Martin Günther

»Webtracking ja - aber...

Derzeit ist bei Websitebetreibern viel Unruhe zu verspüren, was die datenschutzrechtliche Konformität eingesetzter Trackinglösungen angeht. Was ist bei der Verwendung solcher Dienste aus dieser speziellen Rechtsperspektive zu beachten? Für Website Boosting sprach Martin Günther mit den Bundesdatenschutzbeauftragten Peter Schaar.

Was empfehlen Sie Webseitenbetreibern, die Webtrackinglösungen einsetzen?

Peter Schaar: Ohne ausdrückliche Einwilligung der Nutzer dürfen Profile nur unter Pseudonym oder in anonymer Form geführt werden. Allerdings müssen die Nutzer auch dann über die Verwendung der Daten informiert werden. Darüber hinaus haben sie ein Recht auf Auskunft über die unter Pseudonym gespeicherten Daten und können der Registrierung ihrer Daten widersprechen. Websitebetreiber, die eine solche Reichweitenmessung durchführen, müssen deshalb gewährleisten, dass die Nutzer diese Rechte wirksam wahrnehmen können. Vielfach erfolgt die Analyse des Nutzerverhaltens unter Verwendung der vollständigen IP-Adresse, vorrangig um den Nutzer geographisch lokalisieren zu können. Dies ist aus datenschutzrechtlicher Sicht fragwürdig, denn die vollständige IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes, weil sie sich – insbesondere über die Zugangsprovider – in vielen Fällen einzelnen Nutzern zuordnen lässt. Deshalb haben die deutschen Datenschutzbehörden im sogenannten Düsseldorfer Kreis einen Beschluss zur datenschutzkonformen Ausgestaltung von Analyseverfahren veröffentlicht, in dem beispielsweise die Kürzung der IP-Adresse gefordert wird. Eigentlich ist es ja zur Reichweitenmessung gar nicht erforderlich, dass die gesamte IP-Adresse übermittelt wird. Es würde beispielsweise ausreichen, wenn ein Browser-Plugin die Auswertung der Geo-Lokalisierung der Nutzer übernimmt und die Daten in anonymisierter Form, indem z. B. das letzte Oktett der IP-Adresse weggestrichen wird, übermittelt.

Dazu müsste der betroffene Nutzer aber wissen, dass es ein solches Plugin gibt.

Die zentrale Frage ist zunächst, ob der Nutzer überhaupt ein Wahlrecht hat, und die nächste ist die Frage nach der Standardeinstellung von Browsern und sonstiger Software. Bei einem Dienst, der ausschließlich zur Reichweitenmessung und nicht zur individuellen Profilbildung des Nutzers verwendet wird, würde ich es akzeptieren, wenn hier nicht eine Einwilligung, sondern ein Opt-out* realisiert wird, allerdings unter der Voraussetzung, dass weder die IP-Adresse noch längerfristige Cookies verwendet werden. Geht es dagegen um die Profile, d. h. um die Registrierung, welche Interessen ein Nutzer hat und welche Webseiten er wann und von welchen Endgeräten aus besucht hat, ist ein Opt-in* – also eine informierte Einwilligung – erforderlich. Derjenige, der diese Daten erfassen und nutzen will, muss den Nutzer darüber informieren, was mit seinen Daten passieren soll, und er muss sich um seine Einwilligung bemühen.

Wie müsste eine solche informierte Einwilligung aussehen? Reicht dazu ein Hinweis in

* siehe Glossar Seite 96-98

den Datenschutzbestimmungen, zum Beispiel über den Einsatz von Google Analytics, aus? Oder muss der Nutzer die Speicherung aktiv bestätigen, beispielsweise über ein Pop-up-Fenster oder Ähnliches?

Der entscheidende Punkt ist, welche Daten an den Anbieter des Webanalysedienstes übermittelt werden und was er mit diesen Daten macht. Je weitreichender diese Nutzungsmöglichkeiten sind, desto stärker müssen auch die Kontrollmöglichkeiten für den Betroffenen sein. Ich will nicht speziell auf Google Analytics eingehen, weil es eine ganze Reihe anderer Anbieter gibt. Nach meiner Auffassung sind intelligente Lösungen gefragt, die eine Reichweitenmessung ermöglichen, ohne dabei das persönliche Nutzerverhalten – sei es direkt oder indirekt – zu registrieren.

Noch eine abschließende Frage zu Ihrer Keynote auf der SMX. Ist es richtig, dass Sie – bezogen auf den Datenschutz – in Cookies eine größere Gefahr sehen als bei der Speicherung von IP-Adressen?

Solange wir IP-Adressen dynamisch vergeben, sind diese weniger aussagekräftig als andere Identifikatoren, die permanent auf einem Gerät gespeichert sind, wie beispielsweise Cookies, Flash-Cookies und andere vergleichbare Mechanismen. Diese ermöglichen erst die Speicherung des Nutzerverhaltens über mehrere Sitzungen bzw. Nutzungsvorgänge hinweg und machen es dem Anbieter erst möglich, sie gegebenenfalls zusammenzuführen. Es sind aber nicht alle Cookies gleich zu behandeln. Session-Cookies, die nach Beendigung eines Nutzungsvorgangs gelöscht werden, sind datenschutzrechtlich weitestgehend unproblematisch. Längerfristig gespeicherte Cookies in Kombination mit IP-Adressen bilden jedoch den Schlüssel zur Zusammenführung völlig unterschiedlicher Informationen über den Betroffenen. Dadurch wird Dritten ermöglicht, ungeheuer viele Informationen zusammenzuführen und Nutzungs- oder sogar Persönlichkeitsprofile der Betroffenen zu erlangen – womöglich ohne deren Wissen. Bei der Personalisierung eines Dienstes, z. B. über die Anmeldung bei einem E-Mail-Dienst, können diese zunächst unter der Cookie-ID geführten Informationen sogar nachträglich auf einen namentlich bekannten Nutzer zurückgeführt werden.

Herr Schaar, wir danken Ihnen für dieses Gespräch!¶