Handbuch Internet-Suchmaschinen
D. Lewandowski (Hrsg.)
© 2009, AKA Verlag Heidelberg

Datenschutz bei Suchmaschinen

Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98
24103 Kiel
weichert@datenschutzzentrum.de

Abstract. Dieses Kapitel hinterfragt die persönlichkeitsrechtliche Legitimation der Verarbeitung personenbezogener Daten und der Auswertung von Nutzungsdaten bei Suchmaschinen-Betreibern vor dem Hintergrund der deutschen und europäischen datenschutzrechtlichen Situation. Es analysiert die derzeitigen Zugriffsmöglichkeiten durch Suchmaschinen-Anbieter, insbesondere Google, und stellt sie den in der Verfassung und in den bestehenden Gesetzen festgeschriebenen Rechten gegenüber. Die Frage der Anwendbarkeit deutschen und europäischen Rechts auf den internationalen Wirkungsbereich amerikanischer Suchmaschinen-Betreiber wird aufgeworfen und die rechtliche Verantwortlichkeit von Suchmaschinen-Anbietern gegenüber der ungeschützten Vermittlung personenbezogener Information geprüft. Die Rechte der Betroffenen nach dem Bundesdatenschutzgesetz als Objekte der Suche wie nach dem Telemediengesetz als die Nutzenden werden erörtert ebenso wie die Zulässigkeit der Erschließung von Nutzungsdaten zum Zweck der Marktforschung und zielgerichteten Werbung. Im Ergebnis zeigt sich, dass das Recht auf informationelle Selbstbestimmung derzeit im Suchmaschinen-Kontext nicht hinreichend gewahrt ist. Der Grund wird in unzureichenden und nicht an die Technik angepassten gesetzlichen Regelungen und Vollzugsdefiziten gesehen. Forderungen nach Maßnahmen zum Datenschutz richten sich an Suchmaschinen-Betreiber und Gesetzesgeber.

Keywords. Datenschutz, Suchmaschinen, informationelle Selbstbestimmung

Einleitung

Suchmaschinen erfüllen im World Wide Web eine wichtige Rolle bei der Erschließung von Informationen. Sie sind nützlich und notwendig, um den Nutzenden im unstrukturierten Netz einen möglichst unkomplizierten Zugriff auf eingestellte Inhalte zu ermöglichen. Sie dienen insofern der Freiheit zur Informationsbeschaffung. Zugleich sind sie Plattformen zur Verbreitung von Informationen und Meinungen und in einer globalen Informationsgesellschaft ein wichtiges Instrument zur Verwirklichung der Meinungsäußerungsfreiheit und des freien Austauschs von Informationen und Ansichten.

Zugleich begründen Suchmaschinen, in denen personenbezogene Daten verarbeitet werden, Probleme beim Datenschutz und Konflikte mit dem Grundrecht auf informationelle Selbstbestimmung. Über Internet-Suchmaschinen werden im Web gespeicherte Daten von Personen erschlossen und weitergeleitet, auch wenn diese dort illegal allgemein zugänglich gemacht werden. In vielen Fällen haben die Betroffenen von der Veröffentlichung zu ihrer Person keine Kenntnis. Oft haben sie hierzu ihre Zustimmung nicht erteilt. Oft werden falsche und diffamierende Darstellungen und Bewertungen veröffentlicht. Oft erfolgt eine nicht gerechtfertigte oder zumindest unverhältnismäßige Beeinträchtigung der Persönlichkeitsrechte der Betroffenen durch die Darstellung und Bewertung im Web in Wort, Bild und Ton, die durch die Weiterverbreitung über Suchmaschinen verstärkt wird.

Außerdem sammeln manche Betreiber von Suchmaschinen umfangreiche Angaben über die Nutzenden und deren Suchverhalten im Netz. Gespeichert und ausgewertet werden Daten von Cookies und IP-Adressen, die verwendeten Suchbegriffe, Umstände der Suche und angeklickte Suchergebnisse. Diese Daten werden zusammengeführt zu Nutzerhistorien, zu Profilen über die Persönlichkeit, über Interessen, über Einkaufverhalten, über Online-Aktivitäten. Diese Daten werden u.U. kombiniert mit weiteren persönlichen Angaben und werden teilweise eindeutig den Nutzenden zugeordnet. Die derart gesammelten Daten werden für Werbezwecke genutzt, stehen aber u.U. auch für weitere Zwecke zur Verfügung.

Suchmaschinen sind vorrangig ein technisches Angebot für die Internet-Nutzenden: Sie durchforsten mit Hilfe von speziellen Programmen, sog. Robots oder Crawlern, das World Wide Web und speichern den Text der gefundenen Seiten in einer eigenen Datenbank, dem Index. Wird eine Anfrage an eine Suchmaschine gerichtet, so recherchiert diese in ihrer Datenbank, ob sie das Gesuchte findet. Mit Suchmaschinen hat man keinen Zugriff auf das gesamte Internet. Vielmehr müssen die Webseiten von der Datenbank der Suchmaschine erfasst sein. Da die Suchmaschinenbetreiber unterschiedliche Programme zur Durchforstung des Internet verwenden, landen auch verschiedene Seiten im jeweiligen Index. Gesucht wird regelmäßig nach Worten bzw. Textbestandteilen. Möglich sind aber auch Suchen nach Bildern, Videos und Tondokumenten sowie Kombinationen hiervon. Gegenstand der Suchvorgänge können das gesamte öffentlich zugängliche Internet sein, Teile hiervon oder spezifische, über das Web erreichbare Datenbestände.

Suchmaschinen gewinnen voraussichtlich noch stark an Bedeutung. In Deutschland hat sich das Internet innerhalb von 11 Jahren als dritte Säule des Medienkonsums etabliert, indem die Nutzendenzahl von 6,5% auf 62,7% anstieg. 2007 wurde als wichtigster Grund für die Internetnutzung von 91% die Suche nach Informationen genannt, vor der Suche nach Spaß und Unterhaltung mit 72%. Hinsichtlich der verwendeten Anwendungen stehen die E-Mail-Funktion und Suchmaschinen im Vordergrund der Internetnutzung. 76% nutzen wöchentlich Suchmaschinen. Dabei nimmt die zielgerichtete Suche zu. Angesichts der zunehmenden Informationsmasse im Internet gewinnt die professionelle technische Hilfe von Suchmaschinen eine immer wichtigere Bedeutung. Was eine segensreiche Hilfe ist, wird zugleich zum Datenschutzproblem (der vorliegende Beitrag baut auf einem Aufsatz des Autors auf: [1]).

1. Google

In Deutschland wird bei der Internetsuche zu ca. 90 % das Angebot des US-Unternehmens Google genutzt. Dessen Datenschutzpraxis steht im Fokus der Kritik von Datenschützern. Dies gilt insbesondere wegen der Intransparenz der Datenverarbeitung und der übermäßigen Speicherung von personenbezogenen Nutzungsdaten. Google speichert Suchanfragen 18 Monate lang mit folgenden Angaben: IP-Adresse, von dem die Suche durchgeführt wird, die Google-Domain (.com, .de, .at), über welche die Suche gestartet wurde, Tag und Uhrzeit der Suchabfrage, der eingetippte Suchbegriff (bzw. die Suchzeile), Informationen über den Browser (z.B. Explorer, Firefox, Safari) sowie die ID-Nummer des Cookies, über die Google erkennen kann, ob und wie schon einmal der Dienst genutzt wurde. Am 16.07.2007 verkündete der Datenschutzbeauftragte von Google, Peter Fleischer, dass die bisherige Lebensdauer von Google-Cookies (zuvor bis 2038) auf jeweils zwei Jahre beschränkt wird. Die 18- bzw. 24-Monate-Frist dürfte keine tatsächliche Einschränkung für die Datenspeicherung von Google darstellen. Wer vor deren Ablauf erneut seinen Rechner mit einem Google-Dienst nutzt, lässt die Frist wieder von Neuem beginnen. Google registriert weiterhin den ungefähren Standort des Rechners [2]. Entgegen der Bewertung der Datenschutzbehörden in Europa sind nach Ansicht von Google IP-Adressen keine personenbezogenen Daten (s.u. 6.).

Google bietet neben der Nutzung der Suchmaschinenfunktion weitere Dienste an, bei denen die Eingabe einer Benutzerkennung und eines zuvor vergebenen Passworts nötig ist. Hierüber ist dem Unternehmen eine eindeutige Identifikation des Nutzers möglich (sog. Sign-In-Services), z.B. über das E-Mail-Programm. So kann eine namentliche Zuordnung von Suchen erfolgen. Über den Dienst Google Web History [3], für den ein Account bei Google nötig ist, kann ein Nutzer nachschauen, welche Webseiten er an welchem Tag und zu welcher Uhrzeit gesucht und gefunden hat. Das Unternehmen speichert aber nicht nur diese Daten. Das Unternehmen kann detailliertere Profile zu jeder Person erstellen und verwenden. Nutzt jemand erst später einen Sign-In-Service, so kann Google auch nachträglich die über eine Identifikationsnummer erfolgte pseudonyme Datenverarbeitung der konkret bekannt werdenden Person zuordnen. Erfasst wird wohl auch die Browser-History, also welche Seiten ein Nutzer vor der Suche besucht hat und welche Lesezeichen er gesetzt hat.

Zweifellos sind schon die Profile der Suchmaschinennutzung von hoher Aussagekraft. Diese wird jedoch individuell weit übertroffen durch weitere unentgeltliche Dienstleistungen, mit denen Google den Nutzenden hilft, ihr IT-Leben zu organisieren, und in dem Textverarbeitung, Bildbearbeitung und Präsentationsprogramme ebenso enthalten sind wie z.B. ein Virenschutz. Zur Anmeldung bei Gmail bzw. Google Mail müssen Angaben über Name, Wohnort, Alter und einiges mehr gemacht werden – dies sind Daten, die mit den elektronisch schon vorhandenen Daten aus IP-Adressen und Cookies kombiniert werden können. Der Inhalt von erhaltenen wie geschriebenen Gmails wird von Google automatisch analysiert und durch Werbung ergänzt. Die besondere Attraktivität von Gmail für die Nutzenden besteht in der Unentgeltlichkeit sowie in dem großen Speicherplatz, der den Nutzenden über die Online-Festplatte GDrive zur Verfügung gestellt wird. Bei der Nutzung von Google Maps lassen sich Bewegungsprofile ableiten. Über Google Web

History wird der gesamte Browserverlauf abgespeichert und lässt sich später anzeigen, einschließlich der aufgerufenen Webseiten, Bilder, Videos und News. Wer News Alert aktiviert hat, verrät, für welche Nachrichten er sich interessiert. Die Google-Desktop-Suche macht den Nutzer für Google zu einem offenen Buch. Die von Google gespeicherten Daten werden mit Hilfe von Data-Mining-Instrumenten analysiert, ausgewertet und dann v.a. für Werbezwecke genutzt [4].

Die personenbeziehbaren und -bezogenen Nutzungsprofile sind die Grundlage für das Schalten von Werbung in Web-Angeboten. Dies ist die zentrale Einnahmequelle des Unternehmens. Das Wissen über die Nutzer ist somit das wichtigste Kapital des Unternehmens und zugleich die Basis für weitere Entwicklungen und Projekte.

Im Jahr 2007 hat Google den Online-Vermarkter DoubleClick übernommen. DoubleClick hat bei der Internet-Werbung eine marktdominierende Stellung und nutzt praktisch seit Beginn der Internet-Ära Cookies zur Registrierung des Nutzungsverhaltens. Auch DoubleClick speichert Angaben über den genutzten Browser, die IP-Adresse und die Art der Domain. Ein Jahr vor der Übernahme durch Google hatte DoubleClick das Marktforschungsinstitut Abacus Alliance erworben, das über eine umfassende Datenbank mit individualisierten Offline-Informationen über Konsumenten verfügt. Die Übernahme von DoubleClick wurde am 20.12.2007 nach US-Recht von der Federal Trade Commission und am 11.03.2008 nach europäischem Kartellrecht von der Europäischen Kommission genehmigt. Im Rahmen des europäischen Prüfverfahrens musste Google im Januar 2008 garantieren, dass die Datenbanken von Google und DoubleClick nicht verknüpft werden. Außerdem wurde das Unternehmen aufgefordert Informationen vorzulegen, was mit den Nutzungsdaten geschieht [5].

Wie viele Suchanfragen pro Tag getätigt und gespeichert werden, wird von Google als Betriebsgeheimnis behandelt. In der Literatur werden 200 Mio. Suchanfragen täglich genannt. Technisch möglich sein sollen mehr als eine Millionen Anfragen pro Sekunde, was 3,6 Mrd. Anfragen pro Stunde entspräche. Wo diese Anfragen bearbeitet werden, ist auch eines der vielen Geheimnisse des Unternehmens. Es ist ein Netzwerk von Zehntausenden Computern und Servern, auf denen die Daten von ca. 50 % der ca. 1,3 Mrd. Internet-Nutzenden weltweit gespeichert sind und die quer über alle Kontinente verstreut sind. Es wird geschätzt, dass es 7 bis 25 Serverfarmen gibt mit 100.000 bis 450.000 Servern. Das Computernetzwerk von Google dürfte das größte und leistungsfähigste der Welt sein, das unter einer einheitlichen Verfügungsmacht steht. Wichtige Netzknoten liegen in Council Bluff in Iowa; im Bundesstaat Oregon wird derzeit eine weitere Serverfarm errichtet. In Europa gibt es ein Datenzentrum in Holland; ein weiteres soll in Saint-Ghislain in Belgien erbaut werden, ebenso eines im Distrikt Kaisiadoriu in Litauen. Von weiteren Projekten in Taiwan, China und einem Megaprojekt mit einer Kostenhöhe von 750 Mio. Euro in der Zone Andhra Pradesh in Indien ist die Rede.

Gemäß eigenen Angaben speichert Google Daten 18 Monate lang in der Web History oder bei Google Groups: "Gemäß unseren Richtlinien löschen wir eine Nachricht, wenn dies vom ursprünglichen Autor beantragt wird." Dies soll aber bei Diskussionen von Google Groups erst möglich sein, wenn dies von allen Autoren verlangt wird. Jedenfalls kann ein in der Hilfe-Funktion zu findendes "Entfernungstool" genutzt werden.

Die Daten können nicht nur von Google selbst genutzt werden. Ein nicht unerhebliches Risiko besteht auch darin, dass die bei Google gespeicherten Daten auf Forderung oder unter Druck an Regierungsbehörden herausgegeben werden müssen. An derartigen Kooperationen, selbst mit Diktaturen wie China, kommen Firmen wie Google offensichtlich nicht vorbei. Durch die bisher bekannten journalistischen oder sonstigen Recherchen war nicht herauszubekommen, wie viele Anfragen Google von Polizei- und Sicherheitsbehörden in der ganzen Welt erhalten und beantwortet hat.

Die britische Bürgerrechtsorganisation Privacy International (PI) stellte im Sommer 2007 dem Unternehmen die Bewertung "datenschutzfeindlich" aus. Von keinem der 23 untersuchten großen Unternehmen gehe, so PI-Chef Simon Davies, "eine vergleichbare Bedrohung der persönlichen Daten aus wie von Google". Berücksichtigt wurden dabei nicht nur technische Bewertungen und Analysen, sondern auch die Angaben, die die betroffenen Unternehmen selbst übermittelt hatten. Google fiel deshalb unangenehm auf, weil es die mit seinem Suchdienst gesammelten Nutzerdaten mit solchen aus anderen Diensten (z.B. Gmail, Google Maps) verknüpfen kann. Davies: "Die Nutzer haben weder die Möglichkeit, ihre von Google gesammelten Daten einzusehen, noch können sie die Daten löschen lassen." Es habe sich bei genauer Betrachtung herausgestellt, dass Google "viel mehr mit unseren Daten anstellt, als wir jemals für möglich gehalten haben". Auf den PI-Bericht erläuterten Google-Anwälte, die gesammelten Daten dienten dazu, die Nutzer besser zu verstehen und die Google-Dienste verbessern zu können [6].

2. Datenschutz - Recht auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht (BVerfG) hat in einer frühen Entscheidung im Jahr 1969 festgestellt, dass die Erstellung von teilweise oder weitgehend vollständigen Persönlichkeitsbildern aus vorhandenen Daten nicht mit der Menschenwürde vereinbar sei [7]. Dies gilt insbesondere, wenn der Betroffene nicht “dessen Richtigkeit und Vollständigkeit zureichend kontrollieren kann”. Das BVerfG hat das Recht auf Selbstbestimmung nicht nur im Hinblick auf das für eine Person mögliche Gesamtabbild festgeschrieben. Mit der Volkszählungsentscheidung wurde dieses Recht grundsätzlich in Bezug auf jedes zur eigenen Person bestehende Datum begründet und als umfassendes Recht auf informationelle Selbstbestimmung definiert [8]. Diese Rechtsprechung hat das oberste deutsche Gericht auch beibehalten, als sich die Möglichkeiten der informationellen Fremdbestimmung über das Internet erwiesen. Ja es hat gerade im Hinblick auf die damit entstehenden Risiken die Relevanz des Grundrechtsschutzes und des Datenschutzrechtes bekräftigt. Erst jüngst stellte das BVerfG angesichts der technischen Kontrollmöglichkeiten die Bedeutung des Verbots einer Rundumüberwachung dar [9]. In Weiterentwicklung des allgemeinen Persönlichkeitsrechts hat das BVerfG Februar 2008 ein Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme abgeleitet [10]. Diese Antwort auf die modernen Herausforderungen der Informationstechnik bezieht sich insbesondere auf Systeme, die wie global arbeitende Internet-Suchmaschinen schon durch ihre Funktionsweise eine allgemeine Gefährdung für den Datenschutz vieler Menschen begründen.

Mit diesem Grundrechtsschutz geht Deutschland keinen nationalen Sonderweg. Vielmehr findet die Rechtsprechung des BVerfG ihre Bestätigung durch die des Europäischen Gerichtshofes für Menschenrechte und des Europäischen Gerichtshofes. Die Fundierung dieser Rechtsprechung erfolgt über Art. 8 der Europäischen Menschenrechtskonvention, der die Achtung des Privatlebens gewährleistet, sowie über die Europäische Datenschutzkonvention aus dem Jahr 1981. In der Europäischen Grundrechtecharta wird in Art. 8 ausdrücklich der Schutz personenbezogener Daten zugesichert [11]. Damit ist Europa zwar Vorreiter für die internationale Rechtsentwicklung; doch auch in der OECD wie durch die UNO werden Bestrebungen zur weltweiten Anerkennung des Datenschutzes verfolgt.

Zur Konkretisierung des verfassungsrechtlich geforderten Grundrechtsschutzes hat der deutsche Gesetzgeber eine Vielzahl von Datenschutzgesetzen erlassen. Im Hinblick auf die Verarbeitung durch Suchmaschinen sind v.a. das Bundesdatenschutzgesetz (BDSG) und das Telemediengesetz (TMG) anwendbar. Auf europäischer Ebene ist die Europäische Datenschutzrichtlinie (EU-DSRL) anwendbar sowie eine spezielle Richtlinie für die Telekommunikation (EU-TK-DSRL, wird derzeit als ePrivacy-Directive novelliert). Bisher gab es zum Datenschutz bei Suchmaschinen wenig Rechtsprechung, juristische-wissenschaftliche Literatur und Prüferfahrungen der Datenschutzaufsichtsbehörden. Dieses Defizit wurde durch eine Stellungnahme der Art. 29-Arbeitsgruppe der europäischen Datenschutzbeauftragten zumindest teilweise behoben [12]. Doch weiterhin ist in Bezug auf den Datenschutz bei Suchmaschinen vieles ungeklärt.

Als rechtlicher Gegenpol zu den Begrenzungen durch den Datenschutz sind die in Art. 5 GG gewährleisteten Informations- und Meinungsfreiheiten als zentrale Grundlagen einer freiheitlichen und demokratischen Informationsgesellschaft zu berücksichtigen. Art. 11 der Europäischen Grundrechtecharta bekräftigt, dass Informationen überwachungsfrei zugänglich sein sollen.

Es gibt im Grunde zwei große Datenschutzkomplexe bei Suchmaschinen; bei dem einen ist der Mensch das Suchobjekt, beim anderen das suchende Subjekt. Das eine Mal erfolgt die Beeinträchtigung informationeller Selbstbestimmung durch die systematische Zusammenstellung der im Internet auch abseitig gespeicherten und verfügbaren Informationen. Dieses Thema wird v.a. durch das BDSG behandelt. Das andere Mal beeinträchtigt die Analyse des Such- und Surfverhaltens der Nutzenden durch die Suchmaschinenbetreiber deren Möglichkeit selbst festzulegen, “wer was wann und bei welcher Gelegenheit über sie weiß”. Die informationelle Ausbeutung des Nutzungsverhaltens ist Gegenstand des Telekommunikationsrechtes (TKG, TMG).

3. Anwendbarkeit des deutschen und des europäischen Rechtes

Viele großen Suchmaschinenanbieter haben ihren Hauptgeschäftssitz in den USA; deren wesentlichen Datenverarbeitungsvorgänge lassen sich oft nicht lokalisieren, erfolgen jedenfalls in großem Umfang außerhalb der Europäischen Union (EU) bzw. des europäischen Wirtschaftsraumes (EWR). Die Unternehmen versuchen teilweise, sich der deutschen bzw. generell der europäischen Kontrolle mit dem Argument zu

entziehen, für sie gelte das europäische Datenschutzrecht nicht. Die Anwendbarkeit des nationalen Rechtes knüpft gemäß § 1 Abs. 5 BDSG am Ort der Datenverarbeitung an. Tatsächlich wird die Ansicht vertreten, dass es für die Anwendung des BDSG auf den Serverstandort ankommt, da der Anbieter keine Vorstellung davon habe, wer von seinem Angebot Gebrauch machen wird. Es fehle ihm insoweit an einem konkretisierten Erhebungswillen. Der Nutzende gehe in freier Entscheidung darauf ein, seine Daten auf dem Server im Ausland verarbeiten zu lassen.

Richtig ist aber, dass für die Anwendbarkeit des Datenschutzrechtes bei Internet-Suchmaschinen der Ort der Datenverarbeitung maßgeblich ist; dies ist bei Suchmaschinen u.a. der Standort des Clients. Über den Clientstandort erfolgt die wesentliche Verarbeitung, insbesondere die Datenerhebung; auf diesem ist der Cookie des Betreibers gespeichert. Träfe es zu, dass ausschließlich der Serverstandort für die Frage der Anwendbarkeit des jeweiligen nationalen Rechts ausschlaggebend wäre, so könnte sich ein Betreiber einfach dadurch dem deutschen Recht entziehen, dass er seinen Server in einem anderen Land aufstellt. Mit dieser Bewertung werden den Betreibern keine übermäßigen rechtlichen Bürden auferlegt. Wo die Rechner des Anbieters stehen, ist den Nutzenden i.d.R. überhaupt nicht bewusst bzw. bekannt.

Sämtliche großen Internet-Suchmaschinen-Anbieter haben Tochterunternehmen oder Filialen in Deutschland. Sie zielen auf den deutschen Markt, etwa indem sie ein deutschsprachiges Angebot bereithalten oder unter deutscher Länderkennung auftreten. Die Anbieter verfolgen gezielt die Erhebung der Nutzerdaten; diese werden ihnen nicht aufgedrängt. Die großen Suchmaschinen sind unter Domains mit deutscher Länderkennung „.de“ zu erreichen. Google leitet Anfragen, die unter ihrer www.google.com-Adresse von einem Client mit einer deutschen IP-Adresse eingehen, auf die .de-Adresse weiter. Als Option wird die Suche auf deutschsprachigen Seiten angeboten. Es war nicht Intention der europäischen Datenschutzrichtlinie, bei einer Verarbeitung personenbezogener Daten auch im Drittland außerhalb der EU ausschließlich das dortige Rechtsregime für gültig zu erklären. Bei den großen US-Suchmaschinen ist also (auch) deutsches bzw. europäisches Datenschutzrecht anzuwenden (Art. 4 Abs. 1 EU-DSRL).

Für die Anwendbarkeit des Telemediengesetzes (TMG) wird nach § 3 Abs. 1 TMG auf das Herkunftslandprinzip abgestellt. Dies bedeutet, dass Anknüpfungspunkt die Niederlassung des Diensteanbieters in der Bundesrepublik Deutschland ist, wenn der Dienst von einem Anbieter in der Europäischen Union erfolgt. Doch bzgl. spezieller rechtlicher Fragen, u.a. auch des Verbraucherschutzes werden gem. § 3 Abs. 5 TMG Ausnahmen vom Herkunftslandsprinzip zugunsten des Territorialitätsprinzips gemacht. Bei Anbietern von außerhalb der EU gelten die allgemeinen Regelungen. Dies bedeutet: Nutzt ein deutscher Internet-Nutzer eine der großen amerikanischen Suchmaschinen, so ist er nicht auf den Rechtsschutz in den USA angewiesen; vielmehr gilt regelmäßig deutsches Recht, das vor deutschen Gerichten geltend gemacht werden kann.

Die Anwendbarkeitsregeln beim Datenschutz dürfen nicht dazu führen, dass überhaupt kein Schutz gewährt wird. Zugleich soll innerhalb der EU ein möglichst einheitliches Regime gelten. Dennoch lässt sich u.U. nicht vermeiden, dass wegen des transnationalen Charakters der Verarbeitung mehrere nationale Datenschutzregelungen anwendbar sind, insbesondere, wenn Unternehmenssitz und Orte der Datenverarbeitung auch außerhalb des EWR liegen.

4. Personen als Suchobjekt

Suchmaschinen als Fahndungsinstrument für Jedermann und Jedefrau kann für die Objekte der Suchbegierde schlimme existenzielle Konsequenzen haben. Die vom stalkenden Ex-Ehemann verfolgte Frau kann sich nicht vor ihrem Bedränger schützen, wenn im Internet Hinweise auf den aktuellen Aufenthalt zu finden sind. Stellenbewerbende können schnell ein Problem bekommen, wenn der potenzielle Arbeitgeber Negatives aus dem Netz zieht. Versicherungsunternehmen munitionieren sich inzwischen im Netz gegen Leistungsforderungen. Ja selbst Sozialbehörden oder die Polizei bedienen sich der über Suchmaschinen erschlossenen Informationen, um Kriminalität oder Hilfemissbrauch aufzuklären. Dabei ist die Gefahr des Irrtums und der gezielten Täuschung groß, etwa wenn böswillige Personen falsche Fakten, diskreditierende Bilder oder Beleidigungen und Verleumdungen ins Netz stellen. Die Suchmaschinen differenzieren nicht zwischen wahr und falsch, zwischen rechtmäßig und illegal.

Wer Informationen über sich im Klartext in einer Webseite, während eines Chats oder in einer Social Community ins Netz stellt, muss wissen, was er tut. Er erteilt seine Einwilligung nach §§ 4 Abs. 1, 4a BDSG, dass diese Informationen über Suchmaschinen erschlossen werden und in völlig anderen Zusammenhängen genutzt werden können. Die Funktionsweise von Suchmaschinen muss inzwischen jedem Internetnutzenden in groben Zügen bekannt sein. Wer sich selbst im Netz entblößt, mag die sich ergebenden Konsequenzen nicht bedacht haben; den eingesetzten Suchmaschinen kann jedenfalls deshalb kein Vorwurf gemacht werden.

Die meisten Informationen über Menschen im Netz stammen aber nicht von den Betroffenen selbst, sondern von Dritten. Eine Einwilligung in die elektronische Veröffentlichung wird regelmäßig nicht erteilt. In diesen Fällen muss die Veröffentlichung und die Datensuche nach den gesetzlichen Verarbeitungsregeln des BDSG bewertet werden. Dabei ist wenig förderlich, dass die relevanten Regelungen im BDSG aus dem Jahr 1990 stammen und im Jahr 2001 nur wenig an die technische Entwicklung angepasst wurden. Auf Suchmaschinen anwendbar ist § 29 BDSG zur "geschäftsmäßigen Datenerhebung und -verarbeitung zum Zweck der Übermittlung".

Zwar speichern Suchmaschinen personenbezogene Daten im Index und halten diese im Cache über eine gewisse Zeit verfügbar, doch liegt deren Ursprung regelmäßig bei anderen verantwortlichen Betreibern von Webseiten. Diese können die Erfassung bei seriöseren Anbietern dadurch ausschließen, dass sie robots.txt eingeben oder einen Merker Noindex/NoArchie setzen. Einen sicheren Ausschluss kann eine solche Markierung nicht bewirken; entsprechende rechtlich ableitbare Verpflichtungen können derzeit praktisch kaum durchgesetzt werden. Wer seine Internetveröffentlichungen nicht derart markiert, der erstreckt damit seine Verantwortlichkeit nicht auf die Erfassung durch Suchmaschinen, deren Funktionsweise und Verarbeitung von ihm als Webseitenbetreiber praktisch nicht beeinflusst werden kann. Die Betreiber der Suchmaschinen selbst sind vielmehr verantwortliche Stelle. Dies gilt erst recht, wenn die Suche personenspezifisch erfolgt, etwa unter Nutzung von Namen, E-Mail-Adressen, Telefonnummern und anderen Identifikatoren, auch wenn die Auswahl und Zusammenführung vollautomatisch erfolgt.

Fraglich ist, wie weit die Verantwortlichkeit der Betreiber für die durch Suchmaschinen erschlossenen Daten geht. Klar ist insofern die Regelung des § 3 Abs. 7 BDSG, wonach die Verantwortlichkeit bei der jeweiligen speichernden Stelle liegt, auch wenn es sich bei dem Datenspeicher um den Cache einer Suchmaschine handelt. Über die Dauer der Speicherung im Cache bestimmt ausschließlich der Betreiber. Diese Klarheit wird getrübt durch die tatsächliche Verantwortlichkeit: Eine umfassendere inhaltliche Kontrolle über die im Zwischenspeicher ausgewerteten Daten kann auch einem noch so finanziell gut dastehenden Betreiber nicht zugemutet werden. Daraus zieht das Telemediengesetz (TMG), zumindest für Fragen der polizeilichen und zivilrechtlichen Haftung die Konsequenz einer reduzierten Verantwortlichkeit: Nicht verantwortlich sind nach § 10 TMG, wenn Diensteanbieter 1. "keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen ... auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder Information offensichtlich wird oder 2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben." Zwar lassen sich diese Regeln nicht vollständig auf die datenschutzrechtliche Verantwortlichkeit übertragen, doch weisen sie die Richtung für die Lösung des Problems.

Einen weiteren Hinweis zur Problemlösung gibt § 29 BDSG, der die geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung regelt. Danach dürfen Daten zur Auskunftserteilung verarbeitet werden, "wenn die Daten allgemein zugänglich sind". Allerdings steht diese Erlaubnis unter dem Vorbehalt, dass nicht "das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung ... offensichtlich überwiegt". Nach dem BDSG muss diese Abwägung grundsätzlich im Einzelfall erfolgen, eine Anforderung, die eine Suchmaschine allenfalls im Nachhinein auf der Basis einer Beschwerde vornehmen kann. Faktisch unmöglich ist es, technisch das Vorliegen "besonderer Arten personenbezogener Daten", also "über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben" festzustellen, was zwangsläufig zu einem Überwiegen der schutzwürdigen Belange, ja gar zum Erfordernis der Einwilligung führt. Selbst eine pauschale Datenschutz-Abwägung wird derzeit von den Suchmaschinenbetreibern nicht vorgenommen. Die Anzeige der Suchergebnisse in einer Reihenfolge, das sog. Ranking, orientiert sich ausschließlich am vermuteten Interesse der Suchenden bzw. an der kommerziellen Relevanz des Treffers, nicht aber am Schutzbedarf einer gesuchten Person. Dies gilt selbst für gerade im Aufkommen befindliche Personensuchmaschinen, bei denen eine weitgehend maschinelle inhaltliche personenbezogene Aufbereitung der Suchergebnisse erfolgt.

Wendet man die aktuelle Gesetzeslage an, so ist das Ergebnis von verblüffender Eindeutigkeit: Suchmaschinen, mit denen nach Personen gesucht werden kann, sind einfachgesetzlich rechtswidrig. Da diese nicht zwischen sonstigen Begriffen und Personenbezeichnungen, insbesondere Namen unterscheiden, wären Suchmaschinen generell illegal. Diese Konsequenz wird praktisch nicht gezogen. Die Macht des technisch Faktischen beugt das geschriebene Recht. Bei der rechtlichen Bewertung muss das Informationsinteresse nach Art. 5 GG von Anbietern wie von Nachfragenden berücksichtigt werden. Die bestehende rechtliche Diskrepanz muss besser früher als

später vom Gesetzgeber behoben werden. Doch darf dies nicht zu einer Kapitulation des Grundrechtsschutzes vor der Faktizität des Internet führen. Daher sollen im Folgenden einige Lösungsmöglichkeiten aufgezeigt werden.

5. Betroffenenrechte

Die Rechtswidrigkeit einer Datenverarbeitung nach den §§ 28, 29 BDSG hängt in starkem Maße davon ab, in welchem Umfang hierüber für die Betroffenen Transparenz geschaffen ist und in welchem Maße diese eine Einflussmöglichkeit auf die Verarbeitung haben durch Widerspruch, Wahloptionen, Gegendarstellung und Datenlöschung. All diese Betroffenenrechte finden im BDSG sowie im bereichsspezifischen Datenschutzrecht ihre Grundlagen, wenngleich bisher keine dieser Rechte die Besonderheiten des Internet hinreichend berücksichtigt.

Grundlegend für die Sicherung des Datenschutzes durch die Betroffenen selbst, die sog. „Magna Charta", ist der Auskunftsanspruch nach § 34 BDSG (Art. 12 EU-DSRL). Dieses Recht lässt sich leicht durch die Eingabe des eigenen Namens als Suchbegriff realisieren. So elegant diese Lösung ist, so unzureichend ist sie in mancher Hinsicht. Der grundrechtlich fundierte Auskunftsanspruch besteht aus technischer Sicht bedingungslos, er setzt nicht die Verfügbarkeit eines Computers mit Internetanschluss voraus. Nach § 34 Abs. 3 BDSG wird die Auskunft „schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist". In jedem Fall darf bei technisch nicht versierten Personen der Verweis auf das Internet zu keiner Verletzung des Willkürverbotes führen. Der Anspruch auf Auskunft über Herkunft der Daten wird durch die Angabe des Ursprungslinks realisiert, während eine Präzisierung der Angaben zu den Kategorien der Empfänger (potenziell alle) und der Zwecke (zweckfreie Bereitstellung) für den Betroffenen praktisch nicht möglich ist.

Umso wichtiger wäre die Benachrichtigung der Betroffenen (§ 33 BDSG, Art. 11 EU-DSRL), die aber faktisch zumeist nicht durchführbar ist. Zwar sind die zum Zweck der Übermittlung gespeicherten Daten „aus allgemein zugänglichen Quellen entnommen" und wäre „eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig" (§ 33 Abs. 2 Nr. 8a BDSG). Doch ist nur dann die Benachrichtigung rechtlich ausgeschlossen, wenn die Betroffenen selbst „diese Daten veröffentlicht haben". Dies ist bei Daten im Internet oft nicht der Fall. Die Möglichkeit der anderweitigen Kenntnisnahme – eben durch Eigenrecherche – genügt auch nicht zum rechtlichen Ausschluss der Benachrichtigungspflicht. Nach § 33 Abs. 2 Nr. 1 BDSG ist ein Benachrichtigungsverzicht nur bei positiver Kenntniserlangung zulässig.

Notleidend sind auch die weiteren Betroffenenrechte: So sieht § 29 Abs. 4 i.V.m. § 28 Abs. 4 BDSG ein Widerspruchsrecht für Zwecke der Werbung und Markt- und Meinungsforschung vor. Dem mag entgegengehalten werden, dass Internet-Inhaltsdaten typischerweise nicht bzw. nur selten für diese Zwecke genutzt würden. Dieser Einwand ändert nichts daran, dass derartige Nutzungen stattfinden und vom Gesetz nicht erlaubt sind, wenn ein Widerspruch erfolgt. Selbst ein Hinweis auf ein derartiges Nutzungsverbot (vgl. § 29 Abs. 4 i.V.m. § 28 Abs. 5 BDSG) enthalten Suchmaschinen derzeit nicht.

Passen will auch nicht die Regelung des § 29 Abs. 3 BDSG, wonach eine Aufnahme in elektronische Verzeichnisse dann zu unterbleiben hat, „wenn der entgegen stehende Wille des Betroffenen aus dem zugrunde liegenden ... Register ersichtlich ist." Derzeit wird von vielen Suchmaschinen die Markierung einer Webseite mit dem Robots-Metatag oder durch entsprechende Eintragungen in der Datei namens robots.txt beachtet. Diese bezieht sich aber nicht auf ein konkretes personenbezogenes Datum, sondern auf ganze Web-Dokumente. Zudem bedarf es eines Tätigwerdens des Betroffenen gegenüber dem Webseiten-, nicht dem Suchmaschinenbetreiber, um die Suchbarkeit des eigenen Datums auszuschließen.

Über die Anwendung der Verantwortlichkeitsregeln nach dem TMG lässt sich u.U. eine eingeschränkte Rechtspflicht der Suchmaschinenbetreiber gegenüber den Betroffenen legitimieren. Doch auch in diesem Fall besteht zumindest ein Recht zum Widerspruch, mit dem der Betroffene gegenüber diesem eindeutig zum Ausdruck bringt, dass seine überwiegenden schutzwürdigen Interessen der Verarbeitung entgegenstehen; evtl. wird auf die nicht legitimierte Verarbeitung von Daten nach § 3 Abs. 9 BDSG hingewiesen. In diesen Fällen muss der Suchmaschinenbetreiber die beanstandeten Daten umgehend entfernen oder den Zugang zu diesen sperren (§ 10 S. 1 Nr. 2 TMG).

Eine besondere Problematik des Internet allgemein und der Suchmaschinen im Besonderen besteht darin, dass falsche, unrichtig gewordene oder rechtswidrig erhobene Daten auf Grund der Struktur des Internet nur schwer zu korrigieren oder vollständig zu löschen sind (Korrekturansprüche nach § 35 BDSG), da Datensätze im Netz in Caches abgelegt, gespiegelt und gesondert archiviert werden. Werden Daten auf Grund konkreter Ansprüche der Betroffenen im Originaldatenbestand korrigiert, so ist nicht zu gewährleisten, dass auch sämtliche Kopien dieser Daten entsprechend korrigiert werden. Google empfiehlt bei unliebsamen Inhalten, sich an den Seitenbetreiber zu wenden und diesen aufzufordern, Teile seines Angebots für die Google-Suche zu sperren oder Fotos aus der Bildersuche herauszunehmen. Bei Google dauert es nach Firmenangaben ca. 48 Stunden, bis ein Bild nicht mehr zu erreichen ist. Es dauere sechs bis acht Wochen, bis ganz Webseiten nicht mehr erreichbar gemacht werden können, weil sie dazu aus dem Cache gelöscht werden müssen. Die Wahrnehmung der Widerspruchsrechte, die bei Suchmaschinen teilweise nur elektronisch möglich ist, setzt zudem eine komplizierte und oft nicht bekannte Prozedur voraus mit Anmelden, Passwortvergabe und E-Mail-Kommunikation.

Angesichts der technisch und organisatorisch bedingten faktischen Schwierigkeiten der Wahrnehmung der Datenkorrekturansprüche nach § 35 BDSG im Internet gewinnt ein aus dem Presserecht entlehntes Betroffenenrecht gegenüber den Suchmaschinenbetreibern eine zentrale Bedeutung: das Recht auf Gegendarstellung. Lässt sich schon nicht verhindern, dass unzulässige oder falsche Inhalte verbreitet sind, so muss zumindest die Möglichkeit für die Betroffenen gegeben sein, diese richtigzustellen. Dieses Recht richtet sich nicht nur gegen den Erstveröffentlicher, d.h. den u.U. rechtlich nicht greifbaren Verantwortlichen der Webseite, sondern auch den Zweitveröffentlicher und Verbreiter „Suchmaschine".

Die Wahrnehmung der Betroffenenrechte ist wegen der im Internet allgegenwärtigen Homonyme, d.h. der identischen Namen für verschiedene Personen, erschwert. Für die Inanspruchnahme der Rechte bedarf es der zuverlässigen Authentifizierung, d.h. der Identifizierung als Rechteinhaber. Für diese Authentifizierung im Internet werden derzeit technische Lösungen entwickelt, die den

Betroffenen ein Identitätsmanagement und die Wahrnehmung ihrer Datenschutzrechte ermöglichen [13].

6. Nutzungsdaten

Das zweite große Feld des Datenschutzes bei Suchmaschinen wird eröffnet durch die Verarbeitung der Nutzungsdaten der suchenden Personen. Die ökonomische Verwertung der Nutzungsdaten v.a. für Werbezwecke ist die zentrale Triebkraft für das Angebot von Suchmaschinen. Damit kollidiert das Geschäftsmodell mit dem Grundsatz der Datensparsamkeit nach § 3a BDSG. Angesichts der Sensitivität der hinterlassenen Nutzungsdaten hat die 28. Internationale Konferenz der Datenschutzbeauftragten von den Anbietern gefordert, ihre Dienste in einer datenschutzfreundlichen Art und Weise anzubieten. Sie sollten keine Informationen über eine Suche, die Nutzenden von Suchmaschinen zugeordnet werden können, oder über die Nutzenden selbst aufzeichnen. Nach Ende eines Suchvorgangs sollten keine personenbeziehbaren Daten gespeichert bleiben, außer der Nutzende hat seine ausdrückliche informierte Einwilligung dazu gegeben, für die Erbringung weiterer Dienste notwendige Daten speichern zu lassen (z.B. zur Nutzung für spätere Suchläufe). Der Datenminimierung käme eine zentrale Bedeutung zu. Dies käme auch den Anbietern zunutze, da dies die Vorkehrungen bei Forderungen nach der Herausgabe von Nutzungsdaten vereinfachen würde [14]. Diese rechtspolitischen Forderungen müssen nach deutschem Recht zwingend umgesetzt werden.

Teilweise wird behauptet, die bei der Speicherung von Suchanfragen verarbeiteten Daten wären gar nicht personenbezogen, sondern pseudonym, ohne dass eine Identifizierungsmöglichkeit bestünde, diese seien also wie anonyme Daten zu behandeln. Die Art. 29-Gruppe hat in seinem Arbeitspapier 136 inzwischen eindeutig geklärt, dass IP-Adressen und Cookies, die eine personifizierte Zuordnung von Suchen ermöglichen, als personenbezogene Daten zu behandeln sind. Ist, etwa durch die Nutzung von weiteren Sign-In-Service-Diensten, die Zuordnung nicht durch den Betreiber selbst möglich, so kann diese über den Internet-Zugangsdienst erfolgen. Entsprechendes gilt für Cookies. Selbst bei Nutzung von dynamischen IP-Adressen bleibt die Cookie-ID eines Nutzenden gleich. Der Betreiber ist bzgl. der Verarbeitung von Daten auch verantwortliche Stelle: Er hat die Verfügungsmacht über die Daten, bestimmt deren Verarbeitung und die damit verfolgten Zwecke.

Teilweise berufen sich Suchmaschinenbetreiber als Legitimation für die langfristige Speicherung von Nutzungsdaten auf die europäische Richtlinie zur Vorratsdatenspeicherung. Dies zu Unrecht, unabhängig davon, ob diese Richtlinie überhaupt formell und materiell mit europäischen und nationalem Verfassungsrecht vereinbar ist: Suchmaschinen sind keine Telekommunikationsdienste, die den Zugang zu Netzen eröffnen, sondern Telemediendienste, die keiner Aufbewahrungspflicht unterliegen [15]. Angeboten werden nicht Netzzugänge, sondern die Zugänge zu Inhalten bzw. deren Speicherung im Cache und deren Übermittlung.

Betreiber von Suchmaschinen nennen folgende Zwecke der Anfragenspeicherung: Verbesserung des Dienstes, Wahrung der Systemsicherheit, Verhinderung von Betrugsversuchen, Erstellen von Statistiken und die Bereitstellung für Sicherheitsbehörden. Bei Bezahldiensten wird weiterhin die Abrechnung genannt. Die

Personalisierung von Werbung ist die ökonomische Triebfeder für die Speicherung und Auswertung.

Nach § 15 Abs. 1 TMG ist die Verarbeitung personenbezogener Nutzungsdaten zulässig, soweit dies für die Inanspruchnahme des Teledienstes erforderlich ist. Auf der Grundlage dieser Regelung ist die vorübergehende Speicherung und Nutzung der IP-Adresse des Nutzenden und der Suchanfrage zulässig, soweit die Angaben für die Anfragebearbeitung nötig sind. Für eine Speicherung über die Bearbeitung hinaus sowie für die Nutzung weiterer Daten wie z.B. Zeitstempel oder Angaben über den Browser enthält diese Norm keine Rechtsgrundlage.

Nach § 15 Abs. 3 TMG darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Suchmaschine Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzende dem nicht widerspricht. Auf das Widerspruchsrecht ist hinzuweisen. Die Datenschutzerklärungen der größeren Suchmaschinenanbieter weisen darauf hin, dass die Verwendung von Cookies im Browser deaktiviert werden kann, wobei das allerdings dazu führen könne, dass manche Elemente oder Dienste nicht richtig funktionieren. Ob die erteilten Hinweise hinreichend sind, ist zweifelhaft, zumal die Datenschutzerklärung zumeist nicht direkt, sondern über mindestens zwei Klicks erreichbar ist, und da die Deaktivierung von Cookies nicht unbedingt als Ausübung des Widerspruchsrechtes verstanden werden kann. Solange eine Profilbildung über die IP-Adresse als Pseudonym erfolgt, verstößt die derzeitige Praxis gegen § 15 Abs. 3 TMG.

Gemäß § 15 Abs. 3 S. 3 TMG dürfen die Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt, d.h. personifiziert werden. In welchem Umfang dies passiert, ist bei den meisten Suchmaschinenbetreibern nicht bekannt. Es muss aber davon ausgegangen werden, dass dies eine weit verbreitete Praxis ist. Wie dies möglich ist, kann am Beispiel von Google veranschaulicht werden: Google bietet nicht nur pseudonyme, sondern teilweise auch direkt personenbezogene Dienste an, bei denen Identifizierungsdaten zumindest optional angegeben werden. Werden nun über die IP-Adresse, über ein Cookie oder über sonstige Identifier die personenbezogenen Daten des Nutzenden mit denen des Suchdienst-Profiles kombiniert, so erfolgt eine unzulässige Personifizierung. Genutzt wird diese Zuordnung vor allem für die individualisierte Werbung. Über Cookies lässt sich zu einer Vielzahl von Sessions und unter Auswertung zusätzlicher Merkmale ein Interessenprofil erstellen, welches mit den Suchanfragen verdichtet werden kann. Der Umfang des derart möglichen Profils hängt davon ab, wie stark der Anwender den Suchdienst nutzt und Seiten frequentiert, die mit einheitlichen oder koppelbaren Cookies arbeiten.

Sollen Nutzungsdaten zu anderen Zwecken als der Bereitstellung des Dienstes oder der Werbung genutzt werden oder sollen die Daten an ein anderes Unternehmen übermittelt werden, so bedarf es hierfür einer ausdrücklichen Einwilligung nach § 12 Abs. 1 TMG. Dabei darf der Betreiber die Bereitstellung des Suchdienstes nicht von der Einwilligung zur Verwendung für anderen Zwecke abhängig machen, wenn dem Nutzenden ein anderer Zugang zu diesen Telemedien nicht oder in nicht zumutbarer Weise möglich ist (Koppelungsverbot, § 12 Abs. 3 TMG).

Dass die Löschung bzw. Anonymisierung der Nutzungsdaten erfolgt, kann für die Betroffenen u.U. von eminenter Bedeutung sein, da Dritte an einer zweckentfremdenden Nutzung ein großes Interesse haben können und die Betroffenen durch die Nutzung ihrer Daten beeinträchtigt werden können. Selbst staatlicherseits kann an diesen Daten ein – nicht immer legitimes – Interesse bestehen. So sind auf

Grund des Patriot Act (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism) alle Unternehmen in den USA verpflichtet, auf Verlangen alle gespeicherten Nutzungsdaten herauszugeben, auch von deutschen Nutzerinnen und Nutzern. Auch in Deutschland müssen auf der Basis der bestehenden Regelungen u.U. solche Daten an Sicherheitsbehörden herausgegeben werden.

Viele der von Betreibern genannten Zwecke lassen sich mit (teil-) anonymisierten Daten erreichen, bei denen ein Reidentifizierbarkeit ausgeschlossen ist. Dies gilt für die Verbesserung des Dienstes und die Erstellung von Statisiken ebenso wie – zumindest in gewissem Maße – für die Schaltung interessenspezifischer Werbung und für die Verhinderung von Betrug durch die Detektion auffälliger Clicks, deren Zahl zur Grundlage von Werbekosten genommen wird. Auskünfte an Sicherheitsbehörden dürfen nur im Rahmen der Gesetze und unter Beachtung der dort vorgesehenen Verfahren erteilt werden.

Auch im Hinblick auf die Verarbeitung der Nutzungsdaten haben die Betroffenen Rechte. So können sich die Nutzenden gemäß § 5 Abs. 1 TMG umfassend zum Diensteanbieter informieren über Name, Anschrift, Rechtsform, Vertretungsberechtigte, elektronische Kontaktmöglichkeiten und Identifizierungsnummern. Nach § 13 Abs. 1 TMG sind sie zusätzlich zu informieren über die Verarbeitung der Daten außerhalb des Geltungsbereiches der Europäischen Datenschutzrichtlinie. Dabei genügt es nicht, nur auf diesen Umstand hinzuweisen, so wie dies bisher regelmäßig erfolgt, sondern es muss zumindest das Land der Verarbeitung konkret benannt werden. Der Diensteanbieter muss den Nutzenden zudem gemäß § 34 BDSG Auskunft über die zur Person gespeicherten Daten geben, auch über die „zu seinem Pseudonym gespeicherten Daten“ (§ 13 Abs. 7 TMG).

Die Ansprüche auf Datenkorrektur nach § 35 BDSG bestehen auch hinsichtlich der Nutzungsdaten. Der Anbieter der Suchmaschine wie sonstiger Dienste muss zudem technisch-organisatorisch sicherstellen, dass „die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht“ bzw. zumindest gesperrt werden (§ 13 Abs. 4 Nr. 2 TMG).

7. Schlussfolgerungen

Die vorstehende Analyse einiger Datenschutzfragen bei Internet-Suchmaschinen zeigt, dass hier das Recht auf informationelle Selbstbestimmung derzeit i.d.R. nicht hinreichend gewahrt wird. Die gesetzlichen Regelungen sind unzureichend und teilweise auf die eingesetzte Technik nicht anwendbar; die Vollzugsdefizite sind groß; die Aufsichtsbehörden haben keine praktischen Handhaben zur Durchsetzung des Datenschutzes.

Der "schwarze Peter" darf von den Betreibern nicht weitergereicht werden; diese können viel zur Wahrung des Datenschutzes tun: Kurzfristige Anonymisierung der Suchanfragen, Offenlegung der tatsächlich erfolgenden Datenverarbeitungsschritte gegenüber den Nutzenden unter Benennung der verfolgten Zwecke, leicht erreichbare und gut verständliche, praktikable Wahlmöglichkeiten, etwa bzgl. Setzen und Löschen von Cookies, die Verwendung von wirksamen, d.h. hinreichend bestimmten und freiwilligen Einwilligungserklärungen bei dienstübergreifenden Datennutzungen, Benennung der verantwortlichen Stelle und einer für Datenschutzfragen ansprechbaren Person bzw. Stelle.

Bzgl. der Betroffenenrechte als erfasstes Suchobjekt sind die entgegenstehenden Informationsrechte mit abzuwägen. Diese dürfen aber nicht zur vollständigen Negierung der Betroffenenrechte führen. So wäre eine leicht online wie offline erreichbare Beschwerdeinstanz von großem Nutzen, die Auskunfts- und Informationsansprüche unkompliziert beantwortet, Hilfen bei der sonstigen Wahrung von Betroffenenrechte gewährt und um Zweifel Datensperrungen, -löschungen und -berichtigungen veranlassen kann. Zumindest die großen Unternehmen beginnen gerade erst, die Datenschutzimplikationen ihrer Angebote zur Kenntnis zu nehmen und zu reflektieren, um hieraus auch Konsequenzen zu ziehen. Angesichts des bisher bestehenden weitgehenden Monopols ist es bisher kaum möglich, die wettbewerbliche Macht der Verbraucher zu mobilisieren.

Dieser globale Missstand muss und kann sich ändern. Die Aufsichtsbehörden haben begonnen, sich über gemeinsame geforderte Datenschutzstandards selbst auf internationaler Ebene zu verständigen. Hieraus können internationale zwingende Normen zum Schutz informationeller Selbstbestimmung abgeleitet werden. Auf nationaler Ebene ist eine gezieltere Aufsichtstätigkeit nötig, die bisher an der katastrophalen personellen und technischen Ausstattung der zuständigen Stellen wie an einer verbesserungsfähigen Koordination scheitert. Durch die Entwicklung einer europäischen Alternative zu den US-Marktführern kann erreicht werden, dass die (rechtlich erlaubten) Zugriffsmöglichkeiten auf persönliche Daten sowie Betriebs- und Geschäftsgeheimnisse durch US-amerikanische Dienste ausgeschlossen werden.

Unabhängig hiervon muss der nationale Gesetzgeber das Datenschutzrecht an die Notwendigkeiten und Möglichkeiten des globalen Internet anpassen. Neben dem zwingenden Datenschutzrecht müssen gerade in den Bereichen, in denen die „Flucht ins Ausland“ für Anbieter möglich ist, verstärkt Marktmechanismen zum Einsatz gebracht werden. Hierfür bieten sich Datenschutz-Gütesiegel und -Audits an. Parallel hierzu muss die Sensibilisierung der Nutzerinnen und Nutzer vorangebracht werden. Deren Vertretung in Gestalt der Verbraucherverbände hat die Möglichkeit, z.B. über AGB-Kontrollen die Verbraucherrechte generell zu stärken. Das Datenschutzrecht der User und Betroffenen ist nichts anderes als spezifisches Verbraucherrecht [16]. Auch ohne die Mobilisierung des Rechtes sind die Anbieter von Suchmaschinen aufgefordert, ihr Angebot datenschutzkonform (um-) zu gestalten. Um dies zu erreichen, geht kein Weg vorbei an der öffentlichen Diskreditierung schlechter und der positiven Hervorhebung datenschutzfreundlicher Angebote.

Literaturangaben

[1] Weichert, Thilo: Datenschutz bei Suchmaschinen. In: MR Int 4/2007, 188; www.datenschutzzentrum.de/suchmaschinen/20080206-datenschutz-bei-suchmaschinen.html Abruf: 2008-05-07; mit vielen Nachweisen.
[2] vgl. www.ip-adress.com
[3] www.google.com/history
[4] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – ULD, Tätigkeitsbericht 2007, Kap. 10.6-10.9.
[5] Weichert, Thilo: Google übernimmt DoubleClick. In: DuD 2007, 724.
[6] Die Angaben zu Google stammen aus: Reischl, Gerald: Die Google Falle: die unkontrollierte Weltmacht im Internet, München: Ueberreuter, 2008; Speck, Hendrik/Thiele, Frédéric Philipp u. Patzwald, Klaus. In: Lehmann, Kai/Schetsche, Michael: Die Google-Gesellschaft, Bielefeld: transcript 2005, S. 181´; Maurer, Hermann u.a.: Report on dangers and opportunities posed by large search engines, praticularly Google, 30.09.2007, S. 9, 161.

[7] BVerfG NJW 1969, 1707 – Mikrozensus
[8] BVerfG NJW 1984, 419 – Volkszählung
[9] BVerfG NJW 2005, 1341 – GPS
[10] BVerfG NJW 2008, 822 – Online-Durchsuchung
[11] Siemen, Birte: Datenschutz als europäisches Grundrecht, Berlin 2006.
[12] Article 29 Data Protection Working Party, Opinion on data protection issues related to search engines, vom 04.04.2008, 00737/EN WP 148.
[13] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – ULD, Tätigkeitsbericht 2008, Kap. 8.2 u. 8.3; www.prime-project.eu; www.fidis.net; http://www.primelife.eu/
[14] 28. Int. Datenschutzbeauftragten-Konferenz. In: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien, 1983-2006, S. 60.
[15] Article 29 Data Protection Working Party [12], S. 12.
[16] Weichert, Thilo: Datenschutz in Verbraucher- und Wettbewerbsrecht. In: VuR 2006, 377.