LEGAL REVOLUTIONary
Rechtsmagazin der digitalen Wirtschaft

Website-Tracking rechtskonform gestalten (Teil II)

Handlungsempfehlungen nach den Cookie-Entscheidungen von EuGH und BGH

Rainer Robbel | Rechtsanwalt, externer Datenschutzbeauftragter | ETL Rechtsanwälte GmbH

29. Juli 2020

LR 2020, Seiten 200 bis 208 (insgesamt 9 Seiten)

Nach den unlängst ergangenen Entscheidungen von EuGH und BGH sind nahezu alle Website-Betreiber gefordert, sich von den Besuchern ihrer Webseiten eine Einwilligung einzuholen, bevor auf deren Rechnern Cookies gesetzt werden, wollen sie diese und deren Surf- und Nutzungsverhalten auch weiterhin nachverfolgen. Die derzeit einzige bekannte technische Lösung sind sogenannte Consent-Banner[1]. Wie die genau auszusehen haben, lässt die Rechtsprechung bislang jedoch weitestgehend offen. So wird beileibe nicht jede erhältliche Consent-Banner-Lösung am Ende rechtskonform sein. Aber wie gelangt man auf die sichere Seite? Lesen Sie im zweiten Teil dieses Beitrags, was Website-Betreiber nun tun sollten. 1

I. Prognose

Nach dem im ersten Teil dargelegten Meinungsstand scheinen die dänische Aufsichtsbehörde, aber vor allem die Rechtsprechung in Sachen Webtracking dem Schutz der Verbraucher weit mehr Gewicht einzuräumen, als den Interessen der (Werbe-)Wirtschaft. 2

Dem ist zuzustimmen, denn vielen Internetnutzern wird weder die Tragweite ihrer Entscheidung, noch der Umfang der Nutzung ihrer personenbezogenen Daten durch Dritte bewusst sein. Manch einer dürfte nicht einmal merken, dass er in irgendetwas einwilligt, denn die meisten wollen ungestört surfen und klicken die lästigen Banner sofort und ohne sie weiter zu beachten weg. Dabei werden Sie froh sein, wenn diese mit nur einem statt zwei oder mehr Klicks verschwinden. 3

[1] In diesem Beitrag wird der Begriff Consent-Banner verwendet. Hiermit sind die einer Website vorgeschalteten Banner gemeint, mit denen die Einwilligung der Website-Besucher in das Setzen von Cookies oder die Verwendung anderer Tracking-Technologien eingeholt werden. Andere verbreitete Bezeichnungen für Consent-Banner sind z.B. Cookie-Consent-Banner, Cookie-Banner oder Cookie-Management-Tool.

Dazu kommt, dass sich die Websitebetreiber gezielt menschliche Verhaltensmuster zunutze machen, indem sie die Einwilligung der Websitebesucher durch eine geschickte Menüführung „sanft" erzwingen. Oftmals genügen einfachste gestalterische Mittel, z.B. die optische Hervorhebung des Buttons, den der Nutzer klicken soll, das Verstecken von nicht erwünschten Auswahlfeldern im kleingedruckten Fließtext, lange und kaum verständliche „Informationen" usw. Dass dies durchaus gut funktioniert, belegen erste wissenschaftliche Untersuchungen[2].

Die Nutzer messen dem Datenschutz vor allem hierzulande mittlerweile zwar mehr und mehr Bedeutung zu, allerdings möchten sich nur die Wenigsten intensiver damit auseinandersetzen. Dies hatte wohl auch der Gesetzgeber im Blick, als er den Grundsatz des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen mit Art. 25 in die DSGVO aufnahm. Eine Untersuchung der Harvard Law School aus 2019[3] zeigte auf, dass die Menschen zwar verärgert über Unternehmen sind, die ihre Daten sammeln, aber sie oft noch nicht einmal einfache Standardeinstellungen in ihren Browsern oder Apps ändern. Die Wissenschaftler begründen dies mit sogenannter „Informationsvermeidung". Selbst Menschen, die bereit sind, fast einen Stundenlohn für den Schutz der Privatsphäre zu zahlen, sind ebenso bereit, ihre Daten für einen geringwertigen Vorteil quasi zu verschenken, wenn sie die Konsequenzen ihrer Entscheidungen für ihre Privatsphäre nicht erkennen. 4

Versucht man die künftige Rechtsprechung zu diesen Fragen zu prognostizieren, muss man auch den Trend der Rechtsprechung betrachten, den Verbraucher vor „hidden identifiers" und ähnlichen Webtracking-Technologien weitestgehend in Schutz zu nehmen. Die Motivation dafür liegt vor allem im Ungleichgewicht zwischen den technisch und juristisch ahnungs- und arglosen Nutzern auf der einen und den mit Know-How bestens ausgestatteten Unternehmen auf der anderen Seite. Dazu kommt, dass die Verbraucher nicht wissen, was mit ihren Daten tatsächlich geschieht, weil sie nicht ausreichend oder nicht transparent genug informiert werden. In den meisten Fällen wird dies den Website-Betreibern auch gar nicht möglich sein, denn trotz aller Transparenzoffensiven legen Unternehmen wie Google oder Facebook nur das offen, was sie unbedingt müssen und was ihnen nicht schadet. Die großen Leaks der vergangenen Jahre, wie z.B. der Skandal um Oxford Analytica, lässt zumindest befürchten, dass nach wir vor vieles im Verborgenen geschieht und die Webtracking betreibenden Unternehmen kein wirkliches Interesse daran haben, diese Informationen, die zugleich ihre Geschäftsgrundlage bilden, offen zu legen. Demzufolge wird man prophezeien können, dass die Richter*innen an EuGH und BGH jeglichen Versuchen, ein Tracking „durch die Hintertüre" zu betreiben, auch in Zukunft eine Absage erteilen werden. 5

[2] z.B.: https://de.statista.com/statistik/daten/studie/986587/umfrage/umgang-mit-cookies-in-deutschland/.
[3] http://www.law.harvard.edu/programs/olin_center/fellows_papers/pdf/Svirsky_81_revision.pdf.

In diese Richtung zeigt auch der jüngst ergangene Beschluss der Datenschutzkonferenz (DSK) zum Einsatz von Google Analytics im nicht-öffentlichen Bereich[4]. Zwar kommt die DSK zum Ergebnis, dass ein datenschutzkonformer Einsatz möglich ist, diese Aussage ist aber nur theoretischer Natur, denn die DSK fordert, dass der Nutzer umfassend und transparent über die Datenverarbeitung bei Google informiert werden muss, er selbst aber dazu nicht die notwendigen Informationen von Google bereitgestellt bekommt.[5] 6

II. Handlungsalternativen

1. Reduzierung auf das Notwendige

Bevor man als Website-Betreiber darüber nachdenkt, wie man nun am besten an möglichst viele „vorherige" Einwilligungen der Nutzer kommt, empfiehlt es sich zunächst einmal jedes der eingesetzten Trackingtools dahingehend zu hinterfragen, ob man dieses tatsächlich benötigt oder nicht. Es hat schon so manche Geschäftsführung verwundert, wenn ihnen aufgezeigt wird, was die Marketingabteilung oder die Programmierer so alles im Hintergrund an Analysefunktionen aktiviert haben. Häufig heißt es dann, dass man so etwas eigentlich nicht brauche oder das so erhaltene Datenmaterial überhaupt nicht oder nicht zielgerichtet ausgewertet werde. Vor allem kleine oder kleinere mittelständische Unternehmen können, wenn überhaupt nur einen geringen Teil des enormen Funktionsumfangs der meisten dieser Werkzeuge nutzen. Viele wissen erst gar nicht, dass derartige Tools auf ihrer Website aktiviert sind und ausschließlich deren Anbieter schlau und reich machen. 7

Dazu kommt, dass Daten auch Verantwortung bedeuten. Während des Lebenszyklus eines Datums, d.h. von seiner „Geburt", der Erhebung, bis zu seinem „Tod", dem Löschen oder der Vernichtung, muss sich die verantwortliche Stelle darum kümmern, d.h. Ressourcen und Kosten investieren. Daten benötigen Speicherplatz, sie müssen durch geeignete technische und organisatorische Maßnahmen geschützt werden, sie müssen auf vielfältige Weise gemanagt werden, hinzu kommen weitere gesetzlichen Pflichten, wie die Information der Betroffenen und die Dokumentation aller relevanten mit dem Datenschutz in Verbindung stehenden Vorgänge und Prozesse. 8

Im Sinne ökonomischen Handelns sollte also jedes Unternehmen überprüfen, ob der Nutzen, den man aus den gesammelten Daten langfristig ziehen kann, in einem angemessenen Verhältnis zu den Kosten und Ressourcen steht, die man auf der anderen Seite für die Verarbeitung der Daten bereitstellen muss. In nicht wenigen Fällen wird sich so manche Unternehmer*in eingestehen müssen, dass es zwar schön ist zu wissen, wer sich beispielsweise wo wie lange was auf der Website angesehen hat und 9

[4] https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf.

[5] so auch Rechtsanwalt Dr. Bahr, Hamburg (https://www.dr-bahr.com/news/dsk-beschliesst-grundsatzpapier-zum-einsatz-von-google-analytics.html).

vielleicht sogar noch, wo dieser herkommt, aber man dadurch noch lange keine Antworten auf die eigentlich entscheidenden Fragen erhält. Was erforderlich ist, um aus „Big Data" „Smart Data" zu machen und was man mit den Daten macht, die nicht „smart" werden („Dark Data") ist ein ganz anderes Thema und würde den Rahmen dieses Beitrags sprengen. Daher sei hier nur in der gebotenen Kürze erwähnt, dass es des Einsatzes spezieller Technologien und Algorithmen bedarf, um aus einer Unmenge unstrukturierter Daten passgenaue Antworten zu erhalten. Dazu kommt, dass dabei regelmäßig nur ein Teil der gewonnenen Daten von Nutzen ist. Der übrige Rest („Dark Data"), ist für die Unternehmen von keinerlei Wert, dennoch erfordert diese die gleiche datenschutzrechtliche Behandlung, wie die nutzbaren Daten.

Nutzt man ein Trackingtool nur unzureichend oder gar nicht für eigene Zwecke, sind die Ergebnisse der Datenauswertung nicht ausreichend präzise, nur von untergeordneter Bedeutung oder stehen diese nicht im Verhältnis zu Kosten und Aufwand, sollte man sich von diesem trennen. Das gilt analog für Webtracking zu anderen Zwecken wie Marketing oder Erzielung höherer Werbeeinnahmen. Auch wenn hier ein wirtschaftlicher Vorteil in der Regel vorhanden und einfacher messbar ist, sollte in jedem einzelnen Fall geprüft werden, ob dieser im Verhältnis zum Aufwand steht. 10

2. Einsatz eines Consent-Banner

In den meisten Fällen wird man sich gleichwohl nicht gänzlich von Webtracking-Tools trennen können oder wollen. Dann bleibt derzeit als einzige praktikable technische Lösung zur vorherigen Einholung der erforderlichen Einwilligungen nur das Consent-Banner. 11

Rechtlich sicher wird das nach alledem nur so gestaltet sein können, dass ein Button mit der Beschriftung „OK" oder sinngemäß nichts anderes als ein Weitersurfen ohne irgendwelche Cookies oder andere „Hidden Identifiers" bedeuten darf. Bereits an dieser Hürde dürften die meisten aktuell eingesetzten Consent-Banner scheitern. 12

Will der Nutzer hingegen seine Einwilligung in ein oder mehrere Cookies erteilen, muss sich der Button, mit dem man seine Zustimmung erklärt, auf der gleichen Ebene an einer gleich prominenten Stelle befinden und optisch gleichrangig ausgestaltet sein. Unterschiedliche Farbgebung, wie z.B. ein transparenter „OK"-Button neben einem grün unterlegten „Einwilligen"- oder „Einstellungen"-Button dürfte noch zulässig sein, soweit diese sich zumindest in Größe und Schriftbild nicht unterscheiden. Das gilt genauso für einzeln zu setzende Haken in Opt-In-Feldern bei der Nutzung verschiedener funktionaler Cookies zu unterschiedlichen Zwecken. 13

Gleichzeitig muss der Nutzer sich von dort aus unmittelbar und ohne Umwege über die jeweiligen Anbieter der Dienste, welche die Cookies setzen, über den Zweck und die Arten der Datenverarbeitung sowie ggf. die Übermittlung an weitere Unternehmen

unter deren Angabe informieren können. Diese Informationen müssen umfassend und ausreichend transparent sein. Dazu reicht es regelmäßig nicht, lediglich allgemein gehaltene Informationen oder abstrakte Formulierungen zu verwenden. Das sieht auch die Datenschutzkonferenz so: *„Ein bloßer Hinweis wie z.B. „diese Seite verwendet Cookies, um Ihr Surferlebnis zu verbessern" oder „verwendet Cookies für Webanalyse und Werbemaßnahmen" ist nicht ausreichend, sondern irreführend, weil die damit verbundenen Verarbeitungen nicht transparent gemacht werden."* [6]

Die ebenfalls anzutreffende Gestaltung, bei der die Einwilligung mit einem Button „Alle Cookies akzeptieren" erteilt wird, dürfte nicht zulässig sein. Selbst wenn der Nutzer die erforderlichen Informationen über einen anderen Button oder Link abrufen kann, befinden sich diese nicht auf derselben Ebene. Ein solcher "One-Click-Away"-Aufbau erfordert zur Erlangung einer informierten Entscheidung einen zusätzlichen Schritt und ist daher intransparent. Auch eine granulare Entscheidung ist so unmöglich. Zulässig dürfte hingegen sein, wenn sich die Informationen und die Opt-In Felder auf derselben Ebene mit einem „Alle Cookies akzeptieren"- und einem „Einstellungen speichern"-Button befinden. Man könnte auch das durchaus noch verwirrend finden, allerdings darf man die Anforderungen an einen mündigen Verbraucher auch nicht überspannen. Bei diesem Beispiel wird diesem zumindest klar sein, was passiert, wenn er den „Alle Cookies akzeptieren"-Button anklickt und das der andere Button die gegenteilige Alternative bietet. 14

III. Einzelfragen

1. Wann gelten Cookies als „Notwendig" bzw. unbedingt erforderlich?

Derzeit lässt sich keine verbindliche Aussage darüber treffen, welche Cookies unbedingt erforderlich sind. Aufgrund der dargelegten Tendenz wird man aber davon ausgehen können, dass sowohl Rechtsprechung, als auch Aufsichtsbehörden diesen Begriff eng auslegen werden. Session-Cookies, die man z.B. für eine Warenkorb-Steuerung, für den Zugang zu zutrittsbeschränkten Bereichen oder zur Speicherung gerade der Cookie-Einwilligung benötigt, dürften dabei wohl als unbedingt erforderlich gelten. 15

Auch sog. „Remember-Me"-Cookies, die ermöglichen, dass der Nutzer sich bei einem erneuten Besuch eines zutrittsbeschränkten Bereichs nicht immer wieder neu einloggen muss, können i.d.R. als „vom Nutzer verlangt" gelten und daher ohne Einwilligung verwendet werden.

[6] Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12.05.2020 (https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf), S. 4.

Unklarer ist die Rechtslage bei den sog. „Persistent-Cookies“. Wird die Seite für den Nutzer ohne das jeweilige Cookie fehlerfrei angezeigt, dürfte dies aber ein starkes Indiz dafür sein, dass das jeweilige Cookie nicht unbedingt erforderlich ist. Umgekehrt bedeutet das aber auch, wird die Seite ohne das „Persistent-Cookie“ fehlerfrei oder funktionseingeschränkt dargestellt, spricht vieles dafür, dass das jeweilige Cookie eben unbedingt erforderlich ist und damit keine Einwilligung vom Websitebesucher eingeholt werden muss. Diese Aussage gilt aber nicht uneingeschränkt, denn in den Fällen, in denen es auch andere Möglichkeiten gibt, die entsprechende Funktion, z.B. durch Bereitstellung auf dem eigenen Webserver, ohne den Einsatz von Cookies zu nutzen, wird man nicht von einer unbedingten Erforderlichkeit ausgehen können. 16

In manchen Consent-Bannern wird der Einsatz von Analysetools als unbedingt erforderlich dargestellt, da hierfür ein berechtigtes Interesse des Websitebetreibers gemäß Art. 6 Abs. 1 Satz 1 lit. f) DSGVO bestehe und aus diesem Grund eine Einwilligung als Rechtsgrundlage nicht erforderlich sei. Das greift allerdings etwas kurz, denn der EuGH hat bei der „planet49“-Entscheidung nicht (nur) die DSGVO im Auge gehabt, sondern auch andere Rechte, wie z.B. die alte ePrivacy-Richtlinie und insbesondere das Recht auf Privatheit i.S.d. Art. 7 der Charta der Grundrechte der Europäischen Union (GRCh), in welche durch das Setzen von Cookies eingegriffen wird. 17

Der EuGH spricht sich in diesem Zusammenhang mit Blick auf die Erwägungsgründe der ePrivacy-RL klar dafür aus, dass das Einwilligungserfordernis auch dann gelte, wenn die Informationen im Endgerät des Nutzers (wie z.B. in Cookies) nicht personenbezogen sind, es also auf die DSGVO und die dortigen Rechtsgrundlagen nicht ankommt. Das Setzen von Cookies, die nicht aus technischen Gründen unbedingt erforderlich sind, bedarf daher immer der Einwilligung, unabhängig davon, ob es dafür nicht auch andere Rechtsgrundlagen nach der DSGVO gibt, da hierdurch das Recht auf Privatheit i.S.d. Art. 7 GRCh verletzt wird. Demzufolge können auch nicht solche Cookies zu den unbedingt erforderlichen Cookies gezählt werden, für die der Websitebetreiber eine andere Rechtsgrundlage aus der DSGVO hat, in der Regel das berechtigte Interesse nach Art. 6 Abs. 1 Satz 1 lit. f) DSGVO. 18

2. Können Cookies in Cookie-Gruppen zusammengefasst werden?

Laut der FAQ zu Cookies und Tracking[7] des baden-württembergischen Datenschutzbeauftragten, ist die Möglichkeit der Gliederung von Cookies in einzelne Kategorien erlaubt. Auch die Datenschutzkonferenz, die für die deutschen Datenschutzbehörden spricht, scheint keine Einwilligung für jeden einzelnen Anbieter zu fordern. In ihrer Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien[8] ist von der Einwilligung in “Verarbeitungsvorgänge” unter “Nennung der Akteure” und nicht von Einwilligung für einzelne Akteure die Rede. Allerdings ist zu 19

[7] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/FAQ-zu-Cookies-und-Tracking.pdf.
[8] https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

beachten, dass beide Texte vor der EuGH- und der BGH-Entscheidung verfasst und veröffentlicht wurden.

Da eine Voraussetzung einer wirksamen Einwilligung die Informiertheit des Einwilligenden ist, ist es ein nicht von der Hand zu weisendes Argument gegen eine Gliederung in Kategorien. Denn die Information ist eine der Kernpflichten der verantwortlichen Stelle nach der DSGVO und dazu gehört eben auch zu wissen, wer denn letztlich Cookies zu welchem Zweck setzt, in die man einwilligt. 20

Auch hat der BGH im Weiteren entschieden, dass Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können, zu den Informationen zählen, die der Diensteanbieter dem Nutzer einer Website zu geben hat. Dies wird aufgrund der Individualität der Cookies in Kategorien wohl kaum nachvollziehbar gelingen. 21

Dennoch dürfte es durchaus zulässig sein, die Opt-In-Felder lediglich auf Kategorien zu beziehen, wenn über eine weitere Funktion oder einen Link Detailinformationen zu den einzelnen Anbietern abrufbar sind. 22

Im vielen derzeit verwendeten Cookie-Bannern reichen die Detailangaben jedoch nicht aus, da sie lediglich Erläuterungen bzw. Definitionen der einzelnen Kategorien, aber keine Informationen zu den Cookies selbst und zu deren Anbietern enthalten, so wie es EuGH, BGH und die dänische Datenschutzbehörde unmissverständlich fordern (Aufklärung über die die Identität des für die Verarbeitung Verantwortlichen und die Zwecke der Verarbeitung). 23

Auch der Opt-In in Kategorien dürfte unproblematisch sein, wenn sich Informationen zu den einzelnen Anbietern einfach („one click away“) abrufen lassen. Ob das in der Praxis allerdings Sinn macht, ist eine andere Frage. Man könnte nämlich durchaus argumentieren, dass man eher einzelne Einwilligungen erhält, wenn man dem Nutzer diese Auswahl ermöglicht und er sich ohnehin schon die Zeit nimmt, sich Informationen zu beschaffen. 24

Unter bestimmten Umständen kann es sogar zulässig sein, nur zwischen „notwendigen“ und “allen anderen Cookies“ zu unterscheiden, nämlich dann, wenn die einzelnen Anbieter und die Details zu den Cookies (Art, Dauer, Zweck) abrufbar sind, z.B. über einen Button „Details anzeigen“. Da aber schon die Aufsichtsbehörden in ihren Stellungnahmen, die zwar aus der Zeit vor der EuGH-Entscheidung stammen, aber dennoch recht aktuell sind, zumindest eine Gliederung in Kategorien fordern, ist es empfehlenswert, die Opt-In-Felder zumindest in grobe, aber den Zweck beschreibende Kategorien zu unterteilen, damit der Nutzer vor seiner Einwilligung ein Mindestmaß an Informationen erhält. 25

3. Gibt es andere, zulässige Technologien zur Identifikation der Nutzer und zur Analyse deren Nutzerverhalten?

Mit den aktuellen Versionen der meisten auf dem Markt befindlichen Browser und speziellen dafür erhältlichen Add-Ons lassen sich schon jetzt ohnehin alle Third-Party-Cookies abwehren. Dementsprechend haben sich natürlich auch die Unternehmen, die von den Nutzerdaten profitieren, längst neue Technologien zum Nutzer-Tracking erdacht. Dazu zählen z.B. Web-Beacons, Pixel, Tags, Fingerprints und aktuell CNAME Cloaking. 26

Das recht verbreitete Analysetool Matomo lässt sich beispielsweise auch ohne Cookies betreiben, in diesem Fall wird lediglich ein sog. „digital Fingerprint" gespeichert. Nach Meinung des geschätzten Kollegen Dr. Thomas Schwenke sei zwar derzeit rechtlich nicht geklärt, ob ein Fingerprint wie ein Cookie zu behandeln ist, es sei aber gut vertretbar, dass die Cookie-Regelung für den Fingerprint nicht anwendbar ist.[9] 27

Auch wenn in den Entscheidungen von EuGH und BGH nur von Cookies die Rede ist, betreffen diese dennoch alle Technologien, die Daten auf den Geräten der Nutzer speichern und auslesen. Zwar greifen nicht alle Technologien auf den Gerätespeicher zu, aber allen ist gemeinsam, dass sie irgendein Datum benötigen, um den Nutzer zu identifizieren und nachzuverfolgen. Das können die IP-Adresse, Daten zu benutzter Hard- und Software, Metadaten oder andere Daten sein. Die Zusammenfassung all dieser, dem gleichen Zweck dienenden Technologien unter dem Begriff Cookies, hat der EuGH lediglich aus Vereinfachungsgründen vorgenommen. Der EuGH spricht im Weiteren von „Hidden Identifiers", womit deutlich wird, dass es nicht auf die Technologie als solches ankommt, sondern darauf, dass mit dieser (pseudonyme) personenbezogene Daten erhoben werden.

Nach diesseitiger Interpretation fällt auch ein Fingerprint unter den vom EuGH geprägten zusammenfassenden Begriff des „Hidden Identifiers", da mittels diesem zumindest kurzzeitig eine Identifikation des Nutzers und eine Analyse dessen Nutzerverhaltens erfolgen. Es geht letztlich darum, personenbezogene Daten zu analysieren, dabei spielt es keine Rolle, wie lange der Personenbezug i.S.d. DSGVO anhält.

Demzufolge wäre eine Nutzeranalyse ohne Einwilligung quasi unmöglich, aber dies ist im Hinblick auf das Recht auf informationelle Selbstbestimmung – immerhin eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 des Grundgesetzes – hinzunehmen. Dies gilt umso mehr, als dass ja durchaus die Möglichkeit besteht, eine Analyse in zulässiger Weise durchzuführen. Hierzu bedarf es lediglich der wirksamen Einwilligung des Nutzers.

[9] Dr. Thomas Schwenke unter: https://datenschutz-generator.de/bgh-cookies-opt-in-faq-checkliste/.

IV. Zusammenfassung

EuGH und BGH haben mit ihren jüngsten Entscheidungen dem uferlosen Webtracking der Nutzer ohne deren vorherige Einwilligung ein abruptes Ende gesetzt, auch wenn diese Entscheidungen in gewisser Weise vorhersehbar waren. Bereits vor diesen Entscheidungen waren Banner weit verbreitet, welche über den Einsatz von Cookies informierten und die Einwilligung der Nutzer mit dem Aufruf der Seite unterstellten. Nach und nach sind diese Informations-Banner von den Consent-Bannern abgelöst worden, mit denen die Einwilligung der Nutzer eingeholt wird, bevor auf deren Geräten Cookies gesetzt werden. Da nun klar ist, dass ein Opt-Out nicht ausreicht, wird die Einwilligung nunmehr im Wege des Opt-In eingeholt. Gleichwohl versucht die Wirtschaft auch weiterhin so viele Daten wie möglich zu bekommen und bedient sich dabei psychologischer Mittel bei der Gestaltung der Consent-Banner um den Nutzer dazu zu veranlassen, in das Setzen möglichst vieler Cookies einzuwilligen. Zwar gibt es noch keine verbindlichen konkreten Aussagen darüber, wie ein Consent-Banner rechtskonform gestalten werden kann, jedoch kann man den Urteilsbegründungen, wie auch den ersten Aussagen der europäischen Aufsichtsbehörden, insbesondere der dänischen Datenschutzaufsicht entnehmen, was noch erlaubt sein wird und was nicht. Dabei liegt der Schwerpunkt neben der aktiven Handlung des Einwilligenden in dessen Informiertheit. Nur wer weiß in was er einwilligt, wird seinen Willen frei bekunden können. 28

Die einfachste Lösung wäre es, auf Apps, Tools, Plug-Ins und sonstige Tracking-Technologien, die technisch nicht unbedingt erforderlich sind, gänzlich zu verzichten. Den meisten Unternehmen sind aber einige dieser Technologien von erheblichem Nutzen, weshalb ein völliger Verzicht in der heutigen Zeit kaum sinnvoll und möglich sein wird. Dennoch sollte man sich von allem trennen, was man nicht wirklich benötigt. „Nice-to-haves“ sind aufgrund des Aufwands und der Risiken etwaiger Datenschutzverstöße mittlerweile nicht mehr verhältnismäßig. Die Erfahrungen der Vergangenheit zeigen, dass viele Website-Betreiber die Daten aus dem Webtracking nicht oder nicht zielgerichtet analysieren und die Ergebnisse nicht nutzbringend in ihren unternehmerischen Entscheidungen berücksichtigen. 29

Für unverzichtbares Webtracking gilt, dass hierzu eine vorherige Einwilligung des Nutzers erforderlich ist. Diese lässt sich derzeit nur mit einem Consent-Banner einholen, welches dann aber auch rechtskonform ausgestaltet sein muss. 30