Studie

Tracking auf Websites im Gesundheitswesen

Peter Dippold
Dr. jur. Wolfhard Steinmetz

Autoren:
Peter Dippold und Dr. jur. Wolfhard Steinmetz

Sperrfrist: 10.12.2019

Inhaltsverzeichnis

Einführung

In den letzten Jahren, nicht erst mit dem Inkrafttreten der Datenschutzgrundverordnung (DS-GVO), ist die Thematik des „Webtracking“, also des Verfolgens von Benutzern im Internet, auch über die Grenzen von Websites hinweg, ein Thema des öffentlichen Interesses geworden. Den wenigsten Besuchern von Websites dürfte geläufig sein, wie weitreichend heutzutage die Möglichkeiten der Nachverfolgung und Identifikation konkreter Internetuser websiteübergreifend sind. Was können, was dürfen Anbieter im Internet auf ihren Websites und Shops technisch realisieren?
Mit Inkrafttreten der DS-GVO haben sich vor allem zwei Aspekte geändert, einerseits wurden die Rechte von Betroffenen deutlich gestärkt, andererseits müssen Verantwortliche der Datenverarbeitung mit erheblichen Konsequenzen bei Verstößen gegen datenschutzrechtliche Bestimmungen rechnen. Nach unserem Eindruck ist die Sensibilität von Internetusern seit Mai 2018, dem Inkrafttreten der DS-GVO, noch einmal deutlich angestiegen.

Dass Themen, die sich um gesundheitliche Fragestellungen drehen, für die Betroffenen eine besondere Brisanz darstellen, sollte auch ohne einen Blick in die Gesetze jedem klar sein. Nach dem jüngsten Urteil des Europäischen Gerichtshofs vom 1.10.2019 (Planet49/Verbraucherzentrale – AZ C673/17), das sich mit der Frage beschäftigte, welche Voraussetzungen für eine rechtskonforme Erhebung von Daten im Internet seitens der Betreiber realisiert werden müssen, ist die Brisanz der Thematik nochmals deutlicher geworden.

Setting

In der Zeit vom 12.11.2019 bis zum 15.11.2019 wurden insgesamt 45 Websites zu Gesundheitsthemen untersucht. Alle Websites rangierten bei der Suchmaschine DuckDuckGo zu den jeweiligen Suchworten auf den ersten beiden Seiten. Suchworte waren:

- Schwangerschaftsbeschwerden
- AIDS Praxis
- Alkoholentzugsklinik
- Magengeschwür
- Pflegeheim
- Pflegedienst
- Palliativmedizin
- Migräne
- Herointherapie

Die Auswahl der zu analysierenden Websites erfolgte nach dem Sichtprinzip, wobei insbesondere darauf geachtet wurde, nicht nur professionelle Medien aus dem Gesundheitswesen zu analysieren. Unterschiedliche Institutionen, von der Universitätsklinik, über einzelne Ärzte oder Ärzteverbünde, gemeinnützige Organisationen, Behörden, aber auch die erwähnten Medienunternehmen wurden zu den obigen Suchbegriffen auf den ersten Seiten gefunden. Die Studie ist nicht geeignet, repräsentative Zahlen für den gesamten Gesundheitsbereich zu liefern, wohl aber ermöglicht sie einen ersten Eindruck, wie weitgehend die datenschutzrechtlichen Grundlagen der DS-GVO und des BDSG (neu) sowie des Telemediengesetzes in Deutschland umgesetzt werden.

Kurzfassung

Alle untersuchten Websites wiesen zum Zeitpunkt der Analyse datenschutzrechtlich zu kritisierende Verarbeitungen auf. Die Mehrzahl der Websites hatten Drittanbieter eingebunden, Cookies und teilweise auch Einträge in den local storage gesetzt, ohne den Besucher adäquat zu informieren oder gar die Möglichkeit der Verhinderung durch den Besucher zu ermöglichen. Lediglich ein Unternehmen setzte dabei ein Consent-Tool ein, das technisch den Vorgaben des EuGH entspricht, bedauerlicherweise war auch hier eine Zustimmung vorangekreuzt und somit der Einsatz des Tools ebenfalls nicht konform nach dem Urteil des EuGH.

Gemessen an der inhaltlichen Brisanz der aufgerufenen Informationen kann das Analyseergebnis nur als datenschutzrechtlich problematisch bezeichnet werden. In fast allen untersuchten Fällen können Dritte durch die nicht-legitimierte Weitergabe von Informationen über Besucher der Websites Rückschlüsse auf private, gesundheitliche Informationen ziehen, die nicht in fremde Hände gehören.

Rechtliche Grundlagen

Wer eine Webseite betreibt, muss sich zwangsläufig auch mit dem Thema Datenschutz beschäftigen. Dabei geht es nicht (nur) um die Inhalte, die auf der Webseite veröffentlicht werden. Es geht vielmehr und natürlich vor allem mit Bezug auf die vorliegende Studie um die personenbezogenen Daten der Besucher der Webseite. Denn selbst wer seine Webseite in nacktem HTML geschrieben hat, muss seine HTML-Dokumente auf einem Webserver hinterlegen, der zwangsläufig die IP-Adressen der Clients (also personenbezogene Daten der Besucher) in irgendeiner Weise verarbeiten muss. Moderne Webseiten beschränken sich aber kaum auf reine HTML Inhalte. Vielmehr werden Techniken eingesetzt, die den Unzulänglichkeiten des wichtigen Protokolls HTTP, welches „zustandslos“ ist, begegnen sollen, so z.B. das Setzen und Auslesen von Cookies.

Der Anwendungsbereich der DSGVO ist also eröffnet. Als abstrakt generelle Regelung enthält die DSGVO freilich keine expliziten Erlaubnistatbestände für Cookies oder andere Trackingmethoden. Es ist aber mitunter schwierig, die allgemeinen Erlaubnistatbestände des Art. 6 DSGVO auf spezielle Einzelprobleme anzuwenden. Ein Gesetz, das sich speziell mit dem Datenschutz beim Betreiben von Webseiten befasst, wäre also wünschenswert. Die Betreiber von Webseiten warten jedoch bislang vergeblich auf die Verabschiedung der geplanten ePrivacy-Verordnung, die die DSGVO in diesem Punkt (etwas allgemeiner: im Bereich der elektronischen Kommunikation) bereichsspezifisch präzisieren, ergänzen und die alte Richtlinie RL 2002/58/EG ersetzen soll.[1]

Solange eine besondere Regelung auf sich warten lässt, muss der Erlaubnistatbestand in der DSGVO gefunden werden.[2] Die deutschen Aufsichtsbehörden wenden Art. 6 Abs. 1 lit. f DSGVO an. Nach dieser Vorschrift dürfen personenbezogene Daten verarbeitet werden, wenn die

1 Ein aktualisierter Entwurf ist am 04.10.2019 von der finnischen Ratspräsidentschaft veröffentlicht worden. Dieser Entwurf soll in der zuständigen Ratsarbeitsgruppe diskutiert werden, um zu einem gemeinsamen Standpunkt der Mitgliedstaaten zu gelangen.

2 Dass § 15 Abs. 3 TMG keine Erlaubnisnorm in Bezug auf Tracking ist, dürfte mittlerweile herrschende Meinung in der Rechtswissenschaft sein. Praktische Unterschiede dürfte es ohnehin im Vergleich zur Anwendung des Art. 6 Abs. 1 lit. f DSGVO nicht geben.

Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Für Sitzungscookies, die z.B. in einem Internet-Shop eine Warenkorbfunktionalität technisch ermöglichen, dürften die Voraussetzungen dieser Erlaubnisnorm unproblematisch vorliegen. Beim Tracking, das Internetnutzer „gläsern“ und verfolgbar machen soll, kann das nicht so einfach gelten. Die Aufsichtsbehörden fordern beim Einsatz solcher Technologien die Einholung einer Einwilligung der betroffenen Person. Diese Forderung dürfte zu pauschal erhoben sein, vielmehr muss eine Abwägung im Einzelfall erfolgen. Das ist keine leichte Aufgabe, sieht man sich nur die Vielzahl der unbestimmten Rechtsbegriffe an, mit denen Art. 6 Abs. 1 lit. f DSG VO hantiert.

Es kommt daher nicht von ungefähr, dass sich der EuGH mit eben solchen Fragestellungen zu beschäftigen hat, zumal dem EuGH als Hüter der Verträge die Auslegungskompetenz bezüglich europäischer Rechtsetzungsakte wie dem der DSGVO zusteht. Auf Vorlage des BGH[3] erging eine wichtige Entscheidung des EuGH am 01.10.2019.[4] Der EuGH stellt in dieser klar, dass Cookies, die nicht zwingend technisch erforderlich sind, die (aktive) Einwilligung der Nutzer voraussetzen. Ein „opt out“ ist nicht ausreichend, d.h. der Nutzer muss aktiv z.B. durch das Anklicken eines Kästchens in die Datenverarbeitung einwilligen.[5] Das Ankreuzkästchen darf nicht vorausgewählt sein, denn das würde einem passiven Verhalten des Nutzers entsprechen und wäre damit nicht als Einwilligung zu werten. Dem Urteil des EuGH lässt sich indes nicht entnehmen, dass bei jedem Cookie eine Einwilligung vorliegen muss. Webseitenbetreiber werden daher sorgfältig zu den technisch notwendigen Cookies abzugrenzen haben, was im Einzelfall schwierig sein könnte. Dem normalen Rechtsanwender dürfte sich kaum erschließen, was der EuGH mit „hidden identifiers“ meint, die ohne Wissen der Nutzer in deren Endgeräte „eindringen“. Es gibt Spielraum für Auslegung und Diskussionen. Sicher aber ist: Die Regelungs- und Prüfdichte im Datenschutz steigt.

3 BGH GRUR 2018, 96; Vorinstanz OLG Frankfurt a.M. v. 17.12.2015, Az. 6 U 30/15.

4 EuGH, Urt. v. 1.10.2019, Az. C-673/17, abgedruckt u.a. in NJW 2019, 3433 = MMR 2019, 732 m.Anm. Moos, Rothkegel.

5 Damit dürfte § 15 Abs. 3 TMG als nicht richtlinienkonform gelten, eine Anpassung durch den Gesetzgeber steht aus. Die sog. Cookie-Richtlinie (2009/136/EG) sieht ebenjene ausdrückliche Einwilligung vor.

Ergebnisse der Studie

SSL-Verschlüsselung

Zwei der untersuchten 45 Websites verfügten zum Zeitpunkt der Erfassung nicht über eine SSL-Verschlüsselung. Zwei weitere Websites verfügten zwar über die Möglichkeit der SSL-Verschlüsselung, hatten diese aber nicht als Standard voreingestellt. Die Abdeckung der untersuchten Websites mit SSL-Verschlüsselung, die als Standard voreingestellt wurde und beim Aufruf einer Seite ohne https zur sicheren Version umleitete, kann als gut bezeichnet werden. Zu diesem positiven Ergebnis mag neben einer gewachsenen Sensibilität auch die Tatsache, dass es mittlerweile kostenfreie Zertifikate gibt, beigetragen haben. In einem Fall war ein Webformular ohne SSL-Verschlüsselung eingebunden.

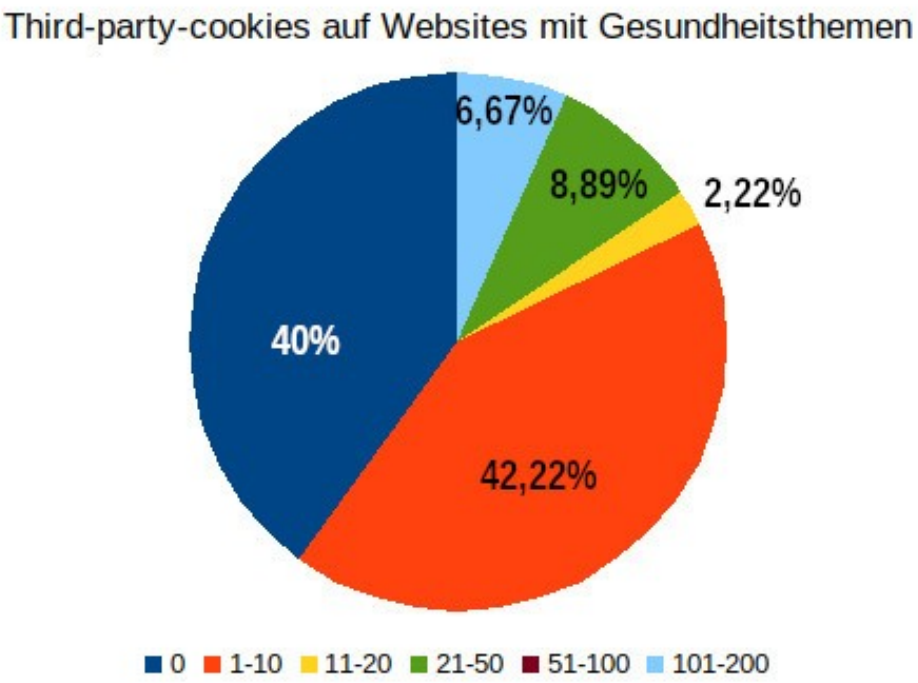
Cookies

Fast alle der untersuchten Websites setzen Cookies ein, insgesamt wurden von 45 Websites 851 Cookies gesetzt, davon waren 590 sogenannte „third-party-cookies“, also Cookies, die von Dritten ausgelesen werden können. Fünf von 45 Websites kamen gänzlich ohne das Setzen von Cookies aus, drei Unternehmen setzten jeweils mehr als 100 Cookies pro Website. Den Rest teilten sich die verbleibenden Unternehmen mit unterschiedlicher Intensität auf.

Grafik: Verteilung der Häufigkeit von Cookies

Die Mehrzahl der untersuchten Websites (62,22%=28 Websites) setzten 1 bis 10 Cookies ein. Der Spitzenwert lag bei 148 Cookies.

Grafik: Verteilung der third-party-cookies



Wie aus der Verteilung sichtbar wird, setzen 40% der untersuchten Websites keine third-party-cookies ein, bei 42,22% waren es bis einschließlich 10 Cookies. Der Rest der untersuchten Websites lag teilweise deutlich über diesen Werten.

Cookie Popup

Obwohl nur fünf Unternehmen auf eine adäquate Information vor dem Setzen von Cookies verzichten konnten, wiesen nur 28 von 43 Unternehmen darauf hin, dass Sie Cookies auf der Website einsetzen. Lediglich ein Unternehmen setzte ein Consent-Tool mit weiteren Informationen und Auswahlmöglichkeiten ein. Bei den 28 Websites, die ein Cookie-Popup einsetzten, handelte es sich in fast allen Fällen um einen unspezifizierten Hinweis. In keinem der untersuchten Fälle bestand die Möglichkeit, dem Setzen von Cookies zu widersprechen und das Setzen wirkungsvoll zu verhindern. Die Anzeige des Cookie-Popup konnte in der Regel lediglich mit dem Klick auf „OK“ oder eine andere Form der „Einwilligung“ unterbunden werden.
Nicht einwilligungspflichtig sind hierbei nur Cookies, die der technischen Funktionsfähigkeit der Website und der Leistungserbringung dienen. Für alle anderen Cookies gilt, dass die informierte und freiwillige Einwilligung nach dem EuGH Urteil die einzige legitime Variante darstellt.

Local Storage („hidden identifiers“)

14 von 45 Unternehmen hatten insgesamt 171 Einträge in den local storage des Besuchers vorgenommen. Im Unterschied zu Cookies ist hier der Speicherplatz nicht begrenzt, so dass erheblich größere Datenmengen übermittelt werden können. Einträge in den local storage können unter Umständen dazu verwendet werden, Besucher zu verfolgen und Profilbildungen zu ermöglichen. Durch eine reine Sichtprüfung kann die konkrete Verwendung von Daten-speichervorgängen im local storage nicht bestimmt werden.

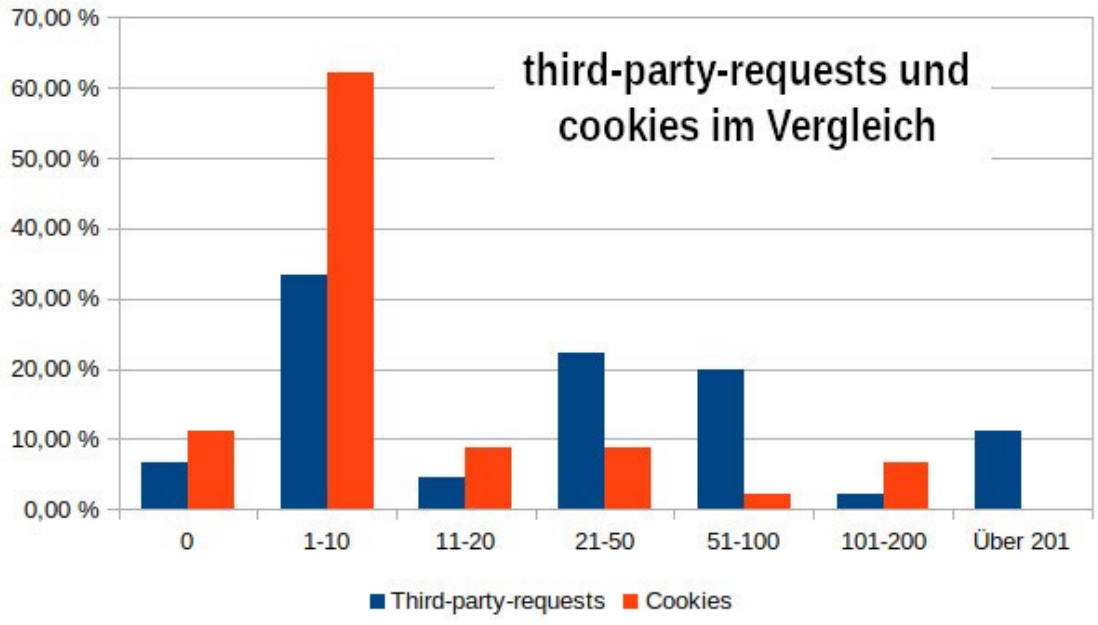
Consent-Tools

Obwohl schon eine Weile auf dem Markt, hat derzeit nur ein Anbieter ein echtes Conset-Tool eingebunden, das vor einem Eingriff in den Rechner des Users, diesen informiert und die freie Wahl der Zustimmung oder Ablehnung lässt. Nicht rechtskonform war dabei das vorangekreuzte Kästchen im Consent-Tool.

Einbindung von Drittanbietern

Lediglich drei von 45 Websites verzichteten auf die Einbindung von Drittanbietern. Die verbleibenden 42 Websites banden insgesamt 2769 sogenannte „third-party-requests“ in ihren Webauftritt ein. 20 Websites nutzten Google Fonts von externen Google Servern, 30 Websites banden andere CDNs in ihrem Auftritt ein.

Grafik: Verteilung third-party-requests und cookies



Zwei der fünf Unternehmen, die keine Cookies einsetzten, banden Drittanbieter in ihr Webangebot ein. In beiden Fällen handelte es sich um die Einbindung von Google Fonts von den Google-Servern. Generell kann festgestellt werden, dass die Anzahl der Cookies mit der Anzahl der third-party-requests korreliert. Je mehr Cookies eingesetzt werden, um so höher ist auch die Anzahl der Einbindung von Drittanbietern auf der Website. Diese werden so zu (ungewollten?) Datenlieferanten vor allem für die großen Datensammler des Internets.

Grafik: Direkte Einbindung von Google Fonts von den Google Servern

20 von 45 untersuchten Websites hatten unnötigerweise Google Fonts per Abruf von den Google Servern eingebunden und damit personenbezogene Daten an das amerikanische Unternehmen übermittelt.
8 von 45 Websites (17,7%) hatten facebook connect direkt eingebunden und damit direkt eine Datenübermittlung an Facebook angestoßen, die es Facebook ermöglicht, die Daten mit weiteren zu einem Profil zusammenzuführen.

Tracking

32 von 45 Websites nutzten Trackingtools externer Anbieter zur Analyse der Besucherströme auf der Website. Der weitaus größte Teil davon entfiel auf Google Analytics. Zwar wurde in den meisten Fällen in der Datenschutzerklärung auf die Nutzung von Analysetools hingewiesen, in

keinem Fall jedoch hatte der Besucher die Möglichkeit, vor der Erfassung zu widersprechen und diese damit wirkungsvoll zu verhindern. Eine rechtskonforme Einwilligung wurde nicht eingeholt.

Fazit

Wer über Gesundheitsthemen informiert, vor allem über solche, bei denen erwartbar der Besucher der Website ein hohes Bedürfnis nach Schutz und Privatheit hat, sollte noch sensibler als andere Betreiber von Websites mit der Weitergabe von Informationen an Dritte umgehen. Diese Form der Rücksichtnahme konnten wir mit wenigen Ausnahmen nicht antreffen. Ein nicht geringer Teil der Betreiber der untersuchten Websites riskiert nicht nur Anfragen und Beschwerden der Besucher, sondern bei Bekanntwerden unter Umständen auch Anordnungen und Bußgelder der Behörden.

Langen und Baden-Baden, den 05.12.2019

Autoren der Studie:
Dr. jur. Wolfhard Steinmetz, Langen
Peter Dippold, Baden-Baden

Impressum:
Peter Dippold
Eichelgartenstr. 6
76530 Baden-Baden

https://www.dsb-baden-baden.de
info@dsb-baden-baden.de
Telefon: 07221 8589943