

# Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

11  
K&R

- Editorial: Europäischer Verbraucherschutz –  
Aktionismus statt Qualität · *Prof. Dr. Stefan Engels*
- 669 Nichts geht mehr? – Das Online-Marketing  
nach Wirksamwerden der DSGVO  
*Dr. Diana Ettig*
- 675 Web-Analytics/Retargeting und automatisierte  
Einzelfallentscheidung · *Christian Galetzka*
- 680 Novelle des Werkvertragsrechts 2018 – Auswirkungen  
auf IT-Verträge · *Dr. Tobias Sedlmeier*
- 686 Das Medienrecht und die Herausforderung  
der technologischen Hybridisierung  
*Prof. Dr. Dr. h.c. Karl-Heinz Ladeur und Prof. Dr. Tobias Gostomzyk*
- 693 Satirische Werbung und die juristische Humorkontrolle  
*Dr. Tobias Hermann*
- 697 Länderreport USA · *Clemens Kochinke*
- 700 EuGH: Kommunikationsdaten müssen auch bei nicht schweren  
Straftaten herausgegeben werden
- 711 BGH: Preisnebenabreden: AGB-Verstoß durch Entgeltklauseln  
beim Online-Ticketkauf  
mit Kommentar von *Dr. Thomas C. Körber* und *Fiona Trabold*
- 716 BGH: Werbeblocker verstößt nicht gegen Wettbewerbsrecht
- 721 BGH: YouTube: Zum Haftungsumfang eines Plattformbetreibers  
bei Urheberrechtsverstößen
- 726 OLG Frankfurt a. M.: Kein „Recht auf Vergessenwerden“  
gegenüber Suchmaschinenbetreiber  
mit Kommentar von *Stefan Michel*
- 733 LG Frankfurt a. M.: Rechtswidrige Bildnisveröffentlichung  
ohne Einwilligung nach KUG und DSGVO  
mit Kommentar von *Dr. Jonas Kahl*

21. Jahrgang

November 2018

Seiten 669 – 740



RAin Dr. Diana Ettig, LL.M., Frankfurt a. M.\*

## Nichts geht mehr? – Das Online-Marketing nach Wirksamwerden der DSGVO

*Egal ob Cookie-Banner, Facebook-Fanpages oder Newsletter-Einwilligungen – in kaum einem Bereich hat die DSGVO für so viel Verunsicherung gesorgt wie im Online-Marketing. Begleitet wurde die Neuregelung von neuen Gerichtsentscheidungen sowie Stellungnahmen der Datenschutzbehörden. Der nachstehende Beitrag gibt einen aktuellen und praxisnahen Überblick über die Entwicklungen der letzten Monate und hinterfragt voreilige Bewertungen über die (Un-)Zulässigkeit der unterschiedlichen Online-Marketing-Anwendungen.*

### I. Einleitung

Das Wirksamwerden der DSGVO am 25. 5. 2018 hat bei nahezu allen Website-Betreibern für ein gewisses Unbehagen gesorgt. Die meisten Unternehmen haben dies – völlig zu Recht – zum Anlass genommen, ihre Datenschutzerklärungen zu überarbeiten und an die neue Rechtslage anzupassen. Zusätzlich wurden zum Teil Funktionen mit einem besonderen datenschutzrechtlichen Risiko abgestellt. Einige Website-Betreiber wussten sich hingegen nur noch dadurch zu helfen, ihre Website ganz vom Netz zu nehmen. Noch immer stößt man daher an der einen oder anderen Stelle auf eine Website im Wartungsmodus.

Ein Revival haben darüber hinaus auch die „Cookie-Banner“ erfahren. Während diese aufgrund der lückenhaften nationalen Umsetzung der Cookie-Richtlinie in Deutschland eher ein Schattendasein führten, müssen wir uns nun auf nahezu jeder Website bereits auf der Startseite zum Thema Cookies verhalten. Verstärkt wurde die diesbezügliche Rechtsunsicherheit noch durch eine Stellungnahme der deutschen Datenschutzbehörden vom April 2018, wonach man nun über die Hintertür der DSGVO in Deutschland endlich der Cookie-Richtlinie zur Wirksamkeit verhelfen will.

Doch damit nicht genug: Nur kurz nach Wirksamwerden der DSGVO kam mit der Entscheidung „Facebook Fanpages“ die nächste schlechte Nachricht für alle Betreiber einer sogenannten Fanpage bei Facebook. Diese sind nach Auffassung der Luxemburger Richter gemeinsam mit Facebook für die Datenerhebung durch das soziale Netzwerk verantwortlich. Während die Entscheidung noch einen gewissen Spielraum für die Gerichte lässt, waren die Datenschutzbehörden in ihrer sich unmittelbar anschließenden Stellungnahme sehr deutlich. Sie sehen aktuell – auch nach ersten Anpassungen durch Facebook – keine Möglichkeit, eine Facebook Fanpage datenschutzkonform zu betreiben.

Überraschend groß war schließlich auch die Verunsicherung der Unternehmer beim Newsletter-Versand. Es dürfte wohl niemanden in Europa geben, der auch nur einen Bruchteil der Newsletter-Informationsmails rund um das Wirksamwerden der DSGVO gelesen hat. Manche Unternehmen haben sich jedoch dafür entschieden, Ihren Newsletter-Verteiler ganz oder zumindest teilweise zu löschen, wenn sie auf besagte Informationsmails nicht noch einmal ein ausdrückliches Opt-in erhalten haben.

Nach alledem stellt sich die Frage: Nichts geht mehr im Online-Marketing? Ist wirklich die einzige Lösung, die Website, die Fanpage und den Newsletter offline zu stellen? Oder kann man durch bestimmte Maßnahmen das Risiko einer rechtlichen Inanspruchnahme durch Betroffene, Wettbewerber oder Datenschutzbehörden vielleicht auch auf ein Minimum reduzieren? Diesen Fragen widmet sich der nachfolgende Beitrag, wobei im Abschnitt II. zunächst das Thema „Website“ näher beleuchtet werden soll, bevor es in Abschnitt III. um das Thema „Social Media“ und in Abschnitt IV. um das Thema „Newsletter“ geht. Schließlich folgt in Abschnitt V. ein kurzes Fazit mit einem Ausblick.

### II. Website und DSGVO

Ob ein Unternehmen sich mit der Datenschutzgrundverordnung auseinandergesetzt hat oder nicht erkennt man am leichtesten an der Website. Denn hier war zumindest die umfassende Überarbeitung der Datenschutzerklärung erforderlich, um die erweiterten Informationspflichten nach Art. 13 DSGVO zu erfüllen. Problematisch wird es dabei vor allem dann, wenn über Funktionen informiert wird, welche auf der Nutzung von Cookies basieren – denn hier stellt sich die zentrale Frage: Setzt man Cookies nur noch mit Einwilligung des Nutzers oder kann man sich in manchen Fällen doch auf das berechtigte Interesse im Sinne von Art. 6 Abs. 1 S. 1 DSGVO berufen?

#### 1. Nutzung von Cookies

Lässt man sich auf einer Website die Cookies anzeigen, die beim Besuch der Seite auf dem eigenen Endgerät gesetzt werden, finden sich häufig Cookies mit den Bezeichnungen „\_gat“, „\_ga“ und „\_gid“ oder „\_utma“, „\_utmb“, „\_utmc“ und „\_utmz“. Das bedeutet, dass der Website-Betreiber auf seiner Seite Google Analytics oder dessen Nachfolger Universal Analytics benutzt. Diese – wie auch die meisten anderen Webanalyse-Dienste – nutzen Cookies, um nachzuvollziehen, wie die Website von den Nutzern angenommen wird. Konkret erfährt der Website-Betreiber, wie viele

\* Mehr über die Autorin erfahren Sie auf S. VIII.

Nutzer seine Seite besuchen und welche Informationen und Unterseiten auf der Seite angeklickt werden. Diese Informationen kann er nutzen, um seine Website zu optimieren und an die Interessen der Nutzer anzupassen.

Um zu ermitteln, wie sich ein einzelner Benutzer auf der Website verhält, speichern Cookies verschiedene Daten wie die IP-Adresse, aber auch Informationen zur verwendeten Hard- und Software. Eine persönliche Identifizierung ist dabei nicht erforderlich, da es lediglich um eine statistische Auswertung des Nutzerverhaltens geht. Aus Gründen des Datenschutzes haben die Anbieter von Webanalyse-Tools – und insbesondere Google Analytics – daher Möglichkeiten entwickelt, die IP-Adresse unmittelbar nach Erhebung zu verkürzen, so dass die erhobenen Daten direkt bei Erhebung anonymisiert oder zumindest pseudonymisiert werden (bei Google Analytics nennt sich diese Erweiterung beispielsweise „AnonymizeIP“).

#### a) Hintergrund

Beim Thema Cookies mag sich der ein oder andere zu Recht fragen, was dies mit der DSGVO zu tun haben soll. Denn die Zulässigkeit der Nutzung von Cookies wurde bereits 2009 durch die sogenannte Cookie-RL,<sup>1</sup> eine Ergänzung der E-Privacy-RL von 2002,<sup>2</sup> umfassend geregelt. Das Wirksamwerden der DSGVO ist jedoch gerade für deutsche Website-Betreiber in dieser Hinsicht äußerst relevant, denn der deutsche Gesetzgeber hat diese Richtlinie, welche für alle Cookies, die zum Betrieb einer Website nicht zwingend erforderlich sind, eine Einwilligung fordert, nie in deutsches Recht umgesetzt.<sup>3</sup> Damit galt in Deutschland bis vor kurzem gemäß § 15 Abs. 3 TMG noch die Widerspruchslösung.

Der BGH, der sich bereits im Oktober 2017 mit der Frage befassen musste, kam jedoch zu dem Ergebnis, dass diese Norm richtlinienkonform auszulegen sei und somit auch in Deutschland bereits vor Wirksamwerden der DSGVO ein Einwilligungserfordernis galt und bis heute gilt.<sup>4</sup> Gleichzeitig haben auch die Karlsruher Richter Zweifel im Hinblick auf die Auslegung von Art. 5 Abs. 3 der E-Privacy-Richtlinie und legten daher dem EuGH eine Reihe von Fragen vor.<sup>5</sup> Konkret geht es dabei um die Form der Einwilligung, wobei der BGH danach differenziert, ob es sich bei den gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht. Denn handelt es sich um solche, so greift nach Auffassung des BGH zusätzlich das Datenschutzrecht und hier ab dem 25. 5. 2018 insbesondere die DSGVO. Insofern müsste die Einwilligung nicht nur den Erfordernissen der E-Privacy-RL, sondern zusätzlich auch der DSGVO genügen. Die letzte Frage des BGH befasst sich schließlich mit den Informationspflichten unter der E-Privacy-RL. Diesbezüglich bitten die Richter um Klarstellung, ob zu den Pflichtinformationen auch die Funktionsdauer der Cookies sowie die Angabe gehören, ob Dritte auf die Cookies Zugriff erhalten.<sup>6</sup> Mit der Frage, ob unter der DSGVO auch eine Speicherung von Cookies aufgrund eines berechtigten Interesses möglich ist, befasst sich die Entscheidung des BGH bedauerlicherweise jedoch nicht.

#### b) Positionspapier der DSK

Demgegenüber gehen die deutschen Datenschutzbehörden bis heute davon aus, dass die Cookie-Richtlinie mangels Umsetzung in deutsches Recht nicht unmittelbar anwendbar ist.<sup>7</sup> Mit Wirksamwerden der DSGVO benötigten Websitebetreiber laut einem Positionspapier der Konfe-

renz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) vom 26. 4. 2018 für die Verarbeitung personenbezogener Daten jedoch eine Rechtfertigung gemäß Art. 6 Abs. 1 DSGVO, wobei insbesondere die Regelungen aus Art. 6 Abs. 1 S. 1 lit. a, b oder f DSGVO in Betracht kommen.

Demnach könne sich ein Websitebetreiber beispielsweise auf Art. 6 Abs. 1 S. 1 lit. b oder f stützen, wenn es sich um Verarbeitungen handelt, die zum Angebot der Website unbedingt erforderlich sind. Bei anderen Verarbeitungen müsse hingegen eine Interessenabwägung im Einzelfall erfolgen. Der Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, sowie die Erstellung von Nutzerprofilen bedürfen nach Auffassung der DSK jedoch stets einer vorherigen Einwilligung.<sup>8</sup> Das bedeutet, dass eine informierte Einwilligung im Sinne der DSGVO in Form einer Erklärung oder sonstigen bestätigenden Handlung vor der Datenverarbeitung eingeholt werden müsste, d. h. bevor beispielsweise ein Cookie platziert wird. Zur Begründung verweist die DSK in dem Positionspapier lediglich darauf, dass ihre Auffassung im Einklang mit dem europäischen Rechtsverständnis zu Art. 5 Abs. 3 der E-Privacy-RL steht, wonach für die Zulässigkeit der Speicherung von Cookies eine Einwilligung erforderlich ist.<sup>9</sup>

Diese Auffassung der Datenschutzbehörden vermag weder dogmatisch noch inhaltlich zu überzeugen. Zwar ist zutreffend, dass die E-Privacy-RL bereits seit 2009 ein Einwilligungserfordernis vorsieht. Allerdings handelt es sich bei der E-Privacy-RL und der DSGVO um zwei völlig verschiedene Gesetzeswerke mit unterschiedlichen Schutzgegenständen: Bei der DSGVO geht es um den Schutz personenbezogener Daten, bei der E-Privacy-RL um den Schutz der elektronischen Kommunikation – unabhängig von einem Personenbezug. Vor diesem Hintergrund wurden die Regelungsgegenstände der E-Privacy-RL auch nicht in die DSGVO aufgenommen, sondern sollen weiterhin Gegenstand einer eigenen gesetzlichen Regelung, der E-Privacy-VO, sein.

Die DSGVO und die E-Privacy-RL stehen mithin unabhängig nebeneinander. Es wäre daher bereits nach dem Sinn und Zweck fraglich, die in der E-Privacy-Richtlinie getroffene Interessenabwägung einfach auf das Datenschutzrecht zu übertragen. Dies gilt umso mehr als die DSGVO gem. Art. 95 den Website-Betreibern gerade keine über die E-Privacy-RL hinausgehenden Pflichten auferlegen soll. Zudem steht die entsprechende Regelung in der E-Privacy-RL ohnehin auf dem Prüfstand. Denn auch der europäische Gesetzgeber hat mittlerweile erkannt, dass er mit der Cookie-RL die Probleme rund um die datenschutzrechtliche Zulässigkeit von Cookies nicht gelöst hat, sondern die Nutzer in der Regel jeder Cookie-Nutzung zustimmen, um den „lästigen“ Cookie-Banner auszublenden. Im Entwurf der Europäischen Kommission für die E-Privacy-VO ist daher vorgesehen, dass die Mes-

1 Art. 5 Abs. 3 RL 2009/136/EG.

2 RL 2002/58/EG.

3 BGH, 5. 10. 2017 – I ZR 7/16, K&R 2018, 54 ff., Rn. 13.

4 BGH, 5. 10. 2017 – I ZR 7/16, K&R 2018, 54 ff., Rn. 13.

5 BGH, 5. 10. 2017 – I ZR 7/16, K&R 2018, 54 ff.

6 Vgl. zu alledem ausführlich *Ettig/Rauer*, ZD 2018, 81.

7 Positionspapier der DSK vom 26. 4. 2018, Nr. 5, [https://www.lidi.nrw.de/mainmenu\\_Datenschutz/submenu\\_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-abdem-25.-Mai-2018/Positionsbestimmung-TMG.pdf](https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-abdem-25.-Mai-2018/Positionsbestimmung-TMG.pdf), Stand: 24. 9. 2018.

8 Positionspapier der DSK (Fn. 7), Nr. 9.

9 Positionspapier der DSK (Fn. 7), S. 4.

sung des Webpublikums – also des Datenverkehrs auf der Website – mittels Cookies oder vergleichbarer Technologien gerechtfertigt ist, soweit diese vom Website-Betreiber selbst vorgenommen wird.<sup>10</sup>

Unklar ist dabei aktuell noch, ob die Rechtfertigung für die Messung des Webpublikums auch dann greift, wenn sich der Website-Betreiber dabei Dritter wie dem Anbieter Google Analytics bedient.<sup>11</sup> Das Parlament sieht in seinem Entwurf für die E-Privacy-Verordnung explizit die Zulässigkeit der Webanalyse durch Dritte vor, wobei jedoch strenge Anforderungen (insbesondere Einräumung von Widerspruchsmöglichkeiten sowie keine Weitergabe personenbezogener Daten an Dritte) gelten sollen.<sup>12</sup> Diese Entwürfe deuten mithin klar auf eine Lockerung des Einwilligungserfordernisses unter der E-Privacy-VO hin.

Darüber hinaus sprechen auch verschiedene inhaltliche Überlegungen gegen die viel zu pauschale Aussage der Datenschutzbehörden: (1) Wenn schon die Direktwerbung als berechtigtes Interesse in Erwägungsgrund 47 der DSGVO ausdrücklich vorgesehen ist, so muss dies erst recht für die Vorstufe der Web- und Marketinganalyse mit deutlich geringerer Eingriffsintensität gelten.<sup>13</sup> (2) Sowohl für die Direktwerbung als auch sogar für das Profiling ist in Art. 21 Abs. 2 DSGVO explizit ein Widerspruchsrecht vorgesehen. Diese Regelung würde schlicht keinen Sinn ergeben, wenn diese Maßnahmen nur mit Einwilligung zulässig wären.<sup>14</sup> (3) Anders als noch 2009 sind die Nutzer heute aufgrund der Cookie-Banner mit der Funktion von Cookies sowie den darauf aufbauenden Mechanismen von Webanalyse und Conversion Tracking vertraut. Der Nutzer rechnet beim Besuch von Websites mit Webtracking.<sup>15</sup> Gerade vor diesem Hintergrund sieht auch der Entwurf für die E-Privacy-VO unter bestimmten Voraussetzungen eine reine Informationslösung für das Tracking vor. Auch dies spricht für eine Zulässigkeit auf Grundlage des berechtigten Interesses. Gerade vor dem Hintergrund dieser aktuellen Entwicklung wäre es völlig absurd, nunmehr über den Umweg der DSGVO die Cookie-Richtlinie in deutsches Recht umzusetzen, die offensichtlich überholt ist.

### c) Rechtliche Bewertung und Empfehlung

Gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO ist eine Datenverarbeitung zulässig, die zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist. Voraussetzung dabei ist jedoch, dass nicht die Interessen oder Grundrechte oder Grundfreiheiten der Betroffenen dieser Datenverarbeitung entgegenstehen. Zudem hat der Betroffene in diesen Fällen ein Widerspruchsrecht, worauf er spätestens zum Zeitpunkt der ersten Kommunikation auch explizit hingewiesen werden muss, Art. 21 DSGVO.

Im ersten Schritt ist dabei zunächst festzustellen, welches berechnete Interesse der Verantwortliche für die Verarbeitung der Daten hat. Gemäß Erwägungsgrund 47 der DSGVO stellt unter anderem die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 S. 1 lit. f DSGVO dar. Im zweiten Schritt ist zu prüfen, inwiefern die Erhebung der Daten zu dem genannten Zweck erforderlich ist. Schließlich setzt Art. 6 Abs. 1 S. 1 lit. f DSGVO voraus, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Dabei ist gemäß Erwägungsgrund 47 zu berücksichtigen, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünft-

licherweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Die Interessenabwägung ist durch den Verantwortlichen vorzunehmen, der dafür auch nachweislich ist.<sup>16</sup>

Unter Zugrundelegung dieser Kriterien sind mithin bei der Prüfung der Zulässigkeit bei der Nutzung von Cookies die folgenden Überlegungen in die Abwägung einzustellen: (1) Werbung stellt nach Erwägungsgrund 47 der DSGVO grundsätzlich ein berechtigtes Interesse im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO dar, das dem Regelungsverständnis der DSGVO nach jedenfalls grundsätzlich nicht von einer Einwilligung abhängig ist. (2) Bei den meisten Cookie-basierten Funktionen wie der Webanalyse oder auch dem Conversion Tracking erfolgt die Datenauswertung nicht personenbezogen. Vorhandene IP-Adressen werden direkt nach Erhebung gekürzt und damit anonymisiert oder zumindest pseudonymisiert.<sup>17</sup> Es werden keine Nutzerprofile gebildet, sondern die Auswertung erfolgt ausschließlich statistisch. Die Eingriffsintensität ist mithin vergleichsweise gering. (3) Die Webanalyse wie auch die Anzeige etwaiger zielgerichteter Werbung ist in der Regel transparent für die betroffene Person. Insofern bestehen gerade bei pseudonymer Nutzung der personenbezogenen Daten der betroffenen Person für die Zwecke des Online-Marketings und der Online-Werbung keine Bedenken, im Rahmen des Art. 6 Abs. 1 lit. f DSGVO die Abwägung zu Gunsten des Verantwortlichen zuzulassen.

Im Ergebnis sprechen daher in vielen Fällen – und insbesondere beim klassischen Webtracking – gute Gründe für eine Rechtfertigung der Nutzung von Cookies über Art. 6 Abs. 1 S. 1 lit. f DSGVO und gegen die Auffassung der deutschen Datenschutzbehörden.<sup>18</sup>

Da es bei der Abwägung der Interessen nach den Erwägungsgründen der DSGVO explizit auf die Erwartungen der Nutzer ankommt, sollte angedacht werden, bereits auf der Startseite mit einem Cookie-Banner oder einer ähnlichen Funktion über die Nutzung von Cookies zum Zwecke des Webtracking sowie über die bestehenden Widerspruchsmöglichkeiten zu informieren. Abzuraten ist dabei jedoch von Formulierungen, die dem Website-Nutzer ein Wahlrecht suggerieren, obwohl tatsächlich keines besteht. Zudem sollte ein eventueller Cookie-Hinweis auf der Startseite konsistent mit den Informationen in der Datenschutzerklärung sein – hier finden sich in der Praxis auf zahlreichen Seiten Widersprüche, welche sicher nicht dem gesetzgeberischen Ziel einer transparenten Datenverarbeitung entsprechen.

## 2. Remarketing

Während „Cookies“ und die klassischen Web-Analyse-Dienste aufgrund der täglichen Cookie-Hinweise mittler-

10 2017/0003 (COD), Art. 8 Abs. 1 lit. d.

11 So *Schleipfer*, ZD 2017, 460, 464; *Rauer/Ettig*, ZD 2018, 255.

12 <http://data.consilium.europa.eu/doc/document/ST-5165-2018-INIT/en/pdf>, Stand: 24. 9. 2018.

13 So bereits *Remmert*, GRUR-Prax 2018, 254.

14 *Remmert*, GRUR-Prax 2018, 254.

15 *Remmert*, GRUR-Prax 2018, 254.

16 *Heberlein*, in: *Ehmann/Selmayr*, Datenschutzgrundverordnung, 2017, Art. 6 Rn. 25; *Ernst*, in: *Paal/Pauly*, DSGVO BDSG, 2. Aufl. 2018, DSGVO, Art. 6 Rn. 31.

17 Zur Frage, ob die Kürzung der IP-Adresse zur Anonymisierung oder nur zur Pseudonymisierung führt, vgl. LG Frankfurt, 18. 2. 2014 – 3-10 O 86/12, K&R 2014, 614 = CR 2014, 266.

18 So auch *Remmert*, GRUR-Prax 2018, 254; a. A. wohl *Jandt*, ZD 2018, 405, 408 – zumindest beim Webtracking durch Drittanbieter und insbesondere beim geräteübergreifenden Tracking.

weile einem Großteil der Internet-Nutzer ein Begriff sind, dürfte die Funktion des Remarketings nur einem Bruchteil bekannt sein. Grundsätzlich geht es dabei um die Anzeige von individualisierten Werbeanzeigen. Besucht ein Internetnutzer die eigene Website, soll er später auf anderen Websites in Werbeanzeigen erneut angesprochen werden. Technische Grundlage für das Remarketing sind in der Regel sogenannte Werbe-IDs, welche von Anbietern von Werbenetzwerken (z. B. Google, Microsoft, Facebook) über Cookies oder andere Technologien wie Device-Fingerprinting oder Tracking-Pixel vergeben werden und auf deren Grundlage bei Aufruf einer Website Werbeanzeigen geschaltet werden.<sup>19</sup>

#### a) Rechtliche Bewertung

Rein technisch betrachtet ist die rechtliche Ausgangslage beim Remarketing grundsätzlich dieselbe wie bei der Webanalyse: Beides basiert auf Cookies oder ähnlichen technischen Funktionsweisen und unterfällt damit zukünftig in erster Linie der E-Privacy-VO, welche sich derzeit jedoch noch im Gesetzgebungsverfahren befindet. Bis zum Abschluss dieses Verfahrens ist jedoch nach Auffassung der Datenschutzbehörden vom Anwendungsvorrang der Datenschutzgrundverordnung auszugehen, d. h. es muss einer der Rechtfertigungsgründe aus Art. 6 Abs. 1 DSGVO vorliegen.

In Betracht kommt auch hier eine Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO, deren Voraussetzungen im Hinblick auf Transparenz und Freiwilligkeit in der Praxis bei den gängigen Remarketing-Anbietern jedoch kaum umsetzbar sind. Dies gilt insbesondere vor dem Hintergrund, dass die Einwilligung eingeholt werden müsste, bevor die ersten Daten erhoben werden und es auch die Möglichkeit der Ablehnung geben muss. In der Praxis stützen daher viele Website-Betreiber, die auf die Funktionen des Remarketing auch nach Wirksamwerden der DSGVO nicht verzichten wollen, deren Nutzung auf berechnete Interessen aus Art. 6 Abs. 1 S. 1 lit. f DSGVO. Wie bei der Webanalyse ist auch hier eine Interessenabwägung vorzunehmen.

Folgt man hingegen der unter Ziffer 1 dargestellten Auffassung der Datenschutzbehörden zum Einwilligungserfordernis für Cookies, wäre für eine solche Interessenabwägung kein Raum.<sup>20</sup> Richtigerweise wird man jedoch zwischen den verschiedenen Funktionalitäten unterscheiden müssen.<sup>21</sup> So differenzierte auch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) in einer Pressemitteilung vom 4. 10. 2017 – und damit noch auf Grundlage der alten Gesetzeslage – bei der Zulässigkeit von Facebook Custom Audiences zwischen der Nutzung mit Kundenliste und der Nutzung mittels Tracking-Pixel. Während die Nutzung von Facebook Custom Audiences i. V. m. dem Hochladen einer Kundenliste danach ganz klar einer Einwilligung bedarf, sei die Nutzung des Facebook-Pixels hingegen unter bestimmten Voraussetzungen auch ohne Einwilligung denkbar.<sup>22</sup> Diese Auffassung setzte das BayLDA in der Folge auch in der Praxis um und erließ gegen Unternehmen, die bei Facebook Custom Audiences ohne Einwilligung ihre Kundenliste hochladen entsprechende Bescheide mit Löschanordnung. Eines der adressierten Unternehmen wehrte sich dagegen sowohl im Eil- als auch im Hauptsacheverfahren, musste nunmehr jedoch vor dem VG Bayreuth eine erste Niederlage hinnehmen. So bestätigte das VG Bayreuth in der Entscheidung vom 8. 5. 2018 die Auffassung der Behörde, wonach das Hochladen einer Kundenliste ohne Einwilligung unzulässig ist.<sup>23</sup>

Auch wenn die Entscheidung noch zur Rechtslage vor Wirksamwerden der DSGVO erging, dürften die Erwägungen weitestgehend auf die neue Rechtslage übertragbar sein.<sup>24</sup> Lediglich die Ausführungen zum Verhältnis zwischen Facebook und dem Website-Betreiber – welches das VG Bayreuth hier als Funktionsübertragung bezeichnet – dürften überholt sein. Hier spricht vieles für eine gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO, die der EuGH auch im Hinblick auf den Betrieb von Fanpages<sup>25</sup> angenommen hatte.<sup>26</sup> Überdies ist auch die vom VG Bayreuth vorgenommene Interessenabwägung insoweit kritikwürdig, als das Gericht dabei argumentiert, dass der Website-Betreiber auch ohne größeren Aufwand eine Einwilligung hätte einholen können. Dabei verkennt das Gericht, dass die datenschutzrechtlichen Rechtfertigungsgründe unabhängig nebeneinander stehen und diese Frage bei der Interessenabwägung insofern gar keine Rolle spielt.<sup>27</sup>

#### b) Empfehlungen

Insgesamt stellt sich das Risiko einer Beanstandung des Remarketings durch die Datenschutzbehörden mithin ungleich höher dar als bei der Webanalyse.<sup>28</sup> Eine sichere Einbindung von Remarketing-Funktionen – insbesondere mit der Übertragung von Kundenlisten – ist aktuell nur mit Einholung einer informierten und ausdrücklichen Einwilligung möglich. Wer dies nicht umsetzen kann und die Funktion dennoch auf Grundlage von berechtigten Interessen nutzen möchte, sollte die von ihm vorgenommene Interessenabwägung sorgfältig dokumentieren, in jedem Fall eine Opt-Out-Möglichkeit implementieren und in der Datenschutzerklärung in transparenter Weise über die eingesetzte Technologie, den Anbieter (einschließlich eines eventuellen Sitzes im Drittland und – in diesem Fall – der Rechtsgrundlage für Datenübertragung ins Drittland), die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. f DSGVO sowie seine konkreten berechtigten Interessen informieren.

### 3. Kontaktformulare

Auch die Implementierung von Kontaktformularen birgt aus datenschutzrechtlicher Sicht gewisse Gefahren. Grund dafür ist eine umstrittene Entscheidung des OLG Köln aus dem Jahr 2016.<sup>29</sup> Darin beanstandet das Gericht fehlende Datenschutzzinformationen in Bezug auf ein Kontaktformular, wobei es jedoch missverständlich sowohl auf die Informationspflichten aus § 13 Abs. 1 TMG als auch auf die Voraussetzungen einer Einwilligung aus § 13 Abs. 2 TMG verweist.<sup>30</sup> Die Entscheidung wurde zu Recht dahingehend kritisiert, dass § 13 Abs. 2 TMG im vorliegenden Fall nicht anwendbar ist und die Bearbeitung einer Anfrage über ein Kontaktformular keiner Einwilligung bedarf.<sup>31</sup>

19 Vgl. ausführlich *Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, Kapitel F. I. 7.

20 So offenbar auch *Jandt*, ZD 2018, 405, 408.

21 Vgl. auch *Gierschmann*, MMR 2018, 7, 9.

22 BayLDA, Pressemitteilung vom 4. 10. 2017, abrufbar unter [www.lda.bayern.de/media/pm2017\\_07.pdf#ua#](http://www.lda.bayern.de/media/pm2017_07.pdf#ua#); Stand: 24. 9. 2018.

23 VG Bayreuth, 8. 5. 2018 – B 1 S 18.105, K&R 2018, 524, bestätigt durch VGH München, 26. 9. 2018 – 5 CS 18.1157, K&R 12/2018.

24 So auch *Nacimiento/Küll*, K&R 2018, 528 f.

25 Dazu unter III.

26 Vgl. ausführlich dazu *Herbrich*, jurisPR-ITR 16/2018 Anm. 2; *Nacimiento/Küll*, K&R 2018, 528, 529.

27 So auch *Herbrich*, jurisPR-ITR 16/2018 Anm. 2; *Nacimiento/Küll*, K&R 2018, 528, 529.

28 Vgl. auch Einschätzung von *Jandt*, ZD 2018, 405, 408.

29 OLG Köln, 11. 3. 2016 – 6 U 121/15, K&R 2016, 429.

30 OLG Köln, 11. 3. 2016 – 6 U 121/15, K&R 2016, 429, Rn. 30.

31 Vgl. nur *Klinger*, jurisPR-ITR 11/2016 Anm. 3.

Darüber hinaus verlangt auch die DSGVO in diesen Fällen keine Einwilligung, da sich die in Rede stehende Verarbeitung auf die Erforderlichkeit zur Durchführung vorvertraglicher Maßnahmen gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO stützen lässt.

In der Praxis führte die Entscheidung dazu, dass nunmehr unsinnigerweise unter nahezu jedem Kontaktformular mit einer gesonderten Tickbox eine Einwilligung in die Verarbeitung personenbezogener Daten zur Beantwortung der Kontaktanfrage verlangt wird. Noch größer wird die Verwirrung indes, wenn dann in der Datenschutzerklärung als Rechtsgrundlage – richtigerweise – Art. 6 Abs. 1 S. 1 lit. b und nicht Art. 6 Abs. 1 S. 1 lit. a DSGVO genannt wird. Wenn überhaupt, sollte hier am Ende des Kontaktformulars mit einem einfachen Hinweis auf die Geltung der Datenschutzerklärung aufmerksam gemacht und diese verlinkt werden.

Doch selbst der Sinn eines solchen Hinweises erschließt sich nicht, wenn die Datenschutzerklärung wie das Impressum ohnehin von jeder Unterseite über einen direkten Link erreichbar sein muss. Denn auch wenn das OLG Köln in der vorstehend zitierten Entscheidung eine explizite Information über die Verarbeitung der in einem Kontaktformular übermittelten Daten fordert, so handelt es sich dabei um eine vergleichsweise transparente Funktion von Websites, welche sich dem Nutzer auch ohne lange Informationen erschließt. Die Entscheidung des OLG Köln führt damit am Ende nur zu unnötigen und teils widersprüchlichen Datenschutzhinweisen und bewirken damit nicht mehr, sondern weniger Transparenz.

Darüber hinaus sorgt mit Blick auf Kontaktformulare auch ein ganz aktueller Beschluss des LG Würzburg<sup>32</sup> für Verunsicherung. Darin bejaht das Gericht im Rahmen eines Verfügungsverfahrens nicht nur eine Wettbewerbsverletzung durch eine unvollständige Datenschutzerklärung,<sup>33</sup> sondern statuiert auch in einem einzigen Satz und ohne weitere Begründung, dass die Bereitstellung eines Kontaktformulars zwingend auch eine Verschlüsselung der Website erfordert. Nicht nur in dieser Hinsicht ist diese erste bekannte Entscheidung zur Umsetzung der DSGVO auf Websites kritikwürdig. Man mag diskutieren, ob man den Nutzer im Rahmen der Datenschutzerklärung darüber informieren sollte, ob die Website verschlüsselt ist oder nicht. Eine Verpflichtung zur Verschlüsselung der Website ist allerdings ebenso fragwürdig wie ein Verbot zum Versenden von Postkarten. Denn ein informierter Nutzer kann durchaus selbst entscheiden, ob er ein solches – unverschlüsseltes – Kontaktformular nutzt oder stattdessen eine andere Kontaktmöglichkeit nutzt.

#### 4. Sonstige datenschutzrelevante Funktionen

Auch wenn eine Aufzählung aller datenschutzrelevanten Funktionen, die in der Datenschutzerklärung Erwähnung finden sollten, den Rahmen des vorliegenden Beitrags sprengen würde, sollen hier noch einige Funktionen angesprochen werden, die in der Praxis häufig von Website-Betreibern übersehen werden. Dabei handelt es sich beispielsweise um Funktionen von Drittanbietern wie Google Maps oder Google Fonts, aber auch die Implementierung von YouTube-Videos, die im erweiterten Datenschutzmodus erfolgen sollte.<sup>34</sup> In der Praxis zeigt sich, dass manchmal selbst der Webdesigner – ganz zu schweigen vom Website-Betreiber – nicht genau weiß, welche personenbezogenen Daten auf der Website erhoben werden. Ein weiteres Problem ist die ungenaue Formulierung des Art. 13 Abs. 2

DSGVO wonach die dort genannten Informationen anzugeben sind, soweit diese „notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten“. Dies führt dazu, dass in den meisten Datenschutzerklärungen sämtliche Informationen aus Art. 13 Abs. 2 DSGVO aufgenommen werden, was leider in der Regel nicht unbedingt zur Transparenz und Übersichtlichkeit der Datenschutzerklärung beiträgt. Insofern bleibt abzuwarten, wann nicht nur die Frage des Vorhandenseins einer Datenschutzerklärung, sondern auch deren Transparenz und Verständlichkeit eine Rolle in gerichtlichen Verfahren spielen wird.

In ihrer Bedeutung deutlich zurückgegangen sind hingegen die bekannten Social Media PlugIns, wie der sogenannte „Like-“ oder „Share-“ Button von Facebook. Mittlerweile sind die damit verbundenen datenschutzrechtlichen Risiken hinreichend bekannt, sodass man in der Praxis häufig nur noch Links zu den entsprechenden Social-Media-Auftritten findet. Diesbezüglich stellen sich aufgrund einer Entscheidung des EuGH nun aber neue Fragen, welche im folgenden Kapitel behandelt werden.

### III. Social Media und DSGVO

Kaum hatten die meisten Website-Betreiber rechtzeitig zum 25. 5. 2018 ihre Datenschutzerklärung auf die DSGVO angepasst, erreichte die Internetgemeinde die nächste schlechte Nachricht. In der Entscheidung „Facebook-Fanpages“ entschied der EuGH, dass der Betreiber einer bei einem sozialen Netzwerk betriebenen Fanpage gemeinsam mit dem sozialen Netzwerk für die Verarbeitung personenbezogener Daten der Besucher der Fanpage verantwortlich ist. Auch diese Entscheidung ist noch zur alten Rechtslage ergangen, ist aber inhaltlich voll und ganz auf die DSGVO übertragbar.<sup>35</sup> Allerdings lässt die Entscheidung insbesondere im Hinblick auf die Verteilung der Verantwortlichkeit zwischen den beiden Verantwortlichen einen nicht unerheblichen Entscheidungsspielraum für die Gerichte.<sup>36</sup>

Dennoch äußerten sich die Datenschutzbehörden noch vor Fortführung des der Entscheidung zu Grunde liegenden Ausgangsverfahrens vor dem BVerwG in einem Positionspapier der DSK vom 6. 6. 2018 und statuierten, dass beim Betrieb von Fanpages dringender Handlungsbedarf bestehe.<sup>37</sup> Gleichzeitig räumte die DSK in dem Papier ein, dass die Betreiber von Fanpages aktuell gar nicht in der Lage sind, über die Verarbeitung personenbezogener Daten durch Facebook hinreichend transparent zu informieren, da ihnen die entsprechenden Informationen nicht vorlägen. Mit Beschluss vom 5. 9. 2018 hat die DSK noch einmal nachgelegt und betont, dass Facebook zwar einige Änderungen in seinem Angebot vorgenommen hätte, doch nach wie vor auch bei Personen, die keine Facebook-Nutzer seien, Daten erhebt.<sup>38</sup> Zudem gebe es entgegen der Ankündigung nach wie vor keine Vereinbarung für gemeinsame Verantwortliche im Sinne von Art. 26 DSGVO. Schließlich fügte die DSK

32 LG Würzburg, 13. 9. 2018 – 11 O 1741/18, K&R 2018, 736 (in diesem Heft).

33 A. A. LG Bochum, 7. 8. 2018 – I-12 O 85/18, K&R 2018, 737 (in diesem Heft), vgl. dazu *Schreiber*, GRUR-Prax 2018, 371.

34 Vgl. *Koreng/Lachenmann* (Fn. 19), Kapitel F 1 6 Rn. 6.

35 Vgl. auch *Härting/Gössling*, NJW 2018, 2523, 2525.

36 *Härting/Gössling*, NJW 2018, 2523, 2524 ff.

37 Entschließung der DSK vom 6. 6. 2018, abrufbar unter: <https://www.datenschutzzentrum.de/uploads/facebook/2018-06-05-Entschliessung-DSK-Fanpages-EuGH-Urteil.pdf>, Stand: 24. 9. 2018.

38 Beschluss der DSK vom 5. 9. 2018, abrufbar unter: <https://www.datenschutzzentrum.de/uploads/facebook/20180905-DSK-Facebook-Fanpages.pdf>, Stand: 24. 9. 2018.

ihrer Entschließung einen 8-Punkte-Fragenkatalog für die Fanpage-Betreiber bei.

Mittlerweile hat Facebook auf das Urteil des EuGH reagiert und ein Page Insights Controller Addendum (deutsch: Seiten-Insights-Ergänzung bezüglich des Verantwortlichen) veröffentlicht.<sup>39</sup> Ob dies den vorstehend in Bezug genommenen Anforderungen der DSK genügt, dürfte bezweifelt werden. Insbesondere die Frage der Speicherung von personenbezogenen Daten von Nicht-Facebook-Nutzern ist nach wie vor nicht geklärt. Es scheint sich hier somit ein Ping-Pong-Spiel zwischen Facebook und den Datenschutzbehörden zu entspinnen, welches bedauerlicherweise auf dem Rücken der Unternehmen ausgetragen wird. Dabei ist zu berücksichtigen, dass nicht primär die großen Unternehmen mit großer Datenschutzabteilung auf eine Präsenz bei Facebook angewiesen sind, sondern vor allem Einheiten mit geringem Werbebudget wie Start-Ups oder auch gemeinnützige Organisationen.

Es wäre daher wünschenswert, wenn die europäischen Datenschutzbehörden ihren Streit mit Facebook direkt austragen würden und nicht über Löschanordnungen gegenüber den Betreibern von Fanpages. Das aktuelle Vorgehen sorgt stattdessen für ein zusätzliches Maß an Rechtsunsicherheit, welche aufgrund des Wirksamwerdens der DSGVO ohnehin schon ein kaum mehr erträgliches Maß angenommen hat. Sowohl die Entscheidung des EuGH als auch die Entschließungen der DSK lassen zudem zahlreiche Fragen offen – wie zum Beispiel die Übertragbarkeit auf andere sozialen Netzwerke.<sup>40</sup>

Wer seine Facebook-Seite bislang kaum aktiv nutzt und eher als zusätzliche Visitenkarte vorhält, der sollte überlegen, ob er das aktuelle rechtliche Risiko dafür tatsächlich eingehen will. Im Übrigen erscheint das Abschalten von Facebook-Seiten aktuell (noch?) nicht angezeigt.<sup>41</sup> Entscheidend ist, dass entsprechende Verträge zur gemeinsamen Verantwortlichkeit, die von Facebook zur Verfügung gestellt werden, auch akzeptiert werden und dass der Nutzer im Rahmen der Datenschutzerklärung – welche auch auf der Fanpage selbst abrufbar sein sollte – so gut wie möglich über die Verarbeitung personenbezogener Daten in dem jeweiligen sozialen Netzwerk informiert wird.<sup>42</sup>

#### IV. Newsletter und DSGVO

Eher überraschend hat man das Wirksamwerden der DSGVO am deutlichsten beim Empfang von Newslettern bemerkt. So gab es in den Wochen um den 25. 5. 2018 zahlreiche E-Mails, mit denen man wahlweise lediglich über die Datennutzung zum Versand des Newsletters informiert oder aber um die aktive Bestätigung des Newsletter-Abonnements gebeten wurde. Überraschend ist dies deswegen, weil sich rein materiell-rechtlich in dieser Hinsicht durch das Wirksamwerden der DSGVO nichts geändert hat. Vielmehr galt auch bisher schon gemäß § 7 UWG ein Einwilligungserfordernis für den Versand von Newslettern. Einziger Ausnahmefall war und ist gemäß § 7 Abs. 3 UWG die E-Mail-Werbung für Bestandskunden, die allerdings nur unter ganz engen Voraussetzungen möglich ist. Die Vorschrift des § 7 UWG basiert auf Art. 13 der E-Privacy-RL von 2002. Anders als bei der Webanalyse sind hier aktuell auch keine Änderungen durch die E-Privacy-VO zu erwarten. Sowohl der Entwurf der Kommission als auch jener des Parlamentes sehen weiterhin ein Einwilligungserfordernis vor. Änderungen wird es voraussichtlich ledig-

lich im Hinblick auf die konkreten Voraussetzungen der Ausnahmeregelung für Bestandskunden geben.<sup>43</sup>

Gleichwohl häufen sich aktuell nicht nur die Abmahnungen wegen unverlangt zugesandter E-Mail-Werbung, sondern auch die Gerichtsentscheidungen zu dem Thema. So hat der BGH erst kürzlich darüber befunden, dass das Übersenden einer Kundenzufriedenheitsanfrage per E-Mail ohne Einwilligung des Nutzers auch dann rechtswidrig ist, wenn sie einer im Übrigen zulässigen E-Mail (im konkreten Fall: Übersendung der Rechnung) beigelegt ist.<sup>44</sup> Weiterhin stellte das OLG Düsseldorf klar, dass die Ausnahmeregelung des § 7 Abs. 3 UWG eine tatsächliche Geschäftsbeziehung voraussetzt. Ein bloßer Interessent, der lediglich eine Anfrage zu einem Produkt stellt, sei hingegen kein Kunde.<sup>45</sup> Überraschend weit fasst hingegen das OLG München den Tatbestand des § 7 Abs. 3 UWG und lässt auch die unentgeltliche Registrierung auf einer Partnervermittlungsplattform als „Verkauf“ einer Dienstleistung im Sinne von § 7 Abs. 3 UWG gelten.<sup>46</sup>

In der Praxis hat sich gezeigt, dass das Einwilligungserfordernis des § 7 UWG bei Weitem nicht allen Unternehmern bekannt war und gerade bei bestehenden Kundenbeziehungen häufig von einer Zulässigkeit des Newsletter-Versands ausgegangen wurde. In diesen Fällen kommt zwar typischerweise eine Rechtfertigung über § 7 Abs. 3 UWG in Betracht, allerdings fehlte es in der Vergangenheit häufig an der dafür erforderlichen Information des Kunden bei Erhebung der Daten. Gerade vor dem Hintergrund, dass der Ausnahmetatbestand für Bestandskunden nach den aktuellen Entwürfen mit überwiegender Wahrscheinlichkeit auch weiterhin gelten wird, kann eine Überarbeitung der Bestellformulare oder Verträge hier für die Zukunft durchaus nützlich sein.

Eine bislang eher selten besprochene Frage ist hingegen die datenschutzrechtliche Zulässigkeit der Auswertung des Nutzerverhaltens beim Newsletterversand. Fast jedes Versand-Tool bietet seinen Kunden die Möglichkeit, das Lese- und Klickverhalten der Empfänger auszuwerten. Dies erfolgt typischerweise über Web-Beacons oder Tracking-Pixel, die im Newsletter enthalten sind. Während der Abmeldelink in jedem Newsletter mittlerweile Standard ist, bieten nur die wenigsten Versand-Tools eine Opt-Out-Möglichkeit für das Newsletter-Tracking. Dies kann daher in der Regel nur dadurch verhindert werden, dass im E-Mail-Programm die Anzeige von Bildern deaktiviert ist.

Rechtsgrundlage für das Newsletter-Tracking kann wiederum entweder eine Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO oder das berechtigte Interesse nach Art. 6 Abs. 1 S. 1 lit. f DSGVO sein. Wie beim Webtracking muss hier jedoch eine sorgfältige Interessenabwägung vorgenommen werden, die insbesondere beim personalisierten Newsletter-Tracking keineswegs immer zugunsten des Unternehmens

39 [https://de-de.facebook.com/legal/terms/page\\_controller\\_addendum](https://de-de.facebook.com/legal/terms/page_controller_addendum), Stand: 24. 9. 2018.

40 So auch *Golland*, K&R 2018, 433, 438; *Wagner*, jurisPR-ITR 15/2018 Anm. 2.

41 So auch *Härtling/Gössling*, NJW 2018, 2523, 2526.

42 *Härtling/Gössling*, NJW 2018, 2523, 2526; *Golland*, K&R 2018, 433, 437.

43 Vgl. Gegenüberstellung der beiden Entwürfe, abrufbar unter: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//DE>; Stand: 24. 9. 2018, vgl. auch *Gierschmann*, MMR 2018, 7, 9.

44 BGH, 10. 7. 2018 – VI ZR 225/17.

45 OLG Düsseldorf, 5. 4. 2018 – I-20 U 155/16.

46 OLG München, 15. 2. 2018, K&R 2018, 409, vgl. dazu ausführlich *Herbrich*, jurisPR-ITR 11/2018 Anm. 5.

ausfallen dürfte. Bei der Einwilligung stellt sich hingegen das Problem des Kopplungsverbot des Art. 7 Abs. 4 DSGVO.<sup>47</sup> Denn die Zusendung eines Newsletters erfordert nicht zwingend die Auswertung des Nutzerverhaltens. Auch wenn hier gute Gründe gegen einen Verstoß gegen das Kopplungsverbot sprechen – der Newsletter ist typischerweise eine kostenlose Leistung – könnte dies wiederum dafür sprechen, das Newsletter-Tracking auf das eigene berechnete Interesse an der Messung des Erfolges und der Reichweite der eigenen Marketing-Maßnahmen zu stützen. In jedem Fall erfordert jede Form des Newsletter-Trackings eine umfassende Information in der Datenschutzerklärung und idealerweise auch eines Hinweises in den korrespondierenden Texten wie zum Beispiel in der Einwilligung selbst oder in der Bestätigungsmail. Darüber hinaus sollte bei der Newsletter-Bestellung stets auch über die Anmeldung im Double-Opt-In-Verfahren sowie die damit einhergehende Datenspeicherung, die Abmeldemöglichkeiten sowie gegebenenfalls den Einsatz eines Versand-Dienstleisters in den USA und die entsprechende Rechtfertigung informiert werden.

## V. Ausblick

Die Beratung von Unternehmen rund um das Thema Online-Marketing ist aktuell schwieriger denn je. Bereits vor Wirksamwerden der DSGVO gab es zahlreiche Unklarheiten wie beispielsweise zum Umgang mit Cookies oder den konkreten Voraussetzungen für die Zulässigkeit des

Newsletter-Versands. Vor diesem Hintergrund verwundert es kaum, dass es aktuell zahlreiche Entscheidungen der unterschiedlichsten Gerichte zu den unterschiedlichen Themen gibt, die allerdings in weiten Teilen noch zur alten Rechtslage ergehen – wie zum Beispiel die Entscheidungen zur Facebook Fanpage oder zu Facebook Custom Audiences.

Auch die DSGVO hat kaum zur Beantwortung der offenen Fragen beigetragen, sondern eröffnet – ganz im Gegenteil – zahlreiche neue Problemfelder. Dies gilt umso mehr, als die E-Privacy-VO, welche die DSGVO gerade im Online-Bereich ergänzen und präzisieren soll, entgegen der ursprünglichen Planung nicht gleichzeitig mit der DSGVO wirksam geworden ist.

Aktuell wird nicht vor Ende des Jahres mit einem gemeinsamen Standpunkt des EU-Rates gerechnet; die Trilog-Verhandlungen zwischen Kommission, Parlament und Rat würden dann voraussichtlich 2019 abgeschlossen werden. Frühestens Ende 2019 wird uns mithin die finale Fassung der E-Privacy-VO vorliegen, die hoffentlich viele Fragen klärt und nicht ihrerseits wieder zu (neuer) Rechtsunsicherheit führt. Bis dahin könnten möglicherweise erste Entscheidungen zur neuen Rechtslage – zum Beispiel in dem erwähnten Vorlageverfahren des BGH zu Cookies – die erhofften Antworten auf die hier diskutierten Fragen geben.

47 Vgl. ausführlich zum Kopplungsverbot *Remmert*, GRUR-Prax 2018, 254, 255.

Christian Galetzka, LL.M., Würzburg\*

# Web-Analytics/Retargeting und automatisierte Einzelfallentscheidung

*Das Thema Web-Analytics bzw. Webtracking und Retargeting wird aktuell nicht nur vor dem Hintergrund des Inkrafttretens der EU Datenschutz-Grundverordnung (DSGVO) verbreitet diskutiert. Befeuert wird die Thematik zusätzlich durch eine im April 2018, also kurz vor Inkrafttreten der DSGVO veröffentlichte, übrigens wenig überzeugende Positionsbestimmung der Datenschutzkonferenz (DSK) unter anderem zur (Nicht-)Anwendbarkeit des TMG und mit dem Statement, dass Webtracking ohne Unterscheidung der Funktionsweise und Art der Datenverarbeitung nur noch mit Einwilligung des Besuchers einer Webseite zulässig sein soll. Der Beitrag beleuchtet diese aktuellen Entwicklungen gleichermaßen wie die technischen Grundlagen des Webtracking und Retargeting als effiziente Möglichkeit für Webseitenbetreiber, statistische Auswertungen über das Nutzungsverhalten ihrer Webseite zu fahren bzw. Nutzer über die gezielte Schaltung von Werbeanzeigen auf anderen Webseiten wieder anzusprechen. Diese Maßnahmen werfen datenschutzrechtliche Fragen auf, die innerhalb des Regelungsgefüges der DSGVO im Vergleich zur alten Rechtslage teilweise neu bewertet werden müssen. Retargeting-Marketingmaßnahmen als automatisierte Entscheidungen im Einzelfall einzuordnen und rechtlich zu bewerten, ist Schwerpunkt des Beitrags.*

## I. Einleitung

Web-Analytics<sup>1</sup> und Retargeting<sup>2</sup> als verbreitete Maßnahmen zielgruppenspezifischer Online-Werbung von Webshop- oder Social Media-Betreibern in einem Atemzug mit der besonderen Thematik der automatisierten Einzelfallentscheidung zu nennen und der Symbiose eine eigene Abhandlung zu widmen, scheint auf den ersten Blick nicht ganz naheliegend. Die thematische Paarung drängt sich aber auf dem zweiten Blick auf, insbesondere wenn man sich die Neuregelung zur automatisierten Einzelfallentscheidung in der seit 25. 8. 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung<sup>3</sup> näher ansieht.

\* Mehr über den Autor erfahren Sie auf S. VIII. Der Beitrag geht auf einen Vortrag des Autors bei der DSRI-Herbstakademie 2018 in Bochum zurück, der im Tagungsband Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, DSRI-Herbstakademie 2018, 2018, dokumentiert ist. Die zitierten Internetquellen wurden zuletzt abgerufen am: 27. 9. 2018.

1 Im Folgenden auch „Webtracking“ genannt.

2 Oder auch Remarketing. Im Folgenden einheitlich „Retargeting“ genannt.

3 VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), ABl. EU L 119/1 v. 4. 5. 2016 (nachfolgend „DSGVO“).