THOMAS HOEREN

Google Analytics – datenschutzrechtlich unbedenklich?

Verwendbarkeit von Webtracking-Tools nach BDSG und TMG

Webseiten-Analyse
Surfprofil
Bestimmtheit der Person
Dynamische IP-Adresse
Zusammenführen von Daten
Cookie-Sperre

■ Google Analytics ist ein kostenloser Dienst von Google, der die Analyse des Zugriffs auf Webseiten ermöglicht. Die Zulässigkeit einer solchen Analyse ist jedoch umstritten, gerade auch nach Maßgabe des deutschen Datenschutzrechts. Daher scheuen sich viele Unternehmen, das Tool einzusetzen. Der folgende Beitrag setzt sich mit der Vereinbarkeit solcher Webtracking-Dienste mit den Vorgaben des TMG und des BDSG auseinander.

■ Google Analytics is a free service offered by Google that allows the analysis of access to Web pages. The admissibility of such an analysis is controversial, especially in view of the legal requirements of German data protection law. Therefore, many companies are reluctant to use the tool. The following article discusses the compatibility of such Web tracking services with the requirements of the Telemedia Act and the Federal Data Protection Act.

I. Beschreibung des Dienstes – Was ist Google Analytics?

Bei dem von *Google* angebotenen Dienst Google Analytics handelt es sich um eine Weiterentwicklung einer ursprünglich von der *Urchin Software Corporation* stammenden Technik. Im März 2005 übernahm *Google* das Unternehmen *Urchin*,[1] welches zu diesem Zeitpunkt bereits ein Programm entwickelt hatte, das durch die Auswertung von Logdateien Informationen über das Nutzerverhalten auf Websites grafisch darstellen konnte. Das Programm wurde als Kaufversion vertrieben sowie als ASP-Lösung unter dem Namen „Urchin on demand". Während die Kaufversion auch nach der Übernahme durch *Google Inc.* weiterentwickelt wurde, benannte man „Urchin on demand" um und veröffentlichte es Ende 2005 kostenfrei als Google Analytics.[2]

Bei dem Programm handelt es sich um ein sog. Tracking-Tool, mit dessen Hilfe nachvollzogen werden kann, von wo aus die zu analysierende Website angesteuert und in welche Richtung sie anschließend wieder verlassen wurde.[3] Dabei werden Nutzungsdaten, wie die Anzahl der Zugriffe, die Zahl der Nutzer und ihre regionale Herkunft, die aufgerufenen Seiten, die Verweildauer auf dem Angebot, Informationen über das vom Nutzer verwendete Endgerät sowie dessen IP-Adresse erhoben.[4] Analytics wird von vielen Webseitenbetreibern zu Zwecken der Marktforschung, Werbung oder bedarfsgerechten Gestaltung ihrer Angebote genutzt.

1. Technische Realisierung

Zur Implementierung des Google-Dienstes bettet der Betreiber der zu analysierenden Website ein JavaScript in seine Seite ein, welches zwei Funktionen übernimmt: Zum einen leitet es die IP-Adresse der Besucher der Seite an *Google Inc.* weiter. Außerdem wird auf den Rechnern der Seitenbesucher ein „First Party Cookie" abgelegt, der mit einer eindeutigen Identifikationsnummer versehen ist. Er dient dazu, den Browser des Nutzers bei einer Wiederkehr auf die Seite unmittelbar wieder für *Google* identifizierbar zu machen. Die Identifikationsnummer des Cookies wird dabei auch direkt an *Google Inc.* übertragen.[5] Diese beiden Nutzungsdaten werden anschließend von *Google* analysiert und die statistischen Auswertungsergebnisse wiederum an den Webseitenbetreiber übermittelt.[6] *Google* selbst kann mit Hilfe des Cookies die Nutzungsdaten verschiedener Webseiten zu einem Surfprofil des Nutzers zusammenfügen, d.h., das Unternehmen hat Kenntnis aller Analytics-basierten Webseiten, die der Nutzer besucht hat. Die so erlangten Nutzungsdaten kann *Google* für weitere eigene Auswertungen verwenden.[7]

2. Wirtschaftliche Bedeutung

Der Google Analytics-Dienst stieß schon bei seiner Markteinführung Ende 2005 auf enormes Interesse. Auf Grund der großen Nachfrage kam es sogar dazu, dass *Google* Anfang 2006 zunächst keine weiteren Anmeldungen zu dem Service mehr zuließ bzw. dies nur noch auf eine Einladung hin möglich war. Dieser Anmeldestopp wurde nach einer Erweiterung der Kapazitäten erst im Sommer 2006 wieder aufgehoben.[8] Heutzutage ist Google Analytics das meistverwendete Webanalyseprogramm überhaupt. Nach einer Kontrolle des *Landesbeauftragten für Datenschutz in Rheinland-Pfalz* nutzten im Januar 2011 z.B. mehr als die Hälfte der 100 größten Unternehmen in dem Bundesland Tracking-Tools für ihre Webseiten. Etwa ein Viertel griff dabei auf Google Analytics zurück.[9] Eine andere Statistik aus dem Jahr 2009 zeigte, dass damals fast die Hälfte der 50.000 beliebtesten deutschen Onlineangebote Google Analytics einsetzten.[10]

II. Rechtliche Probleme

Die Funktionsweise von Google Analytics wirft erhebliche datenschutzrechtliche Bedenken auf.

1 http://www.heise.de/newsticker/meldung/Google-uebernimmt-Hersteller-von-Web-Analysesoftware-148242.html.
2 http://www.heise.de/newsticker/meldung/Google-verschickt-Einladungen-fuer-Analytics-165631.html.
3 *Kirsch*, MMR-Aktuell 2011, 313724.
4 http://www.datenschutz.rlp.de/downloads/oh/Hinweise_Google_Analytics.pdf.
5 Stellungnahme des *ULD Schleswig Holstein*, „Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics, Januar 2009", S. 1, abrufbar unter: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf.
6 https://www.datenschutzzentrum.de/presse/20080807-google-analytics.htm.
7 MMR 8/2008, S. VIII.
8 http://www.heise.de/newsticker/meldung/Google-nimmt-wieder-Anmeldungen-zu-Analytics-an-152846.html.
9 MMR-Aktuell 2011, 313915.
10 http://www.idealobserver.com/component/lyftenbloggie/?view=entry&id=112.

1. Anwendbarkeit des Datenschutzrechts

Zwar könnte man grundsätzliche Zweifel daran äußern, dass das Datenschutzrecht überhaupt auf den typischerweise beim Einsatz von Google Analytics vorliegenden Sachverhalt Anwendung findet. Denn dies ist regelmäßig nur dann der Fall, wenn dabei personenbezogene Daten erhoben, verarbeitet und genutzt werden. Die Frage ist maßgeblich nach dem TMG zu beantworten, da es sich sowohl bei den jeweiligen Webseitenbetreibern als auch bei *Google* um Dienstanbieter i.S.d. § 2 Nr. 1 TMG handelt, auf deren Handeln zunächst gem. § 1 Abs. 1 TMG das Telemediengesetz mit seinen bereichsspezifischen Datenschutzregelungen vorrangig Anwendung findet. Das BDSG kann dagegen nur ergänzend herangezogen werden.

Personenbezogene Daten sind gem. § 12 Abs. 3 TMG, § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Bestimmbarkeit der Person ist dann gegeben, wenn die betroffene Person noch nicht durch die Daten allein, jedoch mit Hilfe anderer Informationen identifiziert werden kann.[11] Im vorliegenden Fall könnte es an der Bestimmtheit oder Bestimmbarkeit der Person fehlen, deren IP-Adresse und Cookie-Identifikationsnummer an *Google* gesendet werden. Denn für einen Dritten lässt sich allein aus diesen Angaben nicht ohne weiteres auf die dahinterstehende real existierende und handelnde natürliche Person schließen. Vor diesem Hintergrund wird es unmittelbar klar, warum die Frage, ob eine IP-Adresse grundsätzlich ein personenbezogenes Datum darstellt, seit einigen Jahren in Rechtsprechung und Literatur hoch umstritten ist. Weitgehende Einigkeit herrscht darüber, dass eine statische IP-Adresse ein personenbezogenes Datum darstellt, lässt sie sich doch eindeutig einem Anschlussinhaber zuordnen.[12] Probleme kann dies nur dann bereiten, wenn die IP-Adresse einem Rechner zugewiesen ist, der von einer Vielzahl von Personen genutzt wird, wie es regelmäßig in großen Firmen der Fall sein wird.[13]

Der Streit beschränkt sich also auf dynamische IP-Adressen, die permanent neu vergeben werden. Hier kommt es maßgeblich darauf an, ob man bei der Frage nach der Bestimmbarkeit der hinter den Daten stehenden Person einen absoluten oder einen relativen Begriff verwendet. Nach der Theorie der absoluten Personenbezogenheit besteht die Bestimmbarkeit bereits dann, wenn abstrakt für irgendjemanden (also auch nicht zwingend für die verarbeitende Stelle) die Möglichkeit besteht, die Daten der dahinterstehenden natürlichen Person zuzuordnen.[14] Anders sehen es die Vertreter der (noch) h.M., die von einem relativen Personenbezug ausgehen. Dieser soll immer dann vorliegen, wenn die konkrete datenverarbeitende Stelle mit vertretbarem Aufwand eine Identifikation der natürlichen Person hinter der IP-Adresse vornehmen könnte,[15] sei es durch eigenes Zusatzwissen,[16] sei es durch frei verfügbares Wissen.[17]

Nach der ersten Theorie stellt eigentlich jede IP-Adresse an sich schon ein personenbezogenes Datum dar, werden doch durch die Access-Provider (teilweise noch) Log-Protokolle geführt, anhand derer sich die IP-Adresse dem jeweiligen Kunden zuordnen lässt, solange diese aufbewahrt werden.

Doch auch nach dem relativen Begriff dürfte im Fall *Google* die IP-Adresse ein personenbezogenes Datum sein. Denn das Unternehmen bietet in der breit gefächerten Palette seiner Dienste eine ganze Reihe von Services an, für die man sich mit dem eigenen Klarnamen bzw. zumindest einer E-Mail-Adresse identifizieren muss. Für *Google* wird daher in einer Vielzahl der Fälle die – zumindest theoretische – Möglichkeit bestehen, die entsprechenden Daten zusammenzuführen und so den Webseitenbesucher eindeutig zu identifizieren.[18] Zwar weist das Unternehmen in den Datenschutzbestimmungen zu Analytics darauf hin, dass es den Analytics-nutzenden Webseitenbetreibern nach den Nutzungsbedingungen des Services untersagt sei, personenbezogene Daten der Besucher mit Webanalysedaten zusammenzuführen.[19] Andererseits behält sich *Google* selber dieses Recht im Rahmen seiner allgemeinen Datenschutzbedingungen vor.[20] Vor diesem Hintergrund dürfte es äußerst zweifelhaft sein, ob es nicht doch zu einer Zusammenführung der entsprechenden Daten kommt. Darüber hinaus ist es auf Grund der schieren Menge der Websites, die mittlerweile Google Analytics nutzen, ebenfalls möglich, umfassende Nutzungs- und „Bewegungs"-Profile der so identifizierten Internetnutzer zu erstellen.

Ähnlich verhält es sich mit der ebenfalls übertragenen ID des Cookies, der durch den Analytics-Dienst auf den Rechnern der Besucher der Website abgelegt wird. Auch diese kann durch Kombination mit weiteren bei *Google* vorhandenen Daten hypothetisch zu einer Identifikation der dahinterstehenden natürlichen Person benutzt werden bzw. zumindest *Google* in die Lage versetzen, ein „Unique-User-Profil" über den jeweiligen Nutzer anzulegen.

Insofern besteht zumindest die ernstzunehmende Gefahr, dass personenbezogene Daten verarbeitet werden. Mithin ist von einer Anwendbarkeit des Datenschutzrechts auszugehen.

2. Rechtlich relevante Vorgänge

Zu fragen ist weiter, ob ein rechtlich relevanter Vorgang vorliegt. Dies wäre dann der Fall, wenn es im Laufe des bei Google Analytics angewandten Verfahrens zu einer Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten käme. Zwar dürfte es vor dem Hintergrund, dass *Google* sich die weitere Nutzung der an das Unternehmen übermittelten Daten vorbehält, kaum möglich sein, genau zu sagen, welche Verarbeitungshandlungen im Detail vorliegen. Zumindest stellt aber die Feststellung der IP-Adresse bzw. der Cookie-ID ein Erheben personenbezogener Daten i.S.d. § 3 Abs. 3 BDSG dar.

Ebenfalls steht fest, dass diese Daten anschließend an *Google* gesendet werden, damit dort die Auswertungsstatistiken für den Webseitenbetreiber erstellt werden können. Mithin liegt im Verhältnis des Webseitenbetreibers zu *Google* eine Datenübermittlung i.S.d. § 3 Abs. 4 Nr. 3a BDSG vor sowie ein anschließendes Speichern und Nutzen der Daten im Hause *Google*, § 3 Abs. 5, 4 Nr. 1 BDSG.

3. Beurteilung der Vorgänge

Grundsätzlich ist gem. § 12 Abs. 1 TMG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn entweder eine Einwilligung des Nutzers oder eine gesetzliche Ermächtigung besteht.

a) Einwilligung

Google schreibt den Nutzern seines Analytics-Services in Ziff. 8.1 der Nutzungsbedingungen[21] vor, die Aufmerksamkeit der Nutzer der Website auf eine Erklärung zu lenken, die im Wesentlichen diesem von *Google* vorgegebenen Text entspricht:

---

11 *Damann*, in: Simitis (Hrsg.), Komm. zum BDSG, 6. Aufl., § 3 Rdnr. 22.
12 *Voigt*, MMR 2009, 377, 378 m.w.Nw.
13 Zu diesem Problem auch *Voigt*, MMR 2009, 377, 380.
14 *AG Berlin* K&R 2007, 600, 601 m.w.Nw.; *Schaar*, Datenschutz im Internet, Rdnr. 175; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Basiskomm. zum BSDG, 3. Aufl., § 3 Rdnr. 13; *Pahlen-Brandt*, DuD 2008, 34 f.
15 *AG München* K&R 2008, 767; *Gola/Schomerus*, BDSG Komm., 9. Aufl., § 3 Rdnr. 10; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl., § 11 TMG Rdnr. 5b; *Damann* (o. Fußn. 11), § 3 Rdnr. 33.
16 *Weichert* (o. Fußn. 14), § 3 Rdnr. 13.
17 *Damann* (o. Fußn.. 11), § 3 Rdnr. 36.
18 So auch *Voigt*, MMR 2009, 377, 379.
19 http://www.google.com/intl/de/analytics/privacyoverview.html.
20 http://www.google.com/intl/de/privacy/privacy-policy.html.
21 Abrufbar unter: http://www.google.at/intl/de_ALL/analytics/tos.html.

„Diese Website benutzt Google Analytics, einen Webanalysedienst der Google Inc. („Google"). Google Analytics verwendet sog. „Cookies", Textdateien, die auf Ihrem Computer gespeichert werden und die eine Analyse der Benutzung der Website durch Sie ermöglichen. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website (einschließlich Ihrer IP-Adresse) wird an einen Server von Google in den USA übertragen und dort gespeichert. Google wird diese Informationen benutzen, um Ihre Nutzung der Website auszuwerten, um Reports über die Websiteaktivitäten für die Websitebetreiber zusammenzustellen und um weitere mit der Websitenutzung und der Internetnutzung verbundene Dienstleistungen zu erbringen. Auch wird Google diese Informationen gegebenenfalls an Dritte übertragen, sofern dies gesetzlich vorgeschrieben ist oder soweit Dritte diese Daten im Auftrag von Google verarbeiten. Google wird in keinem Fall Ihre IP-Adresse mit anderen Daten von Google in Verbindung bringen. Sie können die Installation der Cookies durch eine entsprechende Einstellung Ihrer Browser Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website vollumfänglich nutzen können. Durch die Nutzung dieser Website erklären Sie sich mit der Bearbeitung der über Sie erhobenen Daten durch Google in der zuvor beschriebenen Art und Weise und zu dem zuvor benannten Zweck einverstanden."

Die Voraussetzungen der Einwilligung sind in § 4a BDSG und § 13 Abs. 2 TMG geregelt. Zwar könnte man bei einer Veröffentlichung dieses Textes daran denken, im letzten Satz eine entsprechende Einwilligung zu sehen. Doch hängt dies auch maßgeblich davon ab, ob und wie der jeweilige Webseitenbetreiber den Text auf seiner Internetseite platziert, selbst wenn der von *Google* vorgegebene Originaltext verwendet wird. Denn wenn der Text nur „irgendwo" auf der Internetseite angezeigt wird und der Nutzer die Kenntnisnahme nicht gesondert bestätigen muss, dürfte es fraglich sein, ob er durch das reine Surfen auf der Seite „bewusst und eindeutig" seine Einwilligung erklärt hat, wie es § 13 Abs. 2 Nr. 1 TMG fordert.[22]

b) Gesetzliche Erlaubnis

Eine andere Möglichkeit, um die Datennutzung i.R.v. Google Analytics rechtskonform auszugestalten, ist das Vorliegen einer gesetzlichen Erlaubnis.

■ § 15 Abs. 3 TMG

Die gesetzliche Erlaubnis könnte sich zunächst aus § 15 Abs. 3 TMG ergeben. Hiernach darf der Dienstanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht.

Zunächst ist hierzu anzumerken, dass es vor dem Hintergrund des bereits oben Gesagten mehr als fraglich sein dürfte, ob die Voraussetzungen des § 15 Abs. 3 TMG durch *Google* eingehalten werden. Denn gem. § 15 Abs. 3 Satz 3 TMG dürfen die erstellten Nutzungsprofile nicht anschließend wieder mit Daten über den Träger des Pseudonyms zusammengeführt werden. Hieran bestehen aber – vor allem vor dem Hintergrund der o.g. Ausführungen zu den Datenschutzbestimmungen von *Google* – erhebliche Zweifel.

Außerdem muss der Nutzer, über den ein Profil erstellt wird, gem. § 15 Abs. 3 Satz 2 TMG auf seine Widerspruchsmöglichkeit hingewiesen werden. Dieser Hinweis könnte zwar ebenfalls in der oben abgedruckten Erklärung gesehen werden. Doch merkte bereits der *Datenschutzbeauftragte von Rheinland Pfalz* an, dass der Hinweis auf eine Möglichkeit für den Nutzer, eine Cookie-Sperre einzurichten, nach seiner Ansicht kein ausreichendes Widerspruchsrecht i.S.d. § 15 Abs. 3 TMG darstelle.[23] Dies war früher auch bereits vom *Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein* so geäußert worden, das darauf hinwies, dass die Einrichtung einer entsprechenden Cookie-Sperre sowohl technisch als auch rechtlich nicht zumutbare Belastungen für den Webseitennutzer mit sich bringe. Denn in technischer Hinsicht müsse der Nutzer seinen Browser dann so konfigurieren, dass dieser grundsätzlich keine First-Party-Cookies mehr akzeptiere, was aber die Nutzbarkeit vieler Websites massiv einschränke.

In rechtlicher Hinsicht bestehe für den Dienstanbieter i.R.d. § 15 Abs. 3 Satz 2 TMG die Verpflichtung, die Durchsetzbarkeit des Widerspruchsrechts technisch zu realisieren. Diese Verpflichtung sei aber durch die vorgeschlagene Einrichtung einer Cookie-Sperre auf den Nutzer abgewälzt worden. [24]

Zusammenfassend bleibt festzustellen, dass § 15 Abs. 3 TMG keine taugliche Erlaubnisnorm für die fraglichen Vorgänge darstellt. Weitere gesetzliche Erlaubnisnormen sind nicht ersichtlich, sodass eine Datenverarbeitung nicht auf ein Gesetz gestützt werden kann.

■ § 11 BDSG

Eine gesetzliche Erlaubnis wäre jedoch dann nicht erforderlich, wenn es sich bei der Weiterleitung der Daten an *Google* lediglich um eine Auftragsdatenverarbeitung i.S.d § 11 BDSG handeln würde. Denn in diesem Fall stellt die Weiterleitung der Daten an *Google* kein „Übertragen" derselben an einen Dritten i.S.d. § 3 Abs. 4 Nr. 3a BDSG dar.[25]

Prinzipiell wird das Vorliegen eines Auftragsverhältnisses i.S.d. § 11 BDSG zwischen den Websitebetreibern und *Google* von den zuständigen datenschutzrechtlichen Aufsichtsbehörden bejaht,[26] auch wenn der Websitebetreiber in der Regel keine ausreichenden Kontroll- und Einflussmöglichkeiten auf *Google* habe.[27] Dies spricht aber trotzdem nicht dagegen, dass weiterhin eine Übertragung der Daten vorliegt. Denn gem. § 3 Abs. 8 Satz 3 BDSG ist dies selbst i.R.e. ordnungsgemäßen Auftragsdatenverarbeitung der Fall, wenn die Daten in ein Drittland gesendet werden.[28] Nach den ausdrücklichen Erklärungen von *Google Inc.* (s. z.B. der in den Nutzungsbedingungen empfohlene Text oben) erfolgt die Auswertung der Daten auf Servern in den USA. So entfällt die „Übermittlung" trotzdem nicht.

Mangels gesetzlicher Erlaubnisnorm besteht die einzige Möglichkeit, dieses Problem zu lösen, für den Webseitenbetreiber darin, eine ausdrückliche Einwilligung seiner Nutzer in die Datenübertragung in die USA einzuholen.

III. Verantwortlichkeit

Wie oben bereits ausgeführt, handelt es sich nach Ansicht der zuständigen Datenschützer bei dem Verhältnis des Google Analytics nutzenden Websitebetreibers zu *Google* um eine Auftragsdatenverarbeitung i.S.d. § 11 BDSG. Mithin bleibt nach wie vor der Websitebetreiber verantwortlich dafür, dass die Vorgaben des Datenschutzrechts eingehalten werden. Trägt er hierfür keine Sorge, droht ihm z.B. die Verhängung eines Bußgelds

---

22 Vgl. *Spindler/Nink* (o. Fußn. 15), § 13 TMG Rdnr. 6.

23 http://www.datenschutz.rlp.de/de/aktuell/2011/images/eudstag2011/02_-_Eiermann_-_Profilneurosen.pdf.

24 https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf.

25 Vgl. *Gola/Schomerus* (o. Fußn. 15), § 11 Rdnr. 4.

26 So z.B. der Schleswig-Holsteinische Datenschutzbeauftragte: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf.

27 MMR-Aktuell 2011, 313915.

28 *Gola/Schomerus* (o. Fußn. 15), § 11 Rdnr. 16 m.w.Nw.

gem. § 43 Abs. 2 Nr. 1 BDSG oder sogar eine Strafe nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1 BDSG.

IV. Abhilfemöglichkeiten

Der Einsatz von Google Analytics begegnet erheblichen rechtlichen Bedenken. Von Seiten der Datenschutzbeauftragten wurden daher bereits zahlreiche Maßnahmen vorgeschlagen, um eine rechtskonforme Nutzung von Tracking-Diensten zu ermöglichen.

1. „IP-Masking" und Browser-Erweiterungsmodule

Zum einen sollen an dieser Stelle die Möglichkeiten des IP-Masking sowie der Installation einer Browser-Erweiterung durch den Nutzer genannt werden. Diese Angebote wurden von *Google* als Reaktion auf die massive Kritik der Datenschutzbeauftragten am Analytics-Dienst eingerichtet. Zum einen haben nun die Websitebetreiber die Möglichkeit, durch eine Skriptänderung einen geänderten Websitecode i.R.v. Google Analytics in ihre Website einzubinden, welcher veranlasst, dass die letzten 8 bit der erhobenen IP-Adresse von *Google* gelöscht werden, bevor es zu einer Speicherung und Weiterverarbeitung der Adresse kommt. Damit ist weiterhin eine grobe Lokalisierung des surfenden Nutzers möglich, die für die Zwecke von Analytics genügt, aber keine Identifizierung mehr (sog. „IP-Masking").[29] Weiter hat *Google* eine Browser-Erweiterung[30] entwickelt, welche nach der Installation durch den Nutzer verhindern soll, dass der Analytics-Code bei dem Besuch einer entsprechenden Website ausgeführt wird.

Der *Hamburger Datenschutzbeauftragte* sah diese Lösungen dennoch als unzureichend an. Sein Hauptkritikpunkt am Browser Add-on bestand darin, dass die Erweiterung nicht für Opera und Safari-Browser erhältlich sei, mithin keine ausreichende Schutzmöglichkeit für die Nutzer dieser Programme bestehe.[31] Das Gleiche merkte der *Datenschutzbeauftragte für Rheinland-Pfalz* auch für Smartphone-Browser an.[32] Auch wurden Zweifel daran geäußert, ob wirklich eine ausreichende Anonymisierung der IP-Adressen stattfinde.[33]

2. Alternative Dienste

Eine echte Alternative, wenn man als sich Websitebetreiber einerseits nicht der Gefahr der Nutzung eines rechtswidrigen Dienstes aussetzen möchte, andererseits aber auch nicht auf die Analyse der Besucherströme auf der eigenen Seite zu Marketingzwecken verzichten mag, ist die Nutzung eines Analyse-Programms, dessen Rechtskonformität von den Datenschutzbeauftragten bereits festgestellt worden ist. Hier ist z.B. das Programm „Piwik" zu nennen, welches nach Ansicht des *Landesbeauftragten für Datenschutz des Landes Schleswig-Holstein* mit entsprechenden Einstellungen datenschutzrechtskonform genutzt werden könne.[34]

Professor Dr. Thomas Hoeren
ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der Universität Münster sowie Mitherausgeber der MMR und der ZD.

29 http://www.google.com/support/analytics/bin/answer.py?hl=en&answer=181782.
30 Das Tool kann heruntergeladen werden unter: http://tools.google.com/dlpage/gaoptout.
31 Vgl. MMR-Aktuell 2011, 313915; http://www.heise.de/newsticker/meldung/Datenschuetzer-bricht-Verhandlungen-ueber-Google-Analytics-ab-1167438.html.
32 http://www.datenschutz.rlp.de/de/aktuell/2011/images/eudstag2011/02_-_Eiermann_-_Profilneurosen.pdf; ausführlicher dazu: https://www.datenschutzzentrum.de/material/tb/tb33/kap10.htm.
33 http://www.heise.de/newsticker/meldung/Datenschuetzer-bricht-Verhandlungen-ueber-Google-Analytics-ab-1167438.html.
34 Vgl. die entsprechende Anleitung unter: https://www.datenschutzzentrum.de/tracking/piwik/20110315-webanalyse-piwik.pdf.

JOCHEN SCHNEIDER

Die Datensicherheit – eine vergessene Regelungsmaterie?

Ein Plädoyer für Aufwertung, stärkere Integration und Modernisierung des § 9 BDSG

Technikunterstützung
IT-Sicherheit
Datenschutzkontrolle
Skandalisierung
Instrumente zum Selbstschutz

■ Die Modernisierung des BDSG steht seit langem an. Zu den Forderungen gehört, den Gefahren neuer Techniken und Medien zu begegnen. Weitgehend vernachlässigt wird bei der Artikulierung des Reformbedarfs die „Daten- bzw. IT-Sicherheit". Das BDSG hat schon bislang die Entwicklung des interdisziplinären Bereichs IT-Sicherheit und dessen rechtliche Voraussetzungen und Implikationen verabsäumt – trotz zahlreicher Novellen. Dem BDSG fehlt der Ansatz, dass der Betroffene sich selbst mit Technikunterstützung und eigenen Sicherheitsmaßnahmen besser und aktiv schützen kann (und soll). Auch werden die Anforderungen der DS-RL weit verfehlt, zumindest was den Wortlaut betrifft. Für die Neufassung der DS-RL soll noch 2011 ein Entwurf vorliegen. Vermutlich vergrößert sich dann der Reformbedarf hinsichtlich der Datensicherheit noch.

■ The modernization of the Federal Data Protection Act (BDSG) has been on the agenda for a long time. One of the demands is to address the threat of new technology and media. „Data and IT security" is largely neglected as a factor in the articulation of the need for reform. The BDSG has so far bypassed the development of the interdisciplinary area of IT security, its legal requirements and implications – in spite of numerous amendments. The BDSG fails to address the approach that an individual can (and should) much better protect himself actively with the support of technology and through his own security measures. The requirements of the Data Protection Ordinance (DS-RL) miss this target by far, at least as far as its wording is concerned. For the revision of the DS-RL, a draft is to be expected in 2011. Presumably, there will be a further increase in the need for reform to improve data security.