Michael Knopp

Datenschutzherausforderung Webtracking

Am 26./27.11.2009 hat der Düsseldorfer Kreis in einem Beschluss Kriterien für die rechtskonforme Verwendung von Webtracking-Diensten wie Google Analytics, eTracker oder open tracker vorgelegt. Mehrere Aufsichtsbehörden haben inzwischen ein Vorgehen gegen Verstöße angekündigt. Doch auch seitens der Anbieter erfolgten inzwischen Anpassungen. Der Beitrag gibt Empfehlungen für ein rechtskonformes Vorgehen.

1 Einleitung

In seinem Beschluss vom 26./27. November 2009 hat der Düsseldorfer Kreis, der Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, folgende Kriterien für die rechtskonforme Gestaltung einer Reichweitenmessung von Webangeboten entwickelt:[1]

- Den Betroffenen ist eine wirksam umgesetzte Widerspruchsmöglichkeit gegen die Nutzerprofilerstellung zu geben;
- Nach Erstellen der Nutzungsanalyse sind die Daten zu löschen;
- Es darf nicht zu einer Zusammenführung der pseudonymisierten Daten mit Identifikationsdaten kommen;
- Die Seitenanbieter müssen deutlich auf die Widerrufsmöglichkeit, ihre Datenschutzerklärung und eine Möglichkeit zur pseudonymen Nutzung des Webangebots hinweisen;
- Bei Nutzung einer vollständigen IP-Adresse zu Analysezwecken ist eine Einwilligung des Nutzers einzuholen oder die Personenbeziehbarkeit durch Kürzung der IP-Adresse auszuschließen.

Michael Knopp, Jurist

Berater bei der Secorvo Security Consulting GmbH. Schwerpunkte: Datenschutz und Rechtsfragen im Kontext der IT-Sicherheit.
E-Mail: michael.knopp@secorvo.de

Darüber hinaus sollen auch bei der Erstellung von pseudonymen Nutzungsprofilen die Vorgaben des § 11 BDSG für die Auftragsdatenverarbeitung eingehalten werden.

Während der Beschluss allgemein formuliert ist, hat sich die Aufmerksamkeit schnell auf den meist verbreiteten Dienst, Google Analytics, fokussiert.[2] Bezug nehmend auf den Beschluss oder bereits im Vorfeld haben die Datenschutzaufsichtbehörden von Schleswig-Holstein[3] und Baden-Württemberg[4] angekündigt, Prüfungen durchzuführen bzw. im Kontakt mit Google eine Lösung herbeizuführen. Weitere Aufsichtsbehörden informieren lediglich mehr oder weniger ausführlich über die Rechtswidrigkeit speziell von Google Analytics, ohne konkrete Maßnahmen anzukündigen.[5]

Grundsätzlich betreffen die durch das Webtracking aufgeworfenen Fragen alle Anbieter. Faktisch besteht jedoch zwischen kleineren Anbietern und Google vor allem für die Anhänger eines relativen Personenbezugs ein großer Unterschied: Da Google selbst gegenüber einer Vielzahl von Nutzern als Dienstanbieter auftritt, gegenüber dem sich die Nutzer, etwa im Rahmen von Google-Mail auch identifizieren, verfügt Google auch ohne auf Dritte angewiesen zu sein, über reale Zuordnungsmöglichkeiten hinsichtlich der gebildeten Nutzungsprofile. Ein Teil des Problems mit Google Analytics ergibt sich daher aus der Dienstevielfalt Googles. Als kostenloses Tool eines bekannten Unternehmens hat Google Analytics außerdem einen hohen Verbreitungsgrad.[6] Ein Tracking über einzelne Websitegrenzen hinweg wäre im Fall von Google äußerst ergiebig. Die Fokussierung auf Google ist also jenseits der aktuell verbreiteten allgemeinen Skepsis gegenüber Google als „Datenkrake" durchaus berechtigt.

2 Auswirkungen

Seitens der Webtracking-Nutzer sind bislang wenige Reaktionen erkennbar geworden. Es ist, soweit bekannt, nicht zu einem Einbruch der Google Analytics Nutzung gekommen. Google bietet inzwischen allerdings sowohl eine Ergänzung des Dienstes, die für eine Kürzung der IP-Adressen unmittelbar nach der Übertragung sorgen soll,[7] als auch eine Widerspruchslösung an,[8] auf die die Nutzer auf ihren Seiten verweisen können. Es ist jedoch den Nutzern von Google Analytics selbst überlassen, diese Ergänzungen zu implementieren: Der Dienst wird nicht automatisch mit der Einstellung zum Kürzen der IP-Adressen angeboten, und die Bereitstellung erfolgt auch nicht an prominenter Stelle auf den Google-Seiten.[9] In seinen Nutzungsbedingungen hält sich Google weiterhin die Nutzung der

1 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009 in Stralsund, Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten, abrufbar unter http://www.lfd.m-v.de/dschutz/beschlue/Analyse.pdf

2 Zu Google Analytics siehe auch Hansen, DuD 8/2008, S. 506, sowie ausführlicher Steidle/Pordesch, DuD 5/2008, S. 324-329 und Lepperhoff/Petersdorf, DuD 4/2008, S. 266-269.

3 https://www.datenschutzzentrum.de/tracking/

4 http://www.innenministerium.baden-wuerttemberg.de/fm7/1227/Hinweisblatt%20Web-Analyseprogramme.pdf

5 Bspw. der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, abrufbar unter http://www.datenschutz.rlp.de/downloads/oh/Hinweise_Google_Analytics.pdf

6 Lepperhoff/Petersdorf, s. Fn. 2: der Marktanteil von Google Analytics wurde 2007 auf mehr als 87 % geschätzt, die Nutzung von Trackingdiensten auf 8 %.

7 Der Code ist abrufbar unter http://code.google.com/intl/de-DE/apis/analytics/docs/gaJS/gaJSApi_gat.html

8 Browser Add-on abrufbar unter http://tools.google.com/dlpage/gaoptout?hl=de

9 Unter http://www.google.de/intl/de_ALL/analytics/index.html, der deutschsprachigen Angebotsseite zu Google Analytics, sucht man vergeblich nach Hinweisen auf Rechtsrisiken und die angebotenen Lösungen.

Daten für undefinierte weitere Zwecke offen, beteuert jedoch, keine Zusammenführung von Daten zur Identifizierung der Betroffenen vorzunehmen.[10]

Zahlreiche Konkurrenzprodukte zu Google Analytics haben früher reagiert, sich um eine datenschutzkonforme Gestaltung bemüht und bewerben diese aktiv. Das ULD Schleswig-Holstein hat einem Anbieter bereits 2007 und 2009 ein Datenschutz-Gütesiegel verliehen. Im Gegensatz zu Google wird hier allerdings durch die Verwendung eines „Anonymizers" einer unabhängigen dritten Partei ein deutlich höherer Aufwand zum Zweck der Datensparsamkeit getrieben.[11]

Auch hier konzentrieren sich die Anstrengungen allerdings weitgehend auf die IP-Adresse. Die Identifikatoren der verwendeten Cookies werden ebenso ausgeblendet wie die Möglichkeit der Nutzerbestimmbarkeit durch weitere akkumulierte Profilinhalte. So lässt sich ein bestimmter Browser vielfach auch durch die individuellen Parameter seiner Konfiguration identifizieren,[12] wenn nur genügend Parameter gesammelt werden. Auch dies kann zu einer Zusammenführung von Daten und letztlich zur Herstellung eines Personenbezugs genutzt werden.

3 Würdigung der geforderten Maßnahmen

Zum technischen Ablauf des Webtrackings finden sich inzwischen eine Reihe ausführlicher Darstellungen,[13] so dass hier eine kurze Beschreibung am Beispiel von Google genügen soll: Entscheidet sich ein Dienstanbieter für die Verwendung von Google Analytics, bindet er einen bestimmten Code in den Html-Text der Seiten seiner Website ein. Dieser veranlasst den Browser eines Seitenbesuchers, Script-Code direkt von Google zu beziehen, auszuführen und mehrere Cookies von Google zu setzen. Die Daten über das Nutzerverhalten und die weiteren abgefragten Daten zu z. B. Systemeinstellungen werden so von Google direkt erhoben. Über den gesetzten Cookie werden die verschiedenen Nutzerhandlungen miteinander verknüpft. Dies kann auf eine bestimmte Website beschränkt geschehen; es wäre Google aber auch möglich, über die Identifikationsnummer des Cookies das Verhalten der Seitenbesucher auf sämtlichen Google Analytics einsetzenden Websites zu verknüpfen.

Die datenschutzrechtlichen Risiken des Webtrackings liegen damit auf der Hand. Die Nutzungsprofile zur Werbung, Marktforschung oder Websiteoptimierung können mit den Nutzer identifizierenden Daten zusammengeführt oder personenbeziehbar werden, ohne dass der Seitenbesucher ahnt, dass und in welchem Ausmaß Daten über sein Verhalten gesammelt worden sind.

§ 13 Abs. 1 und 5 sowie § 15 Abs. 3 TMG tragen diesen Risiken Rechnung, indem sie u.a. die Unterrichtung des Seitenbesuchers vorschreiben und das Erstellen von Nutzungsprofilen nur pseudonym oder mit Einwilligung gestatten. Es stellt sich die Frage, ob die vorhandenen Regelungen und die von den Aufsichtsbehörden geforderten Maßnahmen angesichts der Risiken ausreichen, aber auch, ob die geforderten Maßnahmen geeignet sind.

3.1 Gestaltung als Auftragsdatenverarbeitung

Der Düsseldorfer Kreis geht davon aus, dass die Bildung von Nutzungsprofilen durch Webtracking-Dienstanbieter nur in Form einer Auftragsdatenverarbeitung statthaft ist, sofern die Nutzungsprofilbildung und die Datenerhebung nicht anonymisiert erfolgt.

Um diese Annahme zu überprüfen sind zunächst die Verantwortlichkeiten und Verpflichtungen der Beteiligten zu betrachten. Der Website-Anbieter bindet Code des Webtracking-Dienstanbieters in seine Website ein und veranlasst hierdurch eine dem Seitenbesucher nicht bewusste Weiterleitung, das Setzen von Cookies und eine Datenerhebung des Webtracking-Dienstanbieters. Der Website-Anbieter erhebt weder selbst noch übermittelt er Daten an den Webtracking-Dienst. Hierdurch hätte er zunächst den Seitenbesucher nur nach § 13 Abs. 1 S. 2 TMG über das Setzen des Cookies zu unterrichten und die Weitervermittlung nach § 13 Abs. 5 TMG anzuzeigen. Außerdem müsste er, was nur schwer zu realisieren wäre, nach § 13 Abs. 4 Nr. 3 TMG dem Seitenbesucher ermöglichen, die Seite auch geschützt vor einer Kenntnisnahme Dritter in Anspruch zu nehmen, also die Website frei von der unbemerkten Datenerhebung Dritter zu nutzen.

Der Webtracking-Dienstanbieter wäre aus eigenem Recht nach § 15 Abs. 1 TMG nur zum Erheben der ihn betreffenden, den Abruf ermöglichenden Nutzungsdaten berechtigt.[14] Für eine Erhebung weiterer Daten fehlt die nach § 12 Abs. 1 TMG erforderliche gesetzliche Erlaubnis. Im Rahmen der Dienstleistung für den Website-Anbieter kommt es aber gerade auf das Erstellen von Nutzungsprofilen für dessen Website an. Daher muss in der Tat das Erheben des Webtracking-Anbieters in Form einer Auftragsdatenverarbeitung legitimiert werden. In diesem Fall entfällt die Hinweispflicht auf eine Weitervermittlung mangels eines Dritten; es sind jedoch die Pflichten aus § 15 Abs. 3 TMG in Bezug auf die Unterrichtung und die Widerspruchsmöglichkeit hinsichtlich der eigenen Erstellung von Nutzungsprofilen zu erfüllen.

Der Auffassung der baden-württembergischen Aufsichtsbehörde, die eine automatische Begründung einer Auftragsdatenverarbeitung durch die Veranlassung der Datenverarbeitung sieht,[15] kann dagegen nicht gefolgt werden. Eine Auftragsdatenverarbeitung nach § 11 Abs. 1 BDSG liegt nur dann vor, wenn der Betreiber des Webtracking-Dienstes nach Weisung des Auftraggebers handelt und lediglich die technische Ausführung einer Aufgabe für den Auftraggeber übernimmt. Eine Auftragsdatenverarbeitung liegt dagegen nicht vor, wenn der Anbieter des Webtracking-Dienstes vorwiegend im eigenen Interesse handelt. Zudem kann eine Auftragsdatenverarbeitung nur durch einen schriftlichen Vertrag begründet werden.[16]

Im Fall von Google Analytics ist nicht ersichtlich, dass dem Auftraggeber tatsächlich ein Weisungsrecht hinsichtlich der Datenerhebung eingeräumt wird. Es handelt sich auch nicht bloß um ein von Google bereit gestelltes Werkzeug, dass der Website-Anbieter durch seine Einstellungen kontrollieren kann. Der Web-

10 Nutzungsbedingungen, Stand 22.9.2010, abrufbar unter http://www.google.de/intl/de_ALL/analytics/tos.html.

11 Das zugehörige Kurzgutachten findet sich unter https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g070909/070909-kurzgutachten-ptn.html.

12 S. hierzu anschaulich unter https://panopticlick.eff.org.

13 S. bspw. die ausführlichen Erklärungen bei Ott, K&R 2009, S. 308 (309); Steidle/Pordesch, s. Fn. 2, S. 325.

14 Das wäre selbst bei aus dem Ausland agierenden Diensten der Fall, wenn sie in Deutschland erheben, Schaar, Datenschutz im Internet, 2002, S. 81 ff.

15 Hinweise des Innenministeriums Baden-Württemberg, s. Fn. 4.

16 Gola/Schomerus, Bundesdatenschutzgesetz, 10. Aufl. 2010, § 11 Rn. 17.

site-Anbieter kann lediglich konfigurieren, welche Informationen er aus der von Google vorgenommenen Auswertung in welcher Form erhalten möchte.

Die Auftragserteilung erfolgt zudem nicht schriftlich. Die Nichterfüllung der weiteren Anforderungen des § 11 Abs. 2 BDSG stellt dagegen lediglich eine von beiden Seiten begangene Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 2b BDSG dar und schließt nicht das Vorliegen der Auftragsdatenverarbeitung aus. Mit den derzeitigen AGB zu Google Analytics werden allerdings die Anforderungen aus § 11 Abs. 2 Nr. 3, 4, 5, 7, 8, 9 und 10 BDSG nicht erfüllt, so dass selbst bei Zustandekommen einer Auftragsdatenverarbeitung eine Ordnungswidrigkeit vorliegen würde.

Im Fall von Google Analytics liegt aus oben genannten Gründen keine Auftragsdatenverarbeitung vor. Stattdessen handelt es sich um eine Datenerhebung, für die kein gesetzlicher Erlaubnistatbestand besteht. Damit erfüllt Google als Webtracking-Dienstanbieter den Bußgeldtatbestand aus § 16 Abs. 2 Nr. 4 TMG; der Website-Anbieter wird durch die Tatbestände der § 16 Abs. 2 Nr. 2 und 3 TMG erfasst. Die nach Landesrecht zuständige Aufsichtsbehörde (§ 36 Abs. 1 Nr. 2 a), Abs. 2 OWiG) kann damit von Amts wegen Geldbußen von bis zu 50.000 Euro verhängen.

3.2 Außereuropäischer Tracking-Dienstanbieter

Ein weiteres grundsätzliches Problem ist eine Datenverarbeitung durch den Webtracking-Dienstleister im außereuropäischen Ausland. Wie dargestellt ist das Erstellen von Nutzungsprofilen durch Anbieter von Tracking-Diensten nur im Rahmen einer Auftragsdatenverarbeitung möglich, da der Anbieter in diesem Fall kein „Dritter" i. S. des § 3 Abs. 8 BDSG ist und durch die für den Auftraggeber geltenden Erlaubnisse mit erfasst wird. Verarbeitet der Anbieter die Daten aber außerhalb des Europäischen Wirtschaftsraum oder der Europäischen Union, ist eine Auftragsdatenverarbeitung nicht möglich[17] und der Anbieter des Webtrackings wird zum Dritten.

Die Datenverarbeitung von Google Analytics erfolgt laut den Geschäftsbedingungen von Google derzeit in den USA. Ohne Einwilligung des Seitenbesuchers oder vollständige Anonymisierung lässt sich dies nicht mit dem deutschen Datenschutzrecht vereinbaren. Der Verweis der Aufsichtsbehörden auf die Einhaltung der Anforderungen der Auftragsdatenverarbeitung erfasst damit lediglich einen Teil des Problems.

3.3 Kürzung der IP-Adressen

Die Forderung der Aufsichtsbehörden nach einer Kürzung der IP-Adressen steht und fällt mit deren Bewertung als personenbeziehbare, aber nicht pseudonyme Daten. Diese Kategorisierung wird weithin vertreten.[18] Dem ist auch zuzustimmen. Denn der Inhaber auch einer dynamischen IP-Adresse lässt sich zum einen über den Provider, zum anderen aber auch anhand von Registrierungsvorgängen oder durch sonstiges Zusatzwissen bestimmen.

Zwar wird die Bestimmbarkeit des Anschlussinhabers durch Zusatzwissen mit geringem Aufwand regelmäßig nur einen verhältnismäßig kleinen Anteil der Adressen betreffen; für die Bewertung der Datenkategorie als Ganzer ist dieser Anteil jedoch entscheidend, da die Personenbeziehbarkeit für die verarbeitende Stelle zum Zeitpunkt der Erhebung meistens noch nicht erkennbar ist.

Die Einordnung als Pseudonym würde voraussetzen, dass die IP-Adresse als Kennzeichen zum Ersatz eines Identifizierungsmerkmals eingesetzt würde, um einen Personenbezug zu erschweren (§ 3 Abs. 6a BDSG), was nicht der Fall ist.

Da eine Einwilligungslösung für das Webtracking faktisch ausscheidet, ist das Kürzen der IP-Adressen eine erforderliche Mindestmaßnahme. Soweit die Kürzung so erfolgt, dass ein Rückbezug zur vollständigen Adresse nicht mehr möglich ist, führt die Kürzung sogar zu einer Anonymisierung (§ 3 Abs. 6 BDSG).

Bei der Erhebung der Daten durch den Webtracking-Dienst liegt diese Anonymisierung allerdings regelmäßig noch nicht vor, so dass sich die mit dem Webtracking verbundenen Datenschutzprobleme nicht in Wohlgefallen auflösen. Eine frühere Anonymisierung stößt auf technische Grenzen. Die Erfassung der Daten beim Webtracking erfolgt bei und nach dem Herunterladen von Script-Code oder Web-Bugs vom Server des Webtracking-Dienstes. Dieses Herunterladen wird beim Aufruf der getrackten Internetseiten veranlasst. Bei dem Abruf muss noch die vollständige IP-Adresse vorliegen, da sonst der Versand nicht möglich wäre. Die Pseudonymisierung oder Anonymisierung kann also nur durch den Webtracking-Anbieter oder durch einen von diesem zwischengeschalteten Dienst realisiert werden. Somit bleiben die Informationspflichten und das Widerspruchsrecht anwendbar.

Die Fokussierung auf die IP-Adresse als Identifikator darf aber nicht den Blick darauf verstellen, dass Anknüpfungspunkt für § 15 Abs. 3 TMG die Personenbeziehbarkeit bzw. pseudonyme Erstellung des gesamten Nutzerprofils ist.[19] Für die Verknüpfung der einzelnen Handlungen der Website-Besucher und der erhobenen Daten sind als Identifikatoren die regelmäßig gesetzten sitzungsübergreifenden Cookies wesentlich entscheidender. Durch Zusatzwissen sind Cookies wie IP-Adressen personenbeziehbar.[20]

3.4 Cookies

Auch bei den verwendeten Cookies wird in Gestalt einer individuellen Nummer ein potentielles Identifikationsmerkmal gesetzt. Ob in der Identifikationsnummer selbst bereits ein Pseudonym gesehen werden kann,[21] erscheint zweifelhaft, da diese keine zur Identifikation geeigneten Daten ersetzt sondern im Gegenteil ein neues identifizierungstaugliches Datum schafft. Sieht man jedoch in der Identifikationsnummer ein personenbeziehbares Datum, wären genauso wie bei der IP-Adresse weitere Schritte zur Pseudonymisierung oder Anonymisierung des Nutzungsprofils zu unternehmen, um § 15 Abs. 3 TMG zu genügen. Da die Identifikationsnummer im Gegensatz zur IP-Adresse zur Zusammenführung der einzelnen Seitenabrufe und Sitzungen verwendet wird, liegt hierin ein weitaus gravierenderes Problem.

Bezieht man weiter in die Betrachtung ein, dass auch eine Kombination der über den Browser gesammelten Einstellungsdaten unter Umständen dessen Identifizierung ermöglicht, ist das Problem der Personenbeziehbarkeit der Nutzungsprofile nur noch durch eine strikte Reduzierung und Beschränkung der Profilinhalte

17 Gola/Schomerus, s. Fn. 16, § 11 Rn. 16.

18 Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 v. 20.6.2007, Beispiel 15; Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 22. Tätigkeitsbericht 2007/2008, S. 96; Mit einer aktuellen Übersicht über den Meinungsstand Sachs, CR 2010, S. 547, zum relativen und objektiven Personenbezug Pahlen-Brandt, DuD 1/2008, S. 34 ff..

19 Schleiper, RDV 2010, S. 168 (169).

20 Schaar, Datenschutz im Internet, 2002, Rn. 177 ff.; a.A. Härting, CR 2008, S. 743 (744).

21 So Steidle/Pordesch, s. Fn. 2, S. 327.

zu lösen. Die Forderung nach der Kürzung der IP-Adresse kratzt also lediglich an der Oberfläche dieses Problems und vermag für sich allein nicht die Rechtskonformität zu gewährleisten.

3.5 Umsetzung der Widerspruchsmöglichkeit

§ 15 Abs. 3 TMG, um dessen Einhaltung es dem Düsseldorfer Kreis geht, fordert zudem das Bereitstellen einer Widerspruchsmöglichkeit, sofern der Dienstanbieter pseudonyme Nutzungsprofile erstellt. Da bei der durch den Betreiber des Webangebots veranlassten Datenerhebung des Webtracking-Dienstes noch keine Anonymisierung der Daten erfolgt, bleiben das Widerspruchsrecht und die Hinweispflicht bestehen. Zudem stellt das Setzen eines Cookies ein automatisiertes Verfahren dar, das eine spätere Identifizierung des Nutzers ermöglicht, und führt daher nach § 13 Abs. 1 Satz 2 TMG zu einer Unterrichtungspflicht. Als Auftraggeber ist der Website-Anbieter hier der Verpflichtete.

Nach Meinung zumindest einer Aufsichtsbehörde hat die Umsetzung des Widerspruchrechts serverseitig zu erfolgen.[22] Damit würden die branchenübliche Cookie-Lösung und auch Googles Browser-Add-on-Lösung als Umsetzung ausscheiden. In der Tat spricht hierfür, dass der Widerspruch eigentlich eine Erklärung darstellt, dass künftig keine Daten von dem Webseiten-Besucher mehr erhoben werden dürfen. Die angebotenen Lösungen gewährleisten dies zwar zunächst, sie können aber jederzeit unbemerkt faktisch unwirksam werden, z. B. wenn der Nutzer hin und wieder seinen Speicher bereinigt und Cookies umfassend löscht oder den verwendeten Browser wechselt. Hinsichtlich Googles Browserlösung tritt hinzu, dass diese nicht bei allen gängigen Browsern funktioniert. § 15 Abs. 3 TMG verlangt jedoch nicht ausdrücklich, dass der Widerspruch Session übergreifend wirken muss. Allerdings ist zu fordern, dass bei der Unterrichtung über das Widerspruchsrecht auf die beschränkte Wirksamkeit des Widerspruchs hingewiesen wird. Erfolgen entsprechende ergänzende Hinweise, spricht nichts gegen die Umsetzung des Widerspruchs durch das Setzen eines Cookies.

Der Ausschluss von Nutzern des „falschen" Browsers von der Wahrnehmung des Widerspruchsrechts führt jedoch zu einem Verstoß gegen die Verpflichtung aus § 15 Abs. 3 TMG.

3.6 Weitere Anforderungen

Die übrigen Forderungen aus dem Entschluss des Düsseldorfer Kreises und aus § 15 Abs. 3 TMG sind unkritischer für die Tracking-Nutzer und -Anbieter. Dennoch gehört beispielsweise das Löschungsgebot der Nutzungsdaten nach Entfallen der Erforderlichkeit zur Nutzungsanalyse oder nach Widerspruch des Nutzers zu den im Fall von Google nicht nachvollziehbar umgesetzten Anforderungen. Auch daran, dass die verschiedenen Tracking-Dienste sich bei den erhobenen Daten wirklich auf Daten beschränken, die zur Inanspruchnahme oder Abrechnung des angebotenen Telemediendienstes erforderlich sind, darf gezweifelt werden.

4 Ausblick

Die Aufsichtsbehörden haben in verschiedenen Stellungnahmen angekündigt, vor allem mit Google an der Lösung der rechtlichen Probleme arbeiten zu wollen. Angesichts dessen, dass die derzeit angebotene Browser bezogene Widerspruchslösung bereits vom Ansatz her nicht ausreicht, die Datenverarbeitung außerhalb Europas mit geltendem Recht nicht vereinbar ist und die Pseudonymität oder Anonymität der Nutzungsprofile mit den derzeit angewandten Erhebungsmethoden nicht gewährleistet werden kann, erscheint Skepsis hinsichtlich der Erfolgsaussichten dieses Vorhabens angezeigt.

Mangels wirksamer Auftragsdatenverarbeitung und Einwilligung erhebt Google derzeit eine große Menge personenbeziehbarer Daten ohne Rechtsgrundlage. Die getroffenen Maßnahmen bezüglich der Widerspruchsmöglichkeit und des einzufügenden Codes, der die Verkürzung der IP-Adresse anweist, ändern hieran nichts. Ihrer eigenen Einschätzung folgend werden die Aufsichtsbehörden hier einschreiten müssen, sollte keine einvernehmliche Lösung gefunden werden. Dabei bleibt ebenfalls abzuwarten, ob sie sich an Google Analytics selbst oder an dessen Nutzer halten werden. Allerdings ist auch die Selbsteinschätzung zahlreicher anderer Webtracking-Anbieter zur Datenschutzkonformität kritisch zu hinterfragen.

Die Nutzung eines Webtracking-Dienstes ist jedenfalls bei den gängigen Anbietern leicht mittels eines frei verfügbaren Browserzusatzprogramms[23] oder einer Webanwendung[24] festzustellen, so dass das Prüfverfahren den Aufsichtsbehörden keinen großen Aufwand bereiten sollte.

5 Fazit und Handlungsempfehlung

Das Thema Webtracking wird für Unternehmen, Datenschützer und Anbieter noch lange aktuell bleiben und hat mindestens die gleiche Aufmerksamkeit wie der Umgang mit Geoinformationen verdient, die derzeit in aller Munde sind.

Unbestreitbar besteht ein legitimer Bedarf, Statistiken über die Telemediennutzung zu deren Optimierung zu erstellen. Die Auslagerung an Dritte liegt dabei auf der Hand. Angesichts der Risiken, die sich bei der zentralisierten Bildung von Nutzungsprofilen durch Drittanbieter ergeben, ist jedoch eventuell der Augenmerk mehr auf eine Beschränkung der Zusammenführung und des Umfangs von Profilen sowie eine wirkungsvolle Anonymisierung der Profile als Ganzem zu legen.

Die Gestaltung als Auftragsdatenverarbeitung ist angesichts der beschränkten Möglichkeiten einer wirksamen Kontrolle der Webtracking-Dienste und der Beschränkung auf europäische Anbieter keine günstige Lösung.

Den Nutzern von Webtracking-Diensten kann derzeit nur geraten werden, ihren tatsächlichen Bedarf an einer solchen Analyse kritisch zu prüfen. Sollte ein Verzicht oder eine Beschränkung nicht in Frage kommen, sollten sie ihre Verträge mit den Webtracking-Anbietern, ihre datenschutzrechtlichen Hinweise gegenüber ihren Seitenbesuchern mit Bezug auf die Datenerhebung und das Widerspruchsrecht sorgfältig gestalten sowie die von dem Webtracking-Dienst eingesetzte Methode zur Pseudonymisierung oder Anonymisierung der Nutzungsprofile gründlich prüfen.

Bezüglich Google Analytics ist die Erfüllung der rechtlichen Anforderungen vorerst nicht in Sicht, so dass mit der Nutzung das Risiko von Bußgeldern bis zur Höhe von 50.000 € aus § 16 Abs. 2 Nr. 2 und 3 TMG verbunden ist.

22 So auch der Landesbeauftragte Rheinland-Pfalz, s. Fn. 4, S. 1.

23 S. bspw. unter http://www.ghostery.com;

24 S. bespw. unter http://www.ontraxx.net.