Beseitigung und damit zur Unterlassung künftiger Rechtsverletzungen verpflichtet (*BGH* NJW 2007, 2558 [= MMR 2007, 518], Rn. 9; *BGH* NJW 2016, 2106 [= MMR 2016, 418 m. Anm. *Paal* = ZD 2016, 281 m. Anm. *Palzer*], Rn. 23 – Ärztebewertungsportal III).

18 Wird eine Verletzung von Persönlichkeitsrechten behauptet, wird sich eine Rechtsverletzung durch den Betreiber allerdings nicht stets ohne Weiteres feststellen lassen. ...

19 Welcher Überprüfungsaufwand vom Host-Provider im Einzelfall zu verlangen ist, ist auf Grund einer umfassenden Interessenabwägung, bei der die betroffenen Grundrechte der Beteiligten zu berücksichtigen sind, zu ermitteln (*BGH*, a.a.O., Rn. 38 – Ärztebewertungsportal III; *LG Hamburg* MMR 2018, 407, Rn. 46 mwN). Mindestens ist i.d.R. jedenfalls eine Stellungnahme des einstellenden Dritten zu der Rüge des Betroffenen einzuholen. ...

20 In Anwendung dieser Grundsätze hat die Ag. auf die Abmahnung des Ast. hin ihren Pflichten nicht genügt. Der Hinweis des Ast. war insoweit hinreichend konkret, um Pflichten der Ag. auszulösen. Der Ast. hat in seiner Abmahnung unter Angabe der konkreten URL und der konkreten in dem Video enthaltenen Äußerung erläutert, dass die Äußerung unwahr ist und auch i.Ü. unzulässig in sein Persönlichkeitsrecht eingreife. Damit konnte und musste die Ag. auf Grundlage des Vortrags des Ast. prüfen, ob eine Persönlichkeitsrechtsverletzung vorliegt. Dem ist die Ag. offensichtlich nicht in hinreichendem Umfang nachgekommen. Sie hat nämlich trotz Hinweises und Abmahnung lediglich erwidert, dass keine „Beleidigung" vorliege. Die Ag. hat dadurch zu erkennen gegeben, dass sie das Vorbringen des Ast. nicht bzw. nicht in hinreichendem Umfang zur Kenntnis genommen geprüft hat. Der Ast. hat nämlich nicht das Vorliegen einer Beleidigung gerügt, sondern vielmehr die Behauptung unwahrer Tatsachen bzw. eines unwahren Gerüchts sowie den Verstoß gegen die Grundsätze der Verdachtsberichterstattung. Auf dieser Grundlage konnte sich die Ag. nicht darauf beschränken, eine „Beleidigung" zu prüfen, selbst wenn man den englischen Begriff der „defamation" weiter ziehen würde. ...

23 f. Soweit die Ag. rügt, dass das Herkunftslandprinzip nach § 3 Abs. 2 TMG einer Inanspruchnahme der Ag. entgegenstehe, folgt die *Kammer* dem jedenfalls für das vorliegende Eilverfahren nicht. Der *Kammer* ist aus anderen Verfahren vor der *Kammer* bekannt, dass nach dem hier maßgeblichen irischen Recht das entscheidende Merkmal bei der Prüfung der Frage, ob eine „Diffamierung" vorliegt, der Wahrheitsgehalt der entsprechenden Behauptung ist. Im Common Law wird der diffamierende Charakter einer Veröffentlichung daran gemessen, ob die Aussage den Ruf des von der Äußerung Betroffenen beeinträchtigt hat, wobei als Maßstab die Ansicht der „vernünftigen" Mitglieder der Gesellschaft zu Grunde zu legen ist (vgl. *OLG München* U. v. 13.11.2018 – 18 U 1282/16, Rn. 75 ff.).

24 Im Rahmen dieser im Eilverfahren hier nach § 293 ZPO zu Grunde zu legenden Grundsätze ... liegt ein Verstoß gegen das Herkunftslandprinzip nach § 3 Abs. 2 TMG nicht vor, da die angegriffene Äußerung auch nach irischem Recht unzulässig in das Persönlichkeitsrecht des Ast. eingreift. Insoweit hat der Ast. auch hinreichend nach dem Maßstab der §§ 294, 286 ZPO glaubhaft gemacht, dass die angegriffene Äußerung unwahr ist. ...

LG Berlin: Wettbewerbswidrige Angabe von Flugticketpreisen bei Ryanair

Transparenz

VO (EG) 1008/2008 Art. 23 Abs. 1
Urteil vom 1.10.2020 – 91 O 101/18; nicht rechtskräftig

Leitsatz der Redaktion

Ryanair darf bei Angabe von Flugpreisen in GBP nach Eingabe einer deutschen Kreditkartennummer des Kunden nicht automatisch ohne Vorankündigung den Preis in Euro umrechnen und hierbei Gebühren hinzufügen.

Anm. d. Red.: Die Berufung ist beim *KG* anhängig. Vgl. ferner *BGH* MMR 2016, 243.

Schlagworte: Flugbuchung; Preisangabe; Wechselkurs; Umrechnung; Gebühren; Transparenz; Währungswechsel; Gesamtpreis

Sachverhalt

Der *Bundesverband der Verbraucherzentralen und Verbraucherverbände* (Kl.) nimmt eine Fluggesellschaft (Bekl.) auf Unterlassung von Währungsumstellung während des Buchungsvorgange auf ihrer Internetseite in Anspruch.

Die Bekl. ist eine Fluggesellschaft mit Sitz in Irland. Sie betreibt die Internetseite ryanair.com, auf der Verbrauchern die Möglichkeit geboten wird, Onlineflüge zu buchen. Wenn der Kunde die Internetadresse ryanair.de in den Browser eingibt, landet er ebenfalls auf der erstgenannten Seite.

Am 14.3.2018 buchte ein Verbraucher auf der genannten Seite der Bekl. einen einfachen Flug für den 21.5.2018, Abflug ab Glasgow ab 14:10 Uhr, Ankunft in Berlin Schönefeld um 17:20 Uhr. Die Bekl. bot den Flug zunächst für 60,17 GBP an. Diese Preisangabe mit der Währung GBP setzt sich über weitere Buchungsschritte fort. Erst nachdem der Kunde seine Daten der deutschen Kreditkarte eingegeben hatte, zeigte die Buchungsseite unvermittelt und ohne jeden Hinweis einen zu zahlenden Gesamtpreis von 72,16 EUR an. Eine Ermittlung des Umrechnungskurses in dem Währungsrechner Finanzen.net ergab für einen Betrag von 60,17 GBP lediglich einen Betrag von 67,93 EUR. Wenn der Kunde seine Kreditkartendaten eingegeben hat, weist ein Text unter den Kartendaten darauf hin, mit wie viel die

Karte belastet wird. Daneben befindet sich ein klickbarer Link „Klicken Sie hier für weitere Informationen", der bei Anklicken den von der Bekl. verwendeten Wechselkurs angibt. Der Kunde wird darauf hingewiesen, dass er den Wechselkurs ablehnen kann, wenn er ein Häkchen entfernt, ihm wird aber gleichzeitig empfohlen, dies nicht zu tun damit er den garantierten Wechselkurs der Bekl. erhalte. Der Kl. mahnte die Bekl. mit Schreiben v. 21.3.2018 vergeblich ab.

Die Bekl. formuliert in ihren allgemeinen Beförderungsbedingungen, dass der Flugpreis, die Steuern, Gebühren und Abgaben grds. in der Währung des Reiseantrittslands zu entrichten seien, während sie zugleich grundsätzliche Bezahlung in anderen Währungen akzeptiere.

Der Kl. nimmt die Bekl. auf Unterlassung sowie auf Zahlung seiner Abmahnkosten von 200,– EUR in Anspruch. Der Kl. ist der Auffassung, dass die Bekl. mit der angegriffenen Handlung gegen das gesetzliche Verbot aus Art. 23 Abs. 1 VO (EG) 1008/2008 sowie gegen das wettbewerbsrechtliche Irreführungsverbot verstößt, da der zu zahlende Endpreis nicht alle Zuschläge und Entgelte enthalte. Der Währungsaufschlag sei nicht enthalten.

Aus den Gründen

17 Die Klage ist ... begründet.

18 I. Dem als Verband nach §§ 8 Abs. 1, Abs. 3 Nr. 3 UWG klagebefugten Kl. steht gegen die Bekl. als Fluggesellschaft ein Unterlassungsanspruch dahingehend, dass dieser nicht ohne deutlichen Hinweis und nähere weitere Informationen einen Währungswechsel während des Buchungsvorgangs vornimmt, aus § 3a UWG i.V.m. Art. 23 Abs. 1 VO (EG) 1008/2008 zu. Nach der genannten Vorschrift kann der kl. Wettbewerbsverband von der Bekl. Flugunternehmen verlangen, dass dieses nicht gegen europarechtliche Vorschriften zur Transparenz bei Flugpreisen verstößt. Art. 23 verpflichtet die Bekl., den zu zahlenden Endpreis stets auszuweisen, wobei dieser neben dem reinen Flugpreis alle anwendbaren Steuern und Gebühren, Zuschläge und Entgelte, die unvermeidbar zum Zeitpunkt der Veröffentlichung bereits vorhersehbar sind, einschließen muss. Gegen diese Verpflichtung hat die Bekl. verstoßen, weil sie i.R.d. Buchungsvorgangs nach Eingabe einer deutschen Kreditkarte den zunächst in britischen Pfund mitgeteilten Gesamtpreis ohne hinreichenden Hinweis in Euro umgerechnet hat. Dadurch sind dem buchenden Verbraucher Zusatzkosten entstanden, ohne dass er darauf hinreichend deutlich hingewiesen wurde. Der insoweit vorhandene Hinweis der Bekl. erfolgte lediglich über einen der Aufmerksamkeit des durchschnittlichen Verbrauchers nicht zugänglichen Link im Feld zu den Kreditkarten Informationen. Zum Vergleich ist z.B. das Feld, um eine Spende wegen des ökologischen Fußabdrucks des Flugs zu machen, ungleich größer, farblich abgesetzt und damit auffälliger. Dass dem Verbraucher Zusatzkosten durch die Umrechnung entstanden sind, steht zur Überzeugung der *Kammer* trotz des Bestreitens durch den Bekl. auf Grund des unstreitigen Sachverhalts fest. In den von der Bekl. selbst eingereichten Screenshots zu dem Buchungsvorgang ist zu erkennen, dass der zunächst mit 22,98 GBP angegebene Preis dann auf 28,34 EUR umspringt, die die Bekl. selbst wiederum in dem Hinweis ... in 23,26 GBP umrechnet. Bei dem von der Kl. eingereichten Buchungsvorgang war es ebenso. Die Bekl. hat aus Gründen, die sie zu vertreten hat, den Algorithmus, mit dem sie die zunächst in britischen Pfund angegebenen Preise in Euro umrechnet, nicht preisgegeben. Jedoch hat die Kl. hinreichend substanziiert vorgetragen, dass der ... Preis der Bekl. immer über dem ... gängigen [umgerechneten] Preisen liegt.

19 Diese Zusatzkosten hat die Bekl. entgegen ihrer Verpflichtung aus Art. 23 nicht offengelegt, obwohl sie das hätte tun müssen (grds. hierzu *BGH* U. v. 30.7.2015 – I ZR 29/12 [= MMR 2016, 243], mwN).

20 Die Bekl. ist auch passiv legitimiert, denn sie betreibt die streitgegenständliche Seite. Diese unterhält jedenfalls unter ryanair.com das Buchungsportal. Soweit die Bekl. die Auffassung vertreten hat, die Seite sei unzureichend bezeichnet, weil noch ein Zusatz .de erforderlich sei, kann sie damit nicht gehört werden. Der deutsche Kunde landet auf dem Buchungsportal der Bekl., wenn er ryanair.de oder ryanair.com eingibt.

21 Die Wiederholungsgefahr wird auf Grund des Verstoßes vermutet. Die Bekl. hat sich geweigert, eine außergerichtliche Streitbeilegung durch Abgabe einer strafbewehrten Unterlassungserklärung zu ermöglichen.

22 Soweit die Bekl. die Auffassung vertreten hat, die nunmehr tenorierte Unterlassungsverpflichtung sei von ihr nicht erfüllbar, vermag sich die *Kammer* dem nicht anzuschließen. Die Bekl. ist sehr wohl in der Lage die Zusatzkosten auszuweisen, die durch die von ihrem Algorhythmus vorgenommene Währungsumrechnung anfallen. Dass die Bekl. das in diesem Rechtsstreit nicht vorgetragen hat, steht dem nicht entgegen. Schließlich ist die Webseite so programmiert, dass der Buchungsvorgang automatisiert in dieser Form abläuft. Die Bekl. ist auch in der Lage, eine Bezugsgröße für den verwendeten Wechselkurs für den Währungswechsel anzugeben. Denn eine solche steht allein schon auf Grund des Algorithmus zur Verfügung. Schlussendlich steht es der Bekl. auch jederzeit frei, keinerlei Währungsumrechnung vorzunehmen. ...

AG Köln: Retweeten eines Fotos keine Urheberrechtsverletzung

Embedding

UrhG §§ 15 Abs. 2, 16, 19, 31, 97 Abs. 1, 97a
Urteil vom 22.4.2021 – 111 C 569/19

Leitsätze der Redaktion

1. Das Retweeten von Bildern stellt keine Vervielfältigung, öffentliche Zugänglichmachung oder öffentliche Wiedergabe dar, sofern der Inhalt zuvor unbeschränkt abrufbar war.

2. Wer Texte und Fotos auf Social-Media-Plattformen wie Instagram und Twitter hochlädt und sie im Profil öffentlich stellt, willigt konkludent in deren Weiterverbreitung auf der jeweiligen Plattform ein.

Anm. d. Red.: Vgl. ferner *EuGH* MMR 2014, 360 m. Anm. *Dietrich* – Svensson; *EuGH* MMR 2018, 487 – Mops-Foto und *EuGH* MMR 2017, 95 – GS Media.

Schlagworte: Öffentliche Wiedergabe; Social-Media-Plattform; Twitter; Embedding; konkludente Einwilligung

Sachverhalt

Die Parteien streiten über vorgerichtliche Rechtsanwaltskosten. Der Kl. ist Journalist. Der Bekl. ist ebenfalls Journalist. Die Parteien besitzen jeweils einen Account bei der Internetplattform Twitter. Bei Twitter handelt es sich um eine Kommunikationsplattform. Auf Twitter können angemeldete Nutzer telegrammartige Kurznachrichten verbreiten. Die Nachrichten werden „Tweets" genannt. Retweets dienen dazu, den Tweet eines anderen Nutzers mit den eigenen Followern zu teilen. Der Ausgangs-Tweet kann beim Retweeten auch kommentiert werden. Der Kl. ließ von dem Zeugen D. ein Porträtbild von sich erstellen. Dieses Porträtbild verwendete der Kl. auf seinem Twitter-Account als Profilbild. Am 26.10.2019 twitterte der Pressesprecher

einer Bundestagsfraktion (T.) unter der URL https://A. einen Text und lud hierzu dieses Porträtfoto des Kl. hoch. Dieses baute der Bekl. in einen Tweet auf seinem Twitter-Account unter der URL https://B. ein. Der Tweet wurde mehrfach retweetet. Eine ausdrückliche Einwilligung zur Nutzung des Lichtbilds hat der Kl. nicht erteilt. Der Kl. ließ den Bekl. durch seinen jetzigen Prozessbevollmächtigten auffordern, es zu unterlassen das bezeichnete Lichtbildwerk bzw. Lichtbild zu bearbeiten und/oder zu vervielfältigen und/oder zum Abruf bereit zu halten. Der Bekl. gab eine entsprechende Unterlassungsverpflichtungserklärung ab. Die vorgerichtlichen Rechtsanwaltskosten des Kl. zahlte der Bekl. nicht.

Der Kl. behauptet, er habe ein ausschließliches Nutzungsrecht an dem streitgegenständlichen Porträtbild von dem Zeugen D. eingeräumt bekommen.

Aus den Gründen

10 Die … Klage hat in der Sache keinen Erfolg.

11 I. 1. Dem Kl. steht der gegen den Bekl. geltend gemachte Anspruch auf Zahlung … unter keinem rechtlichen Gesichtspunkt zu. Ein solcher folgt insb. nicht aus § 97a Abs. 3 S. 1 UrhG.

12 Nach § 97a Abs. 3 S. 1 UrhG kann Ersatz der erforderlichen Aufwendung verlangt werden, wenn die Abmahnung berechtigt ist und § 97a Abs. 2 Nr. 1 – 4 UrhG entspricht.

13 Der Kl. hat den Bekl. auf Unterlassung abgemahnt. … Die streitgegenständliche Abmahnung des Kl. war jedoch nicht berechtigt.

14 Die Abmahnung ist berechtigt, wenn der Abmahnende ein Anspruch auf Unterlassung hat. Ein solcher besteht nach § 97 Abs. 1 UrhG gegen denjenigen, der das Urheberrecht oder ein anderes nach dem UrhG geschütztes Recht widerrechtlich verletzt. … Ein gem. §§ 31 Abs. 1 S. 2 2. Alt. i.V.m. 31 Abs. 3 UrhG eingeräumtes ausschließliches Nutzungsrecht berechtigt im Fall von dessen Verletzung zur Geltendmachung der in § 97 UrhG normierten Ansprüche (*BGH* GRUR 1987, 37 (39) – Videolizenzvertrag). Es kann vorliegend dahinstehen, ob der Kl. ein ausschließliches Nutzungsrecht an dem streitgegenständlichen Porträtbild innehatte, denn der Bekl. hat das geschützte Recht des Kl. jedenfalls nicht widerrechtlich verletzt.

15 Das Retweeten stellt bereits keine Verbreitung dar. Ob die Verbreitung von Beiträgen auf Social-Media-Plattformen der Zustimmung des Urhebers bedarf, richtet sich nach der rechtlichen Einordnung der jeweiligen Handlung. Ein Retweet auf Twitter stellt eine Nutzungshandlung dar. Werden Beiträge auf Twitter retweetet, liegt ein Fall des sog. „Embeddings" vor. Beim Embedding werden fremde Inhalte nicht kopiert, sondern bestehende Inhalte in das eigene Social-Media-Profil eingebunden. In einem solchen Fall liegt daher weder eine Vervielfältigung i.S.d. § 16 UrhG noch eine öffentliche Zugänglichmachung i.S.d. § 19 UrhG vor. Auch ist in der Wiedergabe des fremden Beitrags auf der eigenen Profilseite i.R.d. Retweetens keine öffentliche Wiedergabe i.S.d. § 15 Abs. 2 UrhG zu sehen. Eine solche Wiedergabehandlung liegt nach der Rspr. des *EuGH* vor, wenn eine recht große und unbegrenzte Anzahl an Personen erreicht und für ein neues Publikum wiedergegeben wird, d.h. für Publikum, an das der Inhaber des Urheberrechts nicht gedacht hatte, als er die ursprüngliche Wiedergabe erlaubte (*EuGH* GRUR 2014, 360 [= MMR 2014, 260 m. Anm. *Dietrich*], Rn. 17 – Svensson; GRUR-RS 2017, 127832 [= MMR 2018, 487] – Mops-Foto). Bei der Frage, ob ein neues Publikum erreicht wird knüpft der *EuGH* daran an, ob der Inhalt zuvor beschränkt oder unbeschränkt abrufbar war. Vorliegend war das streitgegenständliche Porträtbild bereits auf Twitter unbeschränkt abrufbar. Ein Inhalt, der bereits mit Zustimmung des Urhebers der Gesamtheit von Internetnutzern verfügbar war, kann nach Auffassung des *Gerichts* unter Zugrundelegung dieser Rspr. des *EuGH* nicht erneut dieser Öffentlichkeit zugänglich gemacht werden. Kann das Werk ohnehin von jedem Nutzer der Plattform eingesehen werden, weil der Nutzer, der das Werk ursprünglich veröffentlicht hat, die Privatsphäre-Einstellung auf der Plattform so gewählt hat, dass der Beitrag öffentlich, also von jedermann einsehbar ist, liegt ein „neues Publikum" nicht vor. Wie … vom Bekl. … unbestritten vorgetragen wurde, hat der Kl. das streitgegenständliche Porträtbild selbst auf Twitter gestellt und damit der Öffentlichkeit zugänglich gemacht. …

16 Selbst im Fall, dass der Kl. das streitgegenständliche Bild nicht selbst auf Twitter hochgeladen hätte, sondern dieses alleine durch T. auf Twitter gelangt wäre, würde das Retweeten durch den Bekl. keine „öffentliche Wiedergabe" darstellen. Werden ohne Zustimmung des Rechtsinhabers hochgeladene Werke verlinkt oder geteilt, hängt die Einordnung des Hyperlinks als „öffentliche Wiedergabe" entscheidend davon ab, welche Möglichkeiten demjenigen, welcher das Bild retweetet hat, zur Verfügung standen, um die Rechtswidrigkeit des retweeteten Inhalts zu erkennen (vgl. *EuGH* GRUR 2016, 1152 [= MMR 2017, 95] – GS Media). Bei einer mit Gewinnerzielungsabsicht gesetzten Verlinkung geht der *EuGH* davon aus, dass sich derjenige informiert, ob der Inhalt ordnungsgemäß hochgeladen wurde, sodass in einem solchen Fall eine widerlegliche Vermutung für die Kenntnis der Widerrechtlichkeit des verlinkten Inhalts spricht. Ohne Gewinnerzielungsabsicht ist zu ermitteln, ob der Linksetzer wusste oder hätte wissen können, dass der verlinkte Inhalt ohne Zustimmung des Internetnutzers hochgeladen wurde. Eine Gewinnerzielungsabsicht ist nicht vorgetragen und auch nicht ersichtlich, sodass die Vermutung nicht greift. Der Bekl. hat lediglich einen bereits vorhandenen Tweet geteilt und das streitgegenständliche Bild nicht selbst in Twitter eingestellt. Konkrete Anhaltspunkte dafür, dass der Bekl. dabei erkennen hätte können, dass dies ohne Zustimmung des Rechtsinhabers erfolgte, sind nicht vorgetragen. Würde jeder Retweet eines Werks, das ohne Zustimmung des Rechtsinhabers frei verfügbar war, eine Wiedergabehandlung darstellen, müsste jeder Twitternutzer vor einem Retweet herausfinden, ob der Inhalt, welchen er retweeten möchte, rechtmäßig hochgeladen wurde, um sich keinem Haftungsrisiko auszusetzen. Eine solche Recherche ist kaum praktikabel und in den Fällen in denen ein Retweet ohne Gewinnerzielungsabsicht erfolgt nicht zu verlangen.

17 Die Nutzung des Bilds in einem Retweet ist zudem nicht rechtswidrig, da sie mit Zustimmung des Rechtsinhabers erfolgte. Der Kl. hat zwar nicht ausdrücklich zugestimmt. Es ist jedoch eine konkludente Zustimmung des Kl. darin zu sehen, dass der Kl. das streitgegenständliche Profilbild selbst auf Twitter hochgeladen hat. Eine Einwilligung muss nicht ausdrücklich erklärt werden, vielmehr genügt eine konkludente Einwilligung. Wer Texte und Fotos auf Social-Media-Plattformen wie Instagram und Twitter hochlädt und sie im Profil öffentlich stellt, willigt konkludent in deren Weiterverbreitung auf der jeweiligen Plattform ein. Es entspricht der gängigen Praxis von Twitter, dass Inhalte und Bilder geteilt bzw. retweetet werden. Bei Twitter werden Bilder täglich retweetet. Jeder Nutzer von Twitter kann daher davon ausgehen, dass die anderen Nutzer ebenfalls in diese Verwendungspraxis eingewilligt haben und mit dem Retweeten ihrer eingestellten Inhalte einverstanden sind. Innerhalb der Funktionalitäten einer Plattform sind die urheberrechtlichen Nutzungshandlungen daher von einer konkludenten Einwilligung des einstellenden Nutzers gedeckt. Die konkludente Einwilligung folgt auch aus dem Wesen der Social-Media-Plattformen. Diese sind darauf ausgelegt, dass ihre Nutzer mit ihren Äußerungen und Bildern größtmögliche Breitenwirkung erzielen wollen. Wer diese Plattform nutzt und Inhalte darauf stellt, muss

wissen und damit rechnen, dass andere Nutzer von den Möglichkeiten, die die jeweilige Plattform bietet, Gebrauch machen. Stellt man Inhalte auf eine Social-Media-Plattform, muss nach dem allgemeinen Empfängerhorizont i.S.d. §§ 133, 157 BGB davon ausgegangen werden, dass sich der Nutzer zuvor mit der Funktionalität und den Verwendungen dieser Plattform auseinander gesetzt hat. Werden Inhalte daraufhin bewusst eingestellt, darf dies von den anderen Nutzern als Zustimmung gewertet werden, dass diese Inhalte wie die anderen Inhalte der Plattform im Rahmen ihrer Funktionalität genutzt werden dürfen. ...

BAG: Crowdworker sind Arbeitnehmer

Online-Plattform

BGB §§ 611a, 615, 622, 623; ArbGG § 11; KSchG § 4 S. 1; GewO § 106
Urteil vom 1.12.2020 – 9 AZR 102/20 (LAG München, ArbG München)

Leitsatz

Die kontinuierliche Durchführung einer Vielzahl von Kleinstaufträgen („Mikrojobs") durch Nutzer einer Online-Plattform („Crowdworker") auf der Grundlage einer mit dem Betreiber („Crowdsourcer") getroffenen Rahmenvereinbarung kann i.R.d. nach § 611a Abs. 1 S. 5 BGB gebotenen Gesamtbetrachtung zur Annahme eines Arbeitsverhältnisses führen, wenn der Crowdworker zur persönlichen Leistungserbringung verpflichtet ist, die geschuldete Tätigkeit ihrer Eigenart nach einfach gelagert und ihre Durchführungen inhaltlich vorgegeben sind sowie die Auftragsvergabe und die konkrete Nutzung der Online-Plattform i.S.e. Fremdbestimmens durch den Crowdsourcer gelenkt wird.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2020, 41799. Die Berufungsinstanz (*LAG München*) ist veröffentlicht in MMR 2020, 791 (Ls.).

Schlagworte: Kleinstaufträge; Online-Plattform; persönliche Abhängigkeit; Weisungsgebundenheit; Fremdbestimmtheit

Sachverhalt

Die Parteien streiten u.a. über die Wirksamkeit einer ordentlichen Kündigung. Dabei steht die Frage im Vordergrund, ob der Kl. als sog. „Crowdworker" als Arbeitnehmer anzusehen ist. Die Bekl. ist ein sog. „Crowdsourcing-Unternehmen", das u.a. die Kontrolle der Präsentation von Markenprodukten im Einzelhandel und an Tankstellen anbietet. Sie betreibt eine Online-Plattform, über die sie die Aufträge ihrer Kunden in eine Vielzahl einzelner Kleinstaufträge („Mikrojobs") zergliedert, an sog. „Crowdworker" vermittelt, die für sie gegen Bezahlung die entsprechenden Kontrollen durchführen. Der Kl. war für die Bekl. seit dem 4.2.2017 als Crowdworker tätig. Bei einem durchschnittlichen wöchentlichen Arbeitsaufwand von ca. 20 Stunden erzielte er eine durchschnittliche monatliche Vergütung i.H.v. 1.749,34 EUR. Die Parteien schlossen am 13.12.2016/6.2.2017 eine Basis-Vereinbarung, in der es auszugsweise heißt:

„Vorbemerkung
R ist ein Crowdsourcing Unternehmen und bietet über die R App Auftragnehmern verschiedene Aufträge zur Durchführung an. Nimmt der Auftragnehmer einen Auftrag an und führt diesen korrekt durch, wird ihm die im Einzelauftrag vereinbarte Vergütung direkt auf seinem virtuellen R Account gutgeschrieben. Der Auftragnehmer kann sich ein virtuelles Guthaben dann jederzeit per Paypal auszahlen lassen. ...

§ 1 Tätigkeit
... Der Auftraggeber bietet Aufträge der Crowd zur Durchführung an. Dem Auftragnehmer steht es jederzeit frei einen verfügbaren Auftrag anzunehmen, eine Verpflichtung dazu besteht nicht. Umgekehrt besteht keine Verpflichtung für den Auftraggeber Aufträge anzubieten.
Wenn der Auftragnehmer einen Auftrag annimmt, ist dieser entsprechend der Auftragsbeschreibung korrekt durchzuführen. Eine Vergütungspflicht für den Auftraggeber entsteht nur bei vollständiger und korrekter Durchführung des Auftrags gemäß der Auftragsbeschreibung.
Darüber hinaus ist der Auftragnehmer an keinerlei Vorgaben zum Arbeitsort oder Arbeitszeit gebunden. Projektbezogene Zeitvorgaben des Auftraggebers sind ebenso einzuhalten wie fachliche Vorgaben, soweit diese zur ordnungsgemäßen Vertragsdurchführung erforderlich sind. ...
Die Kontrolltätigkeiten für die Bekl. setzten die Installation und Nutzung der firmeneigenen Anwendersoftware für Smartphones („App") und die Nutzung der Website des Unternehmens voraus. In den für die Nutzung der App maßgeblichen „Allgemeinen Geschäfts- und Nutzungsbedingungen (Nutzer)" heißt es auszugsweise:
III. Zustandekommen der Verträge
1. Anmeldung und Accountpflege
Die Annahme von Aufträgen setzt die Anmeldung als Nutzer voraus. Die Anmeldung ist kostenlos. Sie erfolgt durch Eröffnung eines Benutzerkontos („Account"). Mit der Anmeldung stimmt der Nutzer diesen Nutzungsbedingungen zu. Ein Account ist nicht übertragbar. Das Anlegen mehrerer Accounts für dieselbe Person ist unzulässig. Durch die Annahme der Anmeldung kommt ein Nutzervertrag für die von R angebotenen Dienste auf der Website und für die App von R zustande. ...
Das Teilen eines Accounts und/oder Manipulieren der GPS-Lokalisierung, die durch die App protokolliert wird, wird als Missbrauch oder Betrug eingestuft sowie als Verletzung der Nutzungsbedingungen und der EULA angesehen und kann zu Maßnahmen gegen den Account/Nutzer führen, wie insb., aber nicht abschließend, die Sperrung des Accounts.
2. Auftrag, Inhalt und Durchführung
Der Nutzer übernimmt die Verantwortung für sein Handeln während der Durchführung eines Auftrags und verpflichtet sich dazu, sich gut über den jeweiligen Auftrag und wie dieser auszuführen ist, zu informieren und den Auftrag nach bestem Wissen und Gewissen und pünktlich in der App oder auf der Website durchzuführen.
Durch Annahme eines Auftrags innerhalb der App wird vom Nutzer das Angebot zur Erbringung der Leistung innerhalb der im Auftrag genannten Ausführungsfrist, und anhand der im Auftrag angegebenen Leistungsbeschreibung, angenommen.
Der Nutzer wird innerhalb der im Auftrag benannten Frist das Ergebnis an R übersenden. ...
3. Vergütung, steuerliche Pflichten und Hinweise
... Das Vertragsverhältnis zwischen R und dem Nutzer begründet kein Arbeitsverhältnis. Es besteht keine Weisungsgebundenheit.
IV. Beendigung des Vertrags
Jeder Nutzer hat die Möglichkeit, seinen Account und damit den Vertrag für den Zugang zur und die Nutzung der Website und der App von R ohne Einhaltung einer Kündigungsfrist und ohne Angabe von Gründen zu kündigen. Die Kündigung von Nutzern erfolgt über die Website oder direkt über die App. ..."

Der Kl. registrierte sich am 29.7.2016 auf der Plattform der Bekl. als sog. „RPro" und nahm am 4.2.2017 den ersten bezahlten Auftrag an. Nach Freischaltung der App wurden ihm offene Aufträge in einem Radius von bis zu 50 km von seinem aktuellen Standort angezeigt. Hierzu griff die App auf die GPS-Daten sei-

nes Smartphones zurück. Die App enthielt eine Funktion, mit der sich ein angenommener Auftrag abbrechen ließ. Die freigeschalteten Auftragsangebote konnten abhängig vom jeweiligen Kundenauftrag regelmäßig in einem Zeitfenster von zwei bis vier Wochen angenommen werden. Mit zunehmender Verweildauer des Angebots erhöhte sich die Vergütung für dessen Durchführung. Der Kl. führte überwiegend sog. „Tool Checks" durch. Hierbei handelte es sich um Kontrollen, die nach vorheriger Anmeldung vornehmlich in Tankstellen durchgeführt wurden. Zudem führte der Kl. sog. „Mystery Checks" durch, bei denen er sich nicht als Mitarbeiter der Bekl. zu erkennen gab. Die Auftragsangebote enthielten Vorgaben zu Ort und Zeit der Tätigkeit sowie eine genaue Beschreibung der bei der Auftragsdurchführung vorzunehmenden einzelnen Handlungsschritte. Neben der Angabe des voraussichtlichen Zeitaufwands gab die Auftragsbeschreibung ein Zeitfenster vor, innerhalb dessen der Auftrag durchzuführen war. Dieses betrug regelmäßig zwei Stunden. Wurde der Auftrag nicht innerhalb des zeitlichen Rahmens erledigt, wurde er erneut auf der Plattform angeboten. In einem Zeitraum von elf Monaten erledigte der Kl. 2.978 Aufträge.

Die Bekl. nahm die Leistungen der Crowdworker ab und schrieb ihnen neben dem Entgelt Erfahrungspunkte auf ihrem Nutzerkonto gut. Dadurch konnte ein Crowdworker seinen individuellen Nutzerstatus verbessern und eine höhere Anzahl an Aufträgen übernehmen. Auf dem zuletzt erreichten Level 15 konnte er 15 Aufträge gleichzeitig annehmen und deren Bearbeitungsreihenfolge selbst bestimmen. Mit Schriftsatz v. 24.6.2019 kündigte die Bekl. ein etwaig mit dem Kl. bestehendes Arbeitsverhältnis. Das *ArbG* hat die Klage abgewiesen. Das *LAG* hat die Berufung des Kl. zurückgewiesen.

Aus den Gründen

14 Die Revision des Kl. … war … als unbegründet zurückzuweisen. …

22 B. Das *LAG* hat den gegen die Beendigung des Arbeitsverhältnisses der Parteien durch die Kündigung … gerichteten Kündigungsschutzantrag … zwar mit rechtsfehlerhafter Begründung, i.E. aber zu Recht abgewiesen. Der Antrag ist unbegründet. Das zwischen den Parteien bestehende Arbeitsverhältnis wurde durch die Kündigung … beendet. …

27 [I.] 1. In einem Kündigungsschutzverfahren hat das *Gericht* inzident zu prüfen, ob das Rechtsverhältnis der Parteien zum Zeitpunkt des Zugangs der Kündigung als Arbeitsverhältnis zu qualifizieren ist. …

28 2. Entgegen der Auffassung des *LAG* war der Kl. zum Zeitpunkt der Kündigung v. 24.6.2019 als Arbeitnehmer und nicht als selbstständiger Unternehmer für die Bekl. tätig.

29 a) Das *LAG* ist zutreffend von den rechtlichen Grundsätzen ausgegangen, die bei der Abgrenzung eines Arbeitsverhältnisses von dem Rechtsverhältnis eines selbstständigen Unternehmers zu Grunde zu legen sind. Diese ergeben sich seit dem 1.4.2017 aus § 611a Abs. 1 BGB, der eine Legaldefinition des Arbeitsvertrags enthält und damit zusammenhängend regelt, wer Arbeitnehmer ist.

30 aa) Nach § 611a Abs. 1 BGB wird ein Arbeitnehmer durch den Arbeitsvertrag im Dienste eines anderen zur Leistung weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet (Satz 1). Das Weisungsrecht kann Inhalt, Durchführung, Zeit und Ort der Tätigkeit betreffen (Satz 2). Weisungsgebunden ist, wer nicht im Wesentlichen frei seine Tätigkeit gestalten und seine Arbeitszeit bestimmten kann (Satz 3). Der Grad der persönlichen Abhängigkeit hängt dabei auch von der Eigenart der jeweiligen Tätigkeit ab (Satz 4). Für die Feststellung, ob ein Arbeitsvertrag vorliegt, ist eine Gesamtbetrachtung aller Umstände vorzunehmen (Satz 5). Zeigt die tatsächliche Durchführung des Vertragsverhältnisses, dass es sich um ein Arbeitsverhältnis handelt, kommt es auf die Bezeichnung im Vertrag nicht an (Satz 6).

31 bb) Ein Arbeitsverhältnis unterscheidet sich danach von dem Rechtsverhältnis eines selbstständig Tätigen durch den Grad der persönlichen Abhängigkeit des Verpflichteten. Arbeitnehmer ist, wer auf Grund eines privatrechtlichen Vertrags im Dienste eines anderen zur Leistung weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet ist. Die Begriffe der Weisungsgebundenheit und Fremdbestimmung sind eng miteinander verbunden und überschneiden sich teilweise. Eine weisungsgebundene Tätigkeit ist in der Regel zugleich fremdbestimmt. Die Weisungsbindung ist das engere, den Vertragstyp im Kern kennzeichnende Kriterium, das durch § 611a Abs. 1 S. 2 bis S. 4 BGB näher ausgestaltet ist. Es kann, muss aber nicht gleichermaßen Inhalt, Durchführung, Zeit und Ort der Tätigkeit betreffen. Nur wenn jedwede Weisungsgebundenheit fehlt, liegt in der Regel kein Arbeitsverhältnis vor. Das Kriterium der Fremdbestimmung erfasst insb. vom Normaltyp des Arbeitsvertrags abweichende Vertragsgestaltungen (ErfK/*Preis*, 21. Aufl., BGB § 611a Rn. 32). Sie zeigt sich insb. in der Eingliederung des Arbeitnehmers in die Arbeitsorganisation des Arbeitgebers (vgl. *BAG* v. 17.1.2006 – 9 AZR 61/05, Rn. 11; *Bayreuther*, RdA 2020, 241 (246); *Preis*, a.a.O., Rn. 41; MHdB ArbR/*Schneider*, 4. Aufl., § 18 Rn. 19 f. u. 35; *Schubert*, RdA 2020, 248 (251); HWK/*Thüsing*, 9. Aufl., § 611a BGB Rn. 53). …

38 (3) Nach § 611a Abs. 1 S. 5 BGB bedarf es für die Feststellung des Rechtsverhältnisses im konkreten Fall einer Gesamtwürdigung aller maßgeblichen Umstände des Einzelfalls. Anknüpfungspunkt für die Zuordnung des Rechtsverhältnisses zu einem bestimmten Vertragstyp sind insb. die in § 611a Abs. 1 S. 1 BGB genannten Abgrenzungskriterien, können aber auch weitere Umstände sein, die teleologisch zur Abgrenzung beitragen können (vgl. *Preis*, a.a.O., Rn. 47 ff.; *Schneider*, a.a.O., Rn. 43). Vom Vorliegen eines Arbeitsverhältnisses kann (erst) dann ausgegangen werden, wenn den Kriterien, die für eine persönliche Abhängigkeit sprechen, i.R.d. gebotenen Gesamtbetrachtung hinreichendes Gewicht beizumessen ist oder sie dem Rechtsverhältnis ihr Gepräge geben.

39 (4) Leistet der Beschäftigte abweichend von den getroffenen Vereinbarungen tatsächlich weisungsgebundene, fremdbestimmte Arbeit, erklärt § 611a Abs. 1 S. 6 BGB die Bezeichnung im Vertrag für unbeachtlich. Der Widerspruch zwischen Vertragsbezeichnung und Vertragsdurchführung wird durch gesetzliche Anordnung zu Gunsten letzterer aufgelöst. Aus ihr ergibt sich der wirkliche Geschäftsinhalt. Für die Bestimmung des Vertragstyps ist dann allein die tatsächliche Durchführung des Vertragsverhältnisses maßgeblich. Damit wird dem zwingenden Charakter des Arbeitsrechts Rechnung getragen. Die zwingenden gesetzlichen Regelungen für Arbeitsverhältnisse können nicht dadurch abbedungen werden, dass die Parteien ihrem Arbeitsverhältnis eine andere Bezeichnung geben (vgl. *BAG* v. 21.5.2019 – 9 AZR 295/18, Rn. 13; v. 21.11.2013 – 6 AZR 23/12, Rn. 22; v. 25.9.2013 – 10 AZR 282/12, Rn. 16; ähnl. *Schwarze*, RdA 2020, 38 (41 f.); krit. *Riesenhuber*, RdA 2020, 226 (228 ff.)). …

41 b) Gemessen an diesen Grundsätzen hält das Urteil des *LAG* einer revisionsrechtlichen Überprüfung nicht stand.

42 aa) Das *LAG* hat im Ausgangspunkt zutreffend erkannt, dass die Bestimmungen der zwischen den Parteien geschlossenen Basis-Vereinbarung v. 13.12.2016/6.2.2017 nicht die Anforderungen eines Arbeitsvertrags erfüllen. Für die rechtliche Einord-

nung eines Rahmenvertrags kommt es darauf an, ob er der einen Partei das Recht zubilligt, frei über die Annahme der künftigen Einzelverträge zu entscheiden, oder ob einer Partei ein Weisungsrecht zustehen soll, infolge dessen sie die zu erbringende Leistung einseitig und für die andere Partei verbindlich festzulegen berechtigt ist (*BAG* v. 21.5.2019 – 9 AZR 295/18, Rn. 26). Vorliegend begründet die als Rahmenvertrag konzipierte Vereinbarung keine wechselseitigen Rechte und Pflichten. Aus ihr lässt sich weder eine Verpflichtung des Kl. zur Leistung von Diensten für die Bekl. noch zur Annahme eines über die Online-Plattform verfügbaren Auftrags ableiten. Ein Verpflichtungstatbestand folgt auch nicht aus den „Allgemeinen Geschäfts- und Nutzungsbedingungen" für die Bereitstellung und Nutzung der App.

43 bb) Rechtsfehlerhaft ist jedoch die Annahme des *LAG*, auch die tatsächliche Durchführung der durch Angebot und Annahme begründeten einzelnen Auftragsverhältnisse sprächen in ihrer Gesamtheit nicht für ein Arbeitsverhältnis. Die Feststellung, der Kl. habe, ohne mittelbar oder unmittelbar von Anreizen oder drohenden Sanktionen beeinflusst gewesen zu sein, frei darüber entscheiden können, ob und in welchem Umfang er ihm über die Online-Plattform angebotene Aufträge annehme, würdigt wesentliche Umstände der Zusammenarbeit der Parteien nach Annahme eines Auftragsangebots unvollständig. Das *LAG* hat außer Betracht gelassen, dass der Kl. bei der Ausführung der übernommenen Aufträge, d.h. im bereits begründeten Rechtsverhältnis, über keine nennenswerten Entscheidungsspielräume mehr verfügte. Die einzelnen Arbeitsschritte der zu verrichtenden Tätigkeiten wurden durch die Auftragsbeschreibungen auf der Online-Plattform von der Bekl. exakt vorgegeben. Der Kl. hatte diese abzuarbeiten, um die ihm in Aussicht gestellte Vergütung zu erhalten. Auch der zeitliche Rahmen für die Auftragserledigung war stark eingegrenzt. Die übertragenen Kontrolltätigkeiten waren regelmäßig binnen zwei Stunden zu verrichten. Dieses Spannungsverhältnis zwischen der Freiheit bei der Annahme der einzelnen Aufträge und der starken fachlichen, zeitlichen und örtlichen Gebundenheit des Kl. bei der Vertragsdurchführung, mithin beim Vollzug des jeweils angenommenen Auftrags (vgl. dazu allg. *Bayreuther*, RdA 2020, 241 (247)) wurde vom *LAG* weder aufgezeigt noch aufgelöst.

44 c) Dem *Senat* ist es auf der Grundlage der festgestellten Tatsachen ... möglich, eine abschließende Würdigung sämtlicher Umstände vorzunehmen, um den der Rechtsbeziehung der Parteien zu Grunde liegenden Vertragstyp zu bestimmen (vgl. dazu allg. *BAG* v. 13.12.2018 – 2 AZR 370/18, Rn. 47; v. 20.10.2016 – 6 AZR 471/15, Rn. 29). Danach hat der Kl. die ihm erteilten Aufträge nach den aufgezeigten Voraussetzungen tatsächlich in persönlicher Abhängigkeit (aa) i.R.e. einheitlichen Arbeitsverhältnisses (bb) durchgeführt.

45 aa) Die nach § 611a Abs. 1 S. 5 BGB vorzunehmende Gesamtbetrachtung aller Umstände des Einzelfalls ergibt, dass der Kl. i.R.d. tatsächlichen Vertragsdurchführung in arbeitnehmertypischer Weise weisungsgebundene und fremdbestimmte Arbeit leistete. Dafür fällt maßgeblich ins Gewicht, dass der Kl. zur persönlichen Leistungserbringung verpflichtet war (1), die geschuldete Tätigkeit ihrer Eigenart nach einfach gelagert und ihre Durchführung inhaltlich vorgegeben waren (2). Von besonderer Bedeutung ist zudem die konkrete Nutzung der App als Mittel der Fremdbestimmung bei der Auftragsvergabe (3).

46 (1) Der Kl. hatte die Kontrollaufträge persönlich durchzuführen. Beauftragt werden von der Bekl. nur Personen, die sich auf der Grundlage der Basis-Vereinbarung auf ihrer Plattform registriert haben und denen die Anwendersoftware (App) zur Verfügung gestellt wurde. Nach III.1. der Allgemeinen Geschäfts- und Nutzungsbedingungen ist weder das für die jeweilige Person eingerichtete Benutzerkonto übertragbar noch dürfen mehrere Benutzerkonten für dieselbe Person angelegt werden. Das Teilen des Accounts wird von der Bekl. ausdrücklich als „Missbrauch oder Betrug" gewertet und als „Verletzung der Nutzungsbedingungen" angesehen. Da die Aufträge über die App und damit über das individuelle Benutzerkonto abzuwickeln sind, kann der Nutzer ... die übernommenen Aufträge nicht durch Dritte ausführen lassen; er ist vielmehr gehalten, die Kontrollen persönlich vorzunehmen.

47 (2) An die Ausübung der Kleinstaufträge sind nur geringe Qualifikationsanforderungen gestellt. Es handelte sich um eine einfach gelagerte Tätigkeit, die das Rechtsverhältnis schon deshalb in die Nähe eines Arbeitsverhältnisses rücken lässt (vgl. *BAG* v. 30.9.1998 – 5 AZR 563/97 – zu I der Gründe; v. 19.11.1997 – 5 AZR 21/97 – zu B I 1 der Gründe). Der Kl. konnte auf Grund strikter Vorgaben der Bekl. an die Durchführung der ihm obliegenden einfach gelagerten Kontrollaufgaben seine Tätigkeit nicht im Wesentlichen frei gestalten. Er musste diese über die Online-Plattform mit Hilfe der App abwickeln. Dort war im Einzelnen festgelegt, wie er die Tätigkeiten zu verrichten und welche Arbeitsschritte er vorzunehmen hatte. Entgegen der Auffassung der Bekl. stellten diese Vorgaben nicht lediglich eine Beschreibung des Arbeitsergebnisses dar. Durch sie hat die Bekl. die ohnehin nur geringen Gestaltungsmöglichkeiten bei der Art und Weise der Vertragsdurchführung nahezu vollständig ausgeschlossen. Die Möglichkeit des Kl., frei darüber zu entscheiden, ob er zuerst die geforderten Fotos anfertigt und dann die Fragen an die Ansprechperson richtet oder andersherum verfährt, und seine Befugnis, auch die Reihenfolge der inhaltlich vorgegebenen Fragen selbst festzulegen, eröffneten ihm allenfalls minimale Gestaltungsspielräume. Sie führen jedoch nicht dazu, dass der Kl. seine Tätigkeit „im Wesentlichen" frei gestalten konnte.

48 (3) Die über die App einseitig vorgegebenen Beschäftigungsbedingungen sind so gestaltet, dass der jeweilige Nutzer – will er die Kontrolltätigkeiten wirtschaftlich sinnvoll ausüben – über einen längeren Zeitraum regelmäßig Aufträge annehmen und im Einzelnen vorbestimmte Arbeitsvorgänge abarbeiten muss. Lassen sich Crowdworker – wie der Kl. – durch den Abschluss der Basis-Vereinbarung, die Registrierung auf der Plattform und deren Nutzung grds. auf diese Beschäftigungsform ein, lenkt die Bekl. das Nutzerverhalten durch den Zuschnitt und die Kombination der Aufträge nach ihrem Beschäftigungsbedarf, ohne dass konkrete Anweisungen nötig sind. Daraus ergibt sich die Fremdbestimmung der Tätigkeit.

49 (a) Die Bekl. reicht die ihr übertragenen Kontrollaufgaben nicht unverändert an ihre „Subunternehmer" weiter. Sie teilt diese in Mikrojobs auf, um anschließend deren Zusammenfassung über die „Crowd" zu nutzerbezogenen Auftragsbündeln zu ermöglichen. Zunächst wird für die Kontrolle eines bestimmten Produkts bezogen auf jede einzelne Verkaufsstelle ein gesonderter Auftrag ausgeschrieben. Der Annahme und Durchführung eines einzigen Kleinstauftrags kommt – im Gegensatz zu größeren Aufgaben, die ggf. gewisse Fertigkeiten und Kenntnisse voraussetzen, oder zur gebündelten Vergabe mehrerer Mikrojobs – keine nennenswerte wirtschaftliche Bedeutung zu. Erst die Zusammenfassung und tatsächliche Abwicklung mehrerer Kleinstaufträge ermöglichen dem Nutzer eine rentable Beschäftigung. Um eine solche Tätigkeit verrichten zu dürfen, muss der Nutzer dem Einfluss der App nachgeben. Diese bietet ihm in einem Umkreis von bis zu 50 km um seinen aktuellen Aufenthaltsort Aufträge an. Die Anzahl der gleichzeitig anzunehmenden Aufträge und damit die Möglichkeit, eine Route zur Erfüllung mehrerer Aufträge zusammenzustellen und damit faktisch einen Stundenlohn zu erzielen, der den Aufwand rechtfertigt, in einem Umkreis von bis zu 50 km Ziele anzusteuern,

hängt vom erreichten Level im Bewertungssystem ab. Die Funktion der App ist somit nicht auf die Vergabe einzelner Aufträge durch einen selbstständigen Nutzer ausgerichtet, sondern zielt auf eine sich – aus Sicht der Bekl. – selbstvollziehende, automatisierte Disposition der Aufgaben auf dafür bereitstehende eingearbeitete Beschäftigte. Die Attraktivität des für den einzelnen Nutzer jeweils einsehbaren Angebotsportfolio wird durch Inhalt und Zuschnitt der zu einem bestimmten Zeitpunkt ausgelobten Aufträge und damit von der Bekl. bestimmt. Diese Organisation der Plattformarbeit muss einen im eigenen Interesse wirtschaftlich handelnden Crowdworker dazu veranlassen, die Angebotssituation ständig zu prüfen und sich dienstbereit zu halten, um eine sich für ihn auf Grund seiner Filtereinstellungen (Standort, Level, Zeitfenster) ergebende günstige Angebotssituation nutzen zu können.

50 (b) Die Bekl. setzte die Anreizfunktion dieses Bewertungssystems gezielt ein, um den Nutzer dazu zu veranlassen, in dem Bezirk seines gewöhnlichen Aufenthaltsorts kontinuierlich Kontrolltätigkeiten zu erledigen. Der Geschäftsführer der Bekl. hat das „Level-System" ... als „Gamification-Part der App" bezeichnet. Die Bekl. regte somit durch die Inaussichtstellung von Erfahrungspunkten und den damit verbundenen Vorteilen den „Spieltrieb" der Nutzer an mit dem Ziel, diese dadurch zu einer regelmäßigen Beschäftigung zu bewegen. Zugleich verzögerte sie den (zu) schnellen Aufstieg in ein höheres Level durch ein regelmäßig auf zwei Stunden begrenztes Zeitfenster, innerhalb dessen die Aufträge ab dem Zeitpunkt ihrer Übernahme zu bearbeiten sind. Denn zeitgleich können immer nur so viele Einzelangebote angenommen werden, wie der jeweilige Nutzer in der Lage ist, innerhalb von zwei Stunden abzuarbeiten. Inwieweit dieser tatsächlich zeitgleich die seinem Level entsprechende Anzahl an Aufträgen annehmen kann, hängt somit insb. von der räumlichen Nähe der zu kontrollierenden Tankstellen und Einzelhandelsgeschäfte zueinander ab. Je kürzer die Entfernung zwischen den anzusteuernden Orten, desto mehr Kontrollen lassen sich in der vorgegebenen Zeit erledigen.

51 (c) Die Nutzer dürfen die Zeitvorgaben nicht „umgehen". Sie sind nicht berechtigt, auf Vorrat die ihrem Level entsprechende Anzahl von Aufträgen zunächst anzunehmen, um einzelne davon durch Nutzung der Abbruchfunktion in der App wieder abzugeben, wenn sie feststellen, diese nicht in der vorgegebenen Zeit erledigen zu können. Weder die Basis-Vereinbarung noch die Allgemeinen Geschäfts- und Nutzungsbedingungen sehen ein solches Recht vor. Die dort aufgeführten Regelungen verpflichten den Nutzer nach Annahme des Auftrags dazu, „diesen entsprechend der Auftragsbeschreibung korrekt durchzuführen" bzw. die „Leistung innerhalb der im Auftrag genannten Ausführungsfrist" zu erledigen. Die technische Möglichkeit, einen Auftrag durch Nutzung der entsprechenden App-Funktion abzubrechen, lässt nicht auf das Recht schließen, sich einseitig von der eingegangenen Verpflichtung zu lösen. Auch bei einem Auftragsverlust infolge von Zeitablauf liegt eine Verletzung der vom Nutzer eingegangenen Pflicht vor, den Auftrag zeitgerecht auszuführen. Ein solches vertragswidriges Verhalten kann somit kein geeignetes Instrument darstellen, die Zeit-Level-Begrenzung zu umgehen und die sich daraus ergebende Lenkungswirkung zu durchbrechen.

52 bb) Die langfristige und kontinuierliche Beschäftigung des Kl. führte zu einer Verklammerung der einzelnen Aufträge zu einem einheitlichen (unbefristeten) Arbeitsverhältnis.

53 (1) Ein einheitliches Vertragsverhältnis kann durch übereinstimmendes schlüssiges Verhalten begründet werden, wenn die Parteien über einen rechtlich erheblichen Zeitraum einvernehmlich Dienstleistung und Vergütung ausgetauscht haben. Darin kann ihr übereinstimmende Wille zum Ausdruck kommen, einander zu den tatsächlich erbrachten Leistungen arbeitsvertraglich verbunden zu sein (*BAG* v. 9.4.2014 – 10 AZR 590/13, Rn. 26; v. 17.4.2013 – 10 AZR 272/12, Rn. 13).

54 (2) Vorliegend haben die Parteien durch die tatsächliche Vertragspraxis übereinstimmend zu erkennen gegeben, dass ihre Rechtsbeziehung nicht auf die Erledigung einzelner Kleinstaufträge, sondern die kontinuierliche Bearbeitung von Auftragsbündeln gerichtet war. Die in der Zergliederung in Mikrojobs und dem Level-System angelegte und für eine wirtschaftliche Vertragsdurchführung notwendige Bündelung einzelner Aufträge schließt es entgegen der Auffassung der Bekl. aus, dass die Parteien jeden einzelnen angenommenen Kleinstauftrag für sich gesehen als befristetes Arbeitsverhältnis angesehen haben, dessen Rechtsunwirksamkeit innerhalb von drei Wochen nach seinem vereinbarten Ende gem. § 17 S. 1 TzBfG durch Klage beim ArbG geltend gemacht werden muss. Eine rechtlich isolierte Betrachtung eines jeden der allein in einem Zeitraum von elf Monaten vom Kl. erledigten 2.978 Aufträge ließe außer Acht, dass die Bekl. ihr Geschäftsmodell auf eine verstetigte Beschäftigung von Crowdworkern ausgerichtet hat und es auch dem Kl. erkennbar auf eine verstetigte Beschäftigung ankam.

55 3. Entgegen der Auffassung des *LAG* bestand danach zwar bei Zugang der Kündigung ... ein Arbeitsverhältnis zwischen den Parteien. Da dieses jedoch durch die Kündigung der Bekl. ... fristgerecht ... endete, erweist sich die Abweisung des Kündigungsschutzantrags i.E. als zutreffend. ...

LAG Nürnberg: Fristlose Kündigung wegen Installation nicht zugelassener Software

Software-Zugriffsberechtigung

BGB §§ 241 Abs. 2, 626 Abs. 1; KSchG § 1 Abs. 2
Urteil vom 3.11.2020 – 7 Sa 99/20 (ArbG Nürnberg); rechtskräftig

Leitsatz

Das Installieren und Nutzen von Software, die zur Nutzung der Entwicklungsumgebung vorbehalten ist, in der Produktivumgebung ohne entsprechende Genehmigung des Arbeitgebers, kann wegen der damit verbundenen Gefährdung des Netzwerks einen wichtigen Grund an sich für eine außerordentliche Kündigung darstellen.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2020, 46004.

Schlagworte: Produktivumgebung; Software-Zugriffsberechtigung; Rollenkonzept; Sicherheitsrisiko; wichtiger Grund

Sachverhalt

Die Parteien streiten um die Wirksamkeit einer außerordentlichen Arbeitgeberkündigung. Der Kl. hat eine Ausbildung zum Fachinformatiker. Er war bei der Bekl. in der Vergütungsgruppe VII MTA beschäftigt. Ab 1.5.2016 arbeitete der Kl. als erste Fachkraft im Servicebereich Controlling Berichtswesen.

Die Bekl. betreibt zur Erledigung ihrer Aufgaben ein Computernetz mit ca. 120.000 Rechnern in der sog. Produktivumgebung (DST-Umgebung). Dazu zählt auch die Aufgabe des Kl. im Servicebereich Controlling Berichtswesen. Daneben besteht u.a. noch die Umgebung für die Softwareentwicklung (SDST-Umgebung). Die in diesem Bereich beschäftigten Mitarbeiter haben eigene Aufgabenprofile und damit verbunden andere Zugriffsmöglichkeiten auf bei der Bekl. vorhandene Software, darunter

auch Programme zur eigenen Softwareentwicklung. Entsprechende Software ist auf den zentralen Servern der Bekl. abgelegt. Für die Mitarbeiter in der Produktivumgebung ist Installation von Software auf ihren Rechnern grds. verboten.

Durch technische Vorsorge wird bei der Bekl. verhindert, dass Mitarbeiter in der DST-Umgebung Software über CD/DVD-Laufwerk, USB-Anschluss oder dem Internet auf ihren lokalen Rechner holen, dort lokal speichern und nutzbar machen können, die nicht für die DST-Umgebung freigegeben ist. Durch technische Vorsorge wird nicht verhindert, dass Mitarbeiter in der DST-Umgebung sich auf den Servern der Bekl. vorhandene portable Software, die den Mitarbeitern aus der SDST-Umgebung zur Nutzung vorbehalten ist, auf ihren lokalen Rechner laden, dort abspeichern und auch nutzen. Grds. müssen sich Mitarbeiter in der DST-Umgebung die Nutzung solcher Software in einem geregelten Verfahren nach § 7 DV-IKT freigeben lassen. Der Umgang der Mitarbeiter mit der IT wird grds. in einer Dienstvereinbarung über die Nutzung von Einrichtungen der Informations- und Kommunikationstechnik (IKT) geregelt.

In § 6 „Nutzung der Informations- und Kommunikationstechnologie" der DV IKT ist vorgesehen: „... (5) Die elektronische Ablage auf dienstlichen Einrichtungen der IKT ist ausschließlich für die Speicherung von Dateien mit dienstlichem Inhalt zugelassen. Die Nutzung von Speicherkapazitäten dienstlicher IKT-Einrichtungen für private Dateien ohne dienstlichen Bezug ist unzulässig. Dateien mit ausschließlich privatem Inhalt sind unverzüglich aus der dienstlichen oder persönlichen Ablage zu löschen. ..."

In § 7 „Rollen- und Berechtigungskonzepte" der DV IKT ist vorgesehen: „(1) In allen von der BA eingesetzten Verfahren der IKT werden die Zugriffsberechtigungen jeweils in einem Rollen- bzw. Berechtigungskonzept geregelt. Dabei ist festzulegen, welche Art von Zugriff (z.B. „lesender/schreibender Zugriff") zu erteilen ist. Die Berechtigungen werden abhängig von der übertragenen Aufgabe (dienstpostenbezogen) und der Erforderlichkeit für die Dauer der Aufgabenerledigung erteilt. Entfällt das dienstliche Erfordernis, auf das jeweilige Verfahren zugreifen zu müssen, ist die Zugriffsberechtigung zu entziehen. Verantwortlich sind die jeweiligen Vorgesetzten. Sofern darüber hinaus ausnahmsweise Zugriffsberechtigungen im Einzelfall erforderlich sind (z.B. bei Nachwuchskräften während der praktischen Ausbildungsteile), sind die Rollen personenbezogen zuzuweisen und zeitlich auf den erforderlichen Zeitraum zu begrenzen."

In § 10 „Informationssicherheit" der DV IKT ist in Absatz 2 vorgesehen: „... (2) Im Übrigen gelten die einschlägigen Regelungen der Informationssicherheit und die Durchführungsbestimmungen in den Benutzerhandbüchern, die entsprechend den gesetzlichen Regelungen und dieser Dienstvereinbarung zu gestalten sind."

Der Kl. holte sich aus der besonderen Software für die Mitarbeiter, die in der SDST-Umgebung arbeiten, eine portable Version des Webservers „XAMPP" und des Webbrowsers „Google Chrome" und speicherte diese lokal auf seinem Rechner. Mit dem Webserver XAMPP war es u.a. möglich, Webseiten oder Webanwendungen zu erstellen. In der Folgezeit nützte der Kl. diese Möglichkeiten.

Am 8.5.2019 stellte die IT-Sicherheitsabteilung bei der Bekl. (CERT) fest, dass auf dem Rechner des Kl. der Webserver XAMPP aktiviert worden war und betrieben wurde. Dies wurde von der Bekl. als IT-Sicherheitsvorfall gewertet. Dem Kl. wurde wegen Verstoß gegen die IKT-Dienstvereinbarung und die einschlägigen IT-Sicherheitsrichtlinien sowie wegen des Verdachts eines Arbeitszeitbetrugs das Arbeitsverhältnis außerordentlich und fristlos gekündigt. Das *Erstgericht* gab der Kündigungsschutzklage statt. Hinsichtlich der Installation des Webservers XAMPP und der Nutzung von Google Chrome Portable sei nicht nachgewiesen worden, dass der Kl. diese von einer Stelle außerhalb der Bekl. in das System eingespeist und ein erhöhtes Sicherheitsrisiko geschaffen habe.

Aus den Gründen

58 B. Die Berufung der Bekl. gegen das Endurteil des *ArbG Nürnberg* hat keinen Erfolg, sie ist unbegründet. Das *ArbG Nürnberg* hat der Kündigungsschutzklage des Kl. i.E. zu Recht stattgegeben. Das Arbeitsverhältnis der Parteien ist nicht durch die außerordentliche, fristlose Kündigung der Bekl. ... aufgelöst worden. ...

61 I. Die außerordentliche Kündigung ... entbehrt nicht des „wichtigen Grundes an sich".

62 1. Nach § 626 Abs. 1 BGB kann das Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, auf Grund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses selbst bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann. Die Prüfung erfolgt dabei in zwei Stufen. Es ist zunächst zu prüfen, ob der Sachverhalt ohne seine besonderen Umstände „an sich", d.h. typischerweise als wichtiger Grund geeignet ist. Ist dies der Fall, bedarf es in der zweiten Stufe der weiteren Prüfung, ob dem Kündigenden die Fortsetzung des Arbeitsverhältnisses unter Berücksichtigung der konkreten Umstände des Falls und unter Abwägung der Interessen beider Vertragsteile – jedenfalls bis zum Ablauf der Kündigungsfrist – zumutbar ist oder nicht. ...

64 2. An diesen Voraussetzungen gemessen war die Bekl. nicht berechtigt, das Arbeitsverhältnis der Parteien außerordentlich und fristlos zu kündigen.

65 a. Der Kl. hat mit dem Hinüberkopieren und Ausführbarmachen des Webservers XAMPP und des Webbrowsers Google Chrome Portable auf einen ihm zugänglichen Rechner in der DST-Umgebung und deren Nutzung zu privaten Zwecken gegen verschiedene Verbote für die Nutzer der IT-Systeme bei der Bekl. verstoßen. Darin liegt die Verletzung einer vertraglichen Nebenpflicht nach § 241 Abs. 2 BGB. Der Arbeitnehmer ist danach grds. verpflichtet, auf die berechtigten Interessen des Arbeitgebers Rücksicht zu nehmen. Diese Pflicht dient dem Schutz und der Förderung des Vertragszwecks. Zu den berechtigten Interessen der Bekl. zählt es, dass die Mitarbeiter die allgemein gültigen Regeln für die Nutzung der IT-Anlage beachten und befolgen und so dazu beitragen, dass das IT-Netz der Bekl. nicht unnötigen Gefährdungen ausgesetzt ist. Zu den allgemein gültigen und vom Kl. zu beachtenden Regeln zählen hier die DV IKT sowie die weiteren von der Bekl. erlassenen IT-Sicherheitsrichtlinien.

66 (1) Nach § 6 Abs. 5 S. 1 DV IKT ist die elektronische Ablage auf dienstlichen Einrichtungen der IKT ausschließlich für die Speicherung von Dateien mit dienstlichem Inhalt zulässig. Nach § 6 Abs. 5 S. 2 DV IKT ist die Nutzung von Speicherkapazitäten dienstlicher IKT-Einrichtungen für private Dateien ohne dienstlichen Bezug unzulässig. Nach § 10 Abs. 2 DV IKT gelten die einschlägigen Regelungen der Bekl. zur Informationssicherheit. Dazu zählt die IT-Sicherheitsrichtlinie, PC-Richtlinie für IT-Anwender, die das manuelle Installieren von Software untersagt. Dazu zählt ferner die IT-Sicherheitsrichtlinie, IT-Sicherheits-Gateways für IT-Dienstleister, die jeden Anschluss des Intranets der Bekl. an andere Netze verbietet, soweit dies in formaler Hinsicht nicht ausdrücklich erlaubt ist und materiell nicht unbedingt für die Erfüllung der Aufgaben der Bekl. erforderlich ist. Dazu zählt ferner die IT-Sicherheitsrichtlinie Hard- und Softwaremanagement für

IT-Anwender, nach der das Einspielen bzw. Benutzen von nicht freigegebener Soft- oder Hardware unzulässig ist und alle im Produktivbetrieb eingesetzte Soft- bzw. Hardware durch das Test- und Freigabeverfahren der Bekl. freigegeben werden muss. Schließlich ergibt sich aus § 7 DV IKT, dass nach dem Rollenkonzept nicht bestehende Zugriffsberechtigungen, die zur Erfüllung von Sonderaufgaben benötigt werden, nur gesondert personenbezogen und für die notwendige Dauer übertragen werden. Die Verpflichtung zur Beachtung dieser Regelungen hatte der Kl. auch zur Kenntnis genommen mit der Unterzeichnung der Benutzungsbedingungen für die private Nutzung der IT ...

67 (2) Hier hat der Kl. gegen diese Verbote verstoßen. Er hat sowohl den Webserver XAMPP als auch den Webbrowser Google Chrome Portable ohne entsprechendes Genehmigungsverfahren von den Servern der Bekl. hinüberkopiert in die DST-Umgebung. Bei beiden handelt es sich auch um Software. ...

72 Der Verstoß des Kl. gegen seine arbeitsvertraglichen Nebenpflichten, in der DST-Umgebung keine dort nicht freigegebene Software ohne besondere Genehmigung zu installieren durch „Kopieren" und „Ausführbarmachen" und diese anschließend zu nutzen, ist als außerordentlicher Kündigungsgrund an sich geeignet. ...

88 [II.] 1. Nachdem wichtige Gründe an sich für die Kündigung des Kl. vorliegen, ist in die zweite Stufe der Prüfung des wichtigen Grunds einzutreten. Nach dem Wortlaut des § 626 Abs. 1 BGB ist zu prüfen, ob dem Kündigenden die Fortsetzung des Arbeitsverhältnisses unter Berücksichtigung der konkreten Umstände des Falls und unter Abwägung der Interessen beider Vertragsteile – jedenfalls bis zum Ablauf der Kündigungsfrist – zumutbar ist oder nicht. ...

90 b. Hier war jedenfalls das mildere Mittel der ordentlichen Kündigung der Bekl. zumutbar. Die Vertragspflichtverletzungen des Kl. waren noch nicht so schwerwiegend, dass der Bekl. ein Festhalten am Arbeitsverhältnis nicht wenigstens bis zum Ablauf der ordentlichen Kündigungsfrist zumutbar gewesen wäre.

91 Was das Kopieren des Ordners mit dem Webserver XAMPP und dem Webbrowser Google Chrome Portable in die DST-Umgebung hinein und das Nützen dieser Software durch den Kl. betrifft, war die Nutzung von XAMPP mit keinem erhöhten Risiko eines Angriffs auf das Netz der Bekl. von außen verbunden. Die Bekl. hatte ... einen Mitarbeiter aus der IT mitgebracht als Auskunftsperson. Nach dessen Auskunft war mit der Installation von XAMPP kein Angriff von außen auf das System der Bekl. durch sog. „Mal-Software" möglich, da dieser Webserver nicht selbstständig ins Netz geht. Insoweit liegt ein Vertragsverstoß des Kl. vor, der mit keinem Sicherheitsrisiko behaftet war. Das einzige Risiko bestand im Hinblick auf den internen Datenschutz, da mit XAMPP andere Mitarbeiter Zugriff auf den Rechner des Kl. nehmen konnten. Diesem Problem hatte der Kl. aber vorgebeugt, da er nach der Installation von XAMPP sich nicht mehr vom Rechner abgemeldet, sondern seinen Rechner nur noch gesperrt hatte.

92 Was dagegen die Nutzung des Webbrowsers Google Chrome Portable betraf, war diese Nutzung mit einem Sicherheitsrisiko verbunden. Nach Auskunft der Bekl. ... führt das Verwenden einer alten Version, die nicht regelmäßig durch die IT aktualisiert wird, dazu, dass auch keine Sicherheits-Updates aufgespielt werden und so der Webbrowser über längere Zeit zu einem Einfallstor für „Mal-Software" in das Intranet der Bekl. werden kann.

93 Allerdings rechtfertigt nicht jede abstrakte Gefährdungslage und noch so entfernt liegende Möglichkeit eines Schadenseintritts für ein schützenswertes Gut des Arbeitgebers eine fristlose Kündigung. ... Die Bekl. benennt ... keinen einzigen Fall konkret mit Datum und Uhrzeit, an dem [der] Kl. mit dem Webbrowser Google Chrome Portable ins Netz gegangen sein soll. Damit ist auch kein Fall belegt, in dem der Kl. die geschilderte Gefährdungslage realisiert hat. ...

FG München: Aktivierung von Anschaffungskosten und Implementierungskosten einer Software

IT-Systemlandschaft

EStG §§ 4 Abs. 1 u. Abs. 4, 5 Abs. 1 u. Abs. 2, 6 Abs. 1, 6b Abs. 1, 7 Abs. 1; HGB §§ 240 Abs. 1 u. Abs. 2, 242 Abs. 1, 246 Abs. 1, 248 Abs. 2, 255 Abs. 1 S. 1
Urteil vom 4.2.2021 – 10 K 3084/19; rechtskräftig

Leitsätze der Redaktion

1. Bei einem Nutzungsrecht für eine IT-Systemlandschaft handelt es sich um ein immaterielles Wirtschaftsgut. Der Aktivierung des Nutzungsrechts stehen, soweit das Unternehmen Nutzungsentgelte zu zahlen hat, die Grundsätze zur Bilanzierung schwebender Geschäfte entgegen, die während der Laufzeit eines gegenseitigen Rechtsverhältnisses den Ausweis von Forderungen und Verbindlichkeiten verbieten.

2. Die Aufwendungen für Implementierungsleistungen gehören als Betriebsbereitschaftskosten zu den Anschaffungskosten des Wirtschaftsguts „Nutzungsrecht an der IT-Systemlandschaft". Wie die Anschaffungs-(haupt-)kosten können sie nicht aktiviert werden. Bei der Implementierung handelt es sich nicht um ein von dem angeschafften Nutzungsrecht zu unterscheidendes eigenständiges Wirtschaftsgut.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 8563.

Schlagworte: Aktivierung von Nutzungsrechten an Software; Implementierungsleistungen; immaterielles Wirtschaftsgut; Anschaffungskosten; Nutzungsrecht; Aktivierungsverbot; AfA; SAP-Standard-Software; Online-Handel; Backoffice

Sachverhalt

Streitig ist der Abzug von Aufwendungen für die Einführung und Implementierung von Software als Erhaltungsaufwand oder über die AfA verteilt auf die Nutzungsdauer. Gesellschafter der Kl. waren im Streitjahr X-GmbH als Komplementärin mit einer Gewinnbeteiligung i.H.v. 12,55% sowie X-KG als Kommanditistin mit einer Gewinnbeteiligung i.H.v. 87,45%.

Die Kl. ermittelte ihren Gewinn durch Betriebsvermögensvergleich gem. §§ 5 u. 4 Abs. 1 EStG. I.R.e. bei der Kl. durchgeführten Außenprüfung stellten die Prüfer u.a. fest, dass bei „Konzessionen, Schutzrechte, Lizenzen" Anschaffungskosten für Implementierung/Softwareeinführung i.H.v. (350.000,– EUR – AfA 20% von 1 Mio. EUR p.a. 200.000,– EUR =) 150.000,– EUR in 2012 zu aktivieren seien. Seit dem 1.1.2012 werde eine individualisierte *SAP*-Standard-Software eingesetzt, die von der Y-Verlagsgruppe für ihre Zwecke entwickelt worden sei und spezielle Module für das Verlagswesen umfasse (z.B. Online-Handel und Backoffice). Grundlage sei ein Rahmenkooperationsvertrag (RKV) der Kommanditistin mit Y-GmbH vom Mai 2011. Für die einzelnen Projekte seien Unterverträge zwischen der Kl. und Y-KG geschlossen worden. Neben laufenden Lizenzgebühren für die *SAP*-ERP-Software fielen ab 2012 vierteljährliche Lizenzzah-

lungen für die von Y übernommenen Projekte an. Der RKV wie die Unterverträge regelten daneben die Kosten der Einführung des Systems mit dem Ziel der Adaption der X-Gruppe-Prozesse auf die bestehende Systemlandschaft der Y-Gruppe. Die Arbeiten umfassten hauptsächlich die Implementierung und seien neben verschiedenen fremden Dienstleistern hauptsächlich von der Y-Gruppe durchgeführt worden. Diesbezüglich lägen Werkverträge vor, was aus mehreren Vertragsbestandteilen ersichtlich sei, insb. werde ein Erfolg geschuldet, für die Projekte seien Abnahmen und Gewährleistungen vereinbart. In den Vertragstexten werde mehrfach auf das Werkvertragsrecht Bezug genommen. Das Vorliegen von Werkverträgen impliziere allgemein die Anschaffung von Software. Bereits die Kosten der Implementierung und Einführung des Systems stellten zu aktivierende Wirtschaftsgüter dar. Die gesamten Kosten hätten 3.412.649,92 EUR betragen. Geschätzt werde der werthaltige Teil der Aufwendungen einvernehmlich mit ca. 30% (= 1.000.000,– EUR).

Das bekl. *FA* folgte der Auffassung der Prüfer und stellte mit Bescheid für 2012 über die gesonderte und einheitliche Feststellung von Besteuerungsgrundlagen für die Einkommensbesteuerung die Einkünfte aus Gewerbebetrieb auf 5.051.562,13 EUR (bisher 4.893.038,– EUR) fest.

Dagegen legte die Kl. Einspruch ein. Der Einspruch blieb ohne Erfolg.

Aus den Gründen

24 II. Die Klage hat Erfolg.

25 1. Die vom *FA* aktivierten Kosten des Y-Projekts i.H.v. 350.000,– EUR in 2012 sind sofort abzuziehen (§ 4 Abs. 4 EStG). Sie sind zwar als Betriebsbereitschaftskosten Anschaffungskosten des Wirtschaftsguts „Nutzungsrecht an der Y-Systemlandschaft", die die Kl. getätigt hat, um diesen Vermögensgegenstand von der fremden in die eigene Verfügungsmacht zu überführen, und die darum grds. den Periodengewinn nur im Wege der AfA, d.h., verteilt über die Nutzungsdauer des Wirtschaftsguts, beeinflussen (§§ 5 Abs. 1 S. 1, 4 Abs. 1 S. 1 u. S. 6, 6 Abs. 1 Nr. 1 S. 1, 7 Abs. 1 S. 1 EStG; vgl. auch § 255 Abs. 1 HGB). Da die Anschaffungskosten des Wirtschaftsguts „Nutzungsrecht an der Y-Systemlandschaft" aber wegen des Bilanzierungsverbots für schwebende Geschäfte nicht aktiviert werden dürfen, gilt dies auch für die Betriebsbereitschaftskosten.

26 a) Unstreitig hat die Kl. nicht – unter Inanspruchnahme von Dienstleistungen der Y-KG – ein Wirtschaftsgut selbst hergestellt, sodass die Aufwendungen nicht auf Grund des Aktivierungsverbots des § 5 Abs. 2 EStG sofort abzuziehen sind.

27 Nach den vorliegenden Verträgen zwischen der Kommanditistin und Y-GmbH (RKV ...) sowie den vorliegenden Verträgen zwischen der Kl. und Y-KG (Projektvertrag ...) handelt es sich um die Anschaffung des Nutzungsrechts an einer von Y-Gruppe (für sich selbst) individualisierten Software, im Einzelnen von Nutzungsrechten an der IT-Infrastruktur, IT-Prozessen, z.T. an eigenerstellter Software (Lizenzen), z.T. an fremdhergestellter Software (Unterlizenzen) von Y-Gruppe. Die Projektverträge regeln die von Y-KG zu erbringenden Implementierungsleistungen (ausdrücklich nicht den späteren Betrieb der Systeme, s. jeweils unter Nr. 1 der Verträge). Die Vereinbarungen sehen eine weitgehende Adaption der X-Gruppe-Prozesse auf die bestehende Systemlandschaft der Y-Gruppe vor, was i.E. die weitestgehende Übernahme der Y-Gruppe-Prozesse durch die X-Gruppe ohne größere Anpassungsmaßnahmen/Ausprägungen erforderte (so ausdrücklich die Präambeln aller Verträge, Leistungsvereinbarungen zu den Projektverträgen jeweils unter dem Punkt „Vorgehensmodell", was sich in den vereinbarten Leistungen der Y-KG widerspiegelt). Zudem trägt Y-KG das wirtschaftliche Risiko; insb. muss Y-KG bei ordentlicher Kündigung wegen nicht fristgerechter Fertigstellung nach den Projektverträgen die bisherigen Zahlungen der Kl. erstatten (vgl. z.B. Nr. 4 Projektvertrag Backoffice).

28 b) Bei dem der Kl. eingeräumten „Nutzungsrecht an der Y-Systemlandschaft" handelt es sich um ein immaterielles Wirtschaftsgut.

29 aa) Gem. § 5 Abs. 1 S. 1 EStG ist in den jeweiligen Bilanzen der Kl. das Betriebsvermögen anzusetzen, das nach den handelsrechtlichen Grundsätzen ordnungsmäßiger Buchführung (GoB) auszuweisen ist. Diese „handelsrechtlichen" GoB ergeben sich vornehmlich aus §§ 238 ff. HGB.

30 Nach §§ 240 Abs. 2 i.V.m. Abs. 1, 242 Abs. 1 u. 246 Abs. 1 HGB hat der Kaufmann in seiner Bilanz für den Schluss eines Geschäftsjahrs u.a. seine Vermögensgegenstände vollständig auszuweisen.

31 Die Begriffe Vermögensgegenstand und Wirtschaftsgut stimmen inhaltlich überein, sie sind auf der Grundlage einer wirtschaftlichen Betrachtungsweise auszulegen und daher weit gespannt. Beide umfassen nicht nur Sachen und Rechte i.S.d. BGB, sondern auch tatsächliche Zustände und konkrete Möglichkeiten, damit sämtliche Vorteile für den Betrieb, deren Erlangung sich der Kaufmann etwas kosten lässt, die einer besonderen Bewertung zugänglich sind, in der Regel einen Nutzen für mehrere Wirtschaftsjahre erbringen und jedenfalls mit dem Betrieb übertragen werden können. Darunter fallen, wie die Regelungen der § 248 Abs. 2 HGB und § 5 Abs. 2 EStG erkennen lassen, grds. auch – nicht körperliche – immaterielle Wirtschaftsgüter.

32 bb) Die der Kl. eingeräumte Möglichkeit, die Y-Systemlandschaft zu eigener betrieblicher Verwendung zu nutzen, begründet einen Vorteil für den Betrieb, der einer besonderen Bewertung zugänglich ist und auch mit dem Betrieb übertragen werden kann. Ihrer Qualifikation als immaterielles Wirtschaftsgut steht nicht entgegen, dass dieser Nutzungsvorteil nicht auf dinglicher, sondern lediglich schuldrechtlicher (obligatorischer) Grundlage besteht.

33 c) Dieses immaterielle Wirtschaftsgut in Form des Nutzungsvorteils hat – wie § 248 Abs. 2 HGB und § 5 Abs. 2 EStG für dessen Aktivierbarkeit übereinstimmend voraussetzen – die Kl. entgeltlich erworben, nämlich gegen Leistung laufender Nutzungsentgelte sowie gegen Zahlung bestimmter Einmalvergütungen für Implementierung und Hardware.

34 Der Aktivierung des Nutzungsrechts bei der Kl. stehen aber, soweit die Kl. laufende Nutzungsentgelte zu zahlen hat ... , die Grundsätze zur Bilanzierung schwebender Geschäfte entgegen, die während der Laufzeit eines gegenseitigen Rechtsverhältnisses den Ausweis von Forderungen und Verbindlichkeiten verbieten. Denn vorliegend bestand insoweit ein wiederkehrender Leistungsaustausch i.R.e. Dauerschuldverhältnisses (*BFH* U. v. 14.3.2006 – I R 109/04; *Wolffgang*, in: Kirchhof/Söhn/Mellinghoff, EStG, Stand Februar 1998, § 5 Rn. C 107 u. C 166).

35 d) Die Aufwendungen für Implementierungsleistungen gehören als Betriebsbereitschaftskosten zu den Anschaffungskosten des Wirtschaftsguts „Nutzungsrecht an der Y-Systemlandschaft". Wie die Anschaffungs-(haupt-)kosten können sie nicht aktiviert werden.

36 aa) Nach § 255 Abs. 1 S. 1 HGB sind Anschaffungskosten die Aufwendungen, die geleistet werden, um einen Vermögensgegenstand zu erwerben und ihn in einen betriebsbereiten Zustand zu versetzen, soweit sie dem Vermögensgegenstand ein-

zeln zugeordnet werden können. Zu den Anschaffungskosten gehören auch die Nebenkosten sowie die nachträglichen Anschaffungskosten (Satz 2).

37 bb) Soweit die Kl. Einmalvergütungen … für die Implementierung nach den vorliegenden Projektverträgen zu erbringen hat … , handelt [es] sich um Aufwendungen, um das Nutzungsrecht an der Y-Systemlandschaft in einen betriebsbereiten Zustand zu versetzen (vgl. *Kulosa*, in: Schmidt, EStG, 39. Aufl. 2020, § 6 Rn. 140 „Software").

38 cc) Anders als die Kl. meint, stellen die Implementierungsleistungen keine von dem Erwerb des Nutzungsrechts an der Y-Systemlandschaft unabhängig zu beurteilenden und deshalb nicht zu aktivierenden Dienstleistungen dar. Denn diese Leistungen sind Voraussetzung für die Herstellung der Betriebsbereitschaft und somit von Y-KG als Nebenpflicht zur Gewährung des Nutzungsrechts zu erbringen.

39 dd) Entgegen der Meinung des *FA* handelt es sich bei der Implementierung (anteilig) nicht um ein von dem angeschafften Nutzungsrecht zu unterscheidendes, eigenständiges Wirtschaftsgut.

40 Es fehlt an einer selbstständigen Bewertbarkeit, da der Wert der Implementierung vom Bestand des Nutzungsrechts an der Software abhängt. Ohne das Nutzungsrecht ist die Implementierung wertlos. Weiter steht die Implementierung in einem einheitlichen Nutzungs- und Funktionszusammenhang mit dem Nutzungsrecht an der Y-Systemlandschaft, sodass auch bei entsprechender Anwendung der Rechtsprechungsgrundsätze zu Mietereinbauten (*BFH* U. v. 26.2.1975 – I R 32/73; v. 28.7.1993 – I R 88/92) hier keine Aktivierung als selbstständiges Wirtschaftsgut in Betracht käme.

41 ee) Zwar hat der *BFH* für Nebenkosten bei der Bestellung eines anderen Nutzungsrechts, des Erbbaurechts, entschieden, dass diese zu aktivieren sind, da insoweit kein schwebendes Geschäft gegeben ist. Danach steht der grds. Aktivierungspflicht des Erbbaurechts nicht entgegen, dass das durch die Bestellung dieses Nutzungsrechts begründete Rechtsverhältnis als ein Dauerrechtsverhältnis, d.h., seinem rechtlichen und wirtschaftlichen Leistungsinhalt nach, als ein der Miete und der Pacht angenähertes entgeltliches Nutzungsverhältnis anzusehen ist. Dieses ist zwar in seinem Kern auf fortwährenden Leistungsaustausch gerichtet und entzieht sich insoweit als schwebendes Geschäft nach den Grundsätzen ordnungsmäßiger Buchführung einer Bilanzierung. Dieses Bilanzierungsverbot reicht aber dem Grunde wie dem Umfang nach nicht weiter als die für die Dauer des Schwebezustands vermutete „Ausgeglichenheit von Leistung und Gegenleistung".

42 Das Bilanzierungsverbot besteht auch unabhängig von der Art des Gegenstands des schwebenden Geschäfts und besagt nichts über den Rechtscharakter dieses Gegenstands. Das Erbbaurecht verliert daher seine Qualität als Wirtschaftsgut nicht dadurch, dass es zum Gegenstand eines schwebenden Geschäfts gemacht wird; die ungeachtet eines solchen Leistungsaustauschs fortbestehende Bilanzierungsfähigkeit des Erbbaurechts tritt vielmehr in Erscheinung, wenn außerhalb des Dauernutzungsverhältnisses ein Aufwand anfällt und zuzuordnen ist, der vom Erwerber zur Erlangung des Erbbaurechts getätigt worden ist.

43 Solche Zahlungen sind kein vorweggenommenes oder zusätzliches Nutzungsentgelt: Sie beruhen rechtlich wie wirtschaftlich auf einer Rechtsgrundlage, die vom (künftigen) Leistungsaustausch nicht erfasst wird, und können daher auch in der Bilanz nicht etwa wie „vorausgezahlte Nutzungsentgelte" behandelt werden.

44 Auch kommt es beim Ansatz von Anschaffungskosten nicht darauf an, ob der Aufwand tatsächlich zu einer Wertverbesserung des erworbenen Wirtschaftsguts geführt hat und sich entsprechend nachweisen lässt (*BFH* U. v. 4.6.1991 – X R 136/87).

45 ff) Eine abweichende Auffassung hat der *BFH* allerdings bei Kosten für die Begründung eines – wie hier – schuldrechtlichen Nutzungsverhältnisses vertreten. Kann das auf die Nutzung entfallende Entgelt nicht als Anschaffungs-(haupt-)kosten aktiviert werden, können auch Anschaffungsnebenkosten nicht aktiviert werden (*BFH* U. v. 19.6.1997 – IV R 16/95 zu Maklerprovision für Mietvertrag). Nichts anderes kann nach Auffassung des *Senats* für die – hier gegebenen – Betriebsbereitschaftskosten gelten.

46 2. Der vom *FA* vorgenommene AfA-Abzug auf ein Wirtschaftsgut „Implementierung" i.H.v. 200.000,– EUR ist rückgängig zu machen. …

OVG Lüneburg: Verwarnung wegen eines auf einer Facebook-Fanpage einer Partei veröffentlichten Fotos

Sozialsphäre

DS-GVO Art. 6, 58, 85 Abs. 2; GG Art. 21 Abs. 1; KUG §§ 22, 23; ParteienG § 1
Beschluss vom 19.1.2021 – 11 LA 16/20 (VG Hannover)

Leitsätze der Redaktion

1. Die Veröffentlichung eines Fotos auf einer Fanpage bei Facebook, auf dem Personen identifizierbar sind, stellt eine Verarbeitung personenbezogener Daten dar, die einer Legitimation nach datenschutzrechtlichen Vorschriften bedarf.

2. Kann das Ziel einer Datenverarbeitung auch durch die Veröffentlichung anonymisierter Daten erreicht werden, ist eine unanonymisierte Veröffentlichung nicht erforderlich.

3. Bei einem auf einer Fanpage bei Facebook veröffentlichten Foto, auf dem Personen identifizierbar sind, die in die Veröffentlichung nicht eingewilligt haben, ist i.R.d. Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zu Gunsten der betroffenen Personen u.a. zu berücksichtigen, dass eine solche Veröffentlichung auf Grund bestehender Missbrauchsmöglichkeiten sowie auf Grund der großen Reichweite derartiger Netzwerke mit erheblichen Risiken verbunden ist.

4. Art. 21 GG, § 1 ParteienG stellen keine spezifischen Rechtsgrundlagen zur Verarbeitung personenbezogener Daten i.S.v. Art. 6 Abs. 1 lit. e, Abs. 2 u. Abs. 3 DS-GVO dar.

5. Der bloße Umstand, dass eine Datenveröffentlichung auch einen Informationswert für die öffentliche Meinungsbildung hat bzw. ein Ausdruck einer persönlichen Ansicht ist, macht aus der Datenveröffentlichung noch keine journalistische Tätigkeit i.S.d. Art. 85 Abs. 2 DS-GVO.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 555. Die Leitsätze 1-4 sind amtliche Leitsätze; Leitsatz 5 ist ein redaktioneller Leitsatz. Vgl. hierzu auch *OVG Lüneburg* ZD 2021, 224 m. Anm. *Viehweger/Koreng*; ferner *Krüger/Wiencke*, MMR 2019, 76; *Rombey*, ZD 2019, 301; *Benedikt/Kranig*, ZD 2019, 4; *Hanloser*, ZD 2019, 287; *EuGH* MMR 2018, 591 m. Anm. *Moos/Rothkegel* = ZD 2018, 357 m. Anm. *Marosi/Mathé* und m. Anm. *Schulz*; *BVerwG* ZD 2020, 264 m. Anm. *Petri*; *EuGH* MMR 2009, 171; *EuGH* ZD 2017, 324; *EuGH* MMR 2009, 175; *BGH* MMR 2009, 608 m. Anm. *Greve/Schärdel*; *BVerwG* ZD 2016, 193; *EuGH* ZD 2019, 262; *BGH* ZD 2014, 468; *LG Frankfurt/M.* ZD 2018, 587 und *OLG Köln* ZD 2018, 434.

Schlagworte: Öffentlichkeitsarbeit; politische Willensbildung; Interessensabwägung; Sozialsphäre; journalistische Zwecke

Sachverhalt

Der Kl. ist ein Ortsverein der A-Partei. Er wendet sich dagegen, dass ihn die Bekl. i.R.e. aufsichtsbehördlichen Prüfverfahrens nach der DS-GVO wegen der Veröffentlichung eines Fotos bei Facebook verwarnt hat. Im August 2014 führte der Kl. in C eine öffentliche Veranstaltung in Form eines Ortstermins durch, bei der es um den Bau einer Ampelanlage über die viel befahrene D-Straße in C ging. An dieser Veranstaltung nahmen insgesamt ca. 70 Personen teil, darunter zahlreiche Anwohner sowie Vertreter des Kl. und Mitarbeiter der Kommunalverwaltung. Unter den Teilnehmern befanden sich auch die Eheleute F, die in einer Seitenstraße der D-Straße wohnen. Über die Veranstaltung wurde auch in der örtlichen Presse mit Texten und Bildern berichtet, die teilweise immer noch im Internet verfügbar sind. Auf einem von einem Veranstaltungsteilnehmer aufgenommenen Foto, auf dem insgesamt ca. 30 bis 40 Personen zu sehen sind, sind u.a. Frau F (frontal vom Kopf bis zu den Knien), Herr F (frontal nur mit dem Kopf) sowie der Vorsitzende des Kl. (seitlich von Kopf bis Fuß) erkennbar. Der Vorsitzende des Kl. steht dabei in der Mitte eines aus den weiteren Personen geformten Halbkreises. Nachdem im Spätsommer 2018 mit dem Bau der Ampelanlage über die D-Straße begonnen worden war, veröffentlichte der Kl. im September 2018 auf seiner Fanpage bei Facebook, die für sämtliche Facebook-Nutzer frei einsehbar ist, das streitgegenständliche Foto. Daraufhin wandte sich F an den Kl. und führte aus, dass er von einem Kollegen auf das Foto bei Facebook aufmerksam gemacht worden sei, und forderte den Kl. unter Verweis darauf, dass zur Veröffentlichung ein Einverständnis erforderlich sei, zur Stellungnahme und zur Löschung des Fotos auf. Mit E-Mail v. 20.9.2018 antwortete der Vorsitzende des Kl. dem F, dass das Foto seinerzeit von einer ihm unbekannten Person aufgenommen und bereits vor vier Jahren im Internet gepostet worden sei. Jetzt sei es lediglich erneut veröffentlicht worden. Mit Schreiben v. 26.9.2018 wandte sich F zudem unter Bezugnahme und Vorlage seiner Korrespondenz mit dem Vorsitzenden des Kl. mit einer datenschutzrechtlichen Beschwerde an die Bekl. Die Bekl. leitete daraufhin ein aufsichtsbehördliches Prüfverfahren nach Art. 57 Abs. 1 lit. a, lit. f und Art. 58 Abs. 1 lit. b DS-GVO ggü. dem Kl. ein.

Mit Bescheid v. 9.1.2019 verwarnte die Bekl. den Kl. Zur Begründung führte sie im Wesentlichen aus, der Kl. habe für unbestimmte Zeit ohne Wissen und Einverständnis der Eheleute F ein Foto auf seiner Fanpage bei Facebook veröffentlicht, auf dem die Eheleute F abgebildet gewesen seien. Damit habe der Kl. personenbezogene Daten ohne Rechtsgrundlage verarbeitet und gegen Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 lit. f DS-GVO verstoßen. Er sei deshalb gem. Art. 58 Abs. 2 lit. b DS-GVO zu verwarnen.

Aus den Gründen

10 II. Die vom Kl. gegen die Klageabweisung geltend gemachten Zulassungsgründe ... rechtfertigen nicht die Zulassung der Berufung. ...

12 Rechtsgrundlage der Verwarnung der Bekl. v. 9.1.2019 ist Art. 58 Abs. 2 lit. b DS-GVO. Nach dieser Vorschrift hat die Aufsichtsbehörde gem. Art. 51 DS-GVO die Befugnis, einen Verantwortlichen zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen die DS-GVO verstoßen hat. Vorliegend stellt die vom Kl. vorgenommene Veröffentlichung des streitgegenständlichen Fotos auf seiner Fanpage bei Facebook eine Verarbeitung personenbezogener Daten dar, die nicht nach Art. 5 Abs. 1 i.V.m. Art. 6 Abs. 1 DS-GVO gerechtfertigt war und damit gegen die DS-GVO verstoßen hat.

13 Bei der Veröffentlichung des streitgegenständlichen Fotos durch den Kl. auf seiner Fanpage bei Facebook handelt es sich um eine Verarbeitung personenbezogener Daten der abgebildeten Personen i.S.d. Art. 2 Abs. 1, Art. 4 Nr. 1 u. 2 DS-GVO. Als Betreiber der Fanpage bei Facebook ist der Kl. für die streitgegenständliche Datenverarbeitung gemeinsam mit *Facebook* Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO (vgl. *EuGH* U. v. 5.6.2018 – C 210/16 [= MMR 2018, 591 m. Anm. *Moos/Rothkegel* = ZD 2018, 357 m. Anm. *Marosi/Mathé* und m. Anm. *Schulz*], Rn. 30 ff.; *BVerwG* U. v. 11.9.2019 – 6 C 15/18 [= ZD 2020, 264 m. Anm. *Petri*], Rn. 21). Nach Art. 6 Abs. 1 DS-GVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn mindestens eine der insgesamt sechs im Einzelnen in lit. a bis lit. f dieser Vorschrift aufgeführten Voraussetzungen erfüllt ist. Das *VG* ist zutreffend davon ausgegangen, dass die Veröffentlichung des streitgegenständlichen Fotos auf der Fanpage des Kl. bei Facebook nicht nach Art. 6 Abs. 1 lit. f DS-GVO gerechtfertigt war (dazu unter a)) [= Rn. 14]). Entgegen dem Zulassungsvorbringen des Kl. kann er sich auch nicht mit Erfolg darauf berufen, dass die streitgegenständliche Veröffentlichung nach Art. 6 Abs. 1 lit. e DS-GVO i.V.m. Art. 21 GG, § 1 ParteienG (dazu unter b)) [= Rn. 30]) oder nach §§ 22, 23 KUG (dazu unter c) [= Rn. 35]) zulässig war.

14 a) Gem. Art. 6 Abs. 1 lit. f DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. ...

15 aa) Unter dem Begriff der berechtigten Interessen i.S.d. Art. 6 Abs. 1 lit. f DS-GVO sind „die vernünftigen Erwartungen der betroffenen Person" (s. Erwägungsgrund 47 DS-GVO), also sämtliche rechtlichen, wirtschaftlichen oder ideellen Interessen zu verstehen (vgl. *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand: 1.5.2020, Art. 6 DS-GVO Rn. 48 f.; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 57; *Frenzel*, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 6 DS-GVO Rn. 28). Vorliegend diente die Veröffentlichung des streitgegenständlichen Fotos auf der Fanpage bei Facebook dazu, über die parteipolitischen Aktivitäten des Kl. und ihre Erfolge zu informieren und damit – jedenfalls mittelbar – auch an der politischen Willensbildung des Volkes mitzuwirken. Dieses Anliegen stellt ein berechtigtes Interesse i.S.d. Art. 6 Abs. 1 lit. f DS-GVO dar.

16 bb) Die Veröffentlichung des streitgegenständlichen Fotos war jedoch nicht erforderlich i.S.d. Art. 6 Abs. 1 lit. f DS-GVO. Der in der DS-GVO nicht gesondert definierte Begriff der Erforderlichkeit ist unter Berücksichtigung von Erwägungsgrund 39 S. 9 DS-GVO dahingehend auszulegen, dass die Erforderlichkeit zu bejahen ist, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (vgl. *Frenzel*, a.a.O., Rn. 29; *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 6 DS-GVO Rn. 147a). Im Gegensatz zu den weit auszulegenden „berechtigten Interessen" ist der Begriff der Erforderlichkeit eng auszulegen (*Buchner/Petri*, a.a.O.; *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, Art. 6 Abs. 1 DS-GVO Rn. 100, jew. mwN). Zur Bejahung der Erforderlichkeit reicht somit weder eine bloße Zweckdienlichkeit oder eine bestmögliche Effizienz der Datenverarbeitung, noch kann die Erforderlichkeit allein damit begründet werden, dass es sich bei der beabsichtigten Datenverarbeitung um die aus Sicht des Verantwortlichen wirtschaftlich sinnvollste Alternative handelt (vgl. *Buchner/Petri*, a.a.O.). Kann das Ziel einer Datenverarbeitung auch durch die Verarbeitung anonymisierter Daten erreicht werden, ist eine unanonymisierte Verarbeitung nicht erforderlich (vgl. *EuGH* U. v. 16.12.2008 – C-524/06 [= MMR 2009, 171], Rn. 65; *Schantz*, a.a.O.). Die Datenverarbeitung ist somit auf das „absolut Notwendige" zu be-

grenzen (vgl. *EuGH* U. v. 4.5.2017 – C-13/16 [= ZD 2017, 324], Rn. 30; *Schantz*, a.a.O.).

17 Ausgehend von diesen Maßstäben hat das *VG* zu Recht angenommen, dass die Veröffentlichung des streitgegenständlichen Fotos durch den Kl. bei Facebook nicht erforderlich i.S.d. Art. 6 Abs. 1 lit. f DS-GVO war. Zur Begründung hat das *VG* ausgeführt, dass es vorliegend zur Wahrung der berechtigten Interessen des Kl. nicht darauf ankomme, dass gerade die Eheleute F als solche in einen spezifischen Kontext zur politischen Tätigkeit des Kl. gesetzt würden, sondern es dem Kl. nur darum gegangen sei, zu dokumentieren, dass das Thema, für das er sich politisch eingesetzt habe, eine größere Anzahl von Personen interessiere. In diesem Fall reiche es aus, das streitgegenständliche Foto unter Unkenntlichmachung der abgebildeten Personen, z.B. durch Verpixelung der Gesichter, zu verwenden.

18 Die vom Kl. diesbezüglich im Zulassungsverfahren vorgebrachten Einwände begründen keine ernstlichen Richtigkeitszweifel an der angefochtenen Entscheidung. ...

19 Entgegen der Ansicht des Kl. ist ihm eine Unkenntlichmachung derjenigen Personen, die auf dem Foto identifizierbar sind und die in die Veröffentlichung nicht eingewilligt haben, auch zumutbar. Seine Einwände, die Veröffentlichung eines teilweise verpixelten Fotos sei nicht glaubwürdig, nicht authentisch und unseriös, zudem käme die Verpixelung von Personen bzw. ihrer Gesichter einer „unglaublichen Puzzelarbeit gleich", rechtfertigen keine andere Beurteilung. Wie bereits das *VG* in der angefochtenen Entscheidung ausgeführt hat, kann eine Verpixelung mit Hilfe gängiger Bildbearbeitungssoftware ohne erheblichen Kosten- und Zeitaufwand umgesetzt werden. ... Entgegen der Ansicht des Kl. würde eine Unkenntlichmachung der Gesichter der Eheleute F (und ggf. weiterer auf dem Foto identifizierbarer Personen, die in die Veröffentlichung nicht eingewilligt haben) auch nicht dazu führen, dass der Kl. das von ihm mit der Veröffentlichung verfolgte Ziel nicht mehr erreichen kann. Insofern teilt der *Senat* die von der Bekl. im Zulassungsverfahren vorgetragenen Erwägungen, dass eine Unkenntlichmachung von Personen u.a. durch Verpixelung in veröffentlichten Fotos weit verbreitet und allgemein anerkannt ist, um die häufig widerstreitenden Interessen der Öffentlichkeit an Information einerseits und dem Persönlichkeits- und Datenschutzrecht der abgebildeten Personen andererseits in einen angemessenen Ausgleich zu bringen. ...

21 cc) Entgegen der Ansicht des Kl. ist das *VG* auch zutreffend davon ausgegangen, dass die nach Art. 6 Abs. 1 lit. f DS-GVO vorzunehmende Interessenabwägung zu Lasten des Kl. ausgeht, da die Interessen, Grundrechte und Grundfreiheiten der Eheleute F, die den Schutz personenbezogener Daten erfordern, ggü. den berechtigten Interessen des Kl. an der Veröffentlichung des streitgegenständlichen Fotos überwiegen.

22 I.R.d. vorzunehmenden Interessenabwägung sind die jeweils einander gegenüberstehenden Rechte und Interessen einzelfallbezogen zu ermitteln und zu beurteilen (vgl. *Albers/Veit*, a.a.O., Rn. 51, mwN). Unter Beachtung der im Erwägungsgrund 47 DS-GVO enthaltenen Vorgaben sind dabei u.a. die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, sowie die Absehbarkeit bzw. Vorhersehbarkeit der Verarbeitung zu dem maßgeblichen Zweck zu berücksichtigen. Wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, kann sich daraus ein gewichtiger Anhaltspunkt dafür ergeben, dass die Interessen und Grundrechte der betroffenen Person das berechtigte Interesse des Verantwortlichen überwiegen (vgl. *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 28; *Albers/Veit*, a.a.O., Rn. 51, mwN). Entsprechendes gilt, wenn zwischen der betroffenen Person und dem Verantwortlichen keinerlei (vertragliche oder geschäftliche) Beziehung besteht, die die fragliche Datenverarbeitung vernünftigerweise absehbar macht (vgl. *Heberlein*, a.a.O.). Zu berücksichtigen sind auch die mit der Verarbeitung für den Betroffenen verbundenen Risiken sowie die Form der Datenverarbeitung. Danach kommt den Betroffeneninteressen etwa dann ein hohes Gewicht zu, wenn die Daten besonders missbrauchsanfällig sind (*Buchner/Petri*, a.a.O., Rn. 150; *Schantz*, a.a.O., Rn. 107), und/oder z.B. durch eine Veröffentlichung im Internet ein Verlust der Kontrolle über die Daten droht (vgl. *Schantz*, a.a.O., Rn. 107). In die Abwägung einzustellen ist ferner die Art und Weise, wie die Daten erhoben worden sind, insb., ob die Datenerhebung für den Betroffenen erkennbar war oder ob sie heimlich erfolgte (vgl. *Schantz*, a.a.O., Rn. 111). Durch die Grundsätze der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) und der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) ist der Verantwortliche zudem verpflichtet, die Datenverarbeitung auf das notwendige Maß zu beschränken (vgl. *Heberlein*, a.a.O.; *Buchner/Petri*, a.a.O., Rn. 150).

23 Ausgehend von diesen Maßstäben unterliegt die Einschätzung des *VG*, dass die Interessen der Eheleute F am Schutz ihrer personenbezogenen Daten ggü. den Interessen des Kl. an der nicht anonymisierten Veröffentlichung des streitgegenständlichen Fotos überwiegen, keinen ernstlichen Richtigkeitszweifeln. Soweit der Kl. darauf verweist, dass die Eheleute F „lediglich in einer großen Menschenmenge" gezeigt würden, rechtfertigt dies keine andere Beurteilung. Denn nach Art. 4 Nr. 1 DS-GVO kommt es allein darauf an, ob die betroffene Person direkt oder indirekt, insb. mittels Zuordnung zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. ...

25 Soweit der Kl. im Zulassungsverfahren kritisiert, dass das VG i.R.d. Prüfung des § 22 KUG ausgeführt hat, dass die Veröffentlichung von Daten auf einer Fanpage bei Facebook mit unkalkulierbaren Risiken für die betroffenen Personen verbunden sei, lassen sich auch damit keine ernstlichen Richtigkeitszweifel an der angefochtenen Entscheidung begründen. Wie oben ausgeführt, sind auch bei der nach Art. 6 Abs. 1 lit. f DS-GVO vorzunehmenden Interessenabwägung die für die Betroffenen mit der Datenverarbeitung verbundenen Risiken, einschließlich einer evtl. Missbrauchsanfälligkeit, zu berücksichtigen. In diesem Zusammenhang verweist die Bekl. zutreffend darauf, dass eine Veröffentlichung von Fotos im Internet im Allgemeinen und in sog. sozialen Netzwerken wie Facebook im Besonderen mit erheblichen (Missbrauchs-)Risiken für die Betroffenen verbunden sind. Diese Risiken ergeben sich primär daraus, dass ein einmal im Internet veröffentlichtes Foto beliebig oft und von einer unbestimmten Vielzahl von Personen gespeichert, vervielfältigt, verfremdet und an andere Personen übermittelt werden kann. Wird ein Foto verändert und anschließend weitergeleitet, ist es für den Empfänger des veränderten Fotos in der Regel noch nicht einmal erkennbar, ob bzw. in welchen Punkten das Foto vom Original abweicht. Hinzu kommt, dass es sich bei Facebook um ein weltweit verbreitetes und von Millionen von Menschen genutztes Netzwerk handelt. Durch die Kumulation dieser beiden Faktoren – erhebliche Missbrauchsmöglichkeiten und große Reichweite – ist es für die Betroffenen sehr schwierig bis unmöglich, den Überblick über sämtliche über sie veröffentlichte Daten zu behalten und ggf. sämtliche veröffentlichte Daten dauerhaft und restlos aus dem Internet entfernen zu lassen (vgl. *Schantz*, a.a.O., Rn. 131). Vor diesem Hintergrund kommt den Interessen und Rechten der Betroffenen, ihre personenbezoge-

nen Daten vor derartigen Risiken und Missbrauchsmöglichkeiten zu schützen, i.R.d. nach Art. 6 Abs. 1 lit. f DS-GVO vorzunehmenden Interessenabwägung ein besonderes Gewicht zu.

26 Darüber hinaus spricht auch die Art und Weise der Datenerhebung für ein Überwiegen der Interessen der Eheleute F ggü. den Interessen des Kl. Denn das streitgegenständliche Foto wurde ohne Kenntnis der Eheleute F aufgenommen. Es wurde zudem nicht vom Kl. als dem für die weitere Verarbeitung Verantwortlichen, sondern von einem – durch den Kl. nicht identifizierten und daher im vorliegenden Verfahren nicht bekannten – anderen Veranstaltungsteilnehmer erstellt. Damit hatten die Eheleute F bereits zum Zeitpunkt der Datenerhebung keinerlei Kontrolle über ihre Daten und konnten sich bis zur Kenntniserlangung über die streitgegenständliche, erst vier Jahre nach Erstellung des Fotos erfolgte Veröffentlichung nicht gegen die (weitere) Verarbeitung ihrer personenbezogenen Daten wehren.

27 Soweit der Kl. darauf hinweist, dass es sich bei der Veranstaltung am 7.8.2014 um eine öffentliche Veranstaltung gehandelt habe und somit weder die Intim- noch die Privat-, sondern „nur" die Sozialsphäre der Eheleute F betroffen war, ist dies zwar im Ausgangspunkt zutreffend (vgl. zur sog. Sphärentheorie: *Specht-Riemenschneider*, in: Gsell/Krüger/Lorenz/Reymann, Beck-OGK, Stand: 1.11.2020, § 823 BGB Rn. 1397 ff., mwN), rechtfertigt jedoch gleichwohl keine andere Beurteilung. Denn zum einen sind auch personenbezogene Daten, die „nur" die Sozialsphäre betreffen, vom Schutz der Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 DS-GVO erfasst und einer – grds. ergebnisoffenen – Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO zugänglich. Zum anderen wird die Intensität des Eingriffs in die Persönlichkeits- und Datenschutzrechte der Eheleute F vorliegend gerade dadurch erhöht, dass mit der Veröffentlichung des streitgegenständlichen Fotos auf der Facebook-Seite des Kl. die aufgezeigten, besonderen Risiken verbunden sind. Diese Risiken bestehen unabhängig davon, ob es sich um ein Bild von einer öffentlichen oder einer privaten Veranstaltung handelt. Insofern führt auch der Umstand, dass es sich vorliegend um eine öffentliche Veranstaltung gehandelt hat, nicht dazu, dass die Interessen des Kl. an einer unanonymisierten Veröffentlichung des streitgegenständlichen Fotos auf seiner Fanpage bei Facebook höher zu gewichten sind als die Persönlichkeits- und Datenschutzrechte der Eheleute F. …

29 Soweit der Kl. im Zulassungsverfahren darauf verweist, dass er das streitgegenständliche Foto nicht zu kommerziellen Zwecken, sondern zur Erfüllung einer den Parteien verfassungsgemäß zugewiesenen Aufgabe veröffentlicht habe, teilt der *Senat* die vom Kl. vertretene Ansicht, dass dieser Aspekt i.R.d. Interessenabwägung zu Gunsten des Kl. zu berücksichtigen ist. Gleichwohl führt dieser Gesichtspunkt aus den dargelegten Gründen nicht dazu, dass die berechtigten Interessen des Kl. ggü. den schützenswerten Interessen der Eheleute F überwiegen.

30 b) Der Kl. stützt seinen Zulassungsantrag zudem darauf, dass die streitgegenständliche Veröffentlichung auch nach Art. 6 Abs. 1 lit. e DS-GVO i.V.m. Art. 21 GG, § 1 ParteienG gerechtfertigt gewesen sei. …

31 Dieser Vortrag ist nicht geeignet, ernstliche Richtigkeitszweifel an der angefochtenen Entscheidung zu begründen. Art. 6 Abs. 1 lit. e DS-GVO bestimmt, dass die Verarbeitung dann rechtmäßig ist, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Vorschrift kann die streitgegenständliche Veröffentlichung aus drei jeweils selbstständig tragenden Gründen nicht rechtfertigen.

32 aa) Zunächst steht einer erfolgreichen Berufung des Kl. auf Art. 6 Abs. 1 lit. e DS-GVO entgegen, dass die streitgegenständliche Veröffentlichung in unanonymisierter Form nicht zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabenerfüllung durch den Kl. erforderlich war. … Wie bereits oben zu Art. 6 Abs. 1 lit. f DS-GVO ausgeführt, war es zur Wahrung der berechtigten Interessen des Kl. – die Öffentlichkeit über seine parteipolitischen Aktivitäten und ihre Erfolge zu informieren und dadurch auch an der politischen Willensbildung mitzuwirken – nicht erforderlich, ein Foto zu veröffentlichen, auf dem die Eheleute F identifizierbar sind. Die Datenverarbeitung in Form der Veröffentlichung des Fotos hätte vielmehr durch eine Unkenntlichmachung der Eheleute F auf das Notwendigste beschränkt werden können und müssen …

33 bb) Zudem handelt es sich bei Art. 6 Abs. 1 lit. e DS-GVO um eine Regelung, die die Verarbeitung personenbezogener Daten durch die öffentliche Gewalt, insb. in Form der Ordnungs-, Leistungs- und Lenkungsverwaltung, im Blick hat (s. Erwägungsgrund 47 S. 5 DS-GVO; vgl. auch *Schulz*, a.a.O., Rn. 48 u. 51), mithin die Erfüllung von „klassischen Staatsaufgaben" (*Albrecht*, in: Simitis/Hornung/Spiecker, a.a.O., Art. 6 Rn. 8). Der Kl. weist zwar auch in diesem Zusammenhang zutreffend darauf hin, dass Parteien nach Art. 21 Abs. 1 S. 1 GG bei der politischen Willensbildung des Volkes mitwirken und damit eine ihnen nach dem GG obliegende öffentliche Aufgabe erfüllen (§ 1 Abs. 1 S. 2 ParteienG). Dies hat auch das *VG* in der angefochtenen Entscheidung ausdrücklich anerkannt. Das *VG* hat allerdings in Übereinstimmung mit der Rspr. des *BVerfG* zutreffend weitergehend ausgeführt, dass Parteien trotz der Erfüllung einer öffentlichen Aufgabe nicht Teil des Staates sind (*BVerfG* B. v. 6.12.2013 – 2 BvQ 55/13, Rn. 6, mwN). Jedenfalls im hier vorliegenden Kontext, in dem der Kl. durch die Veröffentlichung des streitgegenständlichen Fotos bei Facebook auf seine parteipolitischen Aktivitäten und ihren Erfolg aufmerksam machen wollte, ist die staatliche Sphäre weder unmittelbar noch dergestalt betroffen, dass die Veröffentlichung des Fotos bei Facebook als staatliches Handeln qualifiziert werden könnte (vgl. *BVerfG*, a.a.O., Rn. 7, zum Abschluss einer Koalitionsvereinbarung durch eine Partei). Entsprechendes gilt i.Ü. z.B. für Rechtsanwälte, Insolvenzverwalter, Wirtschaftsprüfer und Steuerberater, die zwar ebenfalls – zumindest teilweise – im öffentlichen Interesse liegende Aufgaben erfüllen, gleichwohl mit ihren berufsbezogenen Tätigkeiten grds. nicht dem Anwendungsbereich des Art. 6 Abs. 1 lit. e DS-GVO unterfallen (vgl. *Buchner/Petri*, a.a.O., Rn. 124, 129a, 135 u. 140; *Roßnagel*, in: Simitis/Hornung/Spiecker, a.a.O., Art. 6 Abs. 1 DS-GVO Rn. 73).

34 cc) Schließlich steht einer Heranziehung des Art. 6 Abs. 1 lit. e DS-GVO vorliegend entgegen, dass diese Regelung … kein eigenständiger Erlaubnistatbestand ist. Vielmehr muss für eine entsprechende Verarbeitung eine konkrete Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen, die den Anforderungen von Art. 6 Abs. 2, Abs. 3 DS-GVO Rechnung trägt (vgl. *Schulz*, a.a.O., Rn. 48; *Buchner/Petri*, a.a.O., Rn. 120; *Albrecht*, a.a.O., Rn. 6). Derartige Regelungen müssen spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DS-GVO mit Bezug auf die Verarbeitung i.S.d. Art. 6 Abs. 1 lit. e DS-GVO enthalten (*Albrecht*, a.a.O., Rn. 6). Bei den vom Kl. im Zulassungsverfahren angeführten Regelungen in Art. 21 GG, § 1 ParteienG handelt es sich nicht um derartige spezifische Rechtsgrundlagen zur Verarbeitung personenbezogener Daten i.S.d. von Art. 6 Abs. 1 lit. e, Abs. 2 u. Abs. 3 DS-GVO, sondern um allgemeine Regelungen zur verfassungsrechtlichen Stellung und zur Aufgabe der Parteien. Folglich kann die Veröffentlichung des streitgegenständlichen Fotos vorliegend entgegen der Ansicht des Kl. auch nicht nach Art. 6 Abs. 1 lit. e, Abs. 2 u. Abs. 3 DS-GVO i.V.m. Art. 21 GG, § 1 ParteienG als rechtmäßig bewertet werden.

35 c) Zur Begründung der ernstlichen Richtigkeitszweifel trägt der Kl. schließlich weiter vor, dass die Veröffentlichung des streitgegenständlichen Fotos auch nach §§ 22, 23 KUG gerechtfertigt gewesen sei, wenn man wegen Art. 85 Abs. 2 DS-GVO von einer fehlenden Anwendbarkeit der DS-GVO ausgehe. Das *VG* habe offengelassen, ob die DS-GVO oder das KUG Anwendung finde. Das Gericht hätte aber weitergehend prüfen und entscheiden müssen, ob die Privilegierung des Art. 85 Abs. 2 DS-GVO für journalistische Zwecke einschlägig sei. Der Kl. verfolge vorliegend auch meinungsbildende Tätigkeiten. ...

39 bb) Die Spezifizierungsklausel des Art. 85 Abs. 2 DS-GVO kann demnach nur dann zur Anwendung gelangen, wenn es sich im konkreten Einzelfall um eine Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken handelt (vgl. *Buchner/Tinnefeld*, in: Kühling/Buchner, a.a.O., Art. 85 Rn. 12; *Lauber-Rönsberg/Hartlaub*, NJW 2017, 1057 (1060); *Krüger/Wiencke*, MMR 2019, 76 (77)). Zwar ist der Begriff der journalistischen Zwecke – auch unter Beachtung von Erwägungsgrund 153 – weit zu verstehen; er ist insb. weder auf bestimmte Medien noch auf bestimmte Formen journalistischer Tätigkeiten beschränkt (vgl. *EuGH* U. v. 16.12.2008 – C-73/07 [= MMR 2009, 175], Rn. 58; *Rombey*, ZD 2019, 301 (303); *Dix*, in: Simitis/Hornung/Spiecker, a.a.O., Art. 85 DS-GVO Rn. 14; *Kröner*, in: Paschke/Berlit/Meyer/Kröner, Hamburger Komm. Gesamtes Medienrecht, 4. Aufl. 2021, Vorbem. §§ 22 ff. KUG, Rn. 3). Allerdings liegen journalistische Zwecke (nur) dann vor, wenn die Verarbeitung im Zusammenhang mit der journalistisch-redaktionellen und damit meinungsrelevanten Tätigkeit eines Medienakteurs steht (vgl. *BGH* U. v. 23.6.2009 – VI ZR 196/08 [= MMR 2009, 608 m. Anm. *Greve/Schärdel*]; *Stender-Vorwachs*, in: Wolff/Brink, a.a.O., Art. 85 Rn. 12). Demgegenüber enthält Art. 85 Abs. 2 DS-GVO kein allgemeines Meinungsprivileg und findet somit nicht auf alle Meinungsäußerungen im Internet Anwendung (vgl. zu § 41 BDSG und § 57 RStV: *BVerwG* B. v. 29.10.2015 – 1 B 32/15 [= ZD 2016, 193], Rn. 5; zu Art. 85 DS-GVO: *Schiedermair*, in: Selmayr/Ehmann, a.a.O., Art. 85 Rn. 1; *Buchner/Tinnefeld*, a.a.O., Art. 85 Rn. 17 a; *Benedikt/Kranig*, ZD 2019, 4 (6); *Rombey*, ZD 2019, 301 (303)). Ebenso wenig bedeutet das weite Begriffsverständnis, dass Journalismus stets allein schon deshalb anzunehmen ist, weil sich jemand mit Informationen an die Öffentlichkeit wendet (*Buchner/Tinnefeld*, a.a.O., Rn. 17 a). Folglich fällt auch nicht jegliche im Internet veröffentlichte Information, die sich auf personenbezogene Daten bezieht, unter den Begriff der journalistischen Tätigkeit (*EuGH* U. v. 14.2.2019 – C-345/17 [= ZD 2019, 262], Rn. 58; *OLG Köln* U. v. 14.11.2019 – I-15 U 89/19, Rn. 40; *Rombey*, ZD 2019, 301 (303)). Zudem gilt die Privilegierung nach dem Erwägungsgrund 153 DS-GVO nur für solche Tätigkeiten, die „ausschließlich" zu journalistischen Zwecken erfolgen. Diese im Erwägungsgrund 153 DS-GVO enthaltene Formulierung ist dabei trotz des Umstands, dass Art. 85 Abs. 2 DS-GVO – anders als zuvor Art. 9 DS-RL – nicht (mehr) ausdrücklich auf eine Verarbeitung „allein" bzw. „ausschließlich" zu journalistischen Tätigkeiten abstellt, jedenfalls i.R.d. Auslegung des Art. 85 Abs. 2 DS-GVO zu berücksichtigen (vgl. auch *Buchner/Tinnefeld*, a.a.O., Rn. 14 u. 16; *Rombey*, ZD 2019, 301 (304)).

40 cc) Ausgehend von diesen Grundsätzen ist das *VG* in der angefochtenen Entscheidung zutreffend davon ausgegangen, dass die Veröffentlichung des streitgegenständlichen Fotos durch den Kl. bei Facebook nicht (ausschließlich) journalistischen Zwecken i.S.d. Art. 85 Abs. 2 DS-GVO diente. ... Vielmehr diente die Veröffentlichung des Posts dazu, auf die parteipolitischen Aktivitäten des Kl. und ihre Erfolge aufmerksam zu machen. Daran ändert auch der – im Ausgangspunkt zutreffende – Hinweis des Kl. darauf nichts, dass mit der Veröffentlichung des Posts auch meinungsbildende Zwecke verfolgt wurden. Denn der bloße Umstand, dass eine Datenveröffentlichung auch einen Informationswert für die öffentliche Meinungsbildung hat bzw. ein Ausdruck einer persönlichen Ansicht ist, macht aus der Datenveröffentlichung noch keine journalistische Tätigkeit i.S.d. Art. 85 Abs. 2 DS-GVO (vgl. *OLG Köln*, a.a.O., Rn. 41; *Benedikt/Kranig*, ZD 2019, 4 (6)). Soweit der Kl. darauf verweist, dass mit einer Tätigkeit mehrere Ziele verfolgt werden könnten und hier neben der Mitwirkung an der Willensbildung auch journalistische Zwecke verfolgt worden seien, rechtfertigt dies ... keine andere Beurteilung. Denn die fragliche Datenverarbeitung muss, wie ausgeführt, ausschließlich journalistischen Zwecken dienen. ...

Anmerkung

Prof. Dr. Wolfgang Ziebarth, Villingen-Schwenningen

Dem vorstehenden Beschluss des *OVG Lüneburg* kann jedenfalls i.E. zugestimmt werden, auch wenn manche Begründung teils zu pauschal erscheint.

Es spricht viel dafür, dass die Fotoveröffentlichung rechtswidrig war. Zur Erinnerung: Der Ortsverein einer politischen Partei stellte ein Foto auf seinem Facebook-Konto ein, das u.a. ein Ehepaar zeigte, das an einem Ortstermin (zur Notwendigkeit einer Verkehrsampel) teilnahm. Das Foto war bereits vor Jahren von seinem Urheber, der mit dem Ortsverein wohl nichts zu tun hatte, ins Internet gestellt worden.

Es ist eine alte Erfahrung aus der Beratungspraxis, dass Fotoveröffentlichungen den Verantwortlichen nicht nur datenschutzrechtliche, sondern auch urheberrechtliche Probleme bereiten. Vermutlich war die Bildveröffentlichung schon aus urheberrechtlichen Gründen rechtswidrig. Denn der Fotograf war auch im Verfahren nicht festzustellen. Mit welchem Recht der kl. Ortsverein Fotos, die ein ihm unbekannter Mensch irgendwo im Internet veröffentlicht hat, einfach auf seine Facebookseite stellt, konnte nur deshalb sein Geheimnis bleiben, weil das Urheberrecht nicht Gegenstand des Verfahrens war.

Das *Gericht* konnte sich daher auf das Datenschutzrecht konzentrieren. Zu Recht sieht es Art. 58 Abs. 2 lit b DS-GVO als richtige Ermächtigungsgrundlage für „Verwarnungen" (Rn. 12). „Verwarnung" in diesem Sinne meint die Feststellung der Rechtswidrigkeit einer Datenverarbeitung durch die Datenschutz-Aufsichtsbehörde (*Ziebarth*, in: Sydow (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 58 Rn. 38 f.; *Körffer*, in: Paal/Pauly, DS-GVO/ BDSG, 3. Aufl. 2021, Art. 58 Rn. 17, 18). Sie ist die mildeste Abhilfebefugnis bei bereits laufender Datenverarbeitung (*Eichler*, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Ed., Stand: 1.2.2021, Art. 58 Rn. 20).

Zutreffend ist auch die Feststellung des *Gerichts*, dass das Einstellen und Veröffentlichen des Fotos auf der Facebookseite eine Verarbeitung personenbezogener Daten darstellt, die rechtfertigungsbedürftig ist (Rn. 13; dazu *Ziebarth/Elsaß*, ZUM 2018, 578 f.). Das *Gericht* misst die Verarbeitung an Art. 5, 6 DS-GVO.

In Rn. 30-35 widerlegt das *Gericht* mit Recht die Ansicht des Ortsvereins, eine politische Partei könne sich auf Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO berufen, weil sie Aufgaben im öffentlichen Interesse wahrnehme, nämlich gem. Art. 21 GG an der politischen Willensbildung des Volks mitwirke.

In Rn. 35-40 legt das *Gericht* dar, warum es nicht über Art. 85 Abs. 2 DS-GVO das Kunsturhebergesetz (KUG) anwendet. Hier begibt es sich in unsichere Fahrwasser, denn ob und in welchen Fällen das KUG über Art. 85 Abs. 2 DS-GVO anwendbar sein könnte, ist unklar und umstritten (vgl. statt vieler *Benedikt/Kranig*, ZD 2019, 4). Darüber hinaus könnte das KUG, was das *Gericht* übersieht, auch gem. Art. 85 Abs. 1 DS-GVO

anwendbar sein (*Viehweger/Koreng* in ihrer Anmerkung zum vorliegenden Beschluss in ZD 2021, 228 (229)).

Das Verhältnis zwischen DS-GVO und KUG ist fünf Jahre nach Inkrafttreten der DS-GVO (Art. 99 Abs. 1 DS-GVO) noch immer unklar. Ist das KUG eine Vorschrift, mit der die widerstreitenden Interessen i.S.d. Art. 85 Abs. 1 DS-GVO in Einklang gebracht werden (vgl. *Krüger/Wiencke*, MMR 2019, 76)? Ist es eine Ausnahmevorschrift i.S.d. Art. 85 Abs. 2 DS-GVO? Kann und soll es nur eines davon oder beides zugleich sein? Wer darf sich in welchen Fällen darauf berufen? Und hat der Bund insoweit überhaupt die Gesetzgebungskompetenz (s. *Benedikt/Kranig*, ZD 2019, 4 (5))?

Die vorliegende Anmerkung kann, muss und will diese Frage nicht beantworten. *Viehweger/Koreng* (a.a.O.) ist darin zuzustimmen, dass die Abwägung nach § 23 Abs. 2 KUG jedenfalls in der Regel zu demselben Ergebnis führen wird, wie die Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO: Denn in beide Abwägungen ist dasselbe Abwägungsmaterial einzustellen.

Hingewiesen werden soll aber auf einen Umstand, der in der Diskussion allzu oft unter den Tisch fällt: § 33 Abs. 1 KUG stellt das unerlaubte Verbreiten oder öffentliche Zurschaustellen von Personenbildnissen unter Strafe, ohne dass (wie etwa in § 42 BDSG) Gewerbsmäßigkeit, Schädigungs- oder Bereicherungsabsicht hinzutreten müssten.

Ist es eines Rechtsstaats würdig, eine Strafvorschrift in Geltung zu halten, von der seit fünf Jahren niemand mit Sicherheit sagen kann, ob und unter welchen Umständen sie anwendbar ist? Ist das mit Art. 103 Abs. 2 GG i.V.m. § 1 StGB vereinbar? Muss nicht konstatiert werden, dass § 33 Abs. 1 KUG die Bestimmtheit abhandengekommen und er deshalb nicht mehr anwendbar ist? Hierfür spricht einiges. Da aber niemand seine Freiheit darauf verwetten sollte, dass Gerichte das genauso sehen, ist jedem zu raten, bei einer Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO vorsichtshalber die Vorgaben des § 23 KUG zu berücksichtigen. Was dort erlaubt ist, wird die Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO sicherlich bestehen.

Jedenfalls sind die widerstreitenden Interessen aber gegeneinander abzuwägen. In Frage kommt eine Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO oder nach KUG. Das *Gericht* entscheidet sich für Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO (Rn. 14 ff.), kommt aber gar nicht erst zur Abwägung, sondern stellt fest, dass auch zur Erreichung des legitimen Interesses des Ortsvereins (das in der Berichterstattung über eigene Aktivitäten und auch in Mitwirkung an der politischen Willensbildung des Volks gesehen wird) eine identifizierende Bebilderung nicht erforderlich sei (Rn. 16).

Dies scheint in der Tat zu pauschal zu sein. Eine Bebilderung völlig ohne Personen oder gar mit schwarzen Balken hat nicht denselben Effekt (so zu Recht *Viehweger/Koreng*, a.a.O.). Es hätte aber auch schlicht ein Foto ohne das Ehepaar verwendet werden können. Das Bild soll den Ortstermin an der Straße dokumentieren, nicht die Anwesenheit des Ehepaars. Zumindest hätte ein Foto genommen (oder ein Bildausschnitt gewählt werden) können, bei dem das Ehepaar wenigstes nicht im Mittelpunkt und Vordergrund steht.

Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO erlaubt Datenverarbeitung, die „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich (ist), sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".

Völlig unberücksichtigt ist ein Aspekt geblieben, der erheblich gegen die Zulässigkeit der Veröffentlichung streitet. Das Ehepaar hat an einem Ortstermin wegen einer Ampel in seiner Nachbarschaft teilgenommen. Es muss nicht damit rechnen und nicht hinnehmen, Jahre später auf dem Facebook-Profil einer politischen Partei zu erscheinen.

Nicht jeder fühlt sich jeder politischen Partei verbunden. Es gibt sogar Parteien, bei denen es erhebliche stigmatisierende Wirkung hat, als ihr Mitglied, Anhänger, Sympathisant, Wähler usw. zu gelten. Durch die Veröffentlichung auf dem Parteiaccount (der Vorsitzende in der Mitte) wird Parteiwerbung gemacht. Sprich: das Ehepaar wird in eine politische Richtung gerückt, die es nicht gutheißen muss – und dies wird (ohne Rücksicht auf Art. 9 DS-GVO) weltweit veröffentlicht.

Viehweger/Koreng (a.a.O., S. 229 f.) meinen, dass dies kein größeres Missbrauchspotenzial eröffnet, weil die Besucher des Accounts sich auf Interessenten des Ortsvereins beschränken. Jedoch sind dies genau diejenigen Kreise, in denen auch das örtlich dort beheimatete Ehepaar bekannt sein dürfte.

Außerdem sehen Plattformen wie Facebook Techniken wie die händische Identifizierung von Personen auf Bildern oder gar automatische Gesichtserkennung vor. Wenn dies auch bisher (angeblich) noch nicht überall durchgeführt werden sollte, so steht die Möglichkeit doch immerhin im Raum. Dass das eigene Gesicht automatisiert mit einer politischen Partei verknüpft und daraus dann Profile über die jeweilige Person gespeist werden, ist ein zutiefst missbrauchsanfälliges Szenario. *Voßkuhle* nennt die Nutzung derartiger Plattformen zu Recht „eine risikogeneigte Tätigkeit" (Focus online, v. 16.12.2013, abrufbar unter: https://www.focus.de/digital/internet/facebook/bundesverfassungsgericht-vosskuhle-warnt-vor-der-sammelwut-von-facebook_aid_681745.html).

Daher streitet die Eigenschaft des Verantwortlichen als politische Partei nicht etwa für die Zulässigkeit der Veröffentlichung einer ungefragten Bildveröffentlichung zur Parteiwerbung (indem Art. 21 GG als besonders gewichtig in die Abwägung eingestellt wird), sondern gegen die Zulässigkeit.

Dieses Argument könnte zu dem Schluss verleiten, umstrittene Parteien mit stigmatisierender Wirkung hätten ggü. „allseits anerkannten" Parteien weniger Möglichkeiten zur Parteiwerbung, sodass der politische Wettbewerb verzerrt sei. Dieser Schluss wiederum könnte gegen das Argument sprechen. Wenn aber auch „allseits anerkannte" Parteien nicht das Recht haben, ohne (informiert, freiwillig, vorherig, aktiv, für den konkreten Einzelfall und separat erklärte sowie jederzeit zumutbar widerrufliche) Einwilligung mit fremder Leute Gesichtern Parteiwerbung zu machen, dann sind die Bedingungen für alle gleich.

Nach hier vertretener Auffassung verbietet es sich daher für politische Gruppierungen jedenfalls grds. politische Werbung mit personenbezogenen Daten Unbeteiligter zu machen. Dabei können die aus § 23 KUG bekannten Ausnahmen (bloßes Beiwerk etc.) durchaus auch für die Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO fruchtbar gemacht werden; gegenläufige Interessen sind dann aber gemäß oder analog § 23 Abs. 2 KUG zu beachten. Damit erscheint jedenfalls die Abbildung von Personen im Vordergrund oder Mittelpunkt des Bilds unzulässig, während bei bloßen Übersichtsaufnahmen eine gegenteilige Einzelfallabwägung möglich und nötig bleibt.

Ein Fall, in dem ein Ereignis der Zeitgeschichte in satirisch-humoristischer Weise für Wahlkampfzwecke mit dem Bildnis einer Person der Zeitgeschichte bebildert wird (so im Fall des *LG Hamburg* U. v. 30.3. 2007 – 324 O 894/06), liegt vorliegend

ersichtlich nicht vor. Zu wirtschaftlicher Werbung mit Bildern von Personen der Zeitgeschichte s. *BGH* U. v. 28.10.1960 – I ZR 87/59; zur Sprachimitation *OLG Hamburg* B. v. 8.5.1989 – 3 W 45/89; zur Vereinnahmung Konrad Adenauers für Wahlwerbezwecke der Partei „Die Republikaner" *OLG Köln* U. v. 24.9.1998 – 15 U 122/98 und für die Unzulässigkeit ungefragter Rekrutierung bekannter Schauspieler für die Bebilderung teils journalistischer, teils kommerzieller Texte zuletzt *BGH* U. v. 21.1.2021 – I ZR 207/19.

VG Berlin: Video im Klassenchat kann vorläufigen Unterrichtsausschluss rechtfertigen

Chatroom-Verhalten

SchulG § 63 Abs. 2, 4, 5, 6 S. 1; VwVfG Berlin §§ 1 Abs. 1, 2 Abs. 2; VwVfG § 3a Abs. 1
Beschluss vom 12.11.2020 – 3 L 649/20

Leitsatz der Redaktion

Die Einschätzung eines Schulleiters, dass das Einstellen eines Videos durch einen Schüler in einen Klassenchat, das einen Mitschüler zeigt, wie dieser einen Stuhl aus dem Fenster der vierten Etage des Schulgebäudes wirft, den schulischen Frieden in erheblichem Maße stört, ist nicht zu beanstanden. Die Beurteilung, der vorläufige Ausschluss des Schülers vom Unterricht für eine Woche sei als Konsequenz erforderlich, begegnet deshalb keinen rechtlichen Bedenken.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2020, 45704. Zur Suspendierung eines Schülers wegen eines beleidigenden Instagram-Posts vgl. *VG Berlin* MMR 2020, 135.

Schlagworte: Chatroom-Verhalten; Videoübertragung; Schulfrieden; Beurteilungsspielraum; Suspendierung

Sachverhalt

Der Ast. ist Schüler in Berlin. Am 3.11.2020 nahm er am Chemie-Unterricht teil, als ein Mitschüler einen Stuhl aus dem Fenster des in der vierten Etage des Schulgebäudes belegenen Klassenzimmers warf. Der Vorfall wurde mit dem Mobiltelefon des Ast. gefilmt. Im Anschluss stellte der Ast. das auf seinem Mobiltelefon gespeicherte Video in einen internen „Klassenchat" ein. Von hier aus verbreitete sich das Video weiter in der Schule und darüber hinaus.

Am 8.11.2020 teilte der Schulleiter den Eltern des Ast. mit, dass er den Ast. vom 9.11.2020 bis einschließlich 16.11.2020 von der Teilnahme am Unterricht suspendiere. Zur Begründung führte er aus, der Ast. habe durch die Verbreitung des Videos, welches eine mögliche massive gesundheitliche Gefährdung von Mitmenschen sowie Vandalismus und Zerstörung schulischen Eigentums zeige, den schulischen Frieden in erheblichem Maße gestört.

Gegen diese Entscheidung legten die Eltern des Ast. Widerspruch ein. Sie machten geltend, dass der Ast. den Vorfall nicht selbst gefilmt habe. Überdies hätten vorrangig Erziehungsmaßnahmen getroffen werden müssen, um sein Fehlverhalten zu ahnden. Mit Schreiben v. 10.11.2020 hat der Ast. um einstweiligen Rechtsschutz nachgesucht.

Aus den Gründen

8 II. Der Antrag hat keinen Erfolg. ...

10 ... Das öffentliche Interesse an der sofortigen Vollziehung der Maßnahme überwiegt das private Interesse des Ast., einstweilen vom Vollzug der Maßnahme verschont zu bleiben. Maßgebend für diese Interessenabwägung ist, dass bei der im Verfahren des vorläufigen Rechtsschutzes allein möglichen und gebotenen summarischen Prüfung der eingelegte Widerspruch voraussichtlich keinen Erfolg haben wird. Es bestehen keine ernstlichen Zweifel an der Rechtmäßigkeit der Maßnahme.

11 ... Ein dringender Fall i.S.d. Norm liegt dann vor, wenn ein Zuwarten auf die Entscheidung über eine Maßnahme durch das grds. hierzu berufene Gremium auf Grund der Störungen des Schulfriedens nicht abgewartet werden kann, mithin sofortiges Handeln der Schulleitung geboten ist. Dabei ist der vorläufige Unterrichtsausschluss keine repressive Ordnungsmaßnahme, sondern hat allein präventive – auf Vermeidung weiterer Ordnungsverstöße gerichtete – Funktion. Er dient dazu, die durch den Konflikt aufgeheizte Situation zu beruhigen und vor allem eine Entscheidung der zuständigen schulischen Stellen (§ 63 Abs. 5 SchulG) über die nach § 63 Abs. 2 SchulG zu ergreifenden Ordnungsmaßnahmen herbeizuführen. Gerade weil es sich nur um eine vorläufige Maßnahme handelt, kommt es nicht darauf an, dass bereits abschließend geklärt wäre, ob die dem Ast. zur Last gelegten Verfehlungen in jeder Hinsicht zutreffen (st. Rspr., vgl. *VG Berlin* B. v. 11.3.2020 – 3 L 80/20; v. 21.9.2018 – 3 L 658.18 u. v. 31.1.2018 – 3 L 68.18). Bei der Verhängung einer Ordnungsmaßnahme kommt der Schule zudem ein pädagogischer Beurteilungsspielraum zu, der nur begrenzt einer gerichtlichen Kontrolle unterliegt. Diese hat sich darauf zu beschränken, ob der Schulleiter Verfahrensvorschriften verletzt hat, von falschen Tatsachen ausgegangen ist, allgemeingültige Bewertungsmaßstäbe nicht beachtet oder sachfremde Erwägungen angestellt hat oder die Bewertung willkürlich ist (vgl. *VG Berlin* B. v. 1.10.2020 – 3 L 361/20 u. B. v. 6.12.2017 – 3 L 1324.17).

12 Bedenken hinsichtlich der formellen Rechtmäßigkeit der Maßnahme bestehen nicht. Der Umstand, dass den Eltern des Ast. der vorläufige Unterrichtsausschluss mittels E-Mail vom privaten Konto des Schulleiters zur Kenntnis gebracht wurde, begründet keine Zweifel an seiner Rechtmäßigkeit oder Wirksamkeit. Bereits die Gestaltung des auf diesem Wege übermittelten Schreibens – mit offizieller Kopfzeile der Schule und Angabe des Geschäftszeichens – macht deutlich, dass der Schulleiter den Eltern die darin enthaltene Anordnung ungeachtet des gewählten Übermittlungswegs in amtlicher Eigenschaft eröffnete. §§ 1 Abs. 1, 2 Abs. 2 VwVfG Bln i.V.m. § 3a Abs. 1 VwVfG stehen der formellen Rechtmäßigkeit der Bekanntgabe ebenfalls nicht entgegen. Schon der Umstand, dass dem Schulleiter die E-Mail-Adresse der Eltern des Ast. bekannt war, deutet darauf hin, dass diese der Schule ggü. einen entsprechenden Zugang eröffnet haben. ...

14 Bei der hier allein möglichen summarischen Prüfung durfte der Schulleiter auch in materieller Hinsicht den vorläufigen Ausschluss des Ast. vom Unterricht veranlassen.

15 Es ist unstreitig, dass der Ast. das mit seinem Mobiltelefon angefertigte Video in den internen Klassenchat eingestellt hat, von wo aus es – vorhersehbarer Weise – weitere Verbreitung gefunden hat. Die Einschätzung des Schulleiters, dass hierdurch die ordnungsgemäße Unterrichts- und Erziehungsarbeit gefährdet wurde, begegnet keinen rechtlichen Bedenken. Zutreffend weist der Schulleiter darauf hin, dass der in dem Video aufgezeichnete Vorfall, der Wurf eines Stuhls aus der vierten Etage des Schulgebäudes, die vorsätzliche Zerstörung von Schuleigentum sowie die grob fahrlässige Gefährdung etwaiger sich im Bereich vor der Schule aufhaltender Menschen beinhalte. Ob der Ast. den gefilmten Vorgang – wie er vorträgt – missbilligt, ist hierbei nicht von Relevanz. Angesichts der rein präventiven und gerade nicht repressiven Zielsetzung des Unterrichtsausschlusses ist hier

nicht die innere Haltung des Ast. ggü. dem eigentlichen Vorfall entscheidend, sondern die Außenwirkung der Versendung und Verbreitung des hiervon angefertigten Videos. Die Einschätzung des Schulleiters, aus der Sicht seiner Mitschüler mache sich der Ast. den Vorfall hiermit zu eigen, ist plausibel und rechtlich nicht zu beanstanden. Ebenso wenig stößt es auf rechtliche Bedenken, wenn der Schulleiter davon ausgeht, dass gerade die absehbar weitläufige Verbreitung des Videos andere Schüler dazu animieren kann, ähnliche Aktionen durchzuführen. Die besondere Dynamik sozialer Online-Medien und virtueller Chatgruppen kann erfahrungsgemäß zu einem regelrechten „Überbietungswettbewerb" führen, in dessen Verlauf versucht wird, durch immer schwerwiegendere Regelübertretungen Aufmerksamkeit zu generieren. Es liegt auf der Hand, dass hierdurch das geordnete Schulleben gefährdet und das Vertrauen der Schülerschaft in einen regelgeleiteten und gewaltfreien schulischen Rahmen fortwährend erschüttert wird. Die Beurteilung des Schulleiters, der vorläufige Ausschluss des Ast. vom Unterricht sei erforderlich, um dieses Vertrauen wiederherzustellen und zu dokumentieren, dass ein entsprechendes ordnungswidriges Verhalten Konsequenzen nach sich zieht, begegnet deshalb keinen rechtlichen Bedenken.

16 Der Dringlichkeit des Unterrichtsausschlusses steht hierbei nicht entgegen, dass zwischen dem gefilmten Vorfall und der Anordnung des vorläufigen Schulausschlusses mehrere Tage liegen. Denn diese zeitliche Verzögerung ist darauf zurückzuführen, dass der Schulleiter erst am 6.11.2020 Kenntnis von dem Vorfall erlangt hat und es erst in den darauffolgenden beiden Tagen gelungen ist, den Ast. als denjenigen auszumachen, der das Video im Klassenchat verbreitet hat. ...

18 Die Maßnahme ist schließlich auch nicht unverhältnismäßig. Die höchstens zulässige Dauer des Unterrichtsausschlusses von 10 Tagen hat die Schulleitung mit der vorläufigen Maßnahme nicht ausgeschöpft. Dass der Ast. infolge des Unterrichtsausschlusses an mehreren Klausuren nicht teilnehmen kann, begründet nicht die Unangemessenheit der Maßnahme. Es ist nicht dargetan, dass der Ast. durch die – bereits in Aussicht gestellte – Nachholung der Klausuren wesentliche Nachteile erleiden wird. ...

LG Bielefeld: Eingeschränkte Händlerpflichten betreffend die Herstellergarantie bei Anbahnung eines Fernabsatzvertrags

UWG §§ 3a, 5a Abs. 2 u. Abs. 4, 8 Abs. 3 Nr. 2, Abs. 4; BGB § 312d Abs. 1; EGBGB Art. 246a § 1 Abs. 1 S. 1 Nr. 9
Urteil vom 26.1.2021 – 15 O 26/19

Leitsatz der Redaktion

Es stellt keinen Verstoß eines Online-Händlers gegen Informationspflichten über die Garantie dar, wenn dieser weder das Bestehen einer Garantie werbend hervorhebt noch sie diese überhaupt erwähnt. Der Händler ist nicht gehalten, i.R.d. Anbahnung eines Fernabsatzvertrags auf das etwaige Bestehen einer gesonderten Herstellergarantie hinzuweisen und sodann die Voraussetzungen über diese Garantie und ihre Ausgestaltung mitzuteilen.

Anm. d. Red.: Vgl. hierzu auch *OLG Hamm* MMR 2013, 375 m. Anm. *Dehißelles*.

Schlagworte: Bewerbung; Informationspflichten; Online-Angebot; Garantie

LG Hamburg: Pflichtangaben bei Angebot von Kleidungsstücken auf eBay als Gebrauchtwaren

VO (EU) Nr. 1007/2011 Art. 17 Abs. 2; UWG §§ 2 Abs. 1 Nr. 3, 3 Abs. 1 u. Abs. 3, 3a, 5 Abs. 1 S. 1 u. 2 Nr. 2, 8 Abs. 1 S. 1; PAngV § 1 Abs. 2 Nr. 1, Abs. 7 S. 2; UStG § 25a Abs. 3 S. 1 u. Abs. 5
Beschluss vom 30.3.2020 – 327 O 84/20

Leitsätze der Redaktion

1. Bei Online-Angeboten von Textilien als Gebrauchtwaren ist die Verwendung der Bezeichnungen „Synthetik" und „Merino" rechtlich zulässig.
2. § 1 Abs. 2 Nr. 1, Abs. 7 S. 2 PAngV ist eine Marktverhaltensregel i.S.v. § 3a UWG.
3. Auch wenn der gewerbliche Verkäufer der Differenzbesteuerung unterliegt, ist er verpflichtet anzugeben, dass die für die angebotenen Waren geforderten Preise die Umsatzsteuer enthalten.
4. Die Angabe „Wir versenden deine Artikel versichert bei DHL" ist nicht als eine unzulässige Werbung mit einer Selbstverständlichkeit oder das Erwecken des unzutreffenden Eindrucks, gesetzlich bestehende Rechte stellten eine Besonderheit des Angebots dar, zu bewerten.

Anm. d. Red.: Vgl. hierzu ferner *LG München I* MMR 2018, 478 m. Anm. *Föhlisch*; *OLG München* MMR 2019, 249 m. Anm. *Föhlisch* sowie *BGH* MMR 2018, 239.

Schlagworte: Online-Handel; Differenzbesteuerung; Preisangabenpflicht; Werbung mit Selbstverständlichkeiten

OVG NRW: Rechtswidrige Suspendierung wegen rechtsextremer Chatnachrichten

BeamtStG §§ 34 S. 3, 39 S. 1; StGB § 86a
Beschluss vom 25.3.2021 – 6 B 2055/20 (VG Düsseldorf)

Leitsätze der Redaktion

1. Das Versenden von Nachrichten mit rassistischen, antisemitischen oder den Nationalsozialismus befürwortenden Inhalten wie auch ihr zustimmendes Kommentieren in Chatgruppen ist grundsätzlich geeignet, Zweifel an der charakterlichen Eignung eines (Polizeivollzugs-)Beamten zu begründen und damit auch ein Verbot der Führung der Dienstgeschäfte zu rechtfertigen.
2. Aus der bloßen Mitgliedschaft in einer rechtsextremen Chatgruppe kann aber nicht auf eine charakterliche Ungeeignetheit geschlossen werden. Es dürfte zu weit gehen, einen Beamten unabhängig von den konkreten Einzelfallumständen bereits bei Erhalt einer einzelnen beanstandungswürdigen Bilddatei stets und uneingeschränkt für verpflichtet zu halten, ihrer Verbreitung aktiv entgegenzuwirken.
3. Werden Nachrichten, Bilder und Videos in ganz erheblicher Zahl in einer Chatgruppe empfangen (hier: durchschnittlich 94 Bilder und 184 Nachrichten täglich), kann nicht ohne Weiteres davon ausgegangen werden, dass alle Nachrichten wahrgenommen werden.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2021, 5594.

Schlagworte: WhatsApp-Gruppe; Polizeibeamte; charakterliche Eignung; freiheitlich-demokratische Grundordnung; Verbot der Führung der Dienstgeschäfte

Christina Etteldorf Belgien: Verfassungsgerichtshof stoppt anlasslose Vorratsdatenspeicherung

MMR-Aktuell 2021, 439468

Der *belgische Verfassungsgerichtshof* hat (E. v. 22.4.2021 – Nr. 57/2021) die nationalen Vorschriften zur Speicherung von elektronischen Kommunikationsdaten durch TK-Anbieter wegen Unvereinbarkeit mit dem Unionsrecht für nichtig erklärt. Damit wurde – wie in vielen weiteren Mitgliedstaaten, darunter auch Deutschland – ein weiterer Fall der gesetzlichen Regulierung der sog. Vorratsdatenspeicherung zu Gunsten eines höheren Schutzes der Privatsphäre der von der Speicherung Betroffenen entschieden.

Im Fokus der Entscheidung stand die Regelung des Art. 126 § 3 des belgischen Gesetzes über die elektronische Kommunikation, der durch das Gesetz v. 29.5.2016 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation reformiert worden war. Darin ist u.a. die Verpflichtung für TK-Anbieter vorgesehen, elektronische Kommunikationsdaten – hier unterteilt in die Kategorien Identifizierungs-, Zugangs- und Verbindungsdaten – zwölf Monate auf Vorrat zu speichern. Einen bestimmten Anlass, der eine solche Speicherpflicht auslöst, sieht die allgemeine Regelung nicht vor. Dagegen hatten die *deutsch- und französischsprachigen Rechtsanwaltskammern Belgiens*, die Menschenrechtsorganisationen *Académie Fiscale*, *Liga voor Mensenrechten* und *Ligue des Droits de l'Homme* sowie weitere Einzelpersonen insbesondere mit der Begründung Klage erhoben, dass dies mit dem Grundrecht auf Schutz der Privatsphäre und den entsprechenden Vorgaben des Unionsrechts nicht vereinbar sei.

Der *Verfassungsgerichtshof* hatte das Verfahren 2018 ausgesetzt und die Frage der Vereinbarkeit der belgischen Regeln mit Art. 15 Abs. 1 RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation dem *EuGH* zur Vorabentscheidung vorgelegt. Der *EuGH* bezog (E. v. 6.10.2020 – C-511/18, C-512/18 und C-520/18, La Quadrature du Net u.a.) klar Stellung: Eine nationale Regelung, die den Betreibern und Anbietern elektronischer Kommunikationsdienste die Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten aller Teilnehmer und Nutzer in Bezug auf alle elektronischen Kommunikationsmittel auferlegt, verstößt gegen Unionsrecht. Unionsrechtswidrig seien nationale Regeln auch dann, wenn sie andere als die in Art. 15 RL 2002/58/EG genannten Ziele verfolgen. Eine Speicherung solcher Kommunikationsdaten, sowie spiegelbildlich Zugriffsmöglichkeiten von Behörden hierauf, sei nur in sehr eng umgrenzten Ausnahmefällen möglich, in denen durch klare und präzise Regeln sichergestellt sein müsse, dass bestimmte materielle und prozedurale Voraussetzungen eingehalten werden und dass Betroffene über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen. Insbesondere, so der *EuGH*, müsse im Lichte der Grundrechte der behördliche Zugang auf bestimmte Fälle beschränkt sein, deren Schwere einen Eingriff unbedingt erforderlich macht, und es müsse (außer in Eilfällen) ggf. eine vorherige Kontrolle durch ein Gericht oder eine unabhängige Behörde gesetzlich vorgesehen sein.

Diesen Vorgaben aus der Entscheidung des *EuGH* entspricht die belgische Regelung nach Auffassung des *belgischen Verfassungsgerichtshofs* nicht, da diese präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehe. Die Vorratsdatenspeicherung sei hier Regelfall und nicht, wie vom *EuGH* auf Basis grundrechtlicher Erwägungen gefordert, Ausnahme. Es mangele an der notwendigen Beschränkung von Eingriffen auf das absolut Notwendige und an objektiven Kriterien, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Hieran ändere auch die Unterscheidung zwischen verschiedenen Arten von Daten in Art. 126 des Gesetzes nichts, da diese sich nur auf den Anfangszeitpunkt der Dauer der Datenspeicherung von in jedem Fall zwölf Monaten und eventuell auf die Möglichkeiten, auf sie zuzugreifen, für die ermächtigten Stellen auswirken. Daher, so der *Verfassungsgerichtshof* i.E., seien sie für nichtig zu erklären.

Der *belgische Ministerrat* hatte hilfsweise für den Fall der Nichtigerklärung des Gesetzes die Aufrechterhaltung der Rechtsfolgen des Gesetzes beantragt, um die Arbeit zur Ermittlung und Verfolgung von Straftaten der Polizei- und Nachrichtendienste nicht zu gefährden. Auch dies lehnte der *belgische Verfassungsgerichtshof* jedoch unter Hinweis auf die betreffende Entscheidung des *EuGH* ab, in der dieser auf die entsprechende Vorlagefrage hin festgestellt hatte, dass auch eine zeitlich begrenzte Anwendung einer unionsrechtswidrigen Vorschrift nicht möglich ist.

■ Vgl. zur Vorabentscheidung des *EuGH* auch ZD-Aktuell 2020, 07333 sowie zur Vorratsdatenspeicherung *Zeitzmann*, MMR-Aktuell 2021, 437661; *Korte*, ZD-Aktuell 2021, 05017; ZD-Aktuell 2020, 07423; *BVerfG* ZD 2020, 580 m. Anm. *Petri*; *BVerwG* ZD 2020, 167; *EuGH* ZD 2017, 124 m. Anm. *Kipker/Schefferski/Stelter* und *Dieterle*, ZD 2016, 517.

Ass. iur. Christina Etteldorf
ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken/Brüssel.

ePrivacy: Bundestag schreibt Einwilligung bei Werbe-Cookies explizit vor

MMR-Aktuell 2021, 439268

Der *Bundestag* hat den Entwurf für ein „Telekommunikations-Telemedien-Datenschutz-Gesetz" (TTDSG) beschlossen. Das Gesetz soll die datenschutzrechtlichen Regelungen aus dem Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG) einheitlich umsetzen und an die DS-GVO anpassen. In diesem Zuge werden erstmals die Vorgaben der ePrivacy-Richtlinie aus dem Jahr 2009 zur Einwilligung von Cookies umgesetzt.

Die EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation ist bereits 2009 in Kraft worden und sieht eine ausdrückliche Einwilligungspflicht für den Einsatz von Cookies vor. Die Umsetzungsfrist der Vorgaben lief bis 2011. Die *Bundesregierung* hat die Verpflichtung zur ausdrücklichen Einwilligung bis heute nicht umgesetzt. Das TMG sieht nur vor, dass Cookies genutzt werden können, wenn der Nutzer nicht widerspricht (Opt-out), es sieht aber keine proaktive Zustimmung (Opt-in) vor. Nach Entscheidungen des *EuGH* (vgl. MMR 2019, 732 m. Anm. *Moos/Rothkegel* – Planet49) und des *BGH*, die eine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG zur Folge hat-

ten, sieht der *Bundestag* im Gesetzesentwurf für ein TTDSG nun eine ausdrückliche vorherige Zustimmung „auf der Grundlage von klaren und umfassenden Informationen" vor, es sei denn es handelt sich um Cookies, die zum Betrieb der Seite notwendig sind. Neben der Umsetzung der Einwilligungspflicht für den Einsatz von Cookies sieht der Entwurf auch Regelungen zu einem „Personal Information Management Service" (PIMS) vor, also einem gesonderten Dienst für eine zentralen Lösung der Nutzer*innen zum Einwilligungsmanagement verschiedener Dienste.

Im Bereich des TKG soll der Missbrauch von TK-Anlagen durch das unbemerkte Abhören oder Aufnehmen von Bildern stärker reguliert werden. Der vermehrte Einsatz von versteckten Kameras oder Mikrofonen in privaten Alltagsgeräten erfordere einen größeren Schutz, sodass insbesondere solche Geräte erfasst sein sollen, deren Aufzeichnungsfunktionen beim regulären Gebrauch nicht ohne Weiteres erkennbar sind. Daneben regelt das TTDSG künftig eine offenere Wahl des Verfahrens für die Vergabe von Mobilfunkfrequenzen; hier soll eine Auktion nicht mehr der Regelfall sein. Weitere Vorgaben betreffen u.a. Vorgaben zur Bestandsdatenauskunft und Herausgabe von Passwörtern, Kompetenzüberschneidungen bei den Datenschutzbehörden im Telemedienbereich und die unerlaubte Unterdrückung von Rufnummern bei Werbeanrufen.

Der Entwurf begegnet kritischen Stimmen von *FDP*, *DIE LINKE* und *AfD*. *Manuel Höferlin*, FDP, warnt, dass das PIMS die informationelle Selbstbestimmung nicht stärke und längst andere Formen des Trackings als Cookies genutzt werden.

Anke Domscheidt-Berg, Partei DIE LINKE, forderte ein Verbot der massenhaften Durchleuchtung von Nutzer*innen und dem missbräuchlichen Design, das eine volle Nutzung einiger Websites nur zulasse, wenn alle Cookies akzeptiert würden. Auch *Enrico Komnig*, AfD, sieht die Regelungen nicht weit genug und fordert untrackbare Bereiche und eine Stärkung der digitalen Bürgerrechte.

■ Vgl. auch *Böhm/Halim*, MMR 2020, 651; *Schwartmann/Benedikt/Reif*, MMR 2021, 99; *BGH* MMR 2021, 48 – Facebook; *BGH* MMR-Aktuell 2020, 429733; *BGH* MMR-Aktuell 2020, 429939 und MMR-Aktuell 2021, 435944.

Christina Etteldorf Italien: 4,5 Mio. EUR Strafe gegen TK-Anbieter wegen rechtswidrigem Telemarketing

MMR-Aktuell 2021, 439470

Mit Entscheidung v. 25.3.2021 hat die italienische Datenschutzbehörde *(Garante per la protezione dei dati personali – GPDP)* dem italienischen TK-Unternehmen *Fastweb S.p.A.*, das u.a. Breitband- und Mobilfunkdienste anbietet, eine Reihe von Abhilfeverpflichtungen sowie eine Geldstrafe i.H.v. 4.501.868,– EUR wegen der rechtswidrigen Verarbeitung von personenbezogenen Daten auferlegt. Die Verstöße gegen datenschutzrechtliche Bestimmungen des EU- und nationalen Rechts erfolgten dabei im Zusammenhang mit der Durchführung von Telemarketing-Maßnahmen.

Grund für die Einleitung des Verfahrens gegen *Fastweb* waren Hunderte von Beschwerden und Berichte von Betroffenen über kontinuierliche Werbeanrufe über die verschiedenen Telefonie- und Internetangebote des Unternehmens, die die *GPDP* erreicht hatten. Die Anrufe erfolgten dabei nicht nur gegenüber dem bestehenden Kundenstamm des Unternehmens, sondern im Laufe der Untersuchung wurde auch ein laut *GPDP* „alarmierender Rückgriff" auf die Verwendung von fiktiven oder nicht im Register der Kommunikationsbetreiber eingetragenen Nummern festgestellt. Einwilligungen der Betroffenen für die Durchführung von Werbemaßnahmen konnte das Unternehmen dabei regelmäßig nicht vorweisen. Nicht nur das Fehlen einer in diesen Fällen erforderlichen Einwilligung bemängelte die Behörde, sondern auch die gesamte damit in Verbindung stehende Organisationstruktur des Unternehmens in Bezug auf den Umgang mit personenbezogenen Daten, wobei von „System-Kritikalität" die Rede ist. Das drückt sich in sieben verschiedenen Verstößen aus, die in der Entscheidung festgehalten werden und die Art. 5 Abs. 1 und 2, Art. 6 Abs. 11, Art. 7, 12, 13, 21, 24, 25, 32, 33 Abs. 1 und Art. 34 DS-GVO betreffen.

Dazu gehört u.a, dass *Fastweb* keine Kontrollsysteme für die Nachverfolgung und entsprechende Organisation der Kette der Sammlung personenbezogener Daten implementiert hat, Listen mit personenbezogenen Daten von Dritten ohne Einwilligung der Betroffenen erworben hat, rechtswidrige Methoden bei der Durchführung des sog. „Call me back"-Services angewendet hat sowie Meldepflichten in Bezug auf Datenschutzverstöße und Pflichten bei der Geltendmachung von Widerspruchs-, Auskunfts- und Berichtigungsansprüchen von Betroffenen nicht oder nicht in geeigneter Weise nachgekommen ist. Auch die Sicherheitsmaßnahmen für Kundenverwaltungssysteme wurden als unzureichend befunden. Die *Behörde* hatte zahlreiche Berichte über Kontaktversuche von selbsternannten Fastweb-Betreibern erhalten, die versuchten, sich über WhatsApp die Daten von Vertragspartnern zu beschaffen – wohl in betrügerischer Absicht. Die *Behörde* ordnete daher an, dass *Fastweb* seine Telemarketing-Verfahren so anpassen muss, dass vorgesehen und nachgewiesen wird, dass die Aktivierung von Angeboten und Dienstleistungen und die Registrierung von Verträgen nur nach Anrufen des Vertriebsnetzes über registrierte Telefonnummern erfolgen. Darüber hinaus soll das Unternehmen seine Sicherheitsmaßnahmen verstärken, um einen unberechtigten Zugriff auf seine Datenbanken zu verhindern. Nicht nur die aggressiven Telemarketing-Techniken ohne entsprechende Einwilligung der Angerufenen, sondern schließlich auch die datensicherheitsrechtlichen Mängel mündeten dann zusätzlich in der Auferlegung eines Bußgelds in besagter Höhe.

Die Maßnahmen gegen *Fastweb* sind dabei nur ein Teil eines größeren Untersuchungsverfahrens, das die *GDPD* derzeit vor allem in Bezug auf Telemarketing-Aktivitäten von TK-Unternehmen durchführt, im Zuge dessen sie in ihrer PM auf ein „Gestrüpp" von illegalen Callcentern hinweist, die unter völliger Missachtung der Bestimmungen zum Schutz personenbezogener Daten Telemarketing-Aktivitäten durchführen. Jüngst hatte die *GDPD* auch Maßnahmen gegen andere Anbieter, darunter *Eni Gas e Luce*, *Tim*, *Wind Tre*, *Iliad Italia* und *Vodafone* ergriffen, die zur Verhängung von Sanktionen i.H.v. insgesamt ca. 70 Mio. EUR geführt haben.

■ Vgl. auch ZD-Aktuell 2020, 07432; *Henrich*, MMR-Aktuell 2020, 425983; *Hemmert-Halswick*, MMR-Aktuell 2019, 422099 und ZD-Aktuell 2019, 06440 sowie ZD-Aktuell 2019, 06677 mwN; außerdem *Paal*, MMR 2020, 14; *Wenzel/Wybitul*, ZD 2019, 290 und *Brink*, ZD 2019, 141.

Ass. iur. Christina Etteldorf
ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken/Brüssel.

BNetzA: Jahresbericht 2020 veröffentlicht

MMR-Aktuell 2021, 439152

Die *Bundesnetzagentur (BNetzA)* hat ihren Jahresbericht für das Jahr 2020 veröffentlicht. Das durch die Corona-Pandemie bedingte veränderte Nutzungsverhalten der Verbraucher*innen führte zu einem höheren Gesprächsvolumen über Festnetze. Zudem ist die Zahl der bei der *BNetzA* eingegangen Beschwerden über unerlaubte Werbeanrufe deutlich gestiegen und erreichte den Höchstwert von über 63.000.

Im Jahr 2020 hat die *BNetzA* wegen unerlaubter Werbeanrufe Bußgelder i.H.v. rund 1,35 Mio. EUR festgesetzt. Im Bereich Rufnummernmissbrauch gingen im Jahr 2020 rund 92.000 Beschwerden ein mit einem Schwerpunkt auf Fax- und SMS-Spam. Wegen Rufnummernmissbrauchs wurden bis Ende April 2021 bereits 214 Rufnummern abgeschaltet und zu 4.304 Rufnummern Rechnungslegungs- und Inkassierungsverbote erlassen.

■ Vgl. auch MMR-Aktuell 2020, 431268; MMR-Aktuell 2020, 426201; MMR-Aktuell 2020, 428121 und MMR-Aktuell 2020, 424514.

BKartA: Verfahren gegen Amazon nach neuen Vorschriften für Digitalkonzerne

MMR-Aktuell 2021, 439348

Nachdem 2021 bereits ein Verfahren gegen *Facebook* (vgl. MMR-Aktuell 2021, 435334) eingeleitet wurde, hat das *Bundeskartellamt (BKartA)* nach der Einführung neuer Vorschriften für Digitalkonzerne ein entsprechendes Verfahren gegen *Amazon* eingeleitet.

Das *BKartA* hat sich in der Vergangenheit bereits vermehrt mit *Amazon* auseinandergesetzt, darunter u.a. mit dem Umgang von Händlern auf dem Amazon Marketplace. Neben zwei ohnehin parallellaufenden Verfahren gegen *Amazon* hat das *BKartA* nun ein weiteres Verfahren eingeleitet, das sich auf Grundlage neuer kartellrechtlicher Möglichkeiten durch die letzte GWB-Novelle zurückführen lässt.

Diese ist in Form des GWB-Digitalisierungsgesetzes im Januar 2021 in Kraft getreten und enthält neue Vorschriften zur kartellrechtlichen Regelung von Digitalkonzernen. Bedeutsam ist dabei besonders der neu eingefügte § 19a GWB, der es dem *BKartA* ermöglichen soll, früher und effektiver gegen die Verhaltensweisen digitaler Konzerne vorzugehen, indem es zunächst nach Absatz 1 die marktübergreifende Bedeutung des Konzerns für den Wettbewerb feststellen kann, um sodann auf Grundlage dessen bestimmte Praktiken zu untersagen, so z.B. die Bevorzugung eigener Angebote nach § 19a Abs. 2 Nr. 1 GWB. Nach dem eingeleiteten Verfahren gegen *Facebook* ist dieses Verfahren bereits das zweite eingeleitete Verfahren nach der GWB-Novelle. Entsprechend § 19a Abs. 1 GWB soll in einem ersten Schritt zunächst festgestellt werden, ob *Amazon* eine überragende marktübergreifende Bedeutung für den Wettbewerb zukommt, ehe dann in weiteren Schritten konkretere Maßnahmen geprüft werden.

■ Vgl. auch MMR-Aktuell 2020, 433515 und MMR-Aktuell 2018, 412549.

BGH: Unzulässige Preisanpassungsklausel von Netflix

MMR-Aktuell 2021, 439416

Der *BGH* (B. v. 15.4.2021 – I ZR 23/20; MMR wird die Entscheidung demnächst veröffentlichen) hat eine Klausel in den Nutzungsbedingungen von *Netflix* für unzulässig erklärt, in der sich der Streaming-Anbieter beliebige Preiserhöhungen vorbehalten hat. Preisanpassungsklausel können zwar grundsätzlich zulässig sein, aber nicht, wenn sie der zusätzlichen Gewinnsteigerung dienen. Daneben hatte das *Gericht* die Gestaltung eines Bestell-Buttons für ein Online-Abo beanstandet, der nicht eindeutig genug auf die Zahlungsverpflichtung hinwies.

Geklagt hatte der *Bundesverband der Verbraucherzentralen (vzbv)* gegen die Klausel von *Netflix* zur beliebigen Preisanpassung: „Unser Abo-Angebot und die Preise für den Netflix-Dienst können sich gelegentlich ändern." Abonnent*innen sollten dann mindestens 30 Tage im Voraus über Änderungen informiert werden.

Bereits die *Vorinstanz* (MMR 2020, 480) hatte sich zur grundsätzlichen Zulässigkeit von Preisanpassungsklauseln geäußert. Diese sei nämlich dann gegeben, wenn die Befugnis der Verwender*innen zu Preisanhebungen von Kostenerhöhungen abhängig gemacht werde und die einzelnen Kostenelemente sowie deren Gewichtung bei der Kalkulation des Gesamtpreises offengelegt werden. Dies gilt nicht, wenn über die Abwälzung konkreter Kostensteigerungen hinaus der zunächst vereinbarte Preis ohne Begrenzung angehoben werden kann, um so nicht nur eine Gewinnschmälerung zu vermeiden, sondern einen zusätzlichen Gewinn zu erzielen. Gegen die Nichtzulassung der Revision hatte *Netflix* Nichtzulassungsbeschwerde beim *BGH* eingelegt. Diese wurde nun als unzulässig verworfen.

■ Vgl. auch *Möllnitz*, MMR 2021, 116; *OLG Köln* MMR 2016, 602; *OLG Köln* MMR 2017, 552 – Bestell-Button II; *BGH* MMR 2012, 600 – Neue Personenkraftwagen sowie *BGH* MMR 2008, 159 – Bezahlfernsehen.

Italien: Kartellbehörde verhängt Strafe gegen Google

MMR-Aktuell 2021, 439414

Die italienische Kartellbehörde *AGCM* hat *Google* eine Strafe von rund 102 Mio. EUR aufgegeben, weil *Google* eine App des Energiekonzerns *Enel* nicht in sein Android-Auto-System für elektronische Fahrzeuge aufgenommen hat.

Android Auto ist ein von *Google* entwickeltes System für Fahrzeuge, durch das Apps von einem gekoppelten Smartphone über das Infotainment-System des Autos genutzt werden können. *Google* nahm eine vom Energiekonzern *Enel* entwickelte App nicht in ihre Android-Auto-Plattform bzw. den Google Play Store auf, sodass die App nicht über das Infotainment-System im Fahrzeug genutzt werden kann. Die App zeigt Fahrer*innen von elektronischen Fahrzeugen Ladestationen für E-Autos in der Nähe an und ermöglicht im gleichen Zuge die Buchung der Säulen und Bezahlung des Stroms. Die *Kartellbehörde* warf *Google* vor, durch den Ausschluss der App die eigene Karten-App (Google Maps) bevorteilt zu haben und sprach eine Strafe von 102.084.433,91 EUR aus. Zwar könne man sich über Google Maps die Ladesäulen nur anzeigen und dorthin lotsen lassen, allerdings bestehe die Möglichkeit, dass dort zukünftig auch ähnliche Bezahlsysteme integriert werden. *Google* prüft derzeit rechtliche Schritte gegen die Strafe.

■ Vgl. auch MMR-Aktuell 2020, 433603; MMR-Aktuell 2020, 432668 und MMR-Aktuell 2018, 407241.

Wolfgang Kuntz HmbBfDI: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch Facebook

MMR-Aktuell 2021, 439258

Der *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI)* hat eine Anordnung erlassen, die der *Facebook Ireland Ltd.* verbietet, personenbezogene Daten von WhatsApp zu verarbeiten, soweit dies zu eigenen Zwecken erfolgt. Der sofortige Vollzug wurde angeordnet.
Dies erfolgt i.R.d. Dringlichkeitsverfahrens der DS-GVO, das den Erlass von Maßnahmen mit einer begrenzten Geltungsdauer im jeweiligen Hoheitsgebiet vorsieht. Hintergrund des Verfahrens ist die Aufforderung an alle Nutzer*innen von WhatsApp, den neuen Nutzungs- und Privatsphärebestimmungen bis zum 15.5.2021 zuzustimmen. Damit lässt sich WhatsApp weitreichende Befugnisse für eine Datenweitergabe an *Facebook* einräumen.

Wolfgang Kuntz
ist Rechtsanwalt und Fachanwalt für IT-Recht in Saarbrücken.

E-Rezept-App ab Juli 2021

MMR-Aktuell 2021, 439263

Die Projektgesellschaft *Gematik* plant den Launch für ihre App zum elektronischen Rezept (E-Rezept) für Verordnungen von apothekenpflichtigen Arzneimitteln für gesetzlich Versicherte. Startpunkt ist der 1.7.2021 mit einer Testphase in den Fokus-Regionen Berlin und Brandenburg.
Mit der App können gesetzlich Versicherte elektronische Rezepte von Ärzt*innen erhalten und weitere Informationen zu Einnahme und Dosierung erfolgen. Das Rezept wird digital erstellt und kann in jeder Apotheke durch Vorzeigen eines Rezeptcodes oder durch eine vorherige unmittelbare Übermittlung eingelöst werden. Technisch erfordert der Einsatz ein NFC-fähiges Smartphone mit mindestens iOS 14 oder Android 6 und den Code der elektronischen Gesundheitskarte. Eine Anwendung der App ist aber auch ohne Registrierung der Gesundheitskarte möglich indem (auch ausgedruckte) Rezeptcodes gescannt und in der Apotheke vorgezeigt werden können.
Die Testphase soll die Grundfunktionen überprüfen und die Anwendung evaluieren. Je nach Feedback der Nutzer*innen sollen in agilen Prozessen weitere Funktionen eingebaut und die App verbessert werden. So soll es z.B. künftig auch möglich sein, unmittelbar am Smartphone an bis zu drei Apotheken automatisch abzufragen, ob das entsprechende Medikament verfügbar ist. Es können Stammapotheken festgelegt werden und eine Anmeldung für mehrere Gesundheitskarten soll möglich sein, sodass z.B. Familienangehörige für die Familie Daten empfangen und verwalten können.
Nach der Testphase in Berlin und Brandenburg im 3. Quartal soll im 4. Quartal 2021 die bundesweite Einführungsphase starten, die die Verfügbarkeit und Akzeptanz steigern soll, ehe eine verpflichtende Nutzung ab 1.1.2022 kommen soll.

■ Vgl. auch MMR-Aktuell 2020, 430406 und MMR-Aktuell 2020, 427506.

MMR MultiMedia und Recht
Zeitschrift für IT-Recht und Recht der Digitalisierung

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (verantwortlich für den Textteil); Katharina Klauser, Redakteurin; Ruth Schrödl, Redakteurin; Eva Wanderer, Redaktionsassistentin; Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-427, Telefax: 089/38189-197, E-Mail: mmr@beck.de

twitter.com/MMRZeitschrift
de.linkedin.com/showcase/zeitschriftmmr

Manuskripte: Manuskripte sind an die Redaktion zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag C.H.BECK an seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Peer-Review-Verfahren: Jeder Beitrag wird vor Abdruck von der Schriftleitung und ferner von zwei Gutachtern in anonymisierter Form gelesen und bewertet.

Anzeigenabteilung: Verlag C.H.BECK, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.
Media-Beratung: Telefon 089/3 81 89-687, Telefax 089/3 81 89-589.
Disposition, Herstellung Anzeigen, technische Daten: Telefon (0 89) 3 81 89-609, Telefax 089/3 81 89-589, E-Mail anzeigen@beck.de.
Verantwortlich für den Anzeigenteil: Bertram Mehling

Verlag: Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Tel.: 089/381 89-0, Telefax: 089/38 18 93 98, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX. Der Verlag ist oHG. Gesellschafter sind Dr. Hans Dieter Beck und Dr. h.c. Wolfgang Beck, beide Verleger in München.

Erscheinungsweise: Monatlich.

Bezugspreise 2021: Jährlich € 449,– (inkl. MwSt.). Vorzugspreis für Mitglieder der davit € 355,– (inkl. MwSt.). Alle Abopreise inklusive Newsdienst MMR-Aktuell und MMRDIREKT. Einzelheft: € 45,– (inkl. MwSt.); Versandkosten jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Abonnement und Bezugspreis beinhalten die Printausgabe sowie eine Lizenz für die Online-Ausgabe. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden. Jahrestitelei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

Bestellungen über jede Buchhandlung und beim Verlag. Vertriebskooperation in der Schweiz: Helbing & Lichtenhahn Verlag AG (CH) & Co.KG, Elisabethenstraße 8, CH-4051 Basel, Tel.: +41 (0)61 228 90 70, Fax: +41 (0)61 228 90 71, E-Mail: zeitschriften@helbing.ch.

KundenServiceCenter: Tel.: 089/3 81 89-750, Fax: 089/3 81 89-358, E-Mail: kundenservice@beck.de

Abbestellungen müssen 6 Wochen vor Jahresschluss erfolgen.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an. Hinweis gemäß § 4 Abs. 3 der Postdienst-Datenschutzverordnung: Bei Anschriftsänderungen des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen des Heftes beim Verlag widersprechen.

Satz: FotoSatz Pfeifer GmbH, 82152 Krailling.

Druck: Druckerei C.H.BECK, Bergerstraße 3–5, 86720 Nördlingen.
ISSN 2698-7988

Datenschutz kompakt.

beck-shop.de/32186236

Von Dr. Georg F. Schröder, RA, LL.M.
4. Auflage. 2021. XVI, 270 Seiten. Kartoniert € 21,90
(dtv-Band 51259) **| Neu im Juni 2021**

Der anschauliche Band

erläutert die praktisch **wichtigsten Aspekte des Datenschutzrechts.** Gut verständlich aufbereitet, mit optischen Hervorhebungen der entscheidenden Elemente und vielen praktischen Beispielen, bietet der Band alles, was ein Unternehmen wissen muss, damit es **datenschutzkonform arbeiten** kann. Zudem sind alle erforderlichen Vertragsvorlagen und Dokumente enthalten.

Die 4. Auflage

berücksichtigt insbesondere **wichtige Anpassungen und Ergänzungen** in den Bereichen:

- Berechnung der Bußgelder
- internationaler Datentransfer nach Schrems II in die USA
- Ransomware Angriffe
- Cookie Consent Management u.v.m.

Im Übrigen ist das Werk auf dem neuesten Stand von Rechtsprechung und Gesetzgebung.

Beck im dtv

Erhältlich im Buchhandel oder bei:
beck-shop.de | Verlag C.H.BECK oHG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 173197

Erfolgreiche Legal Tech-Strategien entwickeln.

beck-shop.de/29076167

Remmertz
Legal Tech-Strategien für Rechtsanwälte
Berufsrecht, Kooperationen, Haftung

2020. XXX, 317 Seiten. Kartoniert € 89,–
ISBN 978-3-406-74372-6

Diese Neuerscheinung

behandelt die berufsrechtlichen Möglichkeiten und Grenzen sowie den **regulatorischen Rahmen** (wie datenschutz-, haftungs-, versicherungs- und steuerrechtliche Fragen) anwaltlicher Legal Tech-Strategien und regt seine Nutzer an, **berufsrechtskonforme Legal Tech-Strategien** zu entwickeln und damit rechtssicher Chancen am lukrativen Markt für **digitale Rechtsdienstleistungen** für sich zu nutzen.

Das perfekte Tool

für Rechtsanwälte und Juristen in Berufsverbänden und -vereinen.

Erhältlich im Buchhandel oder bei:
beck-shop.de | Verlag C.H.BECK oHG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 171922

C.H.BECK

Für den interdisziplinären Austausch zur Digitalisierung.

Vorteile auf einen Blick

- interdisziplinärer und internationaler Ansatz sorgt für umfassende Behandlung der Themen
- befasst sich mit den grundsätzlichen Rechtsfragen der Digitalisierung
- Herausgeber und Autoren sind namhafte Expertinnen und Experten

Die Digitalisierung

dringt immer stärker in unser gesellschaftliches Leben vor und bringt Entwicklungsdynamiken mit sich, die uns **wirtschaftlich, kulturell, technisch und gesellschaftlich** herausfordern. Die dabei entstehenden Rechtsfragen verlangen nach einer intra- und interdisziplinären Diskussion. Die neue ZfDR behandelt fachsäulenübergreifend grundlegende Fragestellungen und bedeutsame **Entwicklungen der Digitalisierung,** zum Beispiel:

- den Verantwortungsbegriff und das Konzept von Wahrheit in Zeiten von »Fake News«
- die Geltung und Reichweite des Rechts
- das Menschenbild in der Digitalisierung
- aktuelle Entwicklungen im Antidiskriminierungsrecht, Datenrecht, Immaterialgüterrecht und Sicherheitsrecht
- die Auseinandersetzung mit den Themenfeldern Künstliche Intelligenz, Autonome Systeme, Blockchain und Legal-Tech-Anwendungen sowie
- die Plattform-Ökonomie und Intermediäre.

ZfDR · Zeitschrift für Digitalisierung und Recht

1. Jahrgang. 2021.
Erscheint vierteljährlich inkl. ZfDR Direkt.
Sie erhalten 1 Ausgabe gratis im Rahmen des Probe-Abos.

Danach bekommen Sie die Zeitschrift im berechneten Abonnement, falls Sie nicht bis 4 Wochen nach Erhalt Ihres Gratis-Heftes abbestellen.

Jahresabonnement für Privatpersonen inkl. ZfDR Direkt für einen Nutzer € 295,–

Jahresabonnement für Institutionen inkl. ZfDR Direkt für 3 Nutzer € 398,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 9,50 jährlich.

beck-shop.de/32324942

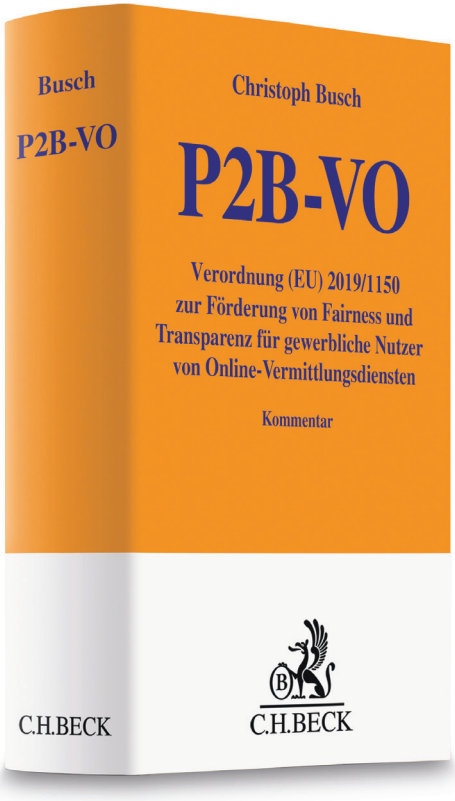
Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 173086
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

Topaktuell zur neuen Platform-to-Business-VO.

Vorteile auf einen Blick

- umfassende Kommentierung der P2B-VO
- Klauselbeispiele aus der Praxis
- erfahrenes Autorenteam



Neue Regeln für Online-Plattformen

Die **Verordnung zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (P2B-VO)** zielt darauf ab, einen fairen, transparenten und berechenbaren Regulierungsrahmen für die Plattformökonomie zu schaffen. Sie enthält insbesondere Transparenzanforderungen und inhaltliche Vorgaben für die AGB der Plattformbetreiber. Hinzu kommen Regeln für das Beschwerdemanagement und die Beilegung von Streitigkeiten zwischen Plattformbetreibern und gewerblichen Plattformnutzern.

Der umfassende Kommentar

bietet eine **detaillierte, wissenschaftlich** und zugleich **praxistaugliche Darstellung** der Neuregelungen. Beispiele aus der **Kautelarpraxis** runden das Werk ab.

Das Autorenteam

Herausgeber ist Prof. Dr. Christoph **Busch,** die Verfasser sind neben dem Herausgeber: Prof. Dr. Thomas **Höppner,** RA; Prof. Dr. Rupprecht **Podszun;** Prof. Dr. Hans **Schulte-Nölke;** Prof. Dr. Friedrich Graf **von Westphalen** und Johannes **Wick,** RA.

Busch
P2B-VO
Verordnung (EU) 2019/1150
zur Förderung von Fairness und
Transparenz für gewerbliche Nutzer
von Online-Vermittlungsdiensten

2021. Rund 500 Seiten.
In Leinen ca. € 119,–
ISBN 978-3-406-75320-6
Neu im August 2021

beck-shop.de/30789420

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 172895
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

20 JAHRE
beck-online
DIE DATENBANK

Urheber-, Presse- und Medienrecht PLUS

Urheber-, Presse- und Medienrecht PLUS

Das aktuelle Fachmodul von beck-online u.a. mit diesen herausragenden Werken:

- **Schricker/Loewenheim, Urheberrecht**
- **Schwarz, Handbuch Filmrecht (bisher Hartlieb/Schwarz)**
- **Spindler/Schuster, Recht der elektronischen Medien**
- **BeckOK Urheberrecht, Hrsg. Ahlberg/Götting**
- **Moser/Scheuermann/Drücke, Handbuch der Musikwirtschaft**

Weiterhin stehen Ihnen zur Verfügung: Drei online zugängliche Standardwerke zum **Presserecht** sowie die **Zeitschrift ZUM** und vieles, was die Arbeit im Urheber- und Medienrecht erleichtert: **einschlägige Rechtsprechung,** alle Gesetzestexte für die Fallbearbeitung, **Formulare und Mustertexte.** Damit macht sich dieses umfassende Informationspaket schnell für Sie bezahlt.

JETZT
4 Wochen
kostenlos
testen
beck-online.de

Infos: beck-shop.de/28120004

▸ schon ab **€ 50,–/Monat**
(Preis für bis zu 3 Nutzer, zzgl. MwSt., 6-Monats-Abo)

Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München | 170861

facebook.com/verlagchbeck | twitter.com/beckonlinede

C.H.BECK