Sven Venzke-Caprarese

Retargeting in der Onlinewerbung

Rechtliche Rahmenbedingungen für zielgenaue Werbung

Werbung ist aus dem Internet kaum wegzudenken. Um diese an den unterschiedlichsten Stellen im Internet noch zielgenauer ausspielen zu können, kommen auch Trackingtechnologien zum Einsatz. Diese ermöglichen es, einzelnen Nutzern personalisierte Werbung anhand ihres vorherigen Nutzungsverhaltens anzuzeigen. Hierbei wird immer häufiger versucht, das entsprechende Tracking durch sog. „Cookie-Banner" zu legitimieren. Dieser Beitrag beleuchtet die damit einhergehenden datenschutz- und telemedienrechtlichen Fragen und stellt die zu beachtenden rechtlichen Rahmenbedingungen dar.

1 Funktionsweise des Retargetings

Mithilfe von Retargeting (teilweise auch Remarketing oder Custom Audience from your Website genannt) versuchen Werbetreibende, Werbung anhand vorheriger Besuche ihrer Website auf anderen Seiten personalisiert auszuspielen.

Ein typisches Anwendungsszenario für Retargeting stellt sich wie folgt dar: Ein Internetnutzer besucht einen Online-Shop und sieht sich dort ein bestimmtes Produkt an. Er verlässt die Seite jedoch, ohne das Produkt zu kaufen. Einige Tage später besucht derselbe Nutzer eine ganz andere Internetseite, z. B. ein Nachrichtenportal. Hier wird ihm nun Werbung für genau das Produkt eingeblendet, welches er sich vor einigen Tagen angesehen hatte. Ein Klick auf die Produktwerbung führt auf die Seite des ursprünglichen Online-Shops und diesmal entschließt sich der Nutzer zum Kauf des Produkts.

Das Beispiel lässt sich fortführen: Ein Nutzer kauft online eine Kaffeekapselmaschine und sieht künftig in regelmäßigen Abständen Zubehör- und Kapselwerbung auf anderen Seiten. Ein Nutzer besucht die Kampagnenseite einer Partei und liest dort mehrere Unterseiten zu einem bestimmten Thema. Kurz vor der Wahl begegnen diesem Nutzer plötzlich auf mehreren Seiten im Internet Bannerwerbungen, die genau dieses Thema aufgreifen und zur Wahl des entsprechenden Kandidaten aufrufen. Ein Nutzer besucht die Informationsseite eines Pharmakonzerns, die über eine bestimmte Erkrankung aufklärt. Wenige Minuten später wird Werbung für ein rezeptfreies Arzneimittel dieses Herstellers auf anderen Seiten angezeigt.

Damit Retargeting in der Praxis funktioniert, müssen technisch einige Voraussetzungen gegeben sein:

1.1 Wiedererkennungsmerkmal schaffen

Retargeting basiert maßgeblich auf der Wiedererkennung eines Nutzers innerhalb eines Werbenetzwerks. Dem Betreiber des Werbenetzwerks stehen zur Wiedererkennung des Nutzers in der Regel eine ganze Reihe von verschiedenen Trackingtechnologien zur Verfügung, etwa HTML-Cookies, Fingerprints, Trackingpixel (Web Beacons), Evercookies[1], Mobile Advertising Identifier, die Auswertung von IP-Adressen, die Verwendung von personenbezogenen Nutzungsdaten etc. Damit ein Nutzer innerhalb des Werbenetzwerks wiedererkannt werden kann, ist es erforderlich, dass alle beteiligten Websitebetreiber dem Betreiber des Werbenetzwerks gestatten, Trackingtechnologien auf ihren Seiten einzubinden. Dies erfolgt in der Regel dadurch, dass sowohl in die Seite des Werbetreibenden[2] als auch in alle Seiten des Werbenetzwerks, auf denen Werbung angezeigt werden kann[3] (sog. Publisher), Javascriptcode des Werbenetzwerkbetreibers durch die jeweiligen Websitebetreiber in den HTML-Code der Seite eingebunden wird. Der Betreiber des Werbenetzwerks ist damit in der Lage, einen Nutzer über alle Seiten, die am Werbenetzwerk teilnehmen, wiederzuerkennen.

1.2 Retargetingkampagne definieren

Werbetreibende, die den entsprechenden Code des Werbenetzwerks in ihre Seiten eingebunden haben, können nun Retarge-

Sven Venzke-Caprarese

Rechtsanwalt und Berater bei der datenschutz nord GmbH mit dem Schwerpunkt Datenschutz in neuen Medien

E-Mail: svenzke@datenschutz-nord.de

1 https://github.com/samyk/evercookie/blob/master/README.md, alle in diesem Artikel aufgeführten Links wurden zuletzt am 2.7.2017 abgerufen.

2 Vgl. z. B. Google Hilfe-Seite „Remarketing einrichten": https://support.google.com/adwords/answer/2454000.

3 Vgl. z. B. Google Hilfe-Seite „Anzeigencode auf Webseiten einfügen": https://support.google.com/adsense/answer/181958.

tingkampagnen definieren. Hierzu müssen Werbetreibende Werbeanzeigen gestalten und festlegen, wann diese ausgespielt werden sollen. Soll bereits der Besuch der Website dazu führen, dass dem Besucher die Werbung auf anderen Seiten des Werbenetzwerks angezeigt wird? Oder soll erst der Besuch einer bestimmten Unterseite die entsprechende Werbeanzeige auslösen? Je nachdem, wofür sich Werbetreibende entscheiden, kann es erforderlich werden, die einzelnen Unterseiten der Website entsprechend zu kennzeichnen.

Dabei müssen Werbetreibende häufig auch Richtlinien und Nutzungsbedingungen des Werbenetzwerkbetreibers akzeptieren. Google verbietet durch eigene Werberichtlinien z. B. Retargeting im Hinblick auf Glücksspiel, politische Neigung (mit Ausnahmen für die USA), die Rekrutierung von Teilnehmern für klinische Studien, eingeschränkt zulässige Arzneimittel, Gesundheit, Informationen zu finanziellen Schwierigkeiten, Straftaten, Missbrauch, sexuelle Orientierung, ethnische Zugehörigkeit, religiöse Überzeugung etc.[4] Andere Werbenetzwerkbetreiber sind an dieser Stelle weniger restriktiv.[5]

1.3 Wiedererkennen und bewerben

Haben alle am Werbenetzwerk teilnehmenden Websitebetreiber sowie der Werbetreibende die entsprechenden Wiedererkennungsmerkmale geschaffen und wurde die Retargetingkampagne definiert, kann der Werbetreibende seine Websitebesucher basierend auf den vorher besuchten Seiten nun innerhalb des Werbenetzwerks gezielt ansprechen lassen.

Da das Wiedererkennungsmerkmal allerdings regelmäßig im Zusammenhang mit dem Client bzw. mit dem Browser erstellt wird, ist es nicht ohne Weiteres möglich, einen Nutzer über mehrere Geräte hinweg zu bewerben.

1.4 Mehrere Geräte verknüpfen, um geräteübergreifend zu bewerben

Um Nutzer geräteübergreifend bewerben zu können, führen einige Werbenetzwerkbetreiber die Wiedererkennungsmerkmale eines Nutzers zusammen. Möglich ist dies immer dann, wenn sich Nutzer gegenüber dem Betreiber des Werbenetzwerks zu erkennen geben. Google bietet das geräteübergreifende Retargeting z. B. seit dem 15. Mai 2017 an und nutzt hierfür die Daten von eingeloggten Nutzern seiner Dienste.[6] Loggt sich ein Nutzer also mit seinem Google Account ein, um z. B. Gmail, Goolge+, den PlayStore, Google Drive, YouTube, Google Maps etc. zu nutzen, kann Google die auf dem Endgerät gespeicherten Wiedererkennungsmerkmale einem übergeordneten Wiedererkennungsmerkmal (z. B. einer von Google vergebenen UserID[7]) zuordnen. Auf diese Weise können die Wiedererkennungsmerkmale aller Endgeräte zusammengeführt werden, auf denen sich ein Nutzer mit seinem Google-Account (und sei es nur für eine logische Sekunde) angemeldet hat. Hierdurch ist es möglich, dass der Besuch einer Internetseite mit dem Smartphone eine Woche später dazu führt, dass der Nutzer entsprechende Werbung auf seinem privaten Desktop-PC, seinem Laptop und seinem Arbeitsplatz-PC angezeigt bekommt.

Google führt hierzu an, dass nur die Nutzer geräteübergreifend beworben werden, die hierfür mittels Opt-In zugestimmt haben.[8] Bei dieser von Google angesprochenen Opt-In-Lösung scheint es sich um die Zustimmung zu einem Text „Datenschutz und Bedingungen" zu handeln, der Nutzern im Rahmen der erstmaligen Registrierung angezeigt wird und der zwei Optionen zulässt: Abbrechen oder zustimmen.

2 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen des Retargetings sind bislang nicht klar definiert und äußerst umstritten.

2.1 Einwilligung versus § 15 Abs. 3 TMG

Zum Teil wird das Retargeting ohne nähere Begründung dem Anwendungsbereich des § 15 Abs. 3 TMG zugeordnet.[9]

Demgegenüber wird aber auch vertreten, dass beim Retargeting davon auszugehen ist, dass die dem Werbenetzwerk angehörigen Webseiten Nutzungsdaten an das Werbenetzwerk übermitteln.[10] Diese Datenübermittlung werde vom einzelnen Websitebetreiber allerdings nicht bewusst herbeigeführt, sondern allenfalls in Kauf genommen. Der am Werbenetzwerk teilnehmende Websitebetreiber habe weder Einfluss auf die Datenverarbeitung noch würden die Nutzungsprofile durch ihn erstellt. Aus diesem Grund sei es bereits fraglich, ob die zugrundeliegende Datenverarbeitung überhaupt durch § 15 Abs. 3 TMG legitimiert werden kann. Auch eine etwaige Ausgestaltung des Retargetings als Auftragsdatenverarbeitung wird vor dem Hintergrund der fehlenden Einflussnahmemöglichkeit des einzelnen Websitebetreibers in Frage gestellt.[11]

Teilweise wird vertreten, dass die bloße Einbindung von Inhalten Dritter noch nicht dazu führe, dass den Websitebetreiber eine datenschutzrechtliche Verantwortung treffe – selbst wenn es sich bei diesen Inhalten offensichtlich um Trackingpixel handelt.[12] Zudem finde auch gar keine Datenübermittlung vom Websitebetreiber an das Werbenetzwerk statt. Denn die Daten würden bei Aufruf der Website direkt vom Nutzer (bzw. seinem Browser) an das Werbenetzwerk übermittelt, ohne dass der Websitebetreiber diese kenne. Der einzelne Websitebetreiber sei somit aus der Verantwortung genommen.[13] Der Werbenetzwerkbetreiber könne sich hingegen auf § 15 Abs. 3 TMG berufen, müsse jedoch dafür Sorge tragen, dass die Nutzer entsprechend informiert werden

4 AdWords-Werberichtlinien-Hilfe zur personalisierten Werbung: https://support.google.com/adwordspolicy/answer/143465?hl=de.

5 Facebook Advertising Policies: https://www.facebook.com/policies/ads, dort Ziffer 7.

6 Google Analytics-Hilfe zum Cross-Device Remarketing: https://support.google.com/analytics/answer/7365094.

7 Vgl. zum geräteübergreifenden Tracking mittels UserID auch *Ertel/Venzke-Caprarese*, Google Universal Analytics, DuD 2014, 181-185. Die dort beschriebene Zusammenführung von Wiedererkennungsmerkmalen erfolgt jedoch nur auf Ebene des Websitebetreibers zur geräteübergreifenden Nutzungsprofilbildung und nicht auf Ebene des Werbenetzwerks.

8 Google Analytics-Hilfe zum Cross-Device Remarketing: https://support.google.com/analytics/answer/7365094.

9 *Koglin* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht (2015), Teil B Kapitel IV Ziffer 2.

10 *Conrad/Klatte* in Forgó/Helfrich/Schneider, Betrieblicher Datenschutz (2014), Teil VIII. Kapitel 4, Rn. 94-95.

11 *Conrad/Klatte, a. a. O.*

12 *Voigt*, Webbrowser Fingerprints – Tracking ohne IP-Adressen und Cookies?, DSRITB 2013, 157-173 (168).

13 *Voigt/Alich*, Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, 3541-3544 (3542).

und über Widerspruchsrechte verfügen. Dies könne dadurch erreicht werden, dass Werbenetzwerkbetreiber mit den Websitebetreibern Verträge schließen, wonach Websitebetreiber verpflichtet werden, auf die Datenverarbeitung in der Datenschutzerklärung hinzuweisen und ggf. eine Widerspruchsmöglichkeit anbieten. Zudem könnten Werbebanner mit Links versehen werden, die zu einer Informationsseite führen, auf welcher dann auch der Datenverarbeitung widersprochen werden kann.[14]

Bei der rechtlichen Bewertung des Retargetings ist festzustellen, dass der Websitebetreiber selbst keine Daten unmittelbar an den Werbenetzwerkbetreiber übermittelt. Allerdings bindet der Websitebetreiber bewusst die Trackingtechnologie des Werbenetzwerkbetreibers in den HTML-Code seiner Seiten ein, damit der Werbenetzwerkbetreiber einen Nutzer diensteanbieterübergreifend wiedererkennen kann. Der Ansicht, dass den Websitebetreiber keinerlei Verantwortung trifft, ist in einer ähnlichen Konstellation zuletzt das LG Düsseldorf entgegengetreten, welches im Falle der unmittelbaren Einbindung von Social Plugins die Verantwortlichkeit des Websitebetreibers bejaht hat.[15] Dabei stellte das Gericht fest, dass die Datenverarbeitung des Dritten erst durch den HTML-Befehl des Websitebetreibers initiiert werde. Zudem machte das Gericht klar, dass der Websitebetreiber, der durch die Einbindung von Drittinhalten in das eigene Angebot einen Verarbeitungsprozess auslöst, hierfür auch datenschutzrechtlich verantwortlich sei. Zwar könnte gegen diese Ansicht des Gerichts angeführt werden, dass die Hürden zu hoch sind, weil sie in der Praxis zu einer Beschränkung der Meinungsfreiheit führen können, da die Einbindung jedweder Drittinhalte somit kaum noch möglich wäre. Sofern allerdings datenschutzkonforme Alternativen zur unmittelbaren Einbindung der Drittinhalte bestehen[16] oder der Websitebetreiber, wie im Falle des Retargetings, weiß, dass die Einbindung der Drittinhalte ausschließlich dem Zweck dient, einem Dritten diensteanbieterübergreifendes Tracking zu ermöglichen, kommt auch diesem Gegenargument kein Gewicht zu. Das Urteil des LG Düsseldorf ist allerdings noch nicht rechtskräftig, sondern befindet sich in der Berufungsinstanz vor dem OLG Düsseldorf. Dieses hat das Verfahren ausgesetzt und dem EuGH im Rahmen eines Vorabentscheidungsverfahrens die relevanten Rechtsfragen vorgelegt.[17] Hierbei geht es insbesondere um die Frage, ob der Websitebetreiber für die Datenverarbeitung des Drittanbieters verantwortlich gemacht werden kann.

Darüber hinaus muss bei der Frage der Rechtmäßigkeit des Retargetings auch die Datenverarbeitung des Werbenetzwerkbetreibers beachtet werden. Dieser wird sich grundsätzlich nicht auf die Privilegierung des § 15 Abs. 3 TMG berufen können. Denn § 15 Abs. 3 TMG erlaubt lediglich dem jeweiligen Diensteanbieter, Nutzungsprofile bei Verwendung von Pseudonymen zu erstellen, sofern der Nutzer dem nicht widerspricht. Der von § 15 Abs. 3 TMG privilegierte Diensteanbieter ist an dieser Stelle aber nur der jeweilige Websitebetreiber und nicht das übergeordnete Werbenetzwerk, welches sich in die Lage versetzt, Nutzer diensteanbieterübergreifend wiederzuerkennen.

Hinzu kommt, dass auch das geräteübergreifende Tracking eines Nutzers regelmäßig nicht von § 15 Abs. 3 TMG umfasst sein wird, da hierzu Identifikationsdaten des Nutzers (seine Logindaten) mit den jeweiligen Wiedererkennungsmerkmalen zusammengeführt werden müssen.[18]

Im Ergebnis ist daher festzustellen, dass sich der Einsatz von Retargeting grundsätzlich außerhalb der Privilegierung des § 15 Abs. 3 TMG bewegt und vieles dafür spricht, dass sowohl der Websitebetreiber als auch der Werbenetzwerkbetreiber an dieser Stelle datenschutzrechtliche Verantwortlichkeiten tragen. Retargeting ist daher nur mit einer Einwilligung der betroffenen Nutzer zulässig.

2.2 Nutzungsbedingungen der Werbenetzwerkbetreiber

Die meisten Werbenetzwerkbetreiber regeln die Nutzung ihrer Trackingtechnologien in Nutzungsbedingungen, die gegenüber den Werbetreibenden, aber auch gegenüber den am Werbenetzwerk teilnehmenden Websitebetreibern (Publisher) gelten.

2.2.1 Google

Insbesondere Google fordert seit Mitte Mai 2015 in unterschiedlichen Nutzungsbedingungen seiner Produkte, dass Werbetreibende und Publisher die sog. „Richtlinie zur Einwilligung der Nutzer in der EU" einhalten müssen. Betroffen hiervon sind insbesondere die Dienste:

- Remarketing mit Google Analytics;
- Berichte zu Impressionen im Google Displaynetzwerk;
- Google Analytics-Berichte zur Leistung nach demografischen Merkmalen und Interessen;
- Integrierte Dienste, für die in Google Analytics Daten mithilfe von Cookies für Anzeigenvorgaben und Kennungen gesammelt werden müssen.

Im Gegensatz zur reinen Nutzung von Google Analytics in der Standardimplementierung, welche bei Beachtung der Hinweise des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit im Rahmen von § 15 Abs. 3 TMG beanstandungsfrei genutzt werden kann[19], zieht Google bei den o.g. Diensten eine Grenze. Und dies aus gutem Grund: Denn wie bereits dargestellt verlässt insbesondere das Retargeting (Google nennt dies Remarketing) den Anwendungsbereich des § 15 Abs. 3 TMG. Google greift insofern auch der Antwort des EuGH auf die Frage der Verantwortlichkeit vor und fordert von Websitebetreibern: *„Sie müssen wirtschaftlich angemessene Maßnahmen ergreifen, um sicherzustellen, dass ein Endnutzer verständliche und umfassende Informationen zur Speicherung von und zum Zugriff auf Cookies und Daten auf dem Gerät des Endnutzers erhält und diesen Aktivitäten*

14 *Voigt*, Webbrowser Fingerprints – Tracking ohne IP-Adressen und Cookies?, DSRITB 2013, 157-173 (170).

15 LG Düsseldorf, Urteil vom 9.3.2016, Az. 12 O 151/15.

16 Im vom LG Düsseldorf behandelten Fall der unmittelbaren Einbindung des Like-Buttons ist hier vor allem an die sog. 2-Klick-Lösung oder die Shariff-Lösung zu denken.

17 OLG Düsseldorf, Beschluss vom 19.1.2017, Az. I-20 U 40/16.

18 Hieran ändert auch eine etwaige Umwandlung der Identifikationsdaten in Hashwerte nichts. Denn obwohl ein Hashwert nicht zurückgerechnet werden kann, ist es doch möglich, innerhalb von Hashwerten nach Identifikationsdaten zu suchen. Hierzu muss lediglich das Hashverfahren bekannt sein, das gesuchte Identifikationsdatum entsprechend gehasht werden und das Ergebnis dann im vorhandenen Hashwertpool gesucht werden. Verläuft die Suche erfolgreich, können die zu dem Hashwert gespeicherten Daten einem Nutzer zugeordnet werden.

19 Google Analytics – Hinweise für Webseitenbetreiber in Hamburg: https://www.datenschutz-hamburg.de/news/detail/article/google-analytics-hinweise-fuer-webseitenbetreiber-in-hamburg.html.

zustimmt, wenn derartige Aktivitäten im Zusammenhang mit der Verwendung eines Produkts erfolgen, für das diese Richtlinie gilt."[20]

Wie die Einwilligung genau eingeholt werden muss, lässt Google zwar offen, verweist aber in der Hilfe zur Richtlinie über die Zustimmung der Nutzer in der EU auf die Website cookiechoices.org, welche Nutzern die Verwendung eines Cookie-Banners zur Einholung der Einwilligung nahelegt.

2.2.2 Facebook

Facebook bezeichnet das Retargeting als „Custom Audience from your Website" und fordert in den entsprechenden Nutzungsbedingungen ebenfalls eine Einwilligung: „*In jurisdictions that require informed consent for the storing and accessing of cookies or other information on an end user's device (such as but not limited to the European Union), you must ensure, in a verifiable manner, that an end user provides the necessary consent before you use Facebook Tools to enable Facebook to store and access cookies or other information on the end user's device.*"[21]

In diesem Rahmen rät auch Facebook ausdrücklich zur Nutzung von Cookie-Bannern und bezeichnet als üblichen Ansatz zur Einwilligungseinholung folgenden Weg: „*Displaying a prominent message when a page loads for the first time (this is usually called a "cookie banner") and informing users what action to take to consent*".[22]

2.3 Die Verwendung von „Cookie-Bannern"

Tatsächlich scheint sich die Verwendung von Cookie-Bannern als Standard der Einwilligungseinholung etabliert zu haben. Bei der Einbindung solcher Banner in die eigene Website gibt es in der Praxis allerdings einiges zu beachten. Dabei müssen Websitebetreiber gleich zu Beginn eine wichtige Entscheidung treffen. Soll über das Banner eine konkludente Einwilligung des Nutzers oder eine ausdrückliche Einwilligung eingeholt werden?

2.3.1 Konkludente Einwilligung

Das Prinzip hinter Cookie-Bannern, mit denen eine konkludente Einwilligung der Nutzer eingeholt werden soll, funktioniert wie folgt: Dem Nutzer wird ein Banner angezeigt, welches z. B. kurz die Verwendung von Trackingtechnologien darstellt, einen Link zu weiterführenden Informationen enthält und dem Nutzer gegenüber deutlich macht, dass er durch die weitere Nutzung der Website seine Einwilligung in diese Datenverarbeitung erklärt. Websitebetreiber können im Rahmen der Bannerimplementierung oftmals definieren, welche Handlung des Nutzers als Weiternutzung der Website gewertet werden soll: Regelmäßig wird ein Weiternutzen der Website angenommen, wenn der Nutzer auf einen Link innerhalb der Website klickt. Darüber hinaus können Websitebetreiber aber auch einstellen, dass die Aktualisierung der Website oder bereits das Scrollen eine Weiternutzung darstellen sollen, welche zur Annahme der konkludenten Einwilligung führt.[23] Datenschutzrechtlich ist diese Form der Einwilligungseinholung sehr riskant, da sich regelmäßig folgende Fragen stellen:

- Hat der Nutzer das Banner überhaupt wahrgenommen?
- Hat der Nutzer die Seite tatsächlich in dem Bewusstsein weitergenutzt, hierdurch eine konkludente Einwilligung zu erklären?
- Kann die Einwilligung des Nutzers nachgewiesen werden?

Problematisch wird an dieser Stelle insbesondere die Einhaltung der Vorgaben des § 13 Abs. 2 Nr. 1 TMG, wonach Einwilligungen zwar elektronisch erklärt werden können, allerdings sichergestellt sein muss, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat. Auch Art. 4 Nr. 11 DS-GVO fordert insofern eine „*unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*".

Als regelmäßig unzulässig erscheinen daher Einstellungen, die bereits im Scrollen oder in der Aktualisierung der Seite eine konkludente Einwilligung sehen. Zudem darf nicht jeder Klick auf einen Link dazu führen, dass eine konkludente Einwilligung angenommen wird. Denn Klicks auf die Datenschutzerklärung der Website, das Impressum oder auf Informationslinks innerhalb des Banners sind regelmäßig noch der Entscheidungsphase des Nutzers zuzuordnen.

2.3.2 Ausdrückliche Einwilligung

Im Gegensatz zu Cookie-Bannern, die auf die Einholung einer konkludenten Einwilligung ausgerichtet sind, kann die Rechtssicherheit durch die Nutzung von Cookie-Bannern, mit deren Hilfe eine ausdrückliche Einwilligung eingeholt werden soll, erhöht werden.

Bei dieser Alternative wird Nutzern ein Banner angezeigt, welches die Möglichkeit bietet, der Datenverarbeitung ausdrücklich zuzustimmen. Erst wenn der Nutzer ausdrücklich zustimmt (etwa durch einen Klick innerhalb des Banners auf „Einverstanden") beginnt das Tracking und die damit verbundene Datenverarbeitung. Zwar bestehen auch bei dieser Alternative noch gewisse Restrisiken, weil § 13 Abs. 2 Nr. 2 TMG sowie Art. 7 Abs. 1 DS-GVO hohe Anforderungen an die Protokollierung bzw. Nachweisbarkeit der Einwilligung stellen. Allerdings ist die Einholung einer ausdrücklichen Einwilligung sehr viel rechtssicherer als die Einholung der konkludenten Einwilligung.

Websitebetreiber haben im Rahmen der Einholung der ausdrücklichen Einwilligung zudem die Wahl, die Einwilligung des Nutzers an die weitere Nutzung der Website zu koppeln. Dies erscheint insbesondere für Websites, die nicht dem öffentlichen Bereich zuzuordnen sind, auch als rechtlich zulässig. Denn ein Kopplungsverbot aus § 28 Abs. 3b BDSG wird sich für die Nutzung von kostenlosen Websites regelmäßig nicht annehmen lassen und auch bei kostenpflichten Websites nur ganz ausnahmsweise bestehen, wenn ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ansonsten nicht besteht. Auch Art. 7 Abs. 4 DS-GVO wird regelmäßig nicht zu einem Kopplungsverbot führen. Insbesondere die Anbieter von kostenlos abrufbaren Web-

20 Google Richtlinie zur Einwilligung der Nutzer in der EU: https://www.google.com/about/company/user-consent-policy.html?hl=de.

21 Facebook Terms For Conversion Tracking, Custom Audiences From Your Website, and Custom Audiences From Your Mobile App: https://www.facebook.com/customaudiences/app/tos/.

22 Facebook Cookie Consent Guide for Sites and Apps: https://developers.facebook.com/docs/privacy.

23 Vgl. hierzu auch die Seite https://www.cookiebot.com/de/demo, welche eine Demo bereithält, mit der verschiedene Einstellungsmöglichkeiten einfach ausprobiert werden können.

sites können an dieser Stelle argumentieren, dass Nutzer mit ihrer Einwilligung in die Datenverarbeitung „bezahlen" und die Datenverarbeitung somit zur Erbringung ihrer Dienste erforderlich ist.[24]

2.3.3 Weitere Wirksamkeitsvoraussetzungen

Unabhängig von den vorgenannten Fragestellungen müssen bei der Implementierung einer Bannerlösung zusätzlich folgende Voraussetzungen beachtet werden:

2.3.3.1 Einblendung des Banners auf der Einstiegsseite

Das Banner muss bereits auf der ersten Seite eingebunden werden, mit welcher der Websitebesucher in Kontakt kommt. Hierbei handelt es sich nicht zwingend um die Startseite der Website. Denn häufig werden Websitebesucher über Deep-Links auf anderen Seiten in die Website einsteigen.

2.3.3.2 Informiertheit der Einwilligung

Sowohl § 4a BDSG und § 13 TMG als auch Art. 4 Nr. 11 DS-GVO sehen als Voraussetzung für eine wirksame Einwilligung die Informiertheit des Einwilligenden vor. Jedes Banner muss daher neben einer kurzen Darstellung der wichtigsten Kernelemente der Datenverarbeitung auch einen Link zu weiterführenden Informationen enthalten, welche den Nutzer im Detail über alle Datenverarbeitungen informiert. Das Banner darf sich dabei nicht nur auf den Umstand einer Verwendung von Cookies beschränken, sondern muss alle Drittanbieter nennen sowie alle Trackingmethoden offenbaren. Die Bezeichnung „Cookie-Banner" ist daher strenggenommen irreführend.

Die Information des Nutzers wird in der Praxis insbesondere dann schwierig, wenn Websitebetreiber eine Vielzahl von Werbenetzwerken und Drittanbieterdiensten nutzen. So ist es keine Seltenheit, dass in Nachrichtenportalen oder Online-Shops Verbindungen zu dutzenden Werbenetzwerken und AdServern aufgebaut werden.

2.3.3.3 Beginn des Trackings erst nach Einwilligung

Websitebetreiber müssen durch technische Maßnahmen zudem dafür Sorge tragen, dass erst nach der Einwilligung der Nutzer das Tracking beginnt. Es muss also mindestens gewährleistet werden, dass auf der Einstiegsseite kein Tracking stattfindet und auch ein Klick auf das Impressum oder die Datenschutzerklärung das Tracking noch nicht in Gang setzt.

2.3.3.4 Widerruf der Einwilligung

Nutzer, die ihre Einwilligung erteilt haben, müssen die Möglichkeit haben, diese zu widerrufen; § 13 Abs. 2 Nr. 4 TMG, Art. 7 Abs. 3 S. 1 DS-GVO. Auch hierüber muss der Nutzer informiert werden. In der Praxis finden sich im Bereich des Retargetings unterschiedliche Ausgestaltungen der Widerrufsmöglichkeit, z. B.:

- Websitebetreiber können eigene Opt-Out-Möglichkeiten implementieren. So wäre es denkbar, dass Tools, die zur Bannerimplementierung genutzt werden, Drittanbieterinhalte und -verbindungen gesteuert blocken (ähnlich wie eine 2-Klick-Lösung bei Social Plugins).
- Websitebetreiber können Nutzer darauf verweisen, ihren Browser so zu konfigurieren, dass Drittanbietercookies nicht akzeptiert werden. Diese Möglichkeit wird jedoch längst nicht allen Trackingtechnologien gerecht, da das Tracking durch klassische Cookies nur noch einen Teil der verwendeten Trackingtechnologie ausmacht.
- Websitebetreiber können Nutzer auf etwaig vorhandene Seiten des Werbenetzwerkbetreibers verweisen, auf denen entsprechende Opt-Out-Möglichkeiten angeboten werden. Problematisch wird dies aber immer dann, wenn eine Website eine Vielzahl an Werbenetzwerken nutzt und der Nutzer einen Widerspruch auf dutzenden Seiten erklären müsste. Zudem ist nicht gewährleistet, dass jeder Werbenetzwerkbetreiber über entsprechende Opt-Out-Seiten verfügt.
- Sofern die entsprechenden Werbenetzwerke dies unterstützen, können Websitebetreiber Nutzer auf Seiten verweisen, die Einstellungsmöglichkeiten für eine Vielzahl verschiedener Werbenetzwerke und Drittanbieter ermöglichen. Zu nennen sind hier etwa die Digital Advertising Alliance[25] und die Initiative www.youronlinechoice.eu der European Interactive Digital Advertising Alliance[26]. Auf diesen Seiten können Nutzer Einstellungen für eine Vielzahl von Werbenetzwerken vornehmen und teilweise mit einem Click Opt-Outs für über hundert Werbenetzwerke setzen. Die Nutzung dieser Opt-Out-Möglichkeiten kann allerdings einige Minuten dauern und basiert auf dem Setzen von Opt-Out-Cookies. Löscht ein Nutzer diese Cookies bei Schließen des Browsers, müssen die Einstellungen neu vorgenommen werden. Allerdings werden hierfür auch erste Browser-Plugins angeboten, welche die entsprechenden Einstellungen dauerhafter speichern sollen. Darüber hinaus können Widersprüche für das Tracking durch Apps über eine eigene App gesteuert werden, die für gängige mobile Betriebssysteme verfügbar ist. Insgesamt ist die Nutzung dieser Möglichkeiten aber immer noch mit nicht unerheblichem Aufwand für den Nutzer verbunden. Das eigentliche Problem ist jedoch, dass die beschriebenen Allianzen lediglich eine Selbstregulierung der teilnehmenden Unternehmen fordern und längst nicht alle relevanten Unternehmen, die Tracking zu Werbezwecken vornehmen, beigetreten sind.

Insgesamt erscheinen die Widerrufsmöglichkeiten gerade auf Websites, die eine Vielzahl von Werbenetzwerken einsetzen, in der Praxis als schwierig umsetzbar.

3 Ausblick auf die ePrivacy-Verordnung

Die anstehende Ablösung der ePrivacy-Richtlinie durch die geplante ePrivacy-Verordnung wird an der dargestellten Situation vermutlich nur wenig ändern:

24 So auch *Frenzel* in Paal/Pauly, Datenschutz-Grundverordnung 1. Auflage 2017, Art. 7, Rn. 21.

25 http://www.aboutads.info/choices/

26 http://www.youronlinechoices.com/de/praferenzmanagement/

3.1 Einwilligung für Drittanbietertracking

So stellt der aktuelle Kommissionsentwurf einer ePrivacy-Verordnung[27] das Tracking durch Drittanbieter zu Werbezwecken unter Einwilligungsvorbehalt. Denn Art. 8 Abs. 1 lit. d des Verordnungsentwurfs sieht vor, dass *„jede vom betreffenden Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware, ... untersagt [ist], außer ... sie ist für die Messung des Webpublikums nötig, sofern der Betreiber des vom Endnutzer gewünschten Dienstes der Informationsgesellschaft diese Messung durchführt."* Für das Retargeting bedeutet dies, dass dies nur zulässig erfolgen kann, wenn der Endnutzer gem. Art. 8 Abs. 1 lit. b des Verordnungsentwurfs seine Einwilligung gegeben hat. Google, Facebook & Co. sind an dieser Stelle gut vorbereitet, da sie, wie bereits dargestellt, bereits seit Jahren die Einholung einer Einwilligung fordern, selbst wenn deren Erfordernis in einzelnen europäischen Ländern auf nationaler Ebene juristisch durchaus umstritten ist.

3.2 Anforderungen an die Einwilligung

Die Anforderungen an eine Einwilligung werden in Art. 9 Abs. 1 des Verordnungsentwurfs näher geregelt, welcher insofern u. a. auf Art. 4 Nr. 11 der DS-GVO verweist. Grundsätzlich ist daher festzustellen, dass die Verwendung von Tracking-Bannern auch nach dem aktuellen Verordnungsentwurf weiterhin die dargestellten Fragen und Kritikpunkte aufwirft. Auch im Hinblick auf das schwache Kopplungsverbot sieht der aktuelle Kommissionsentwurf keine Änderungen vor.[28]

3.3 Einwilligung durch Browsereinstellung

Art. 9 Abs. 2 des Verordnungsentwurfs regelt, dass die Einwilligung in Bezug auf Webtracking auch *„in den passenden technischen Einstellungen einer Software, die den Zugang zum Internet ermöglicht, gegeben werden [kann]."* Klarer wird an dieser Stelle der Erwägungsgrund 24 des Verordnungsentwurfs: *„Damit Webbrowser die in der Verordnung (EU) 2016/679 vorgeschriebene Einwilligung der Endnutzer, z. B. in die Speicherung von Verfolgungs-Cookies von Drittanbietern, einholen können, sollten sie unter anderem eine eindeutige bestätigende Handlung von der Endeinrichtung des Endnutzers verlangen, mit der dieser seine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich erklärte Zustimmung zur Speicherung solcher Cookies in seiner Endeinrichtung und zum Zugriff darauf bekundet. Eine solche Handlung kann als bestätigend verstanden werden, wenn Endnutzer zur Einwilligung beispielsweise die Option „Cookies von Drittanbietern annehmen" aktiv auswählen müssen und ihnen die dazu notwendigen Informationen gegeben werden."*

3.4 Keine Unterstützung eines Do Not Track-Ansatzes

Der aktuelle Verordnungsentwurf vermeidet damit eine Lösung, die Nutzern einen wirksamen Schutz vor ungewolltem Tracking hätte geben können: Zwar wird die Möglichkeit der Erteilung von Einwilligungen und Generaleinwilligungen geregelt. Die verbindliche Unterstützung von Generalwidersprüchen, wie etwa Do Not Track, sowie deren Zusammenspiel mit individuell erklärten konkludenten Einwilligungen bleibt hingegen ungeregelt. Nur eine solche Generalwiderspruchmöglichkeit hätte Nutzer wirksam vor ungewolltem Webtracking schützen können.[29] Insgesamt ist festzustellen, dass Do Not Track in der Vergangenheit mangels klarer gesetzlicher Regelungen sowohl von Betriebssystem- und Browserherstellern verhindert sowie von relevanten Werbenetzwerken bewusst ignoriert wurde.[30] Stattdessen setzen Werbenetzwerke auf die bereits dargestellten Mechanismen von Tracking-Bannern und unterschiedlichsten Widerrufsmöglichkeiten sowie Selbstverpflichtungen.

4 Fazit

Es spricht viel dafür, dass Retargeting aufgrund der verwendeten Trackingtechnologien nur nach vorheriger Einwilligung der betroffenen Nutzer zulässig ist. In diesem Rahmen haben sich Bannerlösungen als Standard der Einwilligungseinholung etabliert. Diese Bannerlösungen werden in der Praxis allerdings häufig keine wirksame Einwilligung darstellen, da je nach Implementierung die Mindestanforderungen an eine informierte und ausdrückliche Einwilligung nicht eingehalten werden. Zudem sind Bannerlösungen in der Praxis kaum geeignet, dem Nutzerwillen gerecht zu werden, da die Möglichkeiten, nicht einzuwilligen, begrenzt sind und auch der Widerruf in der Praxis nur sehr schwer umgesetzt werden kann. Eine Lösung könnte die geplante ePrivacy-Verordnung bringen, allerdings regelt diese den entscheidenden Punkt einer generellen Widerspruchsmöglichkeit gegen den Einsatz von Trackingtechnologien nicht. Angesichts der enormen wirtschaftlichen Bedeutung von Online-Werbung für Werbenetzwerkbetreiber[31] und Publisher wird es schwer werden, deren jeweilige Interessen mit denen der Nutzer in Einklang zu bringen.

27 Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.1.2017, COM (2017) 10 final.

28 Allerdings schlägt der Entwurf der Änderungsempfehlungen des LIBE-Ausschusses vom 9.6.2017 (PE606.011) vor, in Art. 8 Abs. 1a ePrivacy-Verordnung ein ausdrückliches Kopplungsverbot aufzunehmen.

29 Wenngleich auch hier noch Risiken verblieben wären, vgl. *Schleipfer*, Datenschutzkonformer Umgang mit Nutzungsprofilen – Sind IP-Adressen, Cookies und Fingerprints die entscheidenden Details beim Webtracking?, ZD 2015, 399-405.

30 Vgl. *Venzke-Caprarese*, Warum uns Do Not Track nicht schützt – Plädoyer für eine Gesetzesänderung, Blogbeitrag vom 24. August 2016, abrufbar unter https://www.datenschutz-notizen.de/warum-uns-do-not-track-nicht-schuetzt-plaedoyer-fuer-eine-gesetzesaenderung-5615475/ m. w. N.

31 Allein im letzten Jahr verzeichnete Google laut Geschäftsbericht des Mutterkonzerns Alphabet einen Werbeumsatz von 79,38 Milliarden Dollar.