Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

2
K&R

19. Jahrgang Februar 2016 Seiten 73 – 144

dfv Mediengruppe · Frankfurt am Main

RA Dr. Bernd Schmidt, LL.M. (Auckland), Hamburg und RA Tobias Babilon, Bonn*

Anforderungen an den Einsatz von Cookies, Browser-Fingerprinting und ähnlichen Techniken im deutschen Recht

Tracking-Technologien und die Nutzung von Tracking-Daten ermöglichen die Erkennung und Verfolgung von Endgeräten im Netz. Rechtliche Anforderungen an den Einsatz von Cookies als „klassischer Tracking-Technologie" werden in der Literatur schon lange diskutiert und auch die Diskussion um die Zulässigkeit „moderner Tracking-Technologien", wie des Browser-Fingerprintings, hat bereits begonnen. Auf europäischer Ebene fordert die E-Privacy-Richtlinie[1] in der durch die sogenannte Cookie-Richtlinie[2] geänderten Fassung von Webseitenbetreibern, eine Einwilligungserklärung der Nutzer einzuholen (Opt-in), wenn sie Tracking-Technologien einsetzen. Die Umsetzungsfrist für die Cookie-Richtlinie ist seit Mai 2011 abgelaufen, ohne dass es in Deutschland zu einer Änderung oder Ergänzung des Telemediengesetzes (TMG) gekommen ist. Für Webseitenbetreiber stellt sich die Frage, welche Rechtspflichten beim Einsatz von Tracking-Technologien gelten.

I. Tracking-Technologien

Tracking-Technologien ermöglichen es, Endgeräte und deren Nutzer (wieder) zu erkennen und deren Surfverhalten im Netz auch über den Besuch der eigenen Webseite hinaus weiterzuverfolgen. Mit Tracking-Daten lassen sich Interessens- und Verhaltensmuster erkennen und entsprechende Nutzerprofile erstellen, etwa um den Nutzern gezielt Werbung einzublenden.[3] Darüber hinaus ergeben sich weitere Anwendungsmöglichkeiten, etwa im Bereich Fraud Prevention.

1. Klassisches Cookie-basiertes Tracking

„Klassisch" werden zum Tracking Cookies verwendet, die auf dem Endgerät des Nutzers gesetzt werden und es ermöglichen, Endgeräte unmittelbar zuzuordnen und wiederzuerkennen, wenn mit diesen auf eine Webseite zugegriffen wird. Der technische Hintergrund des Trackings mit Cookies ist in der Literatur eingehend dargestellt[4] und soll an dieser Stelle nicht weiter vertieft werden.

Nutzer können das Tracking mit Cookies leicht verhindern, indem sie Cookies löschen oder ihren Browser so konfigurieren, dass Cookies nicht installiert werden. Dies ist bei „klassischen" Cookies mit Standard-Webbrowsern ohne viel Aufwand und vertiefte Kenntnisse möglich.

2. Moderne Tracking-Technologien ohne notwendigen Cookie-Einsatz

Zunehmend wird das klassische Tracking mit Cookies durch modernere Tracking-Technologien ersetzt, wie das Browser-Fingerprinting, Canvas-Fingerprinting oder Clock-Skew-Fingerprinting.[5] Bei modernen Tracking-Technologien müssen keine Informationen auf dem Endgerät des Users hinterlegt werden. Stattdessen werden Informationen ausgelesen, die das Endgerät beim Besuch einer Webseite ohnehin sendet oder abrufbar macht und die sonst insbesondere genutzt werden, um eine optimierte Darstellung der Webseite zu ermöglichen, wie Browsertyp, Betriebssystem, installierte Plugins, Bildschirmauflösung, Spracheinstellung, Zeitzone, Header-Einstellungen oder Zeitstempel für gesendete TCP-Pakete.[6]

Aus diesen Informationen kann ein Webseitenbetreiber durch den Einsatz von Trackingtools einen Hashwert generieren, den sog. Fingerprint. Der Fingerprint ermöglicht in den meisten Fällen eine eindeutige Zuordnung und Wiedererkennung des Endgeräts, ohne dass der User dies wirksam verhindern kann. Diese Methoden weisen Schwächen auf, wenn erhobene Informationen nicht zu einem eindeutigen Fingerprint führen, etwa bei der Erkennung mobiler Endgeräte, deren Browser wenige oder keine Konfigurationsmöglichkeiten bieten. Ähnliche Schwächen bestehen beim Browser-Fingerprinting bei der Erkennung neu installierter und noch nicht konfigurierter Browser sowie bei Änderungen der erfassten Informationen, etwa einer bloßen Aktualisierung der Browserversion.[7] Die Erkennungsraten sollen aber dennoch immerhin zwischen 89 und 93 % liegen.[8]

---

* Dr. Bernd Schmidt, LL.M. ist Rechtsanwalt und Partner bei PLANIT // LEGAL in Hamburg, Tobias Babilon ist Rechtsanwalt bei Scheja & Partner in Bonn. Der Beitrag enthält die weiterentwickelte Fassung eines Vortrags, den die Autoren auf der DSRI-Herbstakademie 2015 in Göttingen gehalten haben; vgl. Schmidt/Babilon in Taeger (Hrsg.), Tagungsband Herbstakademie 2015, 2015, S. 473. Mehr über die Autoren erfahren Sie auf S. VIII.

1 RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12. 7. 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

2 RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25. 11. 2009 zur Änderung der RL 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

3 Vgl. hierzu *Alich/Voigt*, CR 2012, 344 ff.; *Stiemerling/Lachenmann*, ZD 2014, 133, 135.

4 *Alich/Voigt*, CR 2012, 344, 345; *Rammos*, in: Taeger (Hrsg.), Die Welt im Netz – Folgen für Wirtschaft und Gesellschaft, 2011, S. 493, 494 f.; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG, Rn. 4; *Steinhoff*, in: Taeger (Hrsg.), Law as a Service (LaaS), 2013, S. 143, 144 f.; *Stiemerling/Lachenmann*, ZD 2014, 133, 135 f.; *Voigt*, in: Taeger (Fn. 4), S. 157, 160; BVDW Whitepaper Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, http://www.bvdw.org/medien/browsercookies-und-alternative-tracking-technologien-technische-und-datenschutzrechtliche-aspekte?media=7007, S. 5 f.

5 Für eine Übersicht moderner Tracking-Technologien siehe *Puscher*, c't 2014, Heft 11, S. 160; *Zeidler/Brüggemann*, CR 2014, 248, 251 f.; BVDW Whitepaper (Fn. 4), S. 13 ff.; zum Canvas Fingerprinting siehe *Dieterich*, ZD 2015, 199 und *Braun*, c't 2014, Heft 18, S. 36 f.; zum Clock-Skew-Fingerprinting siehe *Hense/Rengers*, in: Taeger (Hrsg.), Tagungsband 2014, 2014, S. 219, 223.

6 Vgl. *Alich/Voigt*, CR 2012, 344, 345 und *Puscher*, c't 2014, Heft 11, S. 160; BVDW Whitepaper (Fn. 4), S. 13 ff.; zur Methodik beim sog. Canvas Fingerprinting siehe *Dieterich*, ZD 2015, 199, 200.

7 Vgl. BVDW Whitepaper (Fn. 4) S. 14 f.

8 Vgl. *Braun*, c't 2014, Heft 18, S. 36; Dieterich, ZD 2015, 199, 200; *Stiemerling/Lachenmann*, ZD 2014, 133, 135.

Das Deaktivieren von Cookies zur Verhinderung des Tracking beim Einsatz moderner Tracking-Technologien ist wirkungslos, da diese nicht mehr auf Cookies angewiesen sind. Vielmehr wird durch eine entsprechende Konfiguration des Browsers dessen Individualität sogar noch erhöht und damit auch die Zuverlässigkeit der Wiedererkennung.[9] Für den User gibt es insofern keine einfach umzusetzenden Maßnahmen, um Tracking-Aktivitäten wirksam zu verhindern, jedenfalls nicht ohne signifikante Einbußen im Hinblick auf den Funktionsumfang der aufgerufenen Seiten und Dienste hinzunehmen (wie etwa bei vollständigem Verzicht auf Java-Script).[10]

II. Europäischer Rechtsrahmen

Der europäische Rechtsrahmen für die Nutzung von Tracking-Technologien ergibt sich aus Art. 5 Abs. 3 der E-Privacy-Richtlinie (in der durch die Cookie-Richtlinie geänderten Fassung). Dort ist geregelt, dass „die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen […] seine Einwilligung gegeben hat."

1. Klassisches Cookie-basiertes Tracking

Tracking-Cookies sind bzw. enthalten auf dem Endgerät des Nutzers gespeicherte Informationen gemäß Art. 5 Abs. 3 S. 1 E-Privacy-Richtlinie.[11] Die Mitgliedstaaten müssen daher gemäß Art. 5 Abs. 3 E-Privacy-Richtlinie Webseitenbetreiber verpflichten, ihre Nutzer klar und umfassend über den Einsatz von Tracking-Cookies zu informieren und Tracking-Cookies nur zu platzieren, wenn der Nutzer zuvor seine Einwilligung erklärt hat (Opt-in).

Eine Ausnahme von dem Einwilligungsvorbehalt darf gemäß Art. 5 Abs. 3 S. 2 E-Privacy-Richtlinie nur für Cookies vorgesehen werden, die „[…] unbedingt erforderlich [sind], um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen." Diese Ausnahme gilt z. B. für Session-Cookies eines Online-Shop-Betreibers zur Speicherung des Inhalts eines Warenkorbs oder zur Speicherung der Spracheinstellungen.[12]

Für Tracking-Cookies ist diese Ausnahme in aller Regel nicht einschlägig,[13] da sie der Verfolgung von Endgeräten und z. B. der gezielten Einblendung von Werbung dienen. Sie sind daher nicht unbedingt erforderlich, um den Dienst der Informationsgesellschaft (die Webseite) zur Verfügung zu stellen.

2. Modernes nicht-Cookie-basiertes Tracking

Der umgangssprachliche Name „Cookie-Richtlinie" suggeriert, dass die Anforderungen gemäß Art. 5 Abs. 3 E-Privacy-Richtlinie nur für klassische, Cookie-basierte Tracking-Technologien gelten. Teilweise wird daher angenommen, der Einsatz moderner Tracking-Technologien finde in einem juristischen Graubereich statt, der jedenfalls nicht eindeutig von der E-Privacy-Richtlinie erfasst werde.[14]

Gegen diese Ansicht sprechen jedoch die bewusst technikneutrale Gestaltung der Cookie-Richtlinie[15] und der klare Wortlaut des Art. 5 Abs. 3 E-Privacy-Richtlinie, der auf „Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind" abstellt. Art. 5 Abs. 3 E-Privacy-Richtlinie ist damit geradezu maßgeschneidert für moderne Tracking-Technologien. Ein Fingerprint im oben erläuterten Sinne besteht nämlich aus einer Vielzahl von Informationen, die im Endgerät des Nutzers gespeichert sind, wie Details der Browserkonfiguration beim Browser-Fingerprinting. Art. 5 Abs. 3 E-Privacy-Richtlinie ist daher auch für moderne Tracking-Technologien anwendbar und verpflichtet die Mitgliedsstaaten, nationale Regelungen zu schaffen, nach denen Webseitenbetreiber beim Einsatz von Tracking-Technologien Opt-in-Mechanismen implementieren müssen.[16]

3. Anforderungen an Informationspflichten und Einwilligungsvorbehalt

Für Webseitenbetreiber ist im Ergebnis entscheidend, wie sie ihre Informationspflichten erfüllen und einen Einwilligungsvorbehalt technisch umsetzen können. Die Artikel 29 Gruppe hat sich hierzu wiederholt geäußert und ihr Verständnis der Pflichten aus Art. 5 Abs. 3 E-Privacy-Richtlinie dargestellt.[17]

Nach Ansicht der Artikel 29 Gruppe muss der Webseitenbetreiber den Nutzer vor der Platzierung von Cookies darüber informieren und der Nutzer muss seine Zustimmung zur Platzierung von Cookies frei von Zwang durch ein aktives Verhalten äußern.[18] Um die Informationspflicht zu erfüllen, könnten Webseitenbetreiber z. B. einen Banner einblenden, sowie einen Link zu weiterführenden Informationen zu den platzierten Cookies, den erhobenen Daten und den verfolgten Zwecken bereitstellen.

Der Nutzer kann seine Einwilligung etwa erklären, indem er eine Schaltfläche oder einen Link anklickt und dadurch aktiviert. Verweilt der Nutzer lediglich auf der Webseite, ist dies hingegen mangels aktiven Verhaltens wohl keine Erklärung der Einwilligung.[19] Denkbar ist nach Einschätzung der Artikel 29 Gruppe auch, dass der Nutzer seine Einwilligung durch das entsprechende Konfigurieren des Browsers erklärt. Lässt der Nutzer lediglich die Standardeinstellungen seines Browsers unverändert, soll dies jedoch keine Erklärung der Einwilligung sein.[20]

III. Deutscher Rechtsrahmen

Ausgangspunkt der Bewertung der Pflichten von Webseitenbetreibern nach deutschem Recht sind die Regelungen des TMG, die den von der E-Privacy-Richtlinie gesetzten Rahmen ausfüllen. Nach dem Inkrafttreten der Cookie-

9 Vgl. *Alich/Voigt*, CR 2012, 344, 345.
10 Art. 29 Gruppe, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (Art. 29 Gruppe, WP 224), S. 7; vgl. BVDW Whitepaper (Fn. 4), S. 14, 18 und 21.
11 Art. 29 Gruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. 6. 2010 (Art. 29 Gruppe, WP 171), S. 10; Art. 29 Gruppe Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies (Art. 29 Gruppe, WP 208), S. 2.
12 Art. 29 Gruppe, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht (Art. 29 Gruppe, WP 194), S. 6 ff.; *Rauer/Ettig*, ZD 2014, S. 27, 29.
13 Art. 29 Gruppe, WP 194 (Fn. 12), Ziffer 2.4/S. 6 und Ziffern 4.1 ff./S. 9 ff.; *Schürmann*, in: Taeger (Fn. 4), 2013, S. 797, 801.
14 *Puscher*, c't 2014, Heft 11, S. 160.
15 *Schürmann*, in: Taeger (Fn. 4) S. 797.
16 Vgl. Art. 29 Gruppe, WP 224 (Fn. 10), S. 7 f.; Art. 29 Gruppe, WP 194 (Fn. 12), Ziffer 1/S. 1.
17 Art. 29 Gruppe, WP 171 (Fn. 11), S. 10; Art. 29 Gruppe WP 208 (Fn. 11); Art. 29 Gruppe, WP 224 (Fn. 10).
18 Art. 29 Gruppe, WP 208 (Fn. 11), S. 3 f.
19 Art. 29 Gruppe, WP 208 (Fn. 11), S. 5.
20 Art. 29 Gruppe, WP 208 (Fn. 11), S. 4 f.; a. A. BVDW Whitepaper (Fn. 4), S. 11, wonach i.V. m. einem hinreichend klaren und eindeutigen Hinweis ein bloßes „Weitersurfen" als konkludente Einwilligungserteilung denkbar sei.

Richtlinie gab es zwei Gesetzesinitiativen zur Umsetzung der Cookie-Richtlinie. In beiden Entwürfen war vorgesehen, Art. 5 Abs. 3 E-Privacy-Richtlinie inhaltsgleich in einem neuen § 13 Abs. 8 TMG in deutsches Recht umzusetzen.[21] Die Entwürfe wurden jedoch nicht verabschiedet.[22] Zur Bewertung von telemedienrechtlichen Pflichten von Webseitenbetreibern beim Einsatz von Tracking-Technologien ist damit weiter von den „alten" Regelungen im TMG auszugehen, wie sie bereits vor Inkrafttreten der Cookie-Richtlinie bestanden.

1. Informationspflicht und Personenbezug von Tracking-Daten

Entsprechend der europarechtlichen Grundlage in Art. 5 Abs. 3 E-Privacy-Richtlinie regulieren auch die datenschutzrechtlichen Bestimmungen des TMG technikneutral das Nutzertracking und insbesondere die darauf basierende Erstellung von Nutzungsprofilen.[23]

Nach deutschem Recht ergibt sich für Webseitenbetreiber, die Tracking-Technologien einsetzen, aus § 13 Abs. 1 TMG unabhängig von der eingesetzten Technologie die Pflicht, „[…] den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten […] in allgemein verständlicher Form zu unterrichten […]", indem er den Einsatz von Tracking-Technologien in der Datenschutzerklärung beschreibt und die Datenschutzerklärung auf der Webseite zum Abruf bereithält. Diese Informationspflicht besteht auch, wenn Daten des Nutzers zunächst ohne Personenbezug erhoben werden, dieser aber nachträglich durch den Dienstanbieter hergestellt werden kann.[24]

Tracking-Daten sind in vielen Fällen personenbezogen. Dies hat zur Folge, dass Webseitenbetreiber auf den Einsatz von Tracking-Technologien hinweisen müssen. Gemäß § 3 Abs. 1 BDSG sind Daten personenbezogen, wenn sie „[…] Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person […]" enthalten. Mit anderen Worten, wenn sie einer Person zugeordnet werden können.

Cookie-Daten sind zwar nicht *per se* personenbezogen.[25] Vielmehr ist ein Cookie eine Art Speicherbehälter für Informationen, die als Identifikatoren zur Zuordnung eines Nutzungsprofils dienen und dabei personenbezogen sein können, aber nicht müssen.[26] Ein Personenbezug bzw. eine Personenbeziehbarkeit ist aber jedenfalls gegeben, wenn der Webseitenbetreiber Cookie-Daten mit weiteren Daten über den Nutzer verknüpfen und so selbst den Personenbezug herstellen kann.[27] Dies ist z. B. der Fall, wenn der Webseitenbetreiber E-Mailadressen bei der Registrierung für einen Newsletter speichert oder Adressdaten bei einer Onlinebestellung. In diesen Fällen stellen Cookie-Daten Pseudonyme im Sinne des § 3 Abs. 6 a BDSG dar und sind für den Webseitenbetreiber personenbezogen bzw. personenbeziehbar.[28]

Wie Cookie-Daten enthalten Browser-, Canvas- und ähnliche Fingerprints technische Informationen, die einzeln keinen Rückschluss auf den Nutzer ermöglichen.[29] Im Ergebnis sind Fingerprints, nicht anders als Cookie-Daten, jedenfalls dann personenbezogen bzw. personenbeziehbar, wenn der Webseitenbetreiber Zusatzinformationen hat, mit denen er eine Zuordnung zu der Person oder Personengruppe, herstellen kann.[30]

Im Zusammenhang mit der Erstellung der Fingerprints wird regelmäßig auch die IP-Adresse erfasst. Sofern man mit den Datenschutzaufsichtsbehörden einen absoluten oder objektiven Begriff der Personenbeziehbarkeit zugrunde legt, wären jedenfalls solche Tracking-Daten personenbeziehbar[31] und deren „Behandlung als personenbezogene Daten geboten".[32] Nach dieser Ansicht der Aufsichtsbehörden müsste daher stets auf den Einsatz von Tracking-Technologien in der Datenschutzerklärung hingewiesen werden. Zur Vermeidung rechtlicher Risiken ist dies zu empfehlen.

2. Erstellung pseudonymer Profile für Werbezwecke und Opt-out

Aus § 15 Abs. 3 TMG folgt, dass Webseitenbetreiber Tracking-Daten zu Werbezwecken in pseudonymen Profilen erheben, speichern und verarbeiten dürfen, soweit der Nutzer nicht widersprochen hat (Opt-out).[33] Soweit Nutzer der Erstellung von Nutzerprofilen widersprechen, müssen Webseitenbetreiber sicherstellen, dass sie von diesen Nutzern ab diesem Zeitpunkt keine Profile mehr erstellen.

Für Cookie-basiertes Tracking müssen Webseitenbetreiber in der Datenschutzerklärung auf die Möglichkeit zur Deaktivierung von Cookies hinweisen. Mit der Deaktivierung können die Nutzer dann erklären, dass sie mit dem Setzen von Cookies nicht einverstanden sind und von ihrem Recht zum Opt-out Gebrauch machen. Eine weitere Möglichkeit zur Erklärung des Opt-out zum Einsatz von (Tracking-)Cookies ist z. B. der „Präferenz-Manager" des Bundesverbands Digitale Wirtschaft e. V., mit dem Nutzer gegenüber den angeschlossenen Unternehmen erklären können, welche Cookies sie nicht akzeptieren.[34]

---

21 Gesetzentwurf des Bundesrats BT-Drs. 17/6765; Gesetzentwurf der SPD Bundestagsfraktion BT-Drs. 17/8454, S. 2.

22 Hierzu *Moos*, K&R 2012, 635, 636 f.

23 *Schleipfer*, ZD 2015, 399, 402.

24 *Spindler/Nink*, in: Spindler/Schuster (Fn. 4), Rn. 3.; vgl. Art. 29 Gruppe, WP 224 (Fn. 10), Ziffer 6/S. 8 zur Anwendbarkeit des Art. 5 Abs. 3 E-Privacy-Richtlinie in diesen Fällen.

25 BVDW Whitepaper (Fn. 4), S. 2 ff.

26 *Schleipfer*, ZD 2015, 399, 400.

27 *Spindler*, GRUR Beilage 2014, 101, 105 f.; *Spindler/Nink*, in: Spindler/Schuster (Fn. 4), Rn. 142.

28 *Moos*, K&R 2012, 635; a. A. *Schürmann*, in: Taeger (Fn. 4), S. 797, 811 f.; BVDW Whitepaper (Fn. 4), S. 3; zum Personenbezug von Tracking-Daten für Betreiber von sozialen Netzwerken siehe Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe „Soziale Netzwerke", S. 7 f.

29 Art. 29 Gruppe, WP 224 (Fn. 10), Ziffer 5/S. 5 f.

30 So auch *Alich/Voigt*, CR 2012, 344, 346; *Voigt*, in: Taeger (Fn. 4), S. 157, 165; *Zeidler/Brüggemann*, CR 2014, 248, 253.

31 Vgl. *Alich/Voigt*, CR 2012, 344, 347; Art. 29 Gruppe, WP 224 (Fn. 10), Ziffer 5/S. 6; a. A. für Canvas-Fingerprinting *Dieterich*, ZD 2015, 199, 202; a. A. BVDW Whitepaper (Fn. 4), S. 3, wo davon ausgegangen wird, dass Tracking-Daten jedenfalls für den Anbieter des Tracking-Dienstes im Grunde nie personenbeziehbar seien.

32 So wörtlich zu dynamischen IP-Adressen: „Orientierungshilfe Datenschutz bei IPv6" der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Arbeitskreis Technische und Organisatorische Datenschutzfragen, Version 1.01 vom 26. 10. 2012, S. 12; s. a. „FAQ IP-Adressen und andere Nutzungsdaten" des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Ziffer I.1.; Die Landesbeauftragte für den Datenschutz Niedersachsen zur „Speicherung und Weitergabe von IP-Adressen", Frage 2, http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=27716&article_id=95008&_psmand=48.

33 *Arning/Moos*, ZD 2014, 242, 243; Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. 11. 2009 in Stralsund zur datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten; Der Landesbeauftragte für den Datenschutz Niedersachsen, Orientierungshilfe für Anbieter von Telemedien, S. 5; *Schneider*, http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html; *Steinhoff*, in: Taeger (Fn. 4), S. 143, 147 f.; *Voigt*, in: Taeger (Fn. 4), S. 157, 170.

34 http://meine-cookies.org/cookies_verwalten/praeferenzmanager-beta.html.

Bei modernen Tracking-Technologien sind das Deaktivieren von Cookies und Änderungen der Browser-Einstellungen zwecklos und ggf. sogar kontraproduktiv (s. o.). Die Nutzer haben jedoch die Möglichkeit, gegenüber den Webseitenbetreibern individuell ihren Widerspruch zu erklären. Alternativ kommt z. B. die Aktivierung eines „Do Not Track HTTP-Header-Felds" in Betracht, das von den deutschen Datenschutzaufsichtsbehörden und der Artikel 29 Gruppe als wirksame Opt-out-Erklärung angesehen wird.[35] Darüber hinaus gibt es Mechanismen zur Erklärung des Opt-out für einzelne Tracking-Technologien, wie das Browser-Add-on zur Deaktivierung von Google Analytics.[36]

Webseitenbetreiber können in ihrer Datenschutzerklärung auf die Möglichkeit der Aktivierung des Do Not Track HTTP-Header-Felds (oder abhängig von den eingesetzten Tracking-Technologien auf andere Opt-out Mechanismen) hinweisen und so ihre Pflicht zur Bereitstellung eines wirksamen Opt-out-Mechanismus erfüllen.

IV. Europarechtliche Überlagerung des TMG

Art. 5 Abs. 3 E-Privacy-Richtlinie sieht für den Einsatz von Tracking-Technologien neben einer Informationspflicht ausdrücklich auch die Pflicht zur Implementierung eines Opt-in-Mechanismus vor. Es besteht damit augenscheinlich ein Konflikt zwischen den Anforderungen aus Art. 5 Abs. 3 E-Privacy-Richtlinie und den telemedienrechtlichen Pflichten von Webseitenbetreibern gemäß § 13 Abs. 1 und § 15 Abs. 3 TMG.[37] Umstritten ist, wie sich dies auf die Rechtspflichten von Webseitenbetreibern nach deutschem Recht auswirkt.

1. Einwilligungsvorbehalt nach § 12 Abs. 1 TMG

Die Bundesregierung vertritt in der Antwort auf einen Fragebogen der EU Kommission zur Umsetzung der Cookie-Richtlinie[38] die Ansicht, die Cookie-Richtlinie müsse in Deutschland nicht umgesetzt werden, da sich den Vorgaben des Art. 5 Abs. 3 E-Privacy-Richtlinie entsprechende Einwilligungsvorbehalte bereits aus dem TMG in der aktuellen Fassung ergäben.[39] Konsequenterweise war die Bundesregierung bereits zuvor dem Gesetzentwurf des Bundesrates entgegengetreten,[40] der die Schaffung eines neuen § 13 Abs. 8 TMG mit einer expliziten Opt-in-Pflicht für den Einsatz von Cookies vorgesehen hatte (s. o.).[41]

Die Pflicht der Webseitenbetreiber zur Information der Nutzer folgt nach Auffassung der Bundesregierung aus § 13 Abs. 1 TMG, der Einwilligungsvorbehalt aus §§ 12 und 15 TMG.[42] § 12 TMG stelle nämlich klar, dass der Dienstanbieter personenbezogene Daten nur erheben dürfe, wenn es hierfür eine ausdrückliche gesetzliche Erlaubnis gebe oder der Betroffene eingewilligt habe. Eine gesetzliche Erlaubnis für die Speicherung und den Abruf von Cookies ergebe sich nicht aus dem TMG, insbesondere nicht aus § 15 TMG, so dass Nutzer ihre Einwilligung hierzu erteilen müssten. Die Regelung in Art. 5 Abs. 3 E-Privacy-Richtlinie sei daher im deutschen Recht umgesetzt.[43]

Für Tracking-Cookies und andere Tracking-Technologien überzeugt diese Argumentation jedoch nicht.[44] Zutreffend geht die Bundesregierung zwar in ihrer Argumentation von dem Verbot der Datenverarbeitung mit Erlaubnisvorbehalt in § 12 Abs. 1 TMG aus.[45] Ein Erlaubnistatbestand zur Erhebung von Tracking-Daten ergibt sich jedoch aus § 15 Abs. 3 TMG. Webseitenanbieter dürfen nach dieser Vorschrift nämlich für Zwecke der Werbung und Marktforschung pseudonyme und damit personenbeziehbare Nutzungsprofile erstellen, soweit die Nutzer keinen Widerspruch (Opt-out) erklärt haben.

Insofern vermag die Auslegung der einschlägigen Regelungen des TMG unter Berücksichtigung des eindeutigen Wortlauts die Annahme der Bundesregierung nicht zu stützen, Art. 5 Abs. 3 E-Privacy-Richtlinie sei im deutschen Recht bereits umgesetzt.[46] Nachdem die EU Kommission zunächst der Argumentation der Bundesregierung gefolgt zu sein schien,[47] findet sich nun in einer Untersuchung der EU Kommission zur Umsetzung der E-Privacy-Richtlinie eine sehr distanzierte Haltung gegenüber dieser Auffassung.[48]

2. Richtlinienkonforme Auslegung des TMG

Um den Widerspruch zwischen europäischem und nationalem Recht zu überwinden, kommt eine richtlinienkonforme Auslegung der Vorschriften des nationalen Rechts in Betracht. Umstritten ist, ob § 15 Abs. 3 TMG richtlinienkonform so ausgelegt werden kann, dass sich ein Einwilligungsvorbehalt zum Einsatz von Tracking-Technologien ergibt.

Nach einer Ansicht[49] besteht diese Möglichkeit der richtlinienkonformen Auslegung von § 15 Abs. 3 TMG nicht. Diese Auslegung stünde nämlich im Widerspruch zum klaren Wortlaut des § 15 Abs. 3 TMG, sei nach den Auslegungsregelungen des nationalen Rechts damit keine mögliche Interpretation der Norm und damit einer richtlinienkonformen Auslegung nicht zugänglich.

Nach der Gegenansicht ist eine richtlinienkonforme Auslegung von § 15 Abs. 3 TMG hingegen geboten, mit der Konsequenz, dass sich hieraus ein Einwilligungsvorbehalt für den Einsatz von Tracking-Technologien ergibt.[50] Zur Begründung wird insbesondere auf die Rechtsprechung des BGH verwiesen.[51] Nach dieser Rechtsprechung erfordert das Gebot der richtlinienkonformen Auslegung auch

35 Art. 29 Gruppe, WP 224 (Fn. 10), S. 7; Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Tätigkeitsbericht 2011, S. 169.
36 Abrufbar unter https://tools.google.com/dlpage/gaoptout/?hl=de.
37 BVDW Whitepaper (Fn. 4), S. 11.
38 Questionnaire on Article 5 (3) of the ePrivacy Directive, COCOM11-20.
39 Questionnaire on Article 5 (3) of the ePrivacy Directive, COCOM11-20, 3 - 5.
40 BT-Drs. 17/6765, S. 14 - 15; siehe auch BT-Drs. 17/5707, S. 3.
41 BR-Drs. 156/11.
42 Questionnaire on Article 5 (3) of the ePrivacy Directive, COCOM11-20, 3 - 5.
43 Questionnaire on Article 5 (3) of the ePrivacy Directive, COCOM11-20, 4 f.
44 So auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung zur Verfolgung des Nutzerverhaltens im Internet; Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis) zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste vom 24./25. 11. 2010; *Rauer/Ettig*, ZD 2014, 27; *Schröder*, in: Taeger (Fn. 4), S. 173, 174; *Schürmann*, in: Taeger (Fn. 4), S. 797.
45 So auch *Moos*, in Taeger/Gabel, BDSG, 2. Aufl. 2013 § 12 TMG, Rn. 5.
46 So auch *Dieterich*, ZD 2015, 199, 202; siehe auch *Moos*, K&R 2012, 635, 635, 640.
47 *Piltz*, http://www.delegedata.de/2015/02/deutsche-datenschutzbehoerden-mangelnde-umsetzung-cookie-richtlinie-in-deutschland-nicht-hinnehmbar/; *Schneider*, http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html; *Schneider*, http://www.telemedicus.info/article/2722-Die-Stellungnahme-der-Bundesregierung-zur-Cookie-Richtlinie.html; BVDW Whitepaper (Fn. 4), S. 11.
48 „When looking at the way Article 5.3 has been transposed by the Member States, a first observation to make is that this provision has not been transposed by the German legislature." ePrivacy Directive: assessment of transposition and compatibility with proposed Data Protection Regulation, S. 63; siehe hierzu http://www.telemedicus.info/article/2965-Cookie-Richtlinie-Das-Imperium-schlaegt-zurueck.html.
49 *Moos*, K&R 2012, 635, 637 f.
50 *Schmitz*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 41. Aufl. 2015, Rn. 275 ff.
51 BGH, 21. 11. 2008 – VIII ZR 200/05, NJW 2009, 427, 429.

eine richtlinienkonforme Rechtsfortbildung.[52] Diese Auffassung kann jedoch nicht überzeugen. Nach der Rechtsprechung des EuGH zur richtlinienkonformen Auslegung sind die nationalen Gerichte verpflichtet, bei der Auslegung der nationalen Gesetze den Wortlaut und Zweck europäischer Richtlinien zu berücksichtigen, um im Rahmen der Auslegungsmethoden des nationalen Rechts die Ziele der Richtlinie zu erreichen.[53]

Die Grenze der Auslegung des nationalen Rechts ist jedoch erreicht, wenn sie dem Zweck der Regelung des nationalen Rechts entgegensteht (*contra legem* Grenze).[54] Dies ist hier der Fall. § 15 Abs. 3 TMG dient dem Zweck für den Nutzer Transparenz zu schaffen[55] und ihn über sein Recht zum Widerruf der Verwendung seiner Daten zu informieren (Opt-out). Die Annahme, Webseitenbetreiber müssten vor dem Einsatz von Tracking-Technologien eine Einwilligung der Nutzer einholen (Opt-in), verstößt gegen diese Wertung.

Zwar ist mit dem BGH davon auszugehen, dass die richtlinienkonforme Auslegung auch zur richtlinienkonformen Rechtsfortbildung (Analogiebildung) verpflichtet.[56] Dies führt jedoch nicht zu einer anderen Bewertung. Eine solche Rechtsfortbildung setzt nämlich eine planwidrige Regelungslücke voraus.[57] Die Annahme, der Gesetzgeber habe bei der Regelung in § 15 Abs. 3 TMG planwidrig vergessen, eine Einwilligungspflicht (Opt-in) für die Bildung von pseudonymen Nutzerprofilen zu begründen, ist jedoch fernliegend. § 15 Abs. 3 TMG setzt nämlich die E-Privacy-Richtlinie in der Fassung vor Inkrafttreten der Cookie-Richtlinie um, in der kein Einwilligungsvorbehalt vorgesehen war.

3. Direkte Anwendbarkeit von Art. 5 Abs. 3 E-Privacy-Richtlinie

In einer Stellungnahme auf dem 13. Deutschen Datenschutzkongress hat der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, die Ansicht vertreten, Art. 5 Abs. 3 E-Privacy-Richtlinie sei in Deutschland unmittelbar anwendbar.[58] Diese Ansicht wird auch von den Datenschutzaufsichtsbehörden[59] und in der Literatur[60] vertreten.

Die direkte Anwendbarkeit einer EU-Richtlinie setzt nach der Rechtsprechung des EuGH voraus, dass die Richtlinie innerhalb der Umsetzungsfrist nicht oder nur unvollständig in nationales Recht umgesetzt wurde und dass der Regelungsgehalt genau bestimmbar ist.[61] Die Umsetzungsfrist für die E-Privacy-Richtlinie in der durch die Cookie-Richtlinie geänderten Fassung ist am 25. 5. 2011 abgelaufen und der deutsche Gesetzgeber hat seitdem keine Regelung zur Umsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie geschaffen.

Art. 5 Abs. 3 E-Privacy-Richtlinie ist auch hinreichend bestimmt, um unmittelbar angewendet zu werden.[62] Hierfür ist es nämlich nicht erforderlich, dass die Norm frei von jeglichem Auslegungsspielraum ist. Die Frage nach der technischen Ausgestaltung des Opt-in-Mechanismus nach Art. 5 Abs. 3 E-Privacy-Richtlinie steht der direkten Anwendbarkeit daher nicht entgegen. Für die Annahme der hinreichenden Bestimmtheit von Art. 5 Abs. 3 E-Privacy-Richtlinie spricht darüber hinaus auch die Tatsache, dass die Regelung in vielen Mitgliedsstaaten (fast) wortgleich in nationales Recht übertragen wurde.

Die direkte Anwendbarkeit von Art. 5 Abs. 3 E-Privacy-Richtlinie begründet jedoch nur eine Verpflichtung des Staates gegenüber seinen Bürgern. Der Zweck der direkten Anwendbarkeit von Richtlinien bei fehlender oder ungenügender Umsetzung in nationales Recht ist es nämlich zu verhindern, dass der Staat von der Nichtbeachtung europarechtlicher Vorgaben zu Lasten seiner Bürger profitiert.[63] Bürger können sich somit dem Staat gegenüber unmittelbar auf die Vorgabe der Richtlinie berufen und aus ihr konkrete Ansprüche ableiten. Staatliche Stellen wie Bundes- und Landesbehörden dürfen folglich auch ohne erfolgte Umsetzung der Vorgabe des Art. 5 Abs. 3 E-Privacy-Richtlinie Cookies nur noch auf Basis eines Opt-in setzen.[64]

Die direkte Anwendbarkeit führt jedoch nicht zur Begründung von Pflichten für private Stellen (keine horizontale Drittwirkung von Richtlinien). Diese unmittelbare Wirkung leitet sich aus Art. 288 Abs. 3 AEUV ab, wonach eine Richtlinie eben nur „für jeden Mitgliedstaat, an den sie gerichtet ist" eine unmittelbare Verbindlichkeit begründet und für niemanden sonst. Eine horizontale Drittwirkung zwischen Privaten würde hingegen eine unzulässige Überschreitung der Kompetenzen der EU bedeuten.[65] Die von Seiten der Datenschutzaufsichtsbehörden teils vertretene gegenteilige Auffassung[66] kann vor diesem Hintergrund nicht überzeugen.

V. Fazit und Praxisempfehlung

Die Anforderung gemäß Art. 5 Abs. 3 E-Privacy-Richtlinie ist im deutschen Recht nicht umgesetzt. Es gibt im deutschen Recht daher keine Rechtspflicht für Webseitenbetreiber, Opt-in-Mechanismen für Tracking-Technologien vorzusehen. Art. 5 Abs. 3 E-Privacy-Richtlinie ist in Deutschland jedoch direkt anwendbar und gilt unmittelbar für öffentlich-rechtliche Webseitenbetreiber. Nur für diese ergibt sich daher die Pflicht zur Implementierung eines Opt-in-Mechanismus für den Einsatz von Tracking-Technologien.

Private Webseitenbetreiber dürfen hingegen weiter gemäß § 15 Abs. 3 TMG klassische und moderne Tracking-Technologien einsetzen und pseudonyme Nutzerprofile bilden, solange die Nutzer keinen Widerspruch erklärt haben (Opt-out). Gemäß § 13 Abs. 1 TMG müssen sie die Nutzer allerdings hierauf hinweisen.

52 *Schmitz*, in: Hoeren/Sieber/Holznagel (Fn. 50), Rn. 277.
53 EuGH, 5. 10. 2004 – C-397/01 - C-403/01, NJW 2004, 3547, 3549; EuGH, 4. 7. 2006 – C-212/04, NJW 2006, 2465, 2467.
54 EuGH, 4. 7. 2006 – C-212/04, NJW 2006, 2465, 2467, hierzu *Auer*, NJW 2007, 1106.
55 Vgl. BT-Drs. 14/6098 zur Vorgängerregelung in § 6 TDDSG.
56 BGH, 21. 11. 2008 – VIII ZR 200/05, NJW 2009, 427, 429.
57 BGH, 21. 11. 2008 – VIII ZR 200/05, NJW 2009, 427, 429.
58 Hierzu http://www.heise.de/newsticker/meldung/Schaar-Cookie-Regeln-der-EU-gelten-unmittelbar-1570745.html.
59 Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe „Soziale Netzwerke" (Fn. 28), S. 33; ULD, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, S. 23.; Beschluss des Düsseldorfer Kreises vom 24./25. 11. 2010 – „Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste".
60 *Moos*, K&R 2012, 635, 638; *Polenz*, VuR 2012, 207, 213.
61 *Moos*, K&R 2012, 635, 638; *Polenz*, VuR 2012, 207, 213; *Schürmann*, in: Taeger (Fn. 4), S. 797.
62 *Moos*, K&R 2012, 635, 637.
63 *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union: EUV/AEUV, 56. Aufl. 2015, Art. 288 AEUV, Rn. 157; *Moos*, K&R 2012, 635, 637.
64 *Moos*, K&R 2012, 635, 638.
65 *Moos*, K&R 2012, 635, 638 f.; EuGH, 14. 7. 1994 – C-91/92, NJW 1994, 2473, 2474.
66 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), 19. 8. 2011, „Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook", S. 23.

Soweit Webseitenbetreiber selbst technisch nicht in der Lage sind, einen Bezug zwischen den Tracking-Daten und den betroffenen Nutzern herzustellen, ist es vertretbar, auf den Einsatz mangels Personenbeziehbarkeit nicht hinzuweisen. Angesichts der restriktiven Sicht der Datenschutzaufsichtsbehörden zur Personenbeziehbarkeit von Daten, die online erhoben werden,[67] sollte jedoch sorgfältig geprüft und sichergestellt werden, dass die Herstellung eines Personenbezugs tatsächlich im Sinne des § 3 Abs. 6 BDSG ausgeschlossen ist. Zur Vermeidung rechtlicher Risiken empfiehlt es sich, im Zweifel auf den Einsatz von Tracking-Technologien hinzuweisen.

Obwohl für private Webseitenbetreiber nach deutschem Recht keine Verpflichtung besteht, einen Opt-in-Mechanismus für den Einsatz von Tracking-Technologien zu implementieren, kann dies dennoch zweckmäßig sein. Etwa wenn für die Webseite nach dem Recht anderer (EU/EWR) Staaten eine Pflicht zur Implementierung eines Opt-in-Mechanismus besteht bzw. für Webseiten mit einem europäischen Adressatenkreis ein einheitliches, richtlinienkonformes Vorgehen zweckmäßig ist. In jedem Fall sollten Webseitenbetreiber die Rechtsentwicklung im Auge behalten und nicht darauf vertrauen, dass die derzeit europarechtswidrige Gestaltung des TMG dauerhaft besteht.

67 S. o. Fn. 27 und 28.

Prof. Dr. Hubertus Gersdorf, Rostock*

Telekommunikationsrechtliche Einordnung von OTT-Diensten am Beispiel von Gmail

Rechtsgutachten im Auftrag der Google Inc.

Ob die über das offene Internet verbreiteten OTT-Dienste wie Gmail Telekommunikationsdienste im Sinne des § 3 Nr. 24 TKG sind, ist umstritten und Gegenstand eines anhängigen gerichtlichen Verfahrens zwischen Google und der Bundesnetzagentur (BNetzA). Der Autor geht zunächst der Frage nach, ob der Begriff der Telekommunikationsdienste sämtliche Dienste der Telekommunikation und nur Dienste der „Übertragung von Signalen" (§ 3 Nr. 24 TKG) erfasst. Sodann wird untersucht, unter welchen Voraussetzungen Dienstanbieter mit der „Übertragung von Signalen" betraut sind.

I. Einleitung und Gegenstand der Untersuchung

Das Internet wirkt auf nahezu sämtliche Lebens- und Wirtschaftsbereiche ein und führt dort zu einem stetig an Dynamik gewinnenden Änderungsprozess. Das Internet ermöglicht neuen Anbietern innovative Dienstleistungen und Produkte, die in komplementäre bzw. substitutive Konkurrenz zu den klassischen Geschäftsmodellen treten. Auch die Massen- und Individualkommunikation hat dieser Strukturwandel erfasst. Im Bereich der Massenkommunikation sind neben die tradierten Fernseh- bzw. Hörfunk- und On Demand-Anbieter sowie die klassischen Plattformbetreiber (Kabel und Satellit) internetbasierte Inhalteanbieter (Netflix, Google Play Filme & Serien, Amazon, Spotify, Apple Music etc.) und internetbasierte Plattformbetreiber mit linearen Medieninhalten (Zattoo, Magine TV etc.) getreten.

Im Bereich der Individual- einschließlich Gruppenkommunikation treten neben die leitungsvermittelten bzw. paketvermittelten (Voice over IP – VoIP) Sprachtelefondienste und Textdienste (SMS) der klassischen Telekommunikationsunternehmen neue rein internetbasierte Dienste-formen wie (Video-)Telefonie-Dienste (Voice over Internet – WhatsApp, Skype etc.) und Instant-Messaging (WhatsApp, Messenger etc.). Aktuelle Marktanalysen zeigen, dass die internetgestützten Telefon- und Instand-Messaging-Dienste immer mehr an Bedeutung gewinnen und klassische Dienste – wie etwa SMS – zum Teil verdrängen.[1]

Die neuen internetbasierten Dienste der Massen- bzw. Individualkommunikation werden als Over The Top-Dienste (OTT-Dienste) bezeichnet. Eine allgemein anerkannte Definition von OTT existiert nicht, geschweige denn eine rechtlich ausgeformte (Legal-)Definition. Das Gremium europäischer Regulierungsbehörden (GEREK) versteht OTT als einen Inhalt, einen Dienst oder eine Anwendung, der/die dem Endnutzer über das offene Internet bereitgestellt wird.[2] Das Charakteristikum von OTT ist daher nicht ein bestimmter Anwendungstyp oder Dienst, sondern die Art und Weise der Bereitstellung eines Inhalts, eines Dienstes oder einer Anwendung. Der Transport erfolgt über das offene Internet unabhängig von dem Internetzugangsanbieter des Endnutzers.[3] OTT-Anbieter haben über den Vorgang des Signaltransports keine Herrschaft. Die Inhalte, Dienste und Anwendungen von OTT-Anbietern werden über das offene Internet nach dem hierfür geltenden Best-Effort-Prinzip transportiert. Die Möglichkeit einer Qualitätssicherung besteht insoweit nicht. Hierin unterscheiden sich OTT-

* Universität Rostock, Gerd Bucerius-Stiftungsprofessur für Kommunikationsrecht und Öffentliches Recht Rostock/Berlin. Mehr über den Autor erfahren Sie auf S. VIII.

1 Vgl. hierzu *Kühling/Schall*, CR 2015, 641, 642 f.; *Schumacher*, K&R 2015, 771, 771 f.

2 Berec, Report on OTT services (draft), BoR (15) 142, p. 14.

3 Monopolkommission, Telekommunikation 2015: Märkte im Wandel, Sondergutachten 73, 2015, Rn. 152.