RDV
Recht der Datenverarbeitung

DataAgenda / RDV Sonderveröffentlichung

Rolf Schwartmann/Kristin Benedikt/Yvette Reif

Datenschutz bei Websites – aktuelle Rechtslage und Ausblick auf das TTDSG

Der Beitrag erläutert die aktuelle Rechtslage in Bezug auf Onlinedatenverarbeitungen im Allgemeinen und Cookies im Besonderen und wagt eine erste Einordnung des Anfang August 2020 geleakten Referentenentwurfs des BMWi für ein Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG), das die Datenschutzvorschriften von TKG und TMG im Vorfeld der Verhandlung der ePrivacy-VO in Deutschland zusammenführen soll.

I. Einführung

Die Bedeutung von Cookies ist in der Onlinewirtschaft nach wie vor hoch. Unterdessen hat ihr Stern zu sinken begonnen. Da viele Nutzer in den Browser-Einstellungen keine Third Party Cookies zulassen oder regelmäßig die Cookies löschen, werden zunehmend alternative Trackingverfahren entwickelt, die eine Nachverfolgung des Nutzers auch ohne das Setzen von Cookies ermöglichen („Cookieless Tracking“).[1] So erfassen etwa beim sog. Browser-Fingerprinting die Webserver unterschiedliche Merkmale der Browser der Besucher und ermitteln auf dieser Basis jeweils einen individuellen digitalen Fingerabdruck, mittels dessen die Nutzer – bzw. genauer: ihre Browser – später wiedererkannt werden können. Die führenden Browseranbieter haben längst reagiert und blockieren Cookies von vornherein. Aber auch Fingerprinting und Geolokalisierung dürfte die Zukunft nicht gehören. Die GAFA-Tech-Giganten setzen auf die Nutzererkennung per Login. So hat Apple kürzlich offengelegt, wie mithilfe der Apple ID die Onlinewelt über iOS 14 per "Sign in with Apple“ noch effizienter erobert werden soll. Die Apple-ID soll künftig nicht nur den Zugang zu den Produkten im App Store erschließen, sondern man soll sie für jeden Onlinekauf benutzen. Anbieter, die sich weigern, den Login per Apple zu implementieren, werden ausgesperrt.[2] Aktuell spielen Cookies aber ungeachtet dessen – insbesondere beim Online-Marketing – immer noch eine zentrale Rolle.

Cookies sind kleine Textdateien, die der Webbrowser auf dem Computer speichert. Anhand von Cookies erkennt eine Website, wer sie gerade besucht, und kann dadurch Nutzerpräferenzen, wie z.B. Sprach- oder Bildschirmeinstellungen, oder Log-in-Informationen speichern, damit der Nutzer die Einstellungen nicht immer wieder neu vornehmen bzw. sich immer wieder neu anmelden muss. Beim Onlineshopping verhindern Cookies, dass sich mit jedem Aufruf einer neuen Unterseite im Rahmen des Webangebots der Warenkorb leert. Im Ausgangspunkt handelt es sich also zunächst einmal um ein sehr nützliches und oft notwendiges Verfahren, ohne das viele Internetseiten nicht in der gewohnten komfortablen Form genutzt werden könnten.

Beim Online-Marketing ermöglicht der Einsatz von Cookies, die Nutzerinteressen auch sessionübergreifend zu ermitteln und so möglichst zielgenaue Onlinewerbung auszuspielen. Dabei handelt es sich um sog. persistente Cookies, die dauerhaft im System des Nutzers hinterlegt werden. Sofern Cookies von der Website gesetzt werden, auf der sich der Nutzer gerade befindet, spricht man von „First Party Cookies“. „Third Party Cookies“ sind demgegenüber Cookies, die nicht vom Betreiber der Website, sondern von einem Dritten platziert werden, dessen Inhalte auf der besuchten Website eingebunden sind. „Third Party Cookies“ liefern ein deutlich klareres Bild der Nutzerpräferenzen, denn mit diesen kann nicht mehr nur nachverfolgt werden, wofür der Nutzer sich innerhalb des eigenen Webauftritts interessiert, sondern über verschiedene Onlineangebote hinweg.

Vor dem Hintergrund dieser noch anhaltenden praktischen Bedeutung befassen sich die Datenschutzaufsicht[3], der Gesetzgeber in Deutschland mit dem Entwurf des TTDSG[4]

1 Zur Zulässigkeit solcher Verfahren vgl. unten II.2.b).

2 Schwartmann, Ein fairer Schlüssel zum Netz? https://web.de/magazine/digital/apple-id-fairer-schluessel-netz-34843646.

und der europäische Gesetzgeber im Rahmen des ePrivacy-VO-Prozesses[5] aktuell intensiv mit einem Rechtsrahmen für Cookies.

Ende Mai 2020 hat nunmehr die BGH-Entscheidung I ZR 7/16 (Cookie-Einwilligung II) in der Praxis für viel Aufruhr gesorgt. Der vorliegende Beitrag soll insofern einen Überblick über die Zulässigkeit von Onlinedatenverarbeitungen allgemein und Cookies und ähnlichen Techniken im Besonderen bieten und die – im Ergebnis beschränkte – Bedeutung der BGH-Entscheidung aufzeigen. Zugleich sollen die wesentlichen Inhalte des vorliegenden TTDSG-Entwurfs dargestellt werden.

II. Rechtliche Rahmenbedingungen von Onlinedatenverarbeitungen

1. Der Rechtsrahmen für Onlinedatenverarbeitungen allgemein

a) Allgemeines

Die DS-GVO ist vorrangig anzuwenden, sodass grundsätzlich datenschutzrechtliche Regelungen der Mitgliedsstaaten verdrängt werden. Dies gilt nur dann nicht, wenn die DS-GVO entweder eine Öffnungsklausel enthält, die den Mitgliedstaaten einen eigenen Gestaltungsspielraum für datenschutzrechtliche Vorschriften einräumt, oder die DS-GVO eine Kollisionsregel enthält.

Eine Öffnungsklausel für bereichsspezifische Regelungen zum Datenschutz im Internet enthält die DS-GVO nicht. Dies würde auch dem Ziel der DS-GVO, einen einheitlichen daten-schutzrechtlichen Rechtsrahmen in der Europäischen Union zu schaffen, zuwiderlaufen. Insbesondere im digitalen Bereich bedarf es eines einheitlichen Rechtsregimes über die Grenzen der Mitgliedstaaten hinaus.

Der Zweck von Kollisionsregeln ist es, das Verhältnis zwischen der DS-GVO und bereits existierendem Recht zu regeln, sodass dieses neben der DS-GVO fortbestehen kann. Eine Kollisionsregel, die das Verhältnis zwischen der DS-GVO und der ePrivacy-Richtlinie (2002/58/EG) regelt, ist in Art. 95 DS-GVO enthalten. Bemerkenswert ist dabei, dass Art. 95 DS-GVO nicht nur das Verhältnis zwischen dem neuen Recht – der DS-GVO – und bereits existierendem Recht – der ePrivacy-Richtlinie (2002/58/EG) – regelt, sondern dass es sich hierbei um Normen unterschiedlicher Wirkung handelt. Im Gegensatz zur DS-GVO, die unmittelbar gilt, müssen Richtlinien gem. Art. 288 AEUV durch die Mitgliedsstaaten in nationales Recht umgesetzt werden.

b) Strittiges Verhältnis zwischen DS-GVO und TMG

Höchst umstritten ist das Verhältnis zwischen dem europäischen Recht, also der DS-GVO und der ePrivacy-Richtlinie (2002/58/EG), sowie dem deutschen TMG.[6] Zu dem Verhältnis zwischen TMG und europäischem Recht haben sich nicht nur die Aufsichtsbehörden geäußert. Seit Mai 2020 gibt es auch eine Entscheidung des BGH.

aa) Aufsichtsbehörden: DS-GVO verdrängt TMG

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im März 2019 die „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien" (OH Telemedien) veröffentlicht. Nach der OH Telemedien sind die datenschutzrechtlichen Vorschriften des TMG, insbesondere die Vorschrift zur Erstellung von Nutzungsprofilen unter Pseudonym gem. § 15 Abs. 3 S. 1 TMG, seit Geltung der DS-GVO nicht mehr anwendbar.

§ 15 Abs. 3 S. 1 TMG bestimmt, dass der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen darf, sofern der Nutzer nicht widerspricht. Das bedeutet, dass dem Nutzer ein Widerspruchsrecht (sog. Opt-out) zusteht, die Datenverarbeitung bis zu diesem Zeitpunkt jedoch rechtmäßig erfolgt. Im Gegensatz dazu verlangt Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG) eine Einwilligung des Nutzers vor Beginn der Verarbeitung und dem Speichern von bzw. dem Zugriff auf Informationen auf dem Endgerät des Nutzers. Die Datenverarbeitung ist nur nach einem Opt-in zulässig.

Im Ergebnis stellt § 15 Abs. 3 S. 1 TMG also eine Opt-out-Regelung dar, während Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG) ein Opt-in voraussetzt. Es handelt sich daher um zwei Vorschriften mit entgegenstehendem Regelungsgehalt, sodass § 15 Abs. 3 S. 1 TMG nach Auffassung der DSK keine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG) darstellen kann.

Die ePrivacy-RL ist auch nicht unmittelbar anwendbar. Zwar können Richtlinien unter bestimmten Voraussetzungen unmittelbare Wirkung entfalten, wenn ein Mitgliedstaat die Richtlinie nicht oder nicht fristgerecht umgesetzt hat. Eine unmittelbare Wirkung kommt aber nur in Betracht, wenn alle folgenden Voraussetzungen vorliegen:

- Die Richtlinie gewährt ein subjektiv-öffentliches Recht, d.h. einen Anspruch des Bürgers gegenüber dem Staat.
- Die Richtlinie muss hinreichend bestimmt sein, d.h., ihre Regelungen müssen inhaltlich klar sein.
- Die Richtlinie wurde nicht oder nicht fristgerecht umgesetzt.

Diese Voraussetzungen liegen im Fall der ePrivacy-RL nicht kumulativ vor. Die ePrivacy-RL regelt keinen Anspruch des Bürgers gegenüber dem Staat, sondern verpflichtet Verant-

3 Art.-29-Datenschutzgruppe, Stellungnahme 01/2017 zum Vorschlag für eine Verordnung über die Privatsphäre (WP 247).

4 Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze, abrufbar unter: https://www.heise.de/downloads/18/2/9/4/6/4/2/1/20200731_RefE_TTDSG_cleaned.pdf. Es handelt sich um einen geleakten Referentenentwurf (Stand: 14.07.2020). Aktuell befindet sich ein geänderter Entwurf in der Ressortabstimmung.

5 Zum diesbezüglichen Stand Spindler, NJW 2020, 2513, 2516. 6 Vgl. dazu Schwartmann/Klein, in: Schwartmann/Jaspers/Thüsing/Kugelmann, HK-DS-GVO Art. 6 Abs. 1 S. 1 f) DS-GVO Rn. 169 ff.

6 Vgl. dazu Schwartmann/Klein, in: Schwartmann/Jaspers/Thüsing/Kugelmann, HK-DS-GVO Art. 6 Abs. 1 S. 1 f) DS-GVO Rn. 169 ff.

wortliche zur Einhaltung datenschutzrechtlicher Vorgaben. Im Ergebnis ist Art. 5 Abs. 3 ePrivacy-RL damit nicht unmittelbar anwendbar.[7]

Nach bisheriger DSK-Auffassung ergeben sich die maßgeblichen Datenschutzregelungen im Zusammenhang mit Websites, Messengern und weiteren Onlinediensten damit im Wesentlichen aus der DS-GVO.

bb) BGH: § 15 Abs. 3 S. 1 TMG gilt fort und ist europarechtskonform zu interpretieren

Demgegenüber hat der BGH mit Urteil vom 28.05.2020 – I ZR 7/16 („Cookie-Einwilligung II") die Ansicht vertreten, dass § 15 Abs. 3 S. 1 TMG trotz DS-GVO weiterhin gilt und richtlinienkonform im Sinne von Art. 5 Abs. 3 S. 1 der ePrivacy-Richtlinie (2002/58/EG) in Fassung der Richtlinie 2009/136/EG („Cookie"-Richtlinie) anzuwenden sei. Bei richtlinienkonformer Auslegung von § 15 Abs. 3 S. 1 TMG ergebe sich, dass für den Einsatz von Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung die Einwilligung des Nutzers erforderlich sei. Der richtlinienkonformen Auslegung von § 15 Abs. 3 S. 1 TMG stehe nicht entgegen, dass der deutsche Gesetzgeber bisher keinen formellen Umsetzungsakt im Hinblick auf Art. 5 Abs. 3 S. 1 der ePrivacy-Richtlinie (2002/58/EG) vorgenommen habe. Denn es sei anzunehmen, dass der Gesetzgeber die bestehende Rechtslage in Deutschland für richtlinienkonform erachtete, so der BGH. Auch mit dem Wortlaut der TMG-Regelung sei eine entsprechende richtlinienkonforme Auslegung noch vereinbar.[8]

Die Entscheidung hat in der Praxis für einigen Wirbel gesorgt. Kritiker werfen dem BGH vor, durch eine ausufernde Auslegungsmethodik die fehlende Anpassung des TMG durch den Gesetzgeber kompensieren zu wollen. Teilweise wird – zu Unrecht – befürchtet, dass diese Entscheidung zur Folge habe, dass nunmehr jeder Websitebetreiber, der Cookies einsetzt, eine Einwilligung einholen müsse.

Für die Verantwortlichen in den Unternehmen ist vor allem wichtig, sich den (eingeschränkten) Aussagegehalt der Entscheidung zu vergegenwärtigen.

Aus der Entscheidung ergibt sich „nur", dass

- sich die Anforderungen einer wirksamen Einwilligung nach der DS-GVO richten,
- voreingestellte Ankreuzkästchen keine wirksame Einwilligung darstellen und
- für den Einsatz von Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung die Einwilligung des Nutzers erforderlich ist.

Der BGH hat insbesondere nicht darüber entschieden,

- ob die §§ 11 ff. TMG insgesamt (richtlinienkonform) anwendbar sind,
- inwiefern Cookies generell einwilligungsbedürftig sind,
- wie das Verhältnis zwischen den Rechtsgrundlagen der DS-GVO und § 15 Abs. 3 TMG ist.

Die deutschen Aufsichtsbehörden sind nicht an die BGH-Entscheidung gebunden. Es bleibt abzuwarten, wie die Datenschutzaufsichtsbehörden sich zu dieser Entscheidung positionieren. Solange keine Stellungnahme der Datenschutzaufsichtsbehörden vorliegt, dürfen sich deutsche Websitebetreiber nach wie vor nach der OH Telemedien richten.

cc) Zwischenfazit

Die Entscheidung des BGH lässt sich in verschiedener Hinsicht kritisieren. Zweifel bestehen insbesondere an der Richtigkeit der Aussage des BGH, der Gesetzgeber habe die bestehende Rechtslage in Deutschland für richtlinienkonform erachtetet.[9] Auch stellt sich die Frage, ob europarechtskonforme Auslegung tatsächlich so weit gehen kann, dass man eine nationale Vorschrift quasi in ihr Gegenteil verkehrt, indem man in eine Regelung, die ihrem Wortlaut nach eine Einwilligung gerade nicht verlangt, ein Einwilligungserfordernis hineininterpretiert.[10] So wird die Auffassung[11] vertreten, dass es „wohl eleganter" gewesen wäre, § 15 Abs. 3 TMG dem Anwendungsvorrang der DS-GVO zum Opfer fallen zu lassen. § 15 Abs. 3 TMG sei, ebenso wie die praktisch wortgleiche Vorgängernorm des § 6 Abs. 3 Teledienstedatenschutzgesetz (TDDSG), originäres mitgliedstaatliches Datenschutzrecht ohne jeden Bezug zu Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG).[12]

Die offenkundige Intention des BGH, den Wertungen von Art. 5 Abs. 3 ePrivacy-Richtlinie zur Anwendung zu verhelfen, hätte über die DS-GVO aber nur unvollständig erreicht werden können. Denn die DS-GVO dient „nur" dem Schutz natürlicher Personen (Art. 1 Abs. 1 DS-GVO) und ist ihrem Anwendungsbereich nach auf die Verarbeitung personenbezogener Daten (Art. 2 DS-GVO) beschränkt. Art. 5 Abs. 3 der ePrivacy-Richtlinie (2002/58/EG) soll den Nutzer aber vor jedem Eingriff in seine Privatsphäre schützen, unabhängig davon, ob dabei personenbezogene Daten oder andere Daten betroffen sind.[13] Die Regelung des Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG) schützt die informationelle Integrität des Endgeräts und geht damit über den Anwendungsbereich der DS-GVO hinaus.[14] Die DS-GVO war insofern für den BGH noch weniger als das TMG ein geeigneter Ansatzpunkt, um die Wertungen des europäischen Rechts „durchzuboxen".[15] Eine unmittelbare Anwendung des Art. 5 Abs. 3 der ePrivacy-Richtlinie (2002/58/EG) kam aus bereits dargestellten Gründen[16]

7 Anders wohl der LfDI BW, der sich in seiner Pressemeldung vom 09.10.2019 unmittelbar auf die Regelung bezieht.

8 BGH, Urteil vom 28.05.2020 – I ZR 7/16, Rz. 54 f.

9 Vgl. dazu Schulz, „Cookie Management 2.0 – Was folgt aus dem Urteil des BGH und den Guidelines der deutschen und europäischen Aufsichtsbehörden für Webseitenbetreiber?", Blogbeitrag vom 02.06.2020.

10 Von einem „waghalsigen rechtsmethodischen Manöver" spricht Spindler NJW 2020, 2513, 2517.

11 Schulz, a.a.O.; ähnlich auch Spindler, NJW 2020, 2513, 2515, der bedauert, dass der BGH einen möglichen „Ausweg" über die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO nicht beschreitet.

12 Schulz, a.a.O.

13 Vgl. EuGH, GRUR 2019, 1198 Rn. 68 f. Verbraucherzentrale Bundesverband/Planet49.

14 BGH, Urteil 28.05.2020 – I ZR 7/16 (Cookie-Einwilligung II), Rn. 61.

15 Kritisch insofern zurecht Spindler, NJW 2020, 2513, 2515. Die Anwendbarkeit von Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG) auch auf nicht personenbezogene Daten lasse sich über § 15 Abs. 3 DS-GVO nicht abbilden. Zum Anwendungsbereich von § 15 TMG vgl. § 11 TMG.

nicht in Betracht. Zum Verhältnis zwischen den Rechtsgrundlagen der DS-GVO und § 15 Abs. 3 TMG äußert sich der BGH nicht. Im Ergebnis wird man aus rechtlicher Sicht zwischen dem Platzieren von Cookies oder vergleichbaren Skripten und dem Auslesen entsprechender Informationen aus den Endgeräten einerseits und der nachgelagerten, auf den Cookies aufbauenden personenbezogenen Datenverarbeitung andererseits zu unterscheiden haben.[17] Für die nachgelagerte Datenverarbeitung gilt, entsprechend den Ausführungen der DSK in der OH Telemedien, die DS-GVO. Setzen bzw. Auslesen der Cookies sind im Ergebnis an den Vorgaben der ePrivacy-Richtlinie (2002/58/EG) zu messen.[18]

2. Besonderheiten beim Einsatz von Cookies und vergleichbaren Techniken bzw. Skripten

a) Allgemeines

Der BGH[19] hat das Einwilligungserfordernis für Cookies, die zu Marketingzwecken zum Einsatz kommen, bejaht. Auch Cookies, die anderen als werblichen Zwecken dienen, werden regelmäßig erst nach Einwilligung der Webseitenbesucher aktiviert werden dürfen. Dies ergibt sich aus Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG) in der Fassung der sog. „Cookie-Richtlinie" (2009/136/EG). Mit dem BGH ist zu unterstellen, dass sich die Wertungen des europäischen Rechts im Ergebnis durchsetzen.[20]

Eine Ausnahme vom Einwilligungserfordernis gilt für „unbedingt erforderliche" Cookies, die nach den Richtlinienvorgaben auch einwilligungsfrei möglich sein sollen. Hierzu zählen etwa Session Cookies, Warenkorbcookies o.Ä. Ob auch Cookies zur Reichweitenmessung/Webanalyse als „unbedingt erforderlich" iSd ePrivacy-Richtlinie anzusehen sind, erscheint zweifelhaft. Jedenfalls erscheint es gesetzgeberisch sinnvoll, solche Cookies vom Einwilligungserfordernis auszunehmen.[21]

Die nachgelagerte (personenbezogene) Datenverarbeitung im Zusammenhang mit den Cookies richtet sich, wie bereits erläutert, nach den Vorgaben der DS-GVO. Hiernach besteht zwar grundsätzlich die Möglichkeit der Datenverarbeitung nach Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO). Sofern der Einsatz von Cookies im konkreten Fall ein Einwilligungserfordernis auslöst, dürfte es aber regelmäßig sinnvoll sein, die Einwilligung auch auf die nachgelagerte Datenverarbeitung zu erstrecken.

b) Cookieless Tracking

Da die Vorgaben der ePrivacy-Richtlinie (2002/58/EG) technologieneutral sind, gelten sie für alternative Verfahren entsprechend, sofern diese die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, voraussetzen. Damit gelten z.B. für das sog. Browser-Fingerprinting[22] die gleichen Spielregeln wie für das Setzen und Auslesen von Cookies.

III. Rechtsgrundlagentabelle

Die nachfolgende Tabelle[23] liefert einen Überblick über Rechtsgrundlagen für mögliche Datenverarbeitungen im Zusammenhang mit einer Website:

Art der Verarbeitung	Unternehmen	Behörden
Dienste-erbringung	*„normaler" Besuch der Website: Art. 6 Abs. 1 lit. f DS-GVO Login-basierte Dienste, z.B. Webshop, Streaming-dienste: Art. 6 Abs. 1 lit. b DS-GVO*	*Art. 6 Abs. 1 lit. e DS-GVO; § 3 BDSG/LDSG*
Auswertung des Nutzungsverhaltens auf der eigenen Seite zu Werbezwecken ohne Hinzuziehung/Verknüpfung von Drittinformationen	*Einwilligung (nach OH Telemedien der DSK gemäß Art. 6 Abs. 1 lit. a DS-GVO; nach BGH – I ZR 7/16 – aufgrund europarechtskonformer Auslegung von § 15 Abs. 3 TMG) Legitimation auch über Art. 6 Abs. 1 lit. f DS-GVO möglich? Zweifelhaft, da entspr. Cookies wohl nicht als unbedingt erforderlich i.S.v. Art. 5 Abs. 3 ePrivacy-Richtlinie angesehen werden können.*	
Werbung unter Hinzuziehung von Drittinformationen/ Werbenetzwerke, weitgreifende Profilbildung	*Einwilligung (nach OH Telemedien der DSK gemäß Art. 6 Abs. 1 lit. a DS-GVO; nach BGH – I ZR 7/16 – aufgrund europarechtskonformer Auslegung von § 15 Abs. 3 TMG)*	
Reichweitenmessung/Web-Analyse	*Einwilligung nötig Datenverarbeitung im Zusammenhang mit entspr. Tools zwar prinzipiell über Art. 6 Abs. 1 lit. f DS-GVO legitimierbar Aber: Cookie Einsatz nicht unbedingt erforderlich i.S.v. Art. 5 Abs. 3 ePrivacy-Richtlinie*	*Einwilligung nötig Datenverarbeitung im Zusammenhang mit entspr. Tools zwar prinzipiell über Art. 6 Abs. 1 lit. e DS-GVO; § 3 BDSG/ LDSG legitimierbar Aber: Cookie Einsatz nicht unbedingt erforderlich i.S.v. Art. 5 Abs. 3 ePrivacy-Richtlinie*

Hinweis: Basiert die Verarbeitung auf Art. 6 Abs. 1 lit. f DS-GVO, sind die Regelungen zum Widerspruchsrecht nach Art. 21 Abs. 1, 4 DS-GVO zu beachten!

16 Siehe II. 1 b) aa).

17 So auch Schulz, a.a.O.

18 Vgl. etwa Pressemeldung des LfDI BW vom 09.10.2019 „Zum Einsatz von Cookies und Cookie-Bannern – was gilt es bei Einwilligungen zu tun (EuGH-Urteil „Planet49")?", die sich ohne nähere Erläuterung unmittelbar auf Art. 5 Abs. 3 ePrivacy-Richtlinie bezieht.

19 Urteil 28.05.2020 – I ZR 7/16 (Cookie-Einwilligung II).

20 Vgl. hierzu im Einzelnen vorstehend unter II. 1. b) bb).

21 So auch die Art.-29-Datenschutzgruppe, „Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht" (WP 194), S. 11 f.

22 Zur Funktionsweise des Browser-Fingerprintings vgl. oben unter I.

23 Auszug aus einer umfassenderen Tabelle aus Schwartmann/Benedikt/Reif, Datenschutz und ePrivacy bei Websites, Social Media und Messengern, 1. Auflage 2020, Abschnitt 4.6.

IV. Referentenentwurf für ein Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG)

Das Bundesministerium für Wirtschaft und Energie plant offenbar die Schaffung eines Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG).[24] Das geplante Gesetz dient der Umsetzung der ePrivacy-Richtlinie (2002/58/EG) in der Fassung der Richtlinie 2009/136/EG („Cookie"-Richtlinie). Das Nebeneinander von DS-GVO, TMG und TKG führe zu Rechtsunsicherheiten bei Verbrauchern, die Telemedien und elektronischen Kommunikationsdienste nutzen, bei Anbietern von diesen Diensten und bei den Aufsichtsbehörden. Der Gesetzentwurf solle insoweit für Rechtsklarheit sorgen.

Das neue TTDSG soll die Bestimmungen enthalten, die bisher in den §§ 88-107 TKG zur Umsetzung der ePrivacy-Richtlinie (2002/58/EG) enthalten waren, sowie weitere Bestimmungen, die bisher dort geregelt sind und die nicht durch die DS-GVO ersetzt wurden. Darüber hinaus werden die TMG-Datenschutzregelungen, soweit diese durch die DS-GVO unberührt geblieben sind, im neuen TTDSG geregelt. Im Übrigen werden die TMG-Datenschutzvorschriften aufgehoben.

Zudem soll eine Rechtsgrundlage für die Anerkennung und Tätigkeit von Diensten zur Verwaltung persönlicher Informationen (Personal Information Management Services – PIMS) als Ansatz einer „Datentreuhand" geschaffen werden. § 3 TTDSG-E regelt insofern, dass Endnutzer ihre Rechte nach diesem Gesetz auch über anerkannte Dienste, die die Verwaltung persönlicher Informationen anbieten, ausüben können. Dies gilt insbesondere für die Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten sowie in das Speichern von Informationen auf Endeinrichtungen und den Zugriff auf Informationen, die bereits auf Endeinrichtungen gespeichert sind. Die Norm geht auf eine Forderung der Datenethikkommission zurück, die im Grundsatz ebenso von Verbraucherschutz- wie Wirtschaftsverbänden unterstützt wird. Ein anerkannter Anbieter soll per PIMS die Einwilligungseinstellungen der Nutzer per Single-Sign-On (SSO) übernehmen und die Einwilligungseinstellungen mit deren Einverständnis an Diensteanbieter (Anbieter von Telemediendiensten) weiterleiten. So entstünde für den Nutzer über den treuhänderisch agierenden SSO-Dienst ein einwilligungsbasierter Kundenkontakt zum Diensteanbieter unter Vermeidung ständig erneut zu erteilender Einwilligungen. Der Ansatz ist datenschutzrechtlich und wirtschaftspolitisch wichtig, weil er dazu führen kann, die Log-ins über Facebook, Google und zunehmend Apple – insofern nach der Vorgabe des EuGH in Schrems II (Urteil vom 16.07.2020 – Rechtssache C-311/18) – in die Hände europäischer Dienste zu legen. Der Entwurf schränkt den Kreis der PIMS-Anbieter auf solche ohne wirtschaftliches Interesse ein. Damit der Kreis der Anbieter von PIMS nicht unzulässig verengt wird, sollte klargestellt werden, dass nur ein Verdienen an der Nutzung der Daten gemeint ist, nicht aber an der Verwaltung.[25]

§ 9 TTDSG-E enthält eine Regelung zum Einsatz von Cookies und vergleichbaren Technologien. Danach ist das Speichern von Informationen auf Endeinrichtungen des Endnutzers oder der Zugriff auf Informationen, die bereits in seinen Endeinrichtungen des Endnutzers gespeichert sind, grundsätzlich nur erlaubt, wenn der Endnutzer darüber gemäß DS-GVO informiert wurde und er eingewilligt hat (§ 9 Abs. 1 TTDSG-E). Ausnahmen vom Einwilligungserfordernis nennt § 9 Abs. 2 TTDSG-E. Das Einwilligungserfordernis besteht nicht, sofern die Speicherung von bzw. der Zugriff auf Informationen

- technisch erforderlich ist, um eine Kommunikation über ein elektronisches Kommunikationsnetz zu übermitteln oder um Telemedien bereitzustellen, deren Inanspruchnahme vom Endnutzer gewünscht wird (Nr. 1),
- vertraglich ausdrücklich mit dem Endnutzer vereinbart wurde, um bestimmte Dienstleistungen zu erbringen (Nr. 2), oder
- zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist (Nr. 3).

Der Nutzer soll seine Einwilligung auch mittels Browser-Einstellungen (§ 9 Abs. 4 TTDSG-E) oder, wie oben bereits angesprochen, über einen PIMS-Anbieter (§ 3 TTDSG-E) abgeben können. Diese Regelung soll die Benutzerfreundlichkeit erhöhen und die bisherige Flut an Cookie-Bannern reduzieren. Der Vorschlag, Einwilligungen des Nutzers zentral einzuholen, wurde bereits im Gesetzgebungsverfahren zur ePrivacy-VO diskutiert, zuletzt aber wieder gestrichen.

Ungeklärt bleibt auch nach dem Entwurf des TTDSG die Frage, unter welchen Umständen Cookies und ähnliche Technologien „technisch erforderlich" sind. Schafft der Gesetzgeber hier keine Klarstellung und nimmt z.B. Verarbeitungen für Zwecke der Reichweitenmessung vom Einwilligungserfordernis aus, bleibt es bei der Rechtsunsicherheit auf Seiten der Verantwortlichen.

Eine weitere Änderung ist bei den Aufsichtsbehörden vorgesehen. § 27 TTDSG-E ordnet die bisherige geteilte Aufgabenwahrnehmung zwischen BNetzA, BfDI und den Datenschutzaufsichtsbehörden der Länder neu. Der Bereich des Internetdatenschutzes soll künftig in Deutschland beim BfDI zentralisiert werden. Bisher sind die Datenschutzaufsichtsbehörden der Länder für den Vollzug des internetspezifischen Datenschutzrechts zuständig, soweit der Verantwortliche z.B. Websites oder Apps betreibt.

V. Fazit und Ausblick

Damit ist der Bogen von der Zulässigkeit in der unterschiedlichen Lesart von DSK und BGH bis hin zum Entwurf des TTDSG gespannt. Auf diesem Entwurf liegen hohe Erwartungen. Er muss sich nicht nur in die bevorstehende ePrivacy-Verordnung einfügen, sondern auch in sich stimmig sein. Denkt man an § 3 TTDSG-E, so fragt sich, was die dort vorgesehene freiwillige Akkreditierung

24 Vgl. Heise Meldung vom 03.08.2020, inklusive Link zum geleakten Referentenentwurf.

25 Mit dieser Differenzierung Abschlussgutachten der Datenethikkommission (2019), S. 133 ff. (134).

von sog. PIMS für europäische Anbieter wie netID oder VERIMI bewirken soll. Die Log-ins der GAFA-Unternehmen sind faktisch nichts anderes als „Anti-PIMS" mit unreguliertem und datenschutzrechtlich fragwürdigem Zugriff auf Nutzerdaten durch Datengiganten. Anders als nach der Idee des TTDSG steuern diese den Zugang zum Nutzer und gerade nicht umgekehrt. Wenn eine Akkreditierung ihren Zweck erfüllen soll, muss die Einhaltung des EU-Datenschutzes und dessen Überprüfung auch für Facebook & Co. verpflichtend sein. Dienste ohne Akkreditierung müssten entweder sanktioniert werden oder gar nicht die Rolle eines Datentreuhänders übernehmen können. Bleibt es bei der aktuellen Entwurfsfassung, gibt die Akkreditierung des § 3 TTDSG-E den rechtstreuen europäischen Anbietern von PIMS Steine statt Brot. Die nicht akkreditierte transatlantische Konkurrenz würde ihr Geschäft ungestört weiter betreiben können, während rechtstreue europäische Dienste ihr Image ohne messbaren Nutzen durch eine freiwillige Anerkennung durch den BfDI aufpolieren könnten. In § 3 TTDSG-E tritt aber noch eine weitere Schwäche zu Tage. Er stellt nämlich nur klar, dass Nutzer per Browser in die Aufzeichnung ihres Onlineverhaltens einwilligen können. Wenn die Norm ihren Zweck erfüllen soll, „Click-Fatigue" zu verhindern, dann muss sie vorgeben, dass das Ablehnen von Tracking im Browser ebenso verbindlich ist. Anderenfalls würden Nutzer, die umfassendes Tracking ablehnen, auch künftig ständig „Cookie-Banner" wegklicken müssen, die das Gesetz unterbinden soll.[26]

Kritisch sind auch die im Entwurf genannten Regelungen zur Einwilligung nach § 9 TTDSG-E. Der Gesetzgeber sollte konkretisieren, welche Anwendungsfälle vom Einwilligungserfordernis ausgenommen sind. Ansonsten ist zu befürchten, dass Verantwortliche aus Rechtsunsicherheit weiterhin im Zweifel auf „Cookie-Banner" zurückgreifen werden. Außerdem sollte berücksichtigt werden, dass schon heute viele Online-Anwendungen ohne Browser auskommen. Beispielsweise verwenden Apps, Smart-Home-Anwendungen, Connected Car und sonstige IoT-Lösungen ausschließlich gerätespezifische Identifier, sodass Cookies keine Rolle mehr spielen. Der Gesetzgeber sollte vor diesem Hintergrund klarstellen, unter welchen Umständen der Zugriff auf oder das Speichern von Informationen auf Endeinrichtungen technisch erforderlich ist. Wünschenswert wäre eine Regelung, die einerseits die wirtschaftlichen Interessen des Verantwortlichen, anderseits das Interesse der Allgemeinheit an Produktverbesserung- und Entwicklung berücksichtigt, um technische Innovationen in Europa zu fördern.

Prof. Dr. Rof Schwartmann
ist Leiter der Kölner Forschungsstelle für Medienrecht, Technische Hochschule Köln, sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn. Zugleich ist er Mitglied im Stiftungsrat der European netID Foundation.

Kristin Benedikt
ist Richterin am Verwaltungsgericht Regensburg.

RAin Yvette Reif, LL.M.
ist stellvertretende Geschäftsführerin der GDD.

Die Autoren dieses Aufsatzes sind zugleich Autoren des kürzlich im Datakontext Verlag erschienen Praxisratgebers „Datenschutz und ePrivacy bei Websites, Social Media und Messengern" (ISBN 978-3-89577-854-4, 1. Auflage 2020).

26 https://netzpolitik.org/2020/online-tracking-lebensverlaengernde-massnahmen-fuer-ein-kaputtes-geschaeftsmodell/.

Stand: *28. August 2020*