

Standpunkt

Spuren im Netz: Google Analytics und das „Computer-Grundrecht“. Die Datenschutzbeauftragten der Bundesländer (Düsseldorfer Kreis) haben einen Beschluss zu Google Analytics gefasst. Der Beschluss vom 26./27. 11. 2009 trägt den sperrigen Titel „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ (www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf). Auch wenn Google in dem Beschluss nicht ausdrücklich erwähnt wird: Es geht um Webtracking. Google Analytics ist dort der überragende Marktführer.

Google Analytics ermöglicht einem Websitebetreiber die Analyse der Besucher der Website durch statistisch aufbereitete Auswertungsergebnisse. Durch Google Analytics lässt sich erfassen, wie Besucher auf die Website gekommen sind, welche Seiten sie aufrufen, an welcher Stelle sie die Website verlassen und wie lange sie sich auf der Website aufhalten. Darüber hinaus gibt Google Analytics darüber Aufschluss, aus welchen Ländern und Regionen die Besucher stammen. Google Analytics ermöglicht damit dem Betreiber einer Website, die Besucher und deren Gewohnheiten kennenzulernen und sich auf diese Gewohnheiten einzustellen.

Google Analytics nutzt die Spuren, die ein Internetnutzer im Netz hinterlässt. Diese Spuren bestehen im Wesentlichen aus Cookies und IP-Adressen und rufen immer wieder den Datenschutz auf den Plan (vgl. *Gabriel/Cornels*, MMR 2008, XIV; *Ott*, K&R 2009, 308; *Steidle/Pordesch*, DuD 2008, 324). Einerseits ist eine Auswertung des Nutzerverhaltens geradezu unerlässlich zur Verbesserung von Internetangeboten – beispielsweise für eine automatische Wahl der Muttersprache des Nutzers. Auch ermöglicht das Tracking eine zielgerechte Lieferung von Informationen und Werbung, abgestimmt auf die Bedürfnisse und Gewohnheiten des Nutzers. Andererseits entsteht eine Big Brother-Situation. Auf Google-Servern werden zahlreiche Daten gespeichert, ohne dass der Nutzer einen genauen Überblick über die gespeicherten Daten und deren Verwendung hat. Dies mag nicht so sehr stören, wenn es um Daten geht aus einer Suchabfrage zum nächsten Urlaubsziel. Anders jedoch bei dem diskreten Besuch von Chat-Foren oder dem Abruf erotischer Internetangebote.

Im Mittelpunkt der datenschutzrechtlichen Diskussion steht die Frage, ob und inwieweit Cookies und IP-Adressen personenbezogene Daten darstellen (vgl. *Härtling*, CR 2008, 743). Die Diskussion ist weitgehend festgefahren. Bei den IP-Adressen stehen sich zwei Lager gegenüber und verweisen auf die beiden einzigen Gerichtsentscheidungen, die es zu dieser Frage gibt: Das *AG Berlin-Mitte* hat die Personenbezogenheit von IP-Adressen bejaht (ZUM 2008, 83); das *AG München* hat die gegenteilige Auffassung vertreten (MMR 2008, 860).

Bei der Diskussion um die Personenbezogenheit geht es im Wesentlichen darum, ob die Gefahr besteht, dass anfallende Datenspuren einem Nutzer zugeordnet werden, der

Google namentlich bekannt ist. Wie groß diese Gefahr ist, ist letztlich eine Glaubensfrage. Wer an das Gute im Menschen glaubt, hält es für sehr fernliegend, dass man sich bei Google die Mühe macht, aus Milliarden Daten herauszufiltern, welche konkreten, namentlich bekannten Personen welche Internetseiten genutzt haben. Wer dagegen ein eher skeptisches Menschenbild hat, glaubt, dass aus theoretischen Möglichkeiten praktische Taten werden. In das Weltbild vieler Skeptiker passt es zudem, dass das „Datenmonster“ auch noch ausgerechnet im fernen Amerika beheimatet ist.

Das Datenschutzrecht in seiner heutigen Form ist in den 70er und 80er Jahren des vergangenen Jahrhunderts entstanden. Damals wurde die elektronische Datenverarbeitung zum Alltag. Spätestens seit dem Volkszählungsurteil des *BVerfG* (NJW 1984, 419) war klar, dass der Bürger davor geschützt werden muss, durch den Staat (und durch Unternehmen) bespitzelt zu werden. Der bespitzelte Bürger war dabei kein anonymes Wesen, sondern Staat und Wirtschaft namentlich bekannt – daher die „Personenbezogenheit“ als zentraler Anknüpfungspunkt der geschützten Daten. Es war die Zeit der Notstandsgesetze und Befehlsverbote, der RAF und Rasterfahndung, der Friedensdemonstrationen und Bürgerinitiativen. Staat und Wirtschaft sollten nicht unkontrolliert Daten der Bürger sammeln. Dies maßgeblich, um den Bürger vor Maßnahmen und Sanktionen wegen „abweichender“ Ansichten, Aktivitäten oder Eigenschaften zu bewahren (*Härtling*, CR 2008, 743 [746]).

Bei Google Analytics geht es um ganz andere Befürchtungen: Am Webtracking beunruhigt nicht die Vorstellung, dass sich ein Mitarbeiter von Google bei einem Nutzer per E-Mail meldet und ihn mit peinlichen Einzelheiten aus den letzten Internetsitzungen konfrontiert. Nicht die Sorge vor der Deanonymisierung ist es, die ein ungutes Gefühl bereitet, sondern der heimliche Blick durch das virtuelle Schlüsselloch. Wie beim Blick durch das Schlüsselloch liegt das Unbehagen nicht darin, dass der Eindringling weiß, wer ich bin. Der Internetnutzer nimmt es vielmehr als freiheitsbeschränkend wahr, dass er sich – anonym – beobachtet fühlt, ohne genau abschätzen zu können, mit welcher Genauigkeit die Beobachtung erfolgt. Bei der Diskussion um Cookies und IP-Adressen geht es letztlich darum, dass ein „potenziell äußerst großer und aussagekräftiger Datenbestand“ entsteht, der den tiefen Einblick in die Persönlichkeit ermöglicht, aus dem das *BVerfG* in seiner Entscheidung zur Online-Durchsuchung das „Computer-Grundrecht“ abgeleitet hat (NJW 2008, 822). Google Analytics ruft das „Computer-Grundrecht“ auf den Plan und nicht die informationelle Selbstbestimmung.

Um das „Computer-Grundrecht“ mit Leben zu erfüllen, bedarf es klarer rechtlicher Regelungen zu der Frage, wie der Nutzer über die Sammlung von Spuren im Netz zu informieren ist. Nur bei einer hinreichenden Information hat der Nutzer die Möglichkeit, frei und autonom zu entscheiden, ob er Dienste nutzt, bei denen ein Webtracking erfolgt. Mit § 15 III TMG gibt es für Nutzerprofile bislang nur eine

Rumpfnorm, die einer Anpassung an die heutigen Internet-Verhältnisse bedarf.

Statt zu diskutieren, ob das *AG Berlin-Mitte* oder das *AG München* bei der Auslegung des Begriffs der Personenbezogenheit gem. § 3 I BDSG recht hat, bedarf es einer rechtspolitischen Diskussion über die Umsetzung der Anforderungen des *BVerfG* an das „Computer-Grundrecht“. Der Gesetzgeber ist gefragt.

Rechtsanwalt Niko Härting, Berlin

Standpunkt

Spuren im Netz: Google Analytics und das „Computer-Grundrecht“. Die Datenschutzbeauftragten der Bundesländer (Düsseldorfer Kreis) haben einen Beschluss zu Google Analytics gefasst. Der Beschluss vom 26./27. 11. 2009 trägt den sperrigen Titel „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ (www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf). Auch wenn Google in dem Beschluss nicht ausdrücklich erwähnt wird: Es geht um Webtracking. Google Analytics ist dort der überragende Marktführer.

Google Analytics ermöglicht einem Websitebetreiber die Analyse der Besucher der Website durch statistisch aufbereitete Auswertungsergebnisse. Durch Google Analytics lässt sich erfassen, wie Besucher auf die Website gekommen sind, welche Seiten sie aufrufen, an welcher Stelle sie die Website verlassen und wie lange sie sich auf der Website aufhalten. Darüber hinaus gibt Google Analytics darüber Aufschluss, aus welchen Ländern und Regionen die Besucher stammen. Google Analytics ermöglicht damit dem Betreiber einer Website, die Besucher und deren Gewohnheiten kennenzulernen und sich auf diese Gewohnheiten einzustellen.

Google Analytics nutzt die Spuren, die ein Internetnutzer im Netz hinterlässt. Diese Spuren bestehen im Wesentlichen aus Cookies und IP-Adressen und rufen immer wieder den Datenschutz auf den Plan (vgl. *Gabriel/Cornels*, MMR 2008, XIV; *Ott*, K&R 2009, 308; *Steidle/Pordesch*, DuD 2008, 324). Einerseits ist eine Auswertung des Nutzerverhaltens geradezu unerlässlich zur Verbesserung von Internetangeboten – beispielsweise für eine automatische Wahl der Muttersprache des Nutzers. Auch ermöglicht das Tracking eine zielgerechte Lieferung von Informationen und Werbung, abgestimmt auf die Bedürfnisse und Gewohnheiten des Nutzers. Andererseits entsteht eine Big Brother-Situation. Auf Google-Servern werden zahlreiche Daten gespeichert, ohne dass der Nutzer einen genauen Überblick über die gespeicherten Daten und deren Verwendung hat. Dies mag nicht so sehr stören, wenn es um Daten geht aus einer Suchabfrage zum nächsten Urlaubsziel. Anders jedoch bei dem diskreten Besuch von Chat-Foren oder dem Abruf erotischer Internetangebote.

Im Mittelpunkt der datenschutzrechtlichen Diskussion steht die Frage, ob und inwieweit Cookies und IP-Adressen personenbezogene Daten darstellen (vgl. *Härtling*, CR 2008, 743). Die Diskussion ist weitgehend festgefahren. Bei den IP-Adressen stehen sich zwei Lager gegenüber und verweisen auf die beiden einzigen Gerichtsentscheidungen, die es zu dieser Frage gibt: Das *AG Berlin-Mitte* hat die Personenbezogenheit von IP-Adressen bejaht (ZUM 2008, 83); das *AG München* hat die gegenteilige Auffassung vertreten (MMR 2008, 860).

Bei der Diskussion um die Personenbezogenheit geht es im Wesentlichen darum, ob die Gefahr besteht, dass anfallende Datenspuren einem Nutzer zugeordnet werden, der

Google namentlich bekannt ist. Wie groß diese Gefahr ist, ist letztlich eine Glaubensfrage. Wer an das Gute im Menschen glaubt, hält es für sehr fernliegend, dass man sich bei Google die Mühe macht, aus Milliarden Daten herauszufiltern, welche konkreten, namentlich bekannten Personen welche Internetseiten genutzt haben. Wer dagegen ein eher skeptisches Menschenbild hat, glaubt, dass aus theoretischen Möglichkeiten praktische Taten werden. In das Weltbild vieler Skeptiker passt es zudem, dass das „Datenmonster“ auch noch ausgerechnet im fernen Amerika beheimatet ist.

Das Datenschutzrecht in seiner heutigen Form ist in den 70er und 80er Jahren des vergangenen Jahrhunderts entstanden. Damals wurde die elektronische Datenverarbeitung zum Alltag. Spätestens seit dem Volkszählungsurteil des *BVerfG* (NJW 1984, 419) war klar, dass der Bürger davor geschützt werden muss, durch den Staat (und durch Unternehmen) bespitzelt zu werden. Der bespitzelte Bürger war dabei kein anonymes Wesen, sondern Staat und Wirtschaft namentlich bekannt – daher die „Personenbezogenheit“ als zentraler Anknüpfungspunkt der geschützten Daten. Es war die Zeit der Notstandsgesetze und Berufsverbote, der RAF und Rasterfahndung, der Friedensdemonstrationen und Bürgerinitiativen. Staat und Wirtschaft sollten nicht unkontrolliert Daten der Bürger sammeln. Dies maßgeblich, um den Bürger vor Maßnahmen und Sanktionen wegen „abweichender“ Ansichten, Aktivitäten oder Eigenschaften zu bewahren (*Härtling*, CR 2008, 743 [746]).

Bei Google Analytics geht es um ganz andere Befürchtungen: Am Webtracking beunruhigt nicht die Vorstellung, dass sich ein Mitarbeiter von Google bei einem Nutzer per E-Mail meldet und ihn mit peinlichen Einzelheiten aus den letzten Internetsitzungen konfrontiert. Nicht die Sorge vor der Deanonymisierung ist es, die ein ungutes Gefühl bereitet, sondern der heimliche Blick durch das virtuelle Schlüsselloch. Wie beim Blick durch das Schlüsselloch liegt das Unbehagen nicht darin, dass der Eindringling weiß, wer ich bin. Der Internetnutzer nimmt es vielmehr als freiheitsbeschränkend wahr, dass er sich – anonym – beobachtet fühlt, ohne genau abschätzen zu können, mit welcher Genauigkeit die Beobachtung erfolgt. Bei der Diskussion um Cookies und IP-Adressen geht es letztlich darum, dass ein „potenziell äußerst großer und aussagekräftiger Datenbestand“ entsteht, der den tiefen Einblick in die Persönlichkeit ermöglicht, aus dem das *BVerfG* in seiner Entscheidung zur Online-Durchsuchung das „Computer-Grundrecht“ abgeleitet hat (NJW 2008, 822). Google Analytics ruft das „Computer-Grundrecht“ auf den Plan und nicht die informationelle Selbstbestimmung.

Um das „Computer-Grundrecht“ mit Leben zu erfüllen, bedarf es klarer rechtlicher Regelungen zu der Frage, wie der Nutzer über die Sammlung von Spuren im Netz zu informieren ist. Nur bei einer hinreichenden Information hat der Nutzer die Möglichkeit, frei und autonom zu entscheiden, ob er Dienste nutzt, bei denen ein Webtracking erfolgt. Mit § 15 III TMG gibt es für Nutzerprofile bislang nur eine

Rumpfnorm, die einer Anpassung an die heutigen Internet-Verhältnisse bedarf.

Statt zu diskutieren, ob das *AG Berlin-Mitte* oder das *AG München* bei der Auslegung des Begriffs der Personenbezogenheit gem. § 3 I BDSG recht hat, bedarf es einer rechtspolitischen Diskussion über die Umsetzung der Anforderungen des *BVerfG* an das „Computer-Grundrecht“. Der Gesetzgeber ist gefragt.

Rechtsanwalt Niko Härting, Berlin