Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

7/8
K&R

Editorial: Vorsicht! Sie haben einen Vertrag mit uns! Die TK-Transparenzverordnung der Bundesnetzagentur · *Dr. Sascha Vander*

445 Zur Zulässigkeit von AdBlock-Detektoren vor dem Hintergrund der E-Privacy-Richtlinie · *Hans Leo Bechtolf* und *Niklas Vogt*

450 Einwilligungserklärungen im Fotorecht · *Dr. Bernd Lorenz*

456 Gesichtserkennung zu Werbezwecken – Erfolgt ein User Tracking bald auch offline? · *Paul Voigt*

462 Erleichterte Informationspflichten bei Fernabsatzverträgen mit Waren · *Dr. Felix Buchmann* und *Anna-Lena Hoffmann*

467 Die Entwicklung des Urheberrechts seit Mitte 2015 *Dr. Alexander R. Klett* und *Maria Ottermann*

474 Hotelzimmer, Zahnarztpraxen und Reha-Einrichtungen – der Begriff der öffentlichen Wiedergabe · *Dr. Diana Ettig* und *Lea Kaase*

478 Der Rundfunkbeitrag im Konflikt mit der Verfassung *Dr. Kay E. Winkler*

482 Länderreport Österreich · *Prof. Dr. Clemens Thiele*

495 BGH: Im Immobiliensumpf: Unterlassungsanspruch gegen anwaltlichen Vorwurf kriminellen Handelns in Pressebericht mit Kommentar von *Martin W. Huff*

509 BGH: Lebens-Kost: Kein Schadensersatzanspruch wegen unzulässiger Telefonwerbung mit Kommentar von *Dr. Carsten Menebröcker*

515 BGH: Kein Werktitelschutz für wetter.de mit Kommentar von *Franz Gernhardt*

530 LG Frankfurt a. M.: Informationspflicht zu Datenübermittlung beim Vertrieb von Smart-TV mit Kommentar von *Sebastian Laoutoumai* und *Orcun Sanli*

544 Glosse: Trauerspiel ums Lachverbot am Feiertag · *Dominik Höch*

19. Jahrgang Juli/August 2016 Seiten 445 – 544

dfv Mediengruppe · Frankfurt am Main

Kommunikation & Recht

K&R 7/8/2016

Hans Leo Bechtolf und Niklas Vogt, Hamburg*

Zur Zulässigkeit von AdBlock-Detektoren vor dem Hintergrund der E-Privacy-Richtlinie

Eine aktuelle Stellungnahme der EU-Kommission auf eine Anfrage des Datenschutzaktivisten Alexander Hanff hat für einen großen Aufschrei in der Medienwelt gesorgt. Die Ausführungen im Schreiben geben Anlass zu der Vermutung, dass die Verwendung von AdBlock-Detektoren gegen bestehendes Europarecht verstoßen könnte. Die Autoren untersuchen in ihrem Beitrag die Rechtmäßigkeit der Verwendung von AdBlock-Detektoren vor dem Hintergrund der nationalen Rechtslage und des europäischen Rechtsrahmens.

I. Einleitung: Der Kampf gegen das AdBlocking

Die werbefinanzierte Contentindustrie steht durch den immer beliebter werdenden Gebrauch von sog. AdBlockern vor einem existenziellen Problem. Solche Tools, die als Erweiterung im Browser der Nutzer installiert werden und die Werbung der jeweils aufgerufenen Seite unterdrücken, sind den Webseitenbetreibern mittlerweile mehr als ein Dorn im Auge; sie sind eine ernsthafte Bedrohung ihres gesamten Geschäftsmodells, das Gratis-Content im Gegenzug für Werbeeinblendungen bereithält.

Allein im Jahr 2015 sind den Anbietern aufgrund von AdBlockern Online-Werbeeinnahmen in Höhe von knapp 21,8 Milliarden US-Dollar entgangen.[1] Für das Jahr 2016 prognostiziert eine Studie von Pagefair und Adobe fast eine Verdoppelung des Schadens auf 41,4 Milliarden US-Dollar weltweit.[2]

Kein Wunder also, dass die Anbieter über Wege nachdenken, wie das AdBlocking verhindert werden kann. Mit dem Versuch, AdBlocker für generell rechtswidrig erklären zu lassen, sind die Anbieter bisher vor dem LG München,[3] LG Hamburg[4] und LG Köln[5] gescheitert. Diese Gerichte gaben mit ihren Urteilen grünes Licht für Adblock Plus – eines der beliebtesten AdBlock-Programme auf dem Markt.

Die Webseitenbetreiber haben außerdem eine weitere Strategie zum Schutz ihres Geschäftsmodells entwickelt, sog. AdBlock-Detektoren. Diese erkennen, ob ein Nutzer einen AdBlocker aktiviert hat und ermöglichen die Sperrung des Contents oder das Einblenden eines Warnhinweises. Viele große Nachrichtenportale setzen mittlerweile auf die Verwendung solcher AdBlock-Detektoren.

Für einen großen Aufschrei[6] sorgte daher die Stellungnahme[7] der EU-Kommission auf eine Anfrage des Datenschutzaktivisten *Alexander Hanff*, in der die Verwendung von AdBlock-Detektoren als Verstoß gegen europarechtliche Datenschutzvorgaben eingeschätzt wurde.

Anlässlich der aktuellen Diskussion soll die Rechtmäßigkeit von AdBlock-Detektoren nach nationalem und europäischem Recht genauer beleuchtet werden.

II. Nationale Rechtslage

Geht es nach deutschem Recht, so kommen beim Einsatz von AdBlock-Detektoren die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Anwendung. Da Webseitenbetreiber Diensteanbieter i. S. v. § 2 Nr. 1 TMG sind, ist auf sie gem. § 1 Abs. 1 TMG zuvorderst das TMG mit seinen bereichsspezifischen Datenschutzregelungen anzuwenden und nur subsidiär das BDSG.

Im TMG sind die datenschutzrechtlichen Vorschriften in den §§ 11 ff. geregelt, deren Anwendungsbereich – wie sich aus dem Wortlaut aller Vorschriften des 4. Abschnitts des TMG ergibt – erst eröffnet ist, wenn bei einem Vorgang „personenbezogene Daten" erhoben werden.[8] Der Begriff der „personenbezogenen Daten" wird aufgrund des Verweises in § 12 Abs. 3 TMG durch § 3 Abs. 1 BDSG genauer bestimmt und erfasst solche Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[9] Eine Person ist dann „bestimmt", wenn sie allein anhand des Datums eindeutig identifiziert werden kann. Ist eine solche Identifizierung nicht direkt möglich, so muss die Person zumindest bestimmbar sein.[10] Wie weit der Begriff der Bestimmbarkeit dabei reicht, ist umstritten. Vermehrt[11] wird vertreten, dass der Begriff relativ zu verstehen sei, es also darauf ankomme, dass die verantwortliche Stelle mit den ihr zur Verfügung stehenden Kenntnissen, Mitteln und Möglichkeiten und ohne unverhältnismäßigen Aufwand den Bezug selbst herstellen könne.[12]

---

* Mehr über die Autoren erfahren Sie auf S. XI, XII.

1 PageFair/Adobe, The cost of ad blocking – PageFair and Adobe 2015 Ad Blocking Report, S. 3, aufrufbar unter https://downloads.pagefair.com/wp-content/uploads/2016/05/2015_report-the_cost_of_ad_blocking.pdf.

2 PageFair/Adobe, The cost of ad blocking (Fn. 1), S. 7.

3 LG München, 27. 5. 2015 – 37 O 11673/14, K&R 2015, 521 ff.

4 LG Hamburg, 21. 4. 2015 – 416 HKO 159/14, K&R 2015, 600 ff.

5 LG Köln, 29. 9. 2015 – 33 O 132/14, MMR 2016, 264 ff. Auch in zweiter Instanz vom OLG nicht beanstandet, das jedoch das Whitelisting-Verfahren für rechtswidrig befand, vgl. OLG Köln, 24. 6. 2016 – 6 U 149/15.

6 S. etwa https://www.telemedicus.info/article/3085-EU-Kommission-Adblocker-Detektoren-fallen-unter-ePrivacy-Richtlinie.html.

7 EU-Kommission, Antwortschreiben an *Alexander Hanff* v. 13. 4. 2016, BL/mp Ares(2016)s-141898, teilweise aufrufbar bei *Grenzer*, CR 2016, 65, 66.

8 Vgl. *Spindler*, in: Schuster/Spindler (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, § 11 TMG Rn. 6.

9 *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 10.

10 *Spindler*, in: Spindler/Schuster (Fn. 8), § 11 TMG Rn. 6.

11 *Gola/Klug/Körffer*, in: Gola/Schomerus (Fn. 9), § 3 Rn. 10; *Plath/Schreiber*, in: Plath (Hrsg.), BDSG, 2013, § 3 Rn. 15; *Wojtowicz*, PinG 2013, 65.

12 *Gola/Klug/Körffer*, in: Gola/Schomerus (Fn. 9), § 3 Rn. 10.

Die Gegenauffassung[13] versteht den Begriff objektiv. Danach reiche es schon aus, wenn die Person anhand des Datums von irgendeiner Person (auch einer Dritten mit Zusatzwissen) bestimmt werden könne.

Letztendlich kann der Streit dahinstehen, wenn die von AdBlock-Detektoren gespeicherten Daten schon nach dem objektiven Verständnis der „Bestimmbarkeit" nicht ausreichen, um einen Personenbezug herzustellen.

Es fragt sich also, welche Daten von AdBlock-Detektoren überhaupt erhoben werden. Zur Beantwortung muss der technische Vorgang dieser Ermittlung betrachtet werden, der jedoch zunächst ein Verständnis der Grundfunktion eines AdBlockers erforderlich macht:

AdBlocker sind Browser-Plugins oder -Erweiterungen, die das Verhalten des Browsers verändern. Kernelement eines AdBlockers ist eine Filterliste, in der zu blockierende Begriffe und Links stehen. Die wohl am häufigsten eingesetzte Filterliste in Deutschland ist die sog. „Easylist".[14] Beim Aufruf einer Webseite wird deren Quelltext auf Begriffe und Links durchsucht, die auf der Filterliste stehen. Erkennt der AdBlocker einen solchen Begriff bzw. Link, wird dessen Abruf durch die Webseite verhindert. Er wird also nicht versteckt, sondern gar nicht erst abgerufen. Dem Nutzer wird dann die Webseite ohne die herausgefilterten Inhalte angezeigt.

AdBlock-Detektoren machen sich diese Funktionsweise der AdBlocker zunutze. Sie stellen dem Nutzer eine „Falle", indem sie ein Inhaltselement, z. B. eine JavaScript-Datei, in den Quelltext der Seite einbinden und dieses so benennen, dass es von einem AdBlocker über die Filterliste ausgeschlossen wird (bspw. „advertise.js"). Per Script wird dann überprüft, ob diese Datei geladen oder unterdrückt wurde. Als weitere Bedingung kann dann festgelegt werden, dass bei unterdrücktem Inhaltselement eine Meldung für den Nutzer erscheint bzw. der Content insgesamt ausgeblendet wird.

Es gibt noch einige weitere Methoden, einen AdBlocker aufzuspüren. Allen Methoden gemein ist aber, dass sie den korrekten Aufruf der Inhaltselemente der Seite durch den Browser des Nutzers testen. Am Ende der AdBlock-Detektion steht somit die Information, ob die Webseite durch den Nutzer korrekt aufgerufen wurde oder nicht. Allein diese Information lässt jedoch nur den Rückschluss zu, dass der betreffende Nutzer höchstwahrscheinlich einen AdBlocker installiert hat. Welcher AdBlocker genau installiert ist, lässt sich nicht sagen.

Eine bestimmte Person kann anhand dieses Datums somit nicht festgestellt werden. Ebenso wird eine Person aufgrund dieser Information noch nicht bestimmbar, denn die Tatsache, dass ein Nutzer einen AdBlocker verwendet, trifft mittlerweile auf knapp ein Viertel der deutschen Internetnutzer zu.[15]

Im Ergebnis wird durch einen AdBlock-Detektor somit kein personenbezogenes Datum erzeugt, so dass das TMG keine Anwendung findet. Nach nationalem Recht ist daher weder ein Hinweis noch ein Opt-in oder Opt-out beim Einsatz von AdBlock-Detektoren erforderlich.

III. Europäischer Rechtsrahmen

Als europarechtliche Vorgabe für die Benutzung von AdBlock-Detektoren könnte Art. 5 Abs. 3 S. 1 der E-Privacy-Richtlinie[16] einschlägig sein. Dieser sieht vor, dass die Mitgliedstaaten sicherstellen, 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 betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der RL 95/45/EG u. a. über die Zwecke der Verbreitung erhält, seine Einwilligung gegeben hat."

Anders als in den Regelungen des TMG ist in Art. 5 Abs. 3 der E-Privacy-Richtlinie nicht vorgesehen, dass die Informationen auch personenbezogen sein müssen.[17] Daher ist zu prüfen, ob der materielle Anwendungsbereich eröffnet ist.

1. Eröffnung des sachlichen Anwendungsbereichs

Der Tatbestand von Art. 5 Abs. 3 S. 1 der E-Privacy-Richtlinie kennt zwei Alternativen: Zum einen die Speicherung von Informationen, zum anderen den Zugang zu Informationen, die bereits im Endgerät eines Nutzers gespeichert sind.

Bei der Anwendung von AdBlock-Detektoren könnte es sich um die „Speicherung von Informationen" handeln. Grundsätzlich werden alle Webinhalte, die beim Abruf einer Webseite mittels HTTP-Request angefragt werden, auf den Rechner des Nutzers heruntergeladen – mithin dort im Cache gespeichert – und vom Browser ausgeführt. Auch AdBlock-Detektoren werden also, z. B. in Form eines eingebundenen JavaScripts, vorübergehend auf dem Computer des Nutzers abgespeichert. Nach dem vollständigen Laden der Webseite wird in der Folge also auch die Information, die durch das AdBlock-Detektions-Script erlangt wurde, auf dem Rechner des Nutzers gespeichert.

Es fragt sich jedoch, ob dies ausreichend ist, um den Schutzmechanismus des Art. 5 Abs. 3 auszulösen, da teilweise angenommen wird, dass dieser nur für die Verwendung von Cookies einschlägig ist.[18]

Gegen ein solch enges Verständnis spricht die technikneutrale Ausgestaltung der Richtlinie. Dem Wortlaut nach ist grundsätzlich nur die Speicherung oder der Zugang zu Informationen maßgeblich, ohne dass nach der eingesetzten Technologie differenziert wird.[19] Hieran zeigt sich die Intention des Richtliniengebers, den Anwendungsbereich nicht bloß auf Cookies zu begrenzen, sondern auch fortgeschrittenen Technologien entgegenwirken zu können.[20]

Dass die Richtlinie gerade nicht nur auf den Einsatz von Cookies Anwendung findet, ergibt sich weiterhin aus dem 24. Erwägungsgrund der E-Privacy-Richtlinie in der Fassung 2002/58/EG. In diesem Erwägungsgrund sind Beispiele aufgeführt, die verdeutlichen, welche Maßnahmen unter den Art. 5 Abs. 3 zu fassen sind. Darunter fallen u. a. die Benutzung von Spähsoftware, Viren, Web-Bugs, Hidden-Identifiers und *ähnlichen Instrumenten*, die ohne Wissen des Nutzers in dessen Endgerät eindringen können, um

13 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 5. Aufl. 2016, § 3 Rn. 13; *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl. 2013, § 3 Rn. 13; *Pahlen-Brandt*, DuD 2008, 34.

14 Hierzu https://easylist.github.io.

15 PageFair/Adobe, The cost of ad blocking (Fn. 1), S. 6.

16 Gemeint ist die Richtlinie vom 25. 11. 2009 in der Fassung 2009/136/EG (auch „Cookie-Richtlinie" genannt).

17 So explizit Art. 29 Gruppe, Opinion 2/2010 on online behavioural advertising (Art. 29 Gruppe, WP 171), S. 9 ff.

18 *Puscher*, c't 2014, Heft 11, S. 160.

19 *Schmidt/Babilon*, K&R 2016, 86, 87; Art. 29 Gruppe, WP 171 (Fn. 17), S. 10.

20 *Schürmann*, in: Taeger (Hrsg.), Die Welt im Netz – Folgen für Wirtschaft und Gesellschaft, 2011, S. 493, 494 f.

Zugang zu Informationen zu erlangen oder die Nutzeraktivität zurückverfolgen zu können.

Auch der 66. Erwägungsgrund der E-Privacy-Richtlinie verdeutlicht, dass grundsätzlich jede Speicherung von Informationen auf der Endeinrichtung des Nutzers untersagt ist. Selbst bei legitimen Gründen (wie manchen Arten von Cookies) soll eine Speicherung auf die Situationen beschränkt sein, in der sie unverzichtbar ist, um Benutzung eines ausdrücklich angeforderten Dienstes zu ermöglichen.

Schließlich sprechen die Stellungnahmen der Art. 29 Datenschutzgruppe zum sog. device fingerprinting dafür, die Richtlinienbestimmung umfänglich auf alle Technologien anzuwenden, denn beim device fingerprinting werden u. a. auch JavaScripte verwendet, die nach Einschätzung der Art. 29 Datenschutzgruppe einwilligungsbedürftig sind.[21]

Materiell-rechtlich erfasst Art. 5 Abs. 3 der E-Privacy-Richtlinie also nicht nur Cookies, sondern alle sonstigen Technologien, die dazu genutzt werden können, Informationen zu speichern oder Zugang zu Informationen zu erhalten, die im Endgerät des Nutzers gespeichert sind.[22] Daher kann ein JavaScript als *ähnliches Instrument* erfasst werden, das unter den Anwendungsbereich der Richtlinie fällt.

Eben jene Gründe macht sich die Kommission in ihrer Stellungnahme auf die Anfrage von *Hanff* zu Eigen und kommt zu dem Ergebnis, dass die Verwendung von Skripten, die feststellen können, ob der Benutzer einen AdBlocker benutzt, materiell-rechtlich von Art. 5 Abs. 3 der E-Privacy-Richtlinie umfasst sind.[23]

Diesem Ergebnis ist auch im Hinblick auf den Telos des Art. 5 Abs. 3 der E-Privacy-Richtlinie zuzustimmen. Wie sich aus dem 24. Erwägungsgrund der RL 2002/58/EG ergibt, verfolgt die Vorschrift den Schutz eines bestimmten Bereichs, der der Privatsphäre des Nutzers aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. Der Schutzzweck richtet sich also nicht gegen den Gewinn einer konkreten Information, sondern gegen das unbefugte Eindringen in einem der Privatsphäre zugeordneten Bereich. Aus diesem Grund ist es auch unerheblich, ob die gewonnene Information Personenbezug aufweist oder nicht.[24]

2. Ausnahmeregelung für AdBlock-Detektoren?

Dies bedeutet jedoch nicht zwingend, dass die Verwendung von AdBlock-Detektoren einen Verstoß gegen die Richtlinienvorgaben begründet. Art. 5 Abs. 3 S. 2 der E-Privacy-Richtlinie sieht zwei Ausnahmetatbestände vor, bei denen die Maßgaben aus Art. 5 Abs. 3 S. 1 einer Speicherung bzw. einem Zugang nicht entgegenstehen. Diese Ausnahmen betreffen zum einen eine Speicherung, deren alleiniger Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist und zum anderen eine Speicherung, die erforderlich ist, damit der Anbieter eines Dienstes, der vom Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Der 66. Erwägungsgrund der E-Privacy-Richtlinie betont das Erfordernis einer restriktiven Auslegung der zweiten Alternative, wonach die Speicherung auch bei legitimen Gründen nur auf jene Situationen beschränkt sein sollte, in denen sie unverzichtbar ist, um die Nutzung eines vom Teilnehmer ausdrücklich aufgeforderten Dienstes zu ermöglichen.

Als Beispiel lässt sich hier die Feststellung der Bildschirmauflösung nennen, die notwendig ist, um eine korrekte Darstellung, beispielsweise auf einem mobilen Endgerät, zu ermöglichen.[25]

Die bei AdBlock-Detektoren verwendete Technologie dient lediglich der Gewährleistung der Einblendung von Werbung und ist daher nicht unbedingt erforderlich, um den Dienst der Webseite zur Verfügung zu stellen. Der Dienst der Seite kann vielmehr auch ohne die Benutzung eines entsprechenden Skripts gewährleistet werden. Zudem ist ihr alleiniger Zweck nicht die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetzwerk, denn gemeint sind nur solche Speicherungen, ohne die die Übertragung einer Nachricht unmöglich wäre.[26]

Aus alledem ergibt sich, dass die Verwendung von AdBlock-Detektoren unter keinen der Ausnahmegründe zu subsummieren ist und dadurch einen Verstoß gegen die Vorgaben des Art. 5 Abs. 3 der E-Privacy-Richtlinie begründet.

IV. Beseitigung des Umsetzungsdefizits

Wie oben bereits erläutert, findet das TMG mangels Personenbezugs der Daten keine Anwendung bei der Verwendung von AdBlock-Detektoren. Hier stehen die Vorgaben des Art. 5 Abs. 3 der E-Privacy-Richtlinie jedoch im klaren Widerspruch zu der nationalen Rechtslage, da dieser das Tatbestandsmerkmal des Personenbezugs nicht verlangt.

Bei der Kollision zwischen europäischem Sekundärrecht und der nationalen Rechtsordnung sind die mitgliedstaatlichen Gerichte zur richtlinienkonformen Auslegung der nationalen Gesetze verpflichtet. Die Pflicht zur richtlinienkonformen Auslegung ergibt sich aus Art. 4 Abs. 3 EUV, dem effet utile, i.V.m. Art. 288 Abs. 3 AEUV sowie der jeweiligen Richtlinie selbst.[27]

Zu betonen ist dabei, dass der Begriff der richtlinienkonformen Auslegung – entgegen seines Wortlauts – nicht nur die Auslegung im engeren Sinne, sondern auch die Rechtsfortbildung als solche erfasst.[28]

1. Methodische Grenzen der richtlinienkonformen Auslegung

Die methodische Grenze der Auslegung muss sich dort ergeben, wo Gesetzeswortlaut und der objektiv manifestierte Wille des Gesetzgebers ihr zuwiderlaufen.[29] Diese – auch vom EuGH anerkannte[30] – „Contra-legem-Grenze“

21 Art. 29 Gruppe, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (Art. 29 Gruppe, WP 224).
22 Vgl. Art. 29 Gruppe, WP 171 (Fn. 17), S. 10; Art. 29 Gruppe, Opinion 04/2012 on Cookie Consent Exemption (Art. 29 Gruppe, WP 194), S. 2; Art. 29 Gruppe, WP 224 (Fn. 21), S. 3.
23 EU-Kommission, Antwortschreiben an *Alexander Hanff* (Fn. 7).
24 So explizit Art. 29 Gruppe, WP 171 (Fn. 17), S. 9 ff.
25 Art. 29 Gruppe, WP 224 (Fn. 21), S. 10 f.
26 Art. 29 Gruppe, WP 194 (Fn. 22), S. 3.
27 *Geismann*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 288 AEUV Rn. 55.
28 BGH, 21. 11. 2008 – VIII ZR 200/05, NJW 2009, 427, 429; *Schroeder*, in: Streinz, EUV/AEUV, 2. Aufl. 2012, Art. 288 AEUV Rn. 128; *Canaris*, Die richtlinienkonforme Auslegung und Rechtsfortbildung, in: Koziol/Hummel (Hrsg.), Im Dienste der Gerechtigkeit, FS Bydlinksi, 2001, S. 47, 81 f.; *Brechmann*, Die richtlinienkonforme Auslegung, 1994, S. 269 ff.; *Classen*, EuZW 1993, 83, 86.
29 BVerfG, 26. 9. 2011 – 2 BvR 2216/06, NJW 2012, 669, Rn. 47; *Canaris*, in: Koziol/Hummel (Fn. 28), S. 91 ff.; *Michael/Payandeh*, NJW 2015, 2392, 2395; *Schlachter*, EuZA 2015, 1, 6.
30 EuGH, 16. 6. 2005 – C-105/03, NJW 2005, 2839, Rn. 47; EuGH, 4. 7. 2006 – C-212/04, NJW 2006, 2465 Rn. 110.

gilt für die nationale Methodenlehre und stellt auch aus europarechtlicher Sicht eine zwingende Grenze dar, die sich aus dem Gewaltenteilungsgrundsatz selbst ergibt.

Die Voraussetzungen für eine richtlinienkonforme Auslegung bzw. Rechtsfortbildung entsprechen also grundsätzlich denen der nationalen Methodik. Erforderlich für eine richtlinienkonforme Rechtsfortbildung ist das Bestehen einer planwidrigen Regelungslücke zwischen status quo im nationalen Recht und den Vorgaben der Richtlinie. Die Planwidrigkeit bedeutet insofern, dass die bestehende Regelungslücke so nicht vom Gesetzgeber intendiert war; also eine abweichende Auslegung unter Berücksichtigung des gesetzgeberischen Willens noch möglich ist.

Im Hinblick auf die richtlinienkonforme Auslegung des TMG herrscht in der Literatur überwiegend die Auffassung, dass diese unter anderem aufgrund des entgegenstehenden Wortlauts des TMG ausscheidet.[31] Dabei erfolgt die Ablehnung häufig zu voreilig: Der Wortlaut ist nur im Rahmen der richtlinienkonformen Auslegung im engeren Sinne von Bedeutung, jedoch nicht bei der richtlinienkonformen Rechtsfortbildung.[32] Erst durch das Überschreiten der Wortlautgrenze kann überhaupt methodisch von einer Rechtsfortbildung gesprochen werden. Entscheidend ist lediglich, ob der gesetzgeberische Wille einer Analogiebildung – insbesondere der Planwidrigkeit – entgegensteht.

In der Rechtsprechung des BGH zeigt sich die Tendenz, dem abstrakten Umsetzungswillen des Gesetzgebers derart viel Gewicht zuzusprechen, dass er alleine aus diesem die Planwidrigkeit herleitet, um bestehende Regelungslücken zu schließen. Betont seien an dieser Stelle die Rechtssachen *Quelle*,[33] *Weber*[34] und zwei jüngere Entscheidungen aus dem Versicherungsrecht,[35] in denen der BGH sogar den abstrakt vermuteten Umsetzungswillen über den konkret geäußerten Willen des Gesetzgebers stellt. So formuliert der BGH: „Strebt der Gesetzgeber eine richtlinienkonforme Umsetzung an, ist diesem – wenn auch möglicherweise unvollkommen verwirklichten – Zweck, Vorrang vor der mit der Einzelnorm verfolgten Zielrichtung zu geben."[36]

Auch der EuGH hielt in seiner Rechtsprechung fest, dass „ungeachtet entgegenstehender Auslegungshinweise, die sich aus den vorbereitenden Arbeiten zu der nationalen Regelung ergeben könnten", die nationalen Gerichte verpflichtet sind, dem Gesetzgeber einen Umsetzungswillen zu unterstellen.[37]

2. Anwendung der Grundsätze auf § 12 TMG

Daher muss eine richtlinienkonforme Auslegung des TMG unter Heranziehung dieser Maßstäbe untersucht werden. Um ein richtlinienkonformes Ergebnis zu erreichen, müsste das Kriterium des Personenbezugs der Daten teleologisch reduziert werden. Dazu müssten die Voraussetzungen für eine Rechtsfortbildung vorliegen.

Aus der Stellungnahme der Bundesregierung auf die Anfrage der Kommission zur Umsetzung des Art. 5 Abs. 3 der E-Privacy-Richtlinie geht hervor, dass die §§ 12 und 15 TMG einen den Vorgaben des Art. 5 Abs. 3 entsprechenden Schutzstandard gewährleisten sollen.[38] Jedoch erkennt die Bundesregierung in ihrer Stellungnahme selbst an, dass es in Deutschland keine spezifischen Regelungen gibt, die darauf abzielen, die technischen Einrichtungen der Nutzer gegen die unberechtigte Speicherung von Informationen zu schützen.[39]

Dies offenbart eine eindeutige Regelungslücke. Für die Planwidrigkeit spricht der Umstand, dass der Gesetzgeber davon ausgeht, mit den §§ 12, 15 TMG einen den europäischen Vorgaben entsprechenden Standard sichergestellt zu haben.[40]

Aus der Gesetzesbegründung des TMG ist jedoch nicht ersichtlich, dass das Gesetz der Umsetzung von Art. 5 Abs. 3 der E-Privacy Richtlinie dient.[41] Der Gesetzgeber hatte vielmehr die Umsetzung der E-Commerce-RL 2000/31/EG vor Augen,[42] die wiederrum in ihrem 14. Erwägungsgrund den Schutz personenbezogener Daten ausschließlich der RL 95/46/EG zuordnet.

Eine klare Positionierung ergibt sich sogar aus der Gesetzesbegründung zum Gesetzentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen vom 4. 5. 2011. Dort äußert der Gesetzgeber explizit, dass die Änderung des Art. 5 Abs. 3 „derzeit Gegenstand umfangreicher Konsultationen auf europäischer Ebene ist und dass das Ergebnis dieses Prozesses vor der Entscheidung über weitergehenden gesetzgeberischen Handlungsbedarf zunächst abgewartet wird".[43]

Hier zeigt sich deutlich, dass der Gesetzgeber von einer Umsetzung des Art. 5 Abs. 3 der E-Privacy-Richtlinie bei der Schaffung des TMG abgesehen hat und sich (zunächst) bewusst gegen eine Umsetzung der Richtlinie entschieden hat.

Selbst wenn grundsätzlich ein abstrakter Umsetzungswille des Gesetzgebers vermutet wird, kann dieser hier keine richtlinienkonforme Auslegung begründen. Denn die Vermutung wurde im Rahmen des TMG durch objektive Anhaltspunkte widerlegt – dem Gesetzgeber kam es gerade darauf an, die Richtlinie nicht umzusetzen. Selbst wenn der Gesetzgeber sich eines Richtlinienverstoßes nicht bewusst war, weil er irrtümlich davon ausging, den Standards der Richtlinie bereits gerecht zu werden, ändert dies nichts an der Betrachtung. Anders als in der *Weber* Entscheidung schuf der Gesetzgeber gerade keine neue Regelung, die der Umsetzung galt und tatsächlich nur irrtümlich unzureichend gestaltet wurde.

3. Unmittelbare Anwendbarkeit des Art. 5 Abs. 3 E-Privacy-Richtlinie

In Rechtsprechung und Literatur herrscht mittlerweile Einigkeit darüber, dass unter gewissen Voraussetzungen Richtlinienbestimmungen unmittelbar angewandt werden

31 Etwa *Moos*, K&R 2012, 635, 638; *Schmidt/Babilon*, K&R 2016, 85, 89 f.
32 BGH, 26. 11. 2008 – VIII ZR 200/05, EuZW 2009, 155 Rn. 20; *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 57. EL 2015, Art. 288 AEUV Rn. 134.
33 BGH, 26. 11. 2008 – VIII ZR 200/05, NJW 2009, 427.
34 BGH, 21. 12. 2011 – VIII ZR 70/08, NJW 2012, 1073.
35 BGH, 7. 5. 2014 – IV ZR 76/11, NJW 2014, 2646, und BGH, 17. 12. 2014 – IV ZR 260/11, NJW 2015, 1023.
36 BGH, 7. 5. 2014 – IV ZR 76/11, NJW 2014, 2646, Rn. 26. Zu Recht kritisch *Michael/Payandeh*, NJW 2015, 2392.
37 EuGH, 29. 4. 2004 – C-371/02, GRUR 2004, 682, Rn. 13; *Roth*, EWS 2005, 385, 389.
38 EU-Kommission, Communications Committee Working Document, 4. 10. 2011, Questionnaire on the implementation of the Article 5 (3) of the ePrivacy Directive, S. 3 f., aufrufbar unter https://www.telemedicus.info/uploads/Dokumente/COCOM11-20QuestionnaireonArt.53e-PrivacyDir.pdf.
39 EU-Kommission, Communications Committee Working Document (Fn. 38), S. 7 f.
40 EU-Kommission, Communications Committee Working Document (Fn. 38).
41 Vgl. BT-Drs. 16/3078.
42 BT-Drs. 16/3078, S. 1, 11.
43 BT-Drs. 17/5707, S. 3.

können.[44] Voraussetzungen für eine unmittelbare Anwendung ist die nicht oder nur unvollständige Umsetzung einer Richtlinie nach Umsetzungsfrist und die inhaltliche Unbedingtheit und hinreichende Genauigkeit des Regelungsgehalts der jeweiligen Bestimmung.[45]

Ob diese Voraussetzungen für Art. 5 Abs. 3 der E-Privacy-Richtlinie vorliegen, ist in der Literatur umstritten. Festhalten lässt sich zunächst, dass die Umsetzungsfrist am 25. 5. 2011 abgelaufen ist und der deutsche Gesetzgeber seitdem bewusst keine legislativen Tätigkeiten im Hinblick auf die E-Privacy-Richtlinie unternommen hat.[46]

Inhaltlich unbedingt ist eine Bestimmung, wenn sie vorbehaltslos und ohne Bedingung anwendbar ist und keine weiteren Maßnahmen der Organe der Mitgliedstaaten erforderlich sind.[47] Hinreichend genau ist die Richtlinienbestimmung, wenn sich ihre Regelungsgehalte mit der erforderlichen Sicherheit ermitteln lassen und von den Gerichten angewandt werden können.[48]

Unbestimmte Rechtsbegriffe stehen dabei einer unmittelbaren Wirkung nicht entgegen.[49] Ein gewisser Auslegungsspielraum, der etwa im Hinblick auf die Ausgestaltung der Opt-in-Verpflichtung besteht, ist daher unerheblich.[50] Der Wortlaut des Art. 5 Abs. 3 der E-Privacy-Richtlinie ist so bestimmt, dass er von Gerichten unproblematisch angewandt werden könnte. Dieses Ergebnis wird insbesondere dadurch bekräftigt, dass in einigen Mitgliedstaaten die Regelung teilweise wortgetreu in das jeweilige nationale Recht umgesetzt wurde.[51] Daher ist Art. 5 Abs. 3 der E-Privacy-Richtlinie unmittelbar anzuwenden.[52]

Allerdings kann eine unmittelbare Wirkung nur im Bürger-Staat-Verhältnis angenommen werden. Dies entspricht gerade dem Sinn und Zweck der unmittelbaren Anwendbarkeit von Richtlinien: Dem Staat sollen keine Vorteile dadurch entstehen, dass er auf eine Umsetzung der einschlägigen Richtlinie verzichtet hat. Der Bürger soll sich daher im Verhältnis zum Staat auf die Richtlinie berufen können.[53] Eine horizontale Wirkung der Richtlinie zwischen Privaten scheidet nach ständiger Rechtsprechung des EuGH allerdings aus.[54] Für öffentlich-rechtliche Webseitenbetreiber gilt Art. 5 Abs. 3 der E-Privacy Richtlinie unmittelbar.[55] Ihnen ist es nach der Richtlinie nicht gestattet, AdBlock-Detektoren ohne Einwilligung zu verwenden.

V. Praktische Gestaltungsmöglichkeiten

Wer seine Webseite europarechtskonform ausgestalten möchte, kommt somit an einer Opt-in-Lösung für AdBlock-Detektoren nicht vorbei. Es muss eine Meldung an alle Besucher der Webseite erfolgen, die zum einen über den Vorgang informiert und zum anderen dem Nutzer die Entscheidung der Überprüfung überlässt.

Es bestehen grundsätzlich zwei praktisch denkbare Ansätze: Der erste Ansatz wäre, den Content der Seite für alle Nutzer zu verstecken und ihn erst anzuzeigen, wenn der Nutzer der AdBlock-Detektion zugestimmt hat. Auf diese Weise muss der Seitenbetreiber noch keinen Content preisgeben und kann AdBlock-Nutzer wirksamer „aussperren". Nachteil dieser Lösung ist, dass dies die Nutzbarkeit der Seite erheblich verschlechtern und damit einhergehend die Besucherzahl sinken würde.

Ein zweiter möglicher Ansatz wäre eine Lösung über eine den Cookie-Hinweisbannern entsprechende Gestaltung, bei der der Content angezeigt wird und am unteren Seitenrand ein Banner mit dem Opt-in-Link erscheint. Diese Lösung hat jedoch den Nachteil, dass die Nutzer den Hinweisbanner einfach ignorieren könnten, der Content trotzdem ausgeliefert und der gesamte Zweck der AdBlock-Detektion somit ausgehöhlt würde.

Beide Ansätze sind sicherlich wenig praktikabel. Am Ende bleibt somit, dass sich die werbefinanzierte Contentindustrie wohl oder übel prinzipielle Gedanken machen muss, wie sie ihr Geschäftsmodell auch ohne AdBlock-Detektoren betreiben kann.

VI. Fazit und Ausblick

Die Nichtumsetzung des Art. 5 Abs. 3 der E-Privacy-Richtlinie schafft einen europarechtswidrigen Zustand, der sich praktisch auf die Benutzung von AdBlock-Detektoren auswirkt. Verstößt deren Einsatz nach deutschem Recht nicht gegen datenschutzrechtliche Bestimmungen, so fordert das Unionsrecht für die Verwendung entsprechender Programme eine Opt-in-Lösung.

Dies wird zwangsläufig zu Konflikten mit der EU-Kommission führen, wie nicht nur die Stellungnahme gegenüber *Alexander Hanff* zeigt.[56]

Da die Beseitigung des Umsetzungsdefizits durch eine richtlinienkonforme Auslegung des TMG aufgrund des explizit entgegenstehenden Willens des Gesetzgebers nicht erreicht werden kann, ist ohne weiteren Legislativakt ein Vertragsverletzungsverfahren der EU-Kommission denkbar. Im öffentlichen Sektor findet Art. 5 Abs. 3 der E-Privacy-Richtlinie hingegen unmittelbare Anwendung gegenüber den Bürgern. Staatlichen Webseitenbetreibern ist die Verwendung von AdBlock-Detektoren ohne vorherige Einwilligung daher versagt.

Auch wenn die Richtlinie für private Webseitenbetreiber keine unmittelbare Anwendung findet, sollten diese auf lange Sicht überdenken, ob sie weiterhin AdBlock-Detektoren ohne Einwilligung der Nutzer verwenden und damit den europarechtlichen Verstoß in Kauf nehmen.

---

44 EuGH, 5. 4. 1979 – C-148/78, NJW 1979, 1764, Rn. 18 ff.; EuGH, 19. 1. 1982 – C-8/81, NJW 1982, 499 Rn. 21; *Schröder*, in: Streinz (Fn. 28), Art. 288 AEUV Rn. 101; *Ruffert*, in: Callies/Ruffert, 4. Aufl. 2011, EUV/AEUV, Art. 288 AEUV Rn. 47 ff.

45 *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 32), Art. 288 AEUV, Rn. 142 ff.; *Ruffert*, in: Callies/Ruffert (Fn. 44), Rn. 51 ff.

46 BT-Drs. 17/5707 S. 3; *Schmidt/Babilon*, K&R 2016, 85, 90.

47 *Ruffert*, in: Callies/Ruffert (Fn. 44), Art. 288 AEUV, Rn. 53.

48 *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 32), Art. 288 AEUV, Rn. 147.

49 *Schröder*, in: Streinz (Fn. 28), Art. 288 AEUV Rn. 108; *Ruffert*, in: Callies/Ruffert (Fn. 44) Art. 288 AEUV Rn. 54; a. A: OVG Münster, 10. 11. 1993 – 23 D 52/92.AK, NVwZ-RR 1995, 10, 11.

50 *Schmidt/Babilon*, K&R 2016, 85, 90.

51 Zu der Umsetzung in den Mitgliedstaaten s. den Bericht der EU-Kommission, ePrivacy Directive: assessment of transposition and compatibility with proposed Data Protection Regulation, S. 63 ff.

52 Im Ergebnis auch *Schaar*, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe „Soziale Netzwerke", S. 33; *Moos*, K&R 2012, 635, 637; *Polenz*, VuR 2012, 207, 213; *Schmidt/Babilon*, K&R 2016, 85, 90.

53 *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 32), Art. 288 AEUV, Rn. 157.

54 EuGH, 7. 1. 2004 – C-201/02, NVwZ 2004, 593, Rn. 56 m. w. N.

55 *Schmidt/Babilon*, K&R 2016, 85, 90.

56 Nachdem die EU-Kommission der Stellungnahme der Bundesregierung zur Umsetzung des Art. 5 Abs. 3 zunächst gefolgt ist, scheint sie sich von dieser Einschätzung wieder zu distanzieren: „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.", in: ePrivacy Directive: assessment of transposition and compatibility with proposed Data Protection Regulation, S. 63; *Schmidt/Babilon*, K&R 2016, 85, 89.