

Hochschule Anhalt (FH)
Hochschule für angewandte Wissenschaften
Abteilung Bernburg
Fachbereich Wirtschaft

Bachelorarbeit

Thema:

Das Recht auf Vergessenwerden

Vorgelegt von: Maximilian Vorwerk
Matrikel-Nr.: 4058394
Vorgelegt am: 26.09.2017
Studiengang: Wirtschaftsrecht
1. Gutachter: Frau Prof. Dr. Zümrüt Gülbay-Peischar
2. Gutachter: Herr Prof. Dr. Sebastian Volkmann

Vorwort

>>Die Erinnerungen verschönern das Leben, aber das Vergessen allein macht es erträglich.<<

- Honoré de Balzac -

Literaturverzeichnis

Vorwort.....	II
Abkürzungsverzeichnis	V
A) Einleitung	1
B) Entwicklung und Popularität von Suchmaschinen	2
I. Was ist eine Suchmaschine?	2
1. Funktionsweise	3
2. Die gesellschaftliche Relevanz von Suchmaschinen	5
3. Geschichte der Suchmaschine	6
4. Suchmaschinen, ein Big-Brother-Albtraum?	6
a) Datenkraken und Datenverkehr.....	8
b) Datensammelwut von sozialen Netzwerken	8
c) Daten über Nichtmitglieder generieren	10
d) Mini-Programm	11
e) Daten bleiben	12
f) Möglichkeit der Anonymisierung?	13
g) Datenverkehr mit Drittstaaten.....	14
5. Suchen ohne Schnüffler	15
C Datenschutz und Suchmaschinen	16
I. Was ist Datenschutz?.....	16
II. Datenschutz = Persönlichkeitsrecht?.....	17
1. Im Spannungsfeld von Datenschutz und Persönlichkeitsrecht – Spickmich-Urteil.....	18
2. Welche Informationen findet eine Suchmaschine über mich?	19
a) Daten im Netz	19
b) Was geschieht mit den Informationen, die eine Suchmaschine bei einer Suche erfasst?..	20
c) Digitale Demenz.....	20
d) Was steckt hinter all dem?	20
e) America Online (AOL) Privacy-Skandal	21
D) Das Recht auf Vergessenwerden.....	21
I. Löschpflichten und Löschantrag Art. 17 EU-DSGVO.....	22
1. Wie ist der Löschantrag geltend zu machen?	23
2. Wann ist zu löschen?	23
3. Mitteilungs- und Informationspflichten	24
4. Ausnahmen von der Löschpflicht	25
5. Irrtümer des Rechts auf Vergessen.....	25
a) Inhalte werden nicht gelöscht. Die betroffenen Seiten bleiben weiterhin online.	25

b)	Die betroffene Seite wird nicht aus den Suchergebnissen „gelöscht“	25
c)	Die betroffene Seite bleibt weiterhin auffindbar	26
d)	Die Suchergebnisse werden allein in den europäischen Versionen der Suchmaschinen entfernt.....	26
e)	Das „Recht auf Vergessenwerden“ ist keine neue Erfindung	26
6.	Verfallsdatum für digitale Daten.....	27
II.	Vereinbarkeit mit dem Grundrecht	28
III.	Datenschutz als Grundrecht im europäischen Recht.....	29
IV.	Urteile zum Recht auf Vergessen.....	29
1.	Volkszählungsurteil von 1983	29
2.	Der Fall Amanda Todd	31
3.	Google-Urteil des EuGH vom 13.05.2014 (C-131/12).....	33
a)	Sachverhalt.....	33
b)	Vorlagefragen und Entscheidung des EuGH	33
aa)	Verantwortlichkeit des Suchindex	34
(1)	Sachlicher Anwendungsbereich	34
(2)	Verantwortliche Stelle	34
bb)	Räumlicher Anwendungsbereich	35
c)	Löschanspruch des Betroffenen	36
aa)	Das Recht auf Vergessenwerden.....	36
bb)	Die Entscheidung des Gerichtshofs	37
d)	Folgen des Urteils	38
aa)	Antragformular	38
bb)	Vorschläge des Löschbeirats	38
cc)	Ablauf einer Löschung.....	39
dd)	Statistik über Löschung.....	39
4.	Daten im Gesellschaftsregister – EuGH-Urteil vom 09.03.2017 (C-398/15)	39
a)	Sachverhalt.....	40
b)	Ist ein unbefristeter Zugang zum Unternehmensregister zulässig?	40
c)	Ausnahme zur Einschränkung des Zugangs	41
V.	Fazit.....	42
	Selbständigkeitserklärung	VII
	Literaturverzeichnis.....	VIII
	Abbildungsverzeichnis	XII

Anmerkung: Da in der deutschen Sprache durch den generischen Maskulin beide Geschlechter gleichermaßen angesprochen werden, wird aus Gründen der besseren Lesbarkeit auf eine geschlechtsspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichberechtigung für beide Geschlechter.

Abkürzungsverzeichnis

Abs.	=	Absatz
AEPD	=	Agencia Española de Protección de Datos
AOL	=	America Online
Art.	=	Artikel
BC	=	British Columbia
BGH	=	Bundesgerichtshof
BDSG	=	Bundesdatenschutzgesetz
bpb	=	Bundeszentrale für politische Bildung
BRD	=	Bundesrepublik Deutschland
BVerfGE	=	Bundesverfassungsgericht
bzw.	=	beziehungsweise
ca.	=	circa
CTO	=	Chief Technology Officer
DRM	=	Digital Rights Management
DS-RL	=	Datenschutz-Richtlinie
EU	=	Europäische Union
EU-DSGVO	=	EU-Datenschutz-Grundverordnung
EuGH	=	Europäischer Gerichtshof
GG	=	Grundgesetz
GRCh	=	Charta der Grundrechte der Europäischen Union
HmbBfDI und Informationsfreiheit	=	Hamburgischen Beauftragten für Datenschutz
HTTP	=	hypertext transfer protocol
ID	=	Identifizierung
Inc.	=	Incorporated
IP	=	Internet Protocol
i.S.d.	=	im Sinne des
i.S.v.	=	im Sinne von
lit.	=	littera

NSA	=	National Security Agency
Nr.	=	Nummer
o.V.	=	ohne Verfasser
PC	=	Personalcomputer
RCMP	=	Royal Canadian Mounted Police
S.	=	Seite
TKG	=	Telekommunikationsgesetz
TMG	=	Telemediengesetz
US	=	United States
USA	=	United States of America
Vgl.	=	Vergleiche
WWW	=	World Wide Web
z.B.	=	zum Beispiel

A) Einleitung

Tagtäglich treffen wir auf verschiedene Fragen, die wir zu beantworten haben, und nicht alle können wir sofort beantworten. Was wird getan? Die Nutzer greifen zum Handy und recherchieren über eine Suchmaschine Informationen über die betreffende Sache. Die Informationen sind allgegenwärtig und wer nicht genau weiß, wo er in der Unübersichtlichkeit des Internets eine bestimmte Information findet, greift in der Regel auf Suchmaschinen zurück. Doch ohne Suchmaschinen wäre das Recherchieren im Internet ohne Suchmaschinen kaum möglich; sie sind sozusagen die Wegweiser bzw. die Navigation durch das Internet, denn mit jeder Suche ergeben sich gleichzeitig neue zum Thema passende Suchvorschläge. Studien legen zu Grunde, dass ca. 90 Prozent aller der aufgerufenen Webseiten über Suchmaschinen und nicht über Werbung in Printmedien, Fernsehen oder durch Empfehlungen von Bekannten und Freunden gefunden werden. Suchmaschinen sind somit Anlaufpunkt und Knotenpunkt in einem. Doch verbirgt sich hinter der Allgegenwärtigkeit von Informationen auch eine große Anzahl an Gefahren.

„Das Internet vergisst nicht!“, so heißt es aus vielen Mündern. Allerdings ist das Vergessen ein natürlicher Vorgang, der wenn man so will, ein Prozess des Selbstschutzes ist, für sich und für andere.

Mittlerweile erkennt ein Großteil die Gefahr hinter der unbegrenzten Möglichkeit, Informationen über das Internet zu erlangen und zu verbreiten. Deshalb fordern Viele ein „Recht auf Vergessenwerden“, um einen Ausweg aus dem „Nichtvergessen“ zu finden und Anreize für das Vergessen zu schaffen.

Diese Arbeit beschäftigt sich mit der Frage der Notwendigkeit des „Rechts auf Vergessenwerden“ und erklärt die Situation der Vereinbarkeit mit dem Grundrecht auf nationaler und europäischer Ebene.

Um dem eigentlichen Thema Verständnis verleihen zu können, wird im ersten Teil der Arbeit über Suchmaschinen und deren Komplexität in der Datenverarbeitung berichtet. Nachdem das geschehen ist, wird mit Hilfe des Themengebietes Datenschutz auf die Relevanz der Persönlichkeitsrecht hingewiesen und wie wichtig der vertrauliche Umgang mit/von personenbezogenen Daten ist. Abschließend dazu wird das „Recht auf Vergessen“ analysiert und interpretiert.

Personenbezogene Daten bedürfen einer besonderen Schützenwürdigkeit; dabei sollte es in der Regel von größter Relevanz sein, den Einzelnen in seinen Persönlichkeitsrechten vor die Allgemeinheit zu stellen.

B) Entwicklung und Popularität von Suchmaschinen

Im Jahr 1240 ließ Abt Hugues de Saint-Cher das erste Stichwortverzeichnis der Bibel aufstellen, mit dieser Aufgabe waren ca. 500 Mönche beschäftigt. Im Vergleich dazu hat die Bibel in ihrer heutigen Druckfassung etwa 800 Seiten, was ca. fünf Megabyte als Computereinheit entspricht.¹

Schätzungen zufolge enthält das Internet zurzeit ca. 50 Millionen Seiten bzw. 400 Gigabyte und wächst monatlich um ungefähr 20 Prozent.² Im Kontext dazu wären weder 500 noch die Gesamtheit der Mönche heute nicht in der Lage diese Informationsflut zu erfassen und durchsuchbar zu machen.³

Um das Informationsinteresse zu stillen und der Informationsflut gerecht zu werden, gibt es Suchmaschinen. Suchmaschinen durchkämmen nicht nur die unübersichtliche Weite des Internets, sie dienen vor allem den Nutzern dazu den Massen an Informationen eine Struktur und Übersichtlichkeit zu geben.

„Wegen der dezentralen Struktur des Internets kann es keinen zentralen Index oder ein Gesamtverzeichnis des Netzes geben.“⁴ Daher ist die Aufgabe von Suchmaschinen, das Internet, speziell das „World Wide Web“, nachfolgend WWW, zu erfassen und über Stichwörter durchsuchbar zu machen.

I. Was ist eine Suchmaschine?

Suchmaschinen sind eine auf einen mathematischen Algorithmus zur Relevanzbewertung von Webseiten bzw. -inhalten aufbauende Anwendung zur Recherche im WWW. Nach Eingabe einer Suchanfrage liefert die Suchmaschine nach bestimmten Kriterien eine geordnete Liste mit Verweisen auf die, für die Suchanfrage am ehesten in Frage kommenden Webseiten bzw. Dateien, und listet diese nach ihrer Qualität bzw. Relevanz geordnet untereinander auf.⁵

¹ Vgl.: (Baumgärtel)

² Vgl.: (Baumgärtel)

³ Vgl.: (Baumgärtel)

⁴ (Baumgärtel)

⁵ (Tippmann, Hemken, Rehberg, & Wienströer)

Wegen der dezentralen Struktur des Internets sind Suchmaschinen erforderlich, um dem Nutzer suchrelevante Informationen zur Verfügung zu stellen.

Im Gegensatz zu Katalogen, die als Vorgänger der Suchmaschinen sich im einfachsten Fall als vorher von Menschen nach alphabetischen oder thematischen Kriterien geordnete Listen erweisen, läuft die Suche automatisiert ab.⁶

„Die Sortierung und Kategorisierung der Adressinformation kann dabei automatisiert über elektronische Agenten oder manuell durch eine Redaktion erfolgen. Suchmaschinen sind attraktiv für Werbetreibende, da sie über hohe Zugriffsraten verfügen und die Möglichkeit kontextsensitiver Werbung bieten. Die mit Abstand meistgenutzte Suchmaschine weltweit ist Google. Weitere Anbieter von Suchdiensten sind etwa Yahoo! oder Microsoft. Neben der heutzutage wichtigsten Gruppe der indexbasierten Suchmaschinen, existieren auch Metasuchmaschinen, die Anfragen gleichzeitig an mehrere Suchmaschinen senden.“⁷

1. Funktionsweise

Suchmaschinen durchsuchen nicht das komplette Internet, sondern nur einen Teil, das WWW. Auch das WWW ist nicht komplett durchsuchbar; hier sind nur jene Webseiten für Suchmaschinen auffindbar, die auch öffentlich zugänglich sind.⁸

Grundsätzlich laufen bei einer Suche im WWW folgende drei Vorgänge ab:⁹

1. Erfassung

Suchmaschinen erfassen laufend neue und veränderte Informationen im World Wide Web. Dies geschieht durch sogenannte Crawler (auch Spider oder Suchroboter genannt). Ein Crawler ist ein System aus Soft- und Hardware, das systematisch und kontinuierlich das Internet durchsucht, die auf den Internetseiten vorhandenen Informationen einsammelt und diese dann auf Servern abspeichert.

2. Informationsaufbereitung und Indizierung

Diese Sammlung von Daten wird nun so aufbereitet, dass effizient ein Index erstellt werden kann. Der Index ist der Kern jeder Websuchmaschine. Er ist vergleichbar mit dem Stichwortregister eines Buches. Der Suchmaschinen-Index enthält einerseits Index-Begriffe, andererseits die Informationen darüber, auf

⁶ (Lackes, Siepermann, & Sjurts)

⁷ (Lackes, Siepermann, & Sjurts)

⁸ (klicksafe.de - Die EU-Initiative für mehr Sicherheit im Netz)

⁹ (klicksafe.de - Die EU-Initiative für mehr Sicherheit im Netz)

welchen Internetseiten die Begriffe vorkommen. Der Suchindex ist also ein virtuelles Verzeichnis, das Milliarden von Begriffen und Verweise auf Webseiten umfasst.

3. Informationsbereitstellung

Für jede Suchanfrage wird somit nicht mehr das gesamte Internet durchsucht, sondern nur noch dieser Index, da dieser besonders schnell und effizient durchsucht werden kann. Abschließend werden die für die Suchanfrage relevantesten Ergebnisse in einer Liste dargestellt.

Das sind die Vorgänge, die für den Nutzer offensichtlich sind. Doch was spielt sich hinter den Kulissen ab? Die folgenden fünf Schritte zum Suchergebnis sind für den Suchenden nicht sichtbar.¹⁰

1. Eingabe der Suchanfrage

Die Suche beginnt mit der Eingabe eines Suchbegriffs, z.B. [Berlin], in das Suchfeld.

2. Die such nach dem richtigen Datenzentrum

Suchmaschinenbetreiber unterhalten weltweit Datenzentren mit Servern, auf denen der Index gespeichert ist. Im Hintergrund werden sofort ein oder mehrere Datenzentren ausgewählt. Bei der Auswahl des richtigen Datenzentrums spielen räumliche Nähe, Geschwindigkeit und Auslastungsgrad eine entscheidende Rolle.

3. Der Suchlauf durch den Index

Bei großen Suchmaschinen ist der Index speziell für eine parallele Abfrage gebaut. Dadurch muss jeder Server nur einen Teil der Suche durchführen und gemeinsam kann so der gesamte Index schneller durchsucht werden. Eine Suchmaschine sucht genau genommen nicht nach einem bestimmten Wort, sondern nach Buchstabenmustern.

Nachdem der Suchlauf durchgeführt und das erste Suchergebnis zusammengestellt ist, muss deshalb noch einmal eine Überprüfung durchgeführt werden. Vielleicht hat sich der Nutzer ja vertippt und wollte etwas ganz anderes suchen? Kann man das Wort auch auseinanderschreiben? Die Suchmaschine versucht, dies nachzuvollziehen, und zeigt bei Bedarf einen besseren Suchvorschlag an. Bei der Eingabe von [berln] wird beispielsweise [Berlin] vorgeschlagen.

¹⁰ (klicksafe.de - Die EU-Initiative für mehr Sicherheit im Netz)

4. *Der Suchlauf nach dem richtigen Dokument*

Die Index-Server enthalten ausschließlich Wörter und Adressen. Sie verweisen auf die sogenannten Doc-Server. Auf den Doc-Servern liegen der Titel, Textauszüge und weitere Daten aus den in der Informationsaufbereitungsphase (siehe oben) gespeicherten Dokumenten. Diese Informationen sind zum einen für die Ausgabe nützlich (z.B. für die kurzen Textauszüge unter den Adressen, genannt Snippets), zum anderen sind sie die Grundlage für den PageRank-Algorithmus. Eine Maßnahme, um den Suchablauf hinter den Kulissen trotz dieses komplexen Verfahrens zu beschleunigen, besteht darin, Ergebnisse häufiger Suchanfragen, wie z.B. [Berlin], zwischen zu speichern, d.h. nicht jedes Mal aufs Neue den Index zu durchsuchen, sondern auf bereits „fertige“ Suchergebnisse zurückzugreifen.

5. *Ausgabe der Suchergebnisse*

Im letzten Schritt müssen die Suchinformationen nun noch nutzerfreundlich angezeigt werden. Schließlich sollen auf den ersten Blick die wichtigsten Internetseiten für den eingegebenen Suchbegriff erkennbar sein. Im Allgemeinen klickt der Nutzer eines der ersten zehn Suchergebnisse an. Ergebnisse, die weiter unten in der Liste auftauchen (also auf nachfolgenden Seiten), werden seltener angeklickt. Die Reihenfolge der Treffer („Ranking“) wird durch einen Algorithmus festgelegt.

2. **Die gesellschaftliche Relevanz von Suchmaschinen**

Aus allgemeingesellschaftlicher Perspektive sind Suchmaschinen von enormer Bedeutung, denn Suchmaschinen ermöglichen Nutzern nicht nur das Suchen von Informationen, sondern bewerten die Informationsquellen an ihrer Relevanz und möglichen Verwendbarkeit.

Ohne Suchmaschinen wäre eine effektive Nutzung des Internets fast unmöglich.¹¹ Die Informationen stünden zwar bereit, allerdings wäre die Wahrscheinlichkeit, dass ein Nutzer, der bestimmte Informationen sucht, diese auch findet, in vielen Fällen äußerst gering. Die praktische Bedeutung von Suchmaschinen für die Nutzung des Internets kann kaum überschätzt werden.¹²

¹¹ (Wolling)

¹² (Wolling)

3. Geschichte der Suchmaschine

1991 entwickelten Paul Lindner und Mark P. McCahill von der University of Minnesota eine Software namens Gopher, mit der es möglich war, Dokumente auf einen bestimmten Server zu durchsuchen. Die Gopher-Seiten wurden thematisch katalogisiert und der komplette Datenbestand konnte mittels der Software „Veronica“ (Very Easy Rodent-Oriented Net-wide Index to Computerized Archives) durchsucht werden. Da es mit Gopher allerdings nicht möglich war, nach Bildern und Grafiken zu suchen, verschwand Gopher drei Jahre später von der Bildfläche, um dem multimedial ausgerichteten WWW zu weichen.

4. Suchmaschinen, ein Big-Brother-Albtraum?

Tagtäglich benutzt ein Großteil der Bevölkerung das Internet und greift dabei auf Suchanbieter zurück. Einer davon, wohl der bekannteste Suchanbieter, heißt Google. „Bei Google handelt es sich um eine der größten Datenkraken, von der unbegrenzt Daten abgeschöpft werden – und die NSA liest mit.“¹³ Mittlerweile entwickelt sich das Internet zum Big-Brother-Albtraum. Permanent werden von den Nutzern jegliche Arten von Daten gespeichert. Ein Ende des Fulltime-Trackings ist mit den anonymen Suchmaschinen in Sicht.

Nach wie vor gilt Google als die am meisten von Usern genutzte Suchmaschine, um nach Informationen und Webseiten zu suchen. Während des Suchens bzw. Surfens hinterlassen die User dem Internetriesen Google eine Vielzahl von Daten. Diese werden genutzt, um passgenaue Anzeigen zu platzieren.¹⁴ „Wer nun der Ansicht ist, dass Bing eine Alternative darstellt, der irrt, denn auch die Suchmaschine von Microsoft sammelt Nutzerinformationen, um gezielt Werbeeinblendungen zu setzen.“¹⁵

Im März 2017 wies Google laut seo-summary.com einen Marktanteil im Vergleich zwischen den Internet-Suchmaschinen von 90,3 % auf, Bing folgte mit 8,1 % und Yahoo mit 1,1 %.¹⁶ Alle anderen sind statistisch gesehen nicht mehr relevant.

¹³ (Wirtschaft.com, 2017)

¹⁴ Vgl.: (Wirtschaft.com, 2017)

¹⁵ (Wirtschaft.com, 2017)

¹⁶ Vgl.: (SEO-Summary.com, 2017)

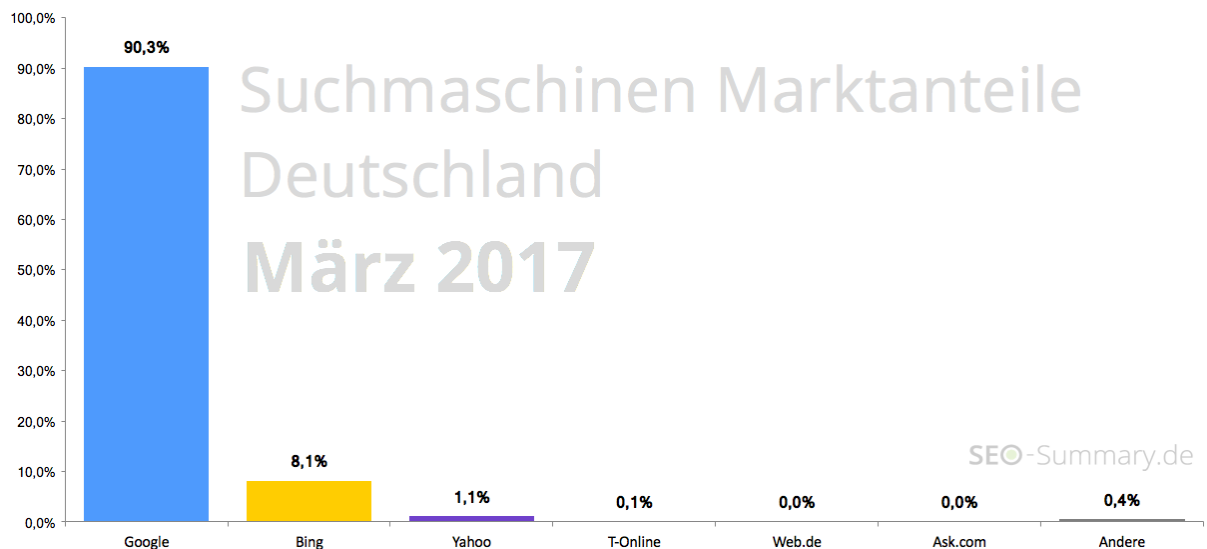


Abbildung 1 Marktanteile Suchmaschinen

Suchmaschine	März 2017	Februar 2017	Januar 2017	12 Monate (03/16)
Google	90,3%	90,2%	89,7%	90,8%
Bing	8,1%	8,2%	8,3%	6,8%
Yahoo**	1,1%	1,1%	1,3%	1,3%
T-Online*	0,1%	0,1%	0,1%	0,8%
Web.de*	0,0%	0,0%	0,0%	0,0%
Ask.com	0,0%	0,0%	0,0%	0,2%
Andere	0,4%	0,4%	0,6%	0,2%

Daten-Quelle: StatCounter, Web-Stats / * = nutzt die Google Suche / ** = nutzt die Bing Suche

Abbildung 2 Statistische Marktanteile in Prozent

Erstaunlich daran ist, dass viele User sich über die „Datensammelwut“ von Google aufregen, letzten Endes aber immer wieder auf diese Suchmaschine zurückgreifen. „Dabei würde es sich lohnen, einmal einen Blick auf andere Suchmaschinen zu werfen, die nicht so „neugierig“ sind.“¹⁷

Sollte jemand den Wunsch besitzen, im Internet anonym auf die Suche gehen zu können, der sollte auf kleinere Anbieter umsteigen. Sogenannte Meta-Suchmaschinen leiten die Anfrage an Suchdienste weiter, sammeln die Ergebnisse und bereiten diese für die User auf.¹⁸

¹⁷ (Wirtschaft.com, 2017)

¹⁸ Vgl.: (Wirtschaft.com, 2017)

Von diesen Suchmaschinen werden keine IP-Adressen oder andere Daten gesammelt, über die der Nutzer identifiziert werden kann.¹⁹ Selbst Cookies kommen kaum zum Einsatz. Allerdings kann ein Zugriff der Behörden auf diese Server nicht immer ausgeschlossen werden.

a) Datenkraken und Datenverkehr

Als eine Datenkrake werden Unternehmen verstanden, die Informationen und Daten sammeln, aggregieren und auswerten. „Insbesondere Internet-Unternehmen aus den USA, in denen gemäßigte Datenschutzbestimmungen herrschen, stehen im Fokus der politischen Diskussion um Informationelle Selbstbestimmung, Schutz vor Datenmissbrauch, Profiling und Netzsicherheit.“²⁰ Im Begriffskomplex Datenkraken wird oftmals von Google gesprochen. Doch nicht nur Google, sondern auch viele andere Internet-Giganten, wie Facebook, WhatsApp, Amazon und Co. profitieren durch das Geschäftsmodell der Erhebung und des Handels von Daten, sie helfen uns durch die Datenspeicherung im Alltag.²¹ „Assistenzsysteme wie Alexa oder Google Assistant erleichtern uns durch Sprachanalysen Aufgaben zu erledigen, Facebook verbindet Menschen in der ganzen Welt, Microsoft Windows und Googles Android sind Betriebssysteme vieler Millionen Internetnutzer und mit dem häufig als Datenkrake bezeichneten Messenger WhatsApp verschicken wir jeden Tag persönliche Nachrichten an Freunde und Familie.“²² Eine „Big Brother“-Wirtschaft ist also Fluch und Segen zugleich.

b) Datensammelwut von sozialen Netzwerken

Unternehmen sammeln und speichern Daten, um ihre Produkte sowie den kommerziellen Handel besser koordinieren und abstimmen zu können. Insbesondere rücken Suchmaschinen und die Sozialen Medien in den Blickpunkt der Datenschützer. Gerade hier wird mit vertraulichen Daten bzw. personenbezogenen Daten leichtsinnig umgegangen. Oftmals tragen jugendliche Nutzer ihre Konflikte auf derartigen öffentlichen Ebenen aus. Nicht nur jetzt sondern auch in der Zukunft ist es Außenstehenden möglich, solche Informationen nachvollziehen zu können.

In Hinblick dessen, dass die meisten sozialen Netzwerke kostenfrei sind, muss die Finanzierung über Werbeeinnahmen erfolgen. Hierzu werden die Werbeanzeigen auf den jeweiligen Nutzer personalisiert. Dies geschieht, in dem der Anbieter Suchanfragen in

¹⁹ Vgl.: (Wirtschat.com, 2017)

²⁰ (datenkraken.de)

²¹ Vgl.: (datenkraken.de)

²² (datenkraken.de)

bestimmte Algorithmen setzt. Bestes Beispiel hierfür ist Facebook. Würde Facebook seine Werbeanzeigen nicht personalisieren, würden dem sozialen Netzwerk, welche mehr als eine Milliarde Nutzer verzeichnet, etliche Millionen an Geldern entgehen. Das größte Problem an der Sache ist, dass die sozialen Netzwerke aus kommerziellen Gründen daran interessiert sind, so viele personenbezogene Daten wie möglich zu erfassen. In diesem Sinne gilt das allgemeine Interesse nicht dem Kunden, vielmehr der Werbeindustrie. Speziell Facebook wird unterstellt, die Datenschutzbedingungen nicht allzu ernst zu nehmen. Im einem offenen Brief von 2010 forderte die Bundesverbraucherschutzministerin Ilse Aigner Facebook zur Verbesserung des Datenschutzes auf: „Grundsätzlich dürfen persönliche Daten nicht ohne Einwilligung automatisch an Dritte zu kommerziellen Zwecken weitergegeben werden.“²³ Allerdings sind die Datenmassen für die sozialen Netzwerke lukrativ und es stehen nicht nur die Daten von Mitgliedern auf der Liste, sondern auch die der Nicht-Mitglieder.²⁴ Wer sich bei Facebook registriert, muss seine E-Mail-Adresse angeben und kann in diesem Zug das ganze Adressbuch synchronisieren oder mit der Smartphone-App die auf dem Handy hinterlegten Kontaktdaten übertragen.²⁵ „In beiden Fällen gleicht Facebook den Teilnehmerstand dann mit den eigenen Datenbeständen ab und schlägt einem „Freund“ vor.“²⁶ Ebenso durch Standortzugriffe oder Registrierungen von Personen aus dem Adressbuch berechnet das System, wer dein Freund sein könnte und schlägt ihn dir vor.²⁷ „Auf diese Weise lassen sich ganze Beziehungsnetze nachzeichnen.“²⁸ Genauso umstritten ist die Nutzung der Gefällt-mir-Schaltflächen, „sobald eine Website den Like-Button [...] eingebunden hat, [werden] personenbezogene Daten [...] an Facebook gesendet [...] – auch wenn der Button gar nicht angeklickt wurde. Und auch, wenn derjenige gar kein Facebook-Mitglied ist. [...] Es bestehen Anhaltspunkte, dass die Verwendung sowohl gegen das TMG als auch gegen das BDSG verstößt.“²⁹ Abschließend sollte erwähnt werden, dass zwar die Mehrheit, aber nicht alle sozialen Netzwerke von Verbraucherschützern gerügt werden.³⁰ „So wird der Microblogging-Plattform Twitter attestiert, relativ wenige Daten von seinen Mitgliedern abzufragen.“³¹

²³ (Aigner, 2010)

²⁴ Vgl.: (Lochmann, Gewehr, & Szugat, 2010)

²⁵ Vgl.: (Schulze, 2013)

²⁶ (Schulze, 2013)

²⁷ Vgl.: (Breithut, 2016)

²⁸ (Auer-Reinsdorf, Jakobs, & Lepperhoff, 2011)

²⁹ (Lochmann, Gewehr, & Szugat, 2010)

³⁰ Vgl.: (Schulze, 2013)

³¹ (Schulze, 2013)

Neben Google gilt Facebook als zweitgrößte Datenkrake, die jeden einzelnen Nutzer in einer in der Weltgeschichte bislang nicht erlebten Art und Weise ausspäht.³² Daten werden nicht nur erhoben, um Werbeanzeigen personenbezogen und zielgenau anzupassen. „Das Gefährliche besteht darin, dass die erfassten Daten zurückwirken. Unser digitaler Zwilling erlaubt nicht allein Rückschlüsse über unser Denken und Fühlen, über politische Entscheidungen und persönliche Präferenzen, sondern die Daten beeinflussen, mit wem wir in Kontakt treten, wie wir gesehen werden und welche Inhalte wir selbst künftig sehen.“³³ Bestes Beispiel hierfür ist die Verbreitung von „Fake News“, wie es 2016 bei der amerikanischen Präsidentenwahl der Fall war.

Während Google mit seinem Quasi-Monopol der Suchmaschinen sowie des mobilen Betriebssystems Android und Marktanteilen von mehr als 85 Prozent durch persönliches Verhalten nicht mehr ausweichbar ist, gibt es bei Facebook einige Lichtblicke.³⁴ Keinem wird auferlegt, Facebook nutzen zu müssen, wenngleich Facebook auch personenbezogene Daten über Menschen erhebt, die kein Facebook-Konto besitzen. Des Weiteren besteht die Möglichkeit, Facebook gewisse Grenzen zu setzen und die Aufzeichnung von Daten zu begrenzen.³⁵

Der erste und wichtigste Schritt besteht darin, genau das Gegenteil dessen zu tun, was Facebook und Co. einem fortwährend vorschlagen. Anstelle der Aufforderung zur Verknüpfung von Konten, Informationen und Diensten mit Facebook zu folgen, weil es dann für den Nutzer leichter wäre, das System zu nutzen oder das Ergebnis mehr Sicherheit bringe, solle dies verneint werden. So nahe liegend, wie es auch klingt, sich mit Facebook zu verbinden, so bedeutet es im Gegenzug auch, dass nicht nur der jeweilige Dienst oder die betreffende App sämtliche persönlichen Daten aus Facebook abziehen, sondern umgekehrt, dass auch Facebook alles erfährt, was eine Fitness-Armbanduhr oder eine Überwachungskamera fürs Heim an Informationen generiert.³⁶

c) Daten über Nichtmitglieder generieren

Facebook ist es möglich, innerhalb der App und im Facebook-System die eigenen Aktivitäten auszuwerten. Das bedeutet, alle selbst eingegebenen Informationen, wie Status-Updates,

³² Vgl.: (Spehr, 2016)

³³ (Spehr, 2016)

³⁴ Vgl.: (Spehr, 2016)

³⁵ Vgl.: (Spehr, 2016)

³⁶ Vgl.: (Spehr, 2016)

geteilte Beiträge und Links und deren implizierte Daten, wie die Inhalte von Fotos mit Hilfe von Bilderkennungsalgorithmen, die von nichtverschlüsselten Chat-Unterhaltungen, Standort- und Bewegungsinformationen, die gelesenen Nachrichten, die Aktivitäten im hauseigenen Newsfeed mitsamt der Frage, welche Beiträge wie lange gelesen wurden und natürlich mit welchem Gerät.³⁷ Mit der IP-Adresse werden Standortdaten jederzeit erhoben, unabhängig davon, ob man den Zugriff auf den Standort in den Berechtigungseinstellungen gewährt hat.

Mit dieser Vorgehensweise wird das eigene Nutzerprofil mit bestimmten Themen in Verbindung gebracht und die fortwährende Nötigung, seine Adressbücher hochzuladen oder die Handynummer anzugeben, soll nicht nur dazu dienen, Verbindungen zu anderen Mitgliedern herzustellen, sondern Daten über Nichtmitglieder zu generieren.³⁸ „Auch mit der Markierung Dritter in Fotos werden Informationen über Nichtmitglieder gesammelt. Unternehmen, die auf Facebook ihre Werbung zeigen wollen, können ihre Kundendatenbanken in Facebook einspeisen, damit diese mit bestehenden Facebook-Profilen abgeglichen werden.“³⁹

d) Mini-Programm

Vorsicht gilt auch außerhalb von Facebook. Dass der Like-Button auf den meisten Internetseiten keineswegs nur einer harmlosen Bezeugung des Gefallens dient, ist den meisten Menschen bekannt. Hinter dem verbirgt sich ein Mini-Programm, das von Facebook nachgeladen wird und die betreffende Seite, Cookies sowie die Sitzungs-ID der gegebenenfalls bei Facebook angemeldeten Person sendet.⁴⁰ „Ist der Besucher der Seite nicht bei Facebook angemeldet, wird ein zwei Jahre gültiges Cookie gesetzt, das bei jeder weiteren Verbindung nach Amerika geschickt wird. So kann Facebook den Besucher der betreffenden Seite gegebenenfalls später einer Person zuordnen, nämlich wenn sie sich auf dem Gerät anmeldet.“⁴¹

Mit der aktuell laufenden Werbekampagne möchte Facebook allerdings den Eindruck erwecken, dass jeder Nutzer jederzeit die volle Kontrolle über die Verbreitung seiner Beiträge besitzt. In diesem Sinne ist es der Nutzer, der bestimmt, wie was verbreitet wird, welche Mitglieder oder Gruppen daran teilhaben bzw. Zugriff darauf erlangen; und dem Nutzer ist es

³⁷ Vgl.: (Spehr, 2016)

³⁸ Vgl.: (Spehr, 2016)

³⁹ (Spehr, 2016)

⁴⁰ Vgl.: (Spehr, 2016)

⁴¹ (Spehr, 2016)

möglich, sofort unerwünschte und versehentliche Veröffentlichung zu löschen. Sind diese entsprechenden Einstellungen tatsächlich nur Placebo-Pillen, die an der Datensammelwut des Imperiums nicht einmal kratzen, weil die Privatsphäre-Funktionalität bloß die Sichtbarkeit eigener Daten gegenüber anderen betrifft? „Was dem Facebook-Nutzer in Gänze vorenthalten wird, ist jedweder Einblick in die Rückschlüsse und Erkenntnisse, die Facebook aus dem Nutzerverhalten generiert hat. Die vom Nutzer selbst hochgeladenen Informationen sind nur ein kleiner Bruchteil dessen, was Facebook über ihn weiß.“⁴²

e) **Daten bleiben**

Jeder Nutzer von sozialen Netzwerken beschäftigt sich früher oder später mal mit der Frage: Sollte ich mein Konto löschen und was bedeutet die Löschung für mich? Denn selbst eine Kontolöschung bei Facebook bedeutet lediglich, dass die vom Nutzer erstellten Beiträge gelöscht werden, dass die über ihn erhobenen Informationen ebenfalls getilgt werden, ist unwahrscheinlich. „Fachleute nehmen an, dass Facebook ohnehin nie etwas löscht, sondern mit Löschvermerken arbeitet, also nur Markierungen setzt, dass etwas als gelöscht zu gelten hat. Die Daten bleiben.“⁴³

Facebook sammelt Daten nicht allein in seinem eigenen Ökosystem, sondern auch mit Hilfe seiner Tochterunternehmen. Aktuell wurde die Weitergabe von Telefonnummern und Nutzungszeiten von Whatsapp an Facebook in Europa vorübergehend stillgelegt. Doch das ebenfalls zum Konzern gehörende Instagram sammelt weiterhin fleißig und reicht laut eigener Datenschutzbestimmungen Cookies, Protokolldateien, Gerätekennungen sowie Ortungs- und Nutzungsdaten an Facebook weiter.⁴⁴ Der nächste geplante Schritt ist Free Basics. Hinter dieser Idee verbirgt sich der Gedanke, dass in Afrika, Ostasien und Lateinamerika unentgeltlich mobil im Netz gesurft werden kann, allerdings nur auf von Facebook und einigen anderen Seiten ausgewählten Websites.⁴⁵ Facebook stellt sich damit gegen das freie und offene Internet und untersagt den Einsatz von Verschlüsselungsprotokollen wie HTTPS. Indien hat das Programm bereits verboten, weil es die Netzneutralität verletzt. In den Geschäftsbedingungen von Free Basic nimmt sich Facebook das Recht, als Internet-

⁴² (Spehr, 2016)

⁴³ (Spehr, 2016)

⁴⁴ Vgl.: (Spehr, 2016)

⁴⁵ Vgl.: (Spehr, 2016)

Zugangspvovider nahezu alle verfügbaren Informationen der Nutzer zu verwenden, selbst die Batteriestärke des eingesetzten Geräts.⁴⁶

f) Möglichkeit der Anonymisierung?

Der einfachste Weg, Facebook so wenig personenbezogene Informationen wie möglich zu generieren, ist der, es in einer geschlossenen Umgebung laufen zu lassen, sprich abgeschottet und nicht permanent eingeloggt. Auf dem PC wäre es notwendig, einen zweiten Browser, in dem nichts Persönliches gespeichert ist, zu verwenden. „Wer mit Chrome arbeitet, nehme Firefox - und umgekehrt.“⁴⁷ Mit dem Nutzen des „anonymen“ Browserfensters öffne man Facebook, erledige das, was zu tun ist und meldet sich wieder ab. So wäre dafür gesorgt, dass der Browser nach dem Schließen sämtliche Cookies, sowie weitere Chroniken oder Spuren löscht.⁴⁸

„Smartphone-Apps lassen sich in ihrer Neugier nicht einfach bremsen. Wer es richtig machen will, installiert Facebook auf einem zweiten Smartphone, das keine eigenen Daten, Konten, Adressbücher, E-Mails enthält. Was Facebook interessiert, lässt sich auf den mobilen Plattformen in den Einstellungen für die App-Berechtigungen einsehen. Facebook fordert den Zugriff auf so gut wie alles und überträgt zum Beispiel, wie eine Kontroll-Software für den Datenverkehr zeigt, auch so gut wie alles im Minutentakt nach Amerika. Insbesondere den eigenen Standort. Mit der „laufenden Synchronisierung“ werden neben den eigenen Daten auch jene von Dritten an Facebook gesendet; in diesem Fall das Adressbuch mitsamt Details. Ein europäischer Facebook-Nutzer müsste jeden seiner Kontakte fragen, ob er einverstanden ist, dass seine Daten an Facebook weitergeleitet werden.“⁴⁹

Im Sommer 2016 machte ein Bild Schlagzeilen die Runde, das Facebook-Gründer und -Chef Mark Zuckerberg in seinem Hauptquartier zeigt. Im Hintergrund ist der Schreibtisch mit seinem Notebook zu sehen, zu sehen sind zwei Details: Das Mikrofon links und die Kamera über der Anzeige sind abgeklebt. Eine sehr aufschlussreiche analoge Abwehr digitaler Spähangriffe.⁵⁰

⁴⁶ Vgl.: (Spehr, 2016)

⁴⁷ (Spehr, 2016)

⁴⁸ Vgl.: (Spehr, 2016)

⁴⁹ (Spehr, 2016)

⁵⁰ (Spehr, 2016)

g) Datenverkehr mit Drittstaaten

Auf Grund der Tatsache, dass das Internet den Unternehmen die Möglichkeit bietet, seine Server weltweit so zu platzieren, wie die örtlichen Datenschutzrichtlinien am besten dem Geschäftsmodell entsprechen, sind die Datenströme im Internet kaum zu kontrollieren. „Doch auch für die Seitenbetreiber stellt dies eine Herausforderung dar. So soll die Seite in möglichst vielen Ländern gleich oder zumindest ähnlich betrieben werden und die Konnektivität sichergestellt sein.“⁵¹ Jedoch unterscheiden sich die gesetzlichen Vorgaben teilweise zu deutlich voneinander. Speziell der nordamerikanische Raum kann als eher datenschutzunfreundlich beurteilt werden, während in weiten Teilen Europas ein größeres Bewusstsein für die Datensicherheit besteht.⁵² Im Vergleich dazu bieten autoritäre Staatsformen wie China eine ganz andere Herausforderung. Insbesondere Newsportale, Blogs und Suchmaschinenbetreiber können zur Zielscheibe der staatlichen Zensur werden. Ebenso kann die digitale Infrastruktur eines Landes, wie beim Georgienkonflikt, den Attacken fremder Mächte zum Opfer fallen.⁵³ Aus diesem Grund sind Organisationen wie Anonymus in der Lage, einzelne Seiten anzugreifen. Je nach Weltregion finden die Seitenbetreiber unterschiedlichste Bedingungen vor. „Unternehmen, die ein Interesse an möglichst großen Datenbeständen haben, sind so auf der einen Seite an politisch stabilen Verhältnissen und auf der anderen an weniger strikten Datenschutzgesetzen interessiert.“⁵⁴ Die Schnittmenge der in Betracht kommenden Staaten ist überschaubar. Der Datenverkehr selbst ist auch in einem globalen Netz keineswegs ungeklärt, so heißt es im BDSG §1 Abs. 5: „Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle die nicht in einem Mitgliedstaat der EU [...] zu belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt.“ Noch deutlicher ist die Datenschutz-Grundverordnung in Art. 3 Abs. 2: „Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen.“ Art. 25 sagt weiter, dass jeder in einem Drittland, das laut Beschluss der Kommission keinen angemessenen Schutz im Sinne von Art. 41 bietet, ansässigen Verantwortlichen einen Vertreter in der Union benennen muss. Art. 41 bewertet, ob ein angemessener Schutz vorliegt danach, ob unabhängige Aufsichtsbehörden sowie Rechtsstaatlichkeit in den betreffenden Drittländern oder Organisationen gegeben sind.

⁵¹ (Schulze, 2013)

⁵² Vgl.: (Schulze, 2013)

⁵³ Vgl.: (Schulze, 2013)

⁵⁴ (Schulze, 2013)

5. Suchen ohne Schnüffler

Wer nicht möchte, dass personenbezogene Daten durch Suchmaschinen erhoben werden, hat immer noch die Möglichkeit seinen Suchanbieter zu wechseln, denn auf dem Markt sind nicht nur Google, Bing oder Yahoo.

Anders als Google speichert die niederländische Suchmaschine Startpage by Ixquick weder die IP-Adresse des Users (anhand der User eindeutig identifizierbar sind), noch den genutzten Browser oder die eigentliche Suchanfrage.⁵⁵ Abgesehen davon, wird die Suchanfrage nach dem besonders sicheren Perfect Forward Secrecy-Verfahren verschlüsselt. Das stellt sicher, dass keine anderen Webseiten und nicht einmal die NSA das Surfverhalten verfolgen können.⁵⁶



Abbildung 3 ixquick Logo

„Search anonymously, find instantly" lautet das Motto von DuckDuckGo und das bedeutet: Wie Startpage speichert die Seite keine Suchergebnisse, keine IP-Adresse und auch nicht den genutzten Browser. Auch hier werden die bei einer Suchanfrage trotzdem anfallenden Daten nach dem besonders sicheren Perfect Forward Secrecy-Verfahren verschlüsselt.“⁵⁷



Abbildung 4 DuckDuckGo Logo

„Die deutsche Suchmaschine YaCy geht einen komplett anderen Weg als der Rest im Suchmaschinen-Business und speichert die Software und den Suchindex dezentral auf der Festplatte eines jeden Users, statt auf zentralen Firmenservern. Die gesammelten Daten können also nirgends zentral eingesehen werden.“⁵⁸



Abbildung 5 YaCy Logo

⁵⁵ Vgl.: (Funk, 2017)

⁵⁶ Vgl.: (Funk, 2017)

⁵⁷ (Funk, 2017)

⁵⁸ (Funk, 2017)

C Datenschutz und Suchmaschinen

I. Was ist Datenschutz?

„Der Datenschutz beruht in Deutschland auf den beiden ersten Artikeln des Grundgesetzes (Art. 2 I GG, Art. 11 GG); das Bundesverfassungsgericht hat im sogenannten Volkszählungsurteil im Jahr 1983 daraus das „Recht auf informelle Selbstbestimmung“ abgeleitet.“⁵⁹ In den Datenschutzgesetzen des Bundes und der Länder sowie in Spezialgesetzen wie dem Telemediengesetz (TMG) oder dem Telekommunikationsgesetz (TKG) ist der Datenschutz im Einzelnen geregelt. Sinn dieser Gesetze ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.⁶⁰ Im wesentlichen dient der Datenschutz dazu, die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zu verhindern, es sei denn, es gibt eine klare Rechtsgrundlage oder der Einzelne gibt seine ausdrückliche Zustimmung (sogenanntes Verbotsprinzip mit Erlaubnisvorbehalt).

„Im Zusammenhang mit Suchmaschinen wird Datenschutz vor allem in Bezug auf die Zugriffsmöglichkeiten auf personenbezogene Daten und deren Verarbeitung diskutiert sowie in Bezug auf die Anwendbarkeit deutschen und europäischen Rechts auf internationale Suchmaschinenbetreiber.“⁶¹ Insbesondere werden durch den Datenschutz die Suchmaschinen in dem Sinne kritisiert, dass der Umgang mit Nutzerdaten intransparent ist. Viele Suchmaschinennutzer sind besorgt, dass mit der Verwendung einer Suchmaschine durch eine Suchanfrage individuelle Nutzerprofile erstellt werden und mit jeder weiteren Suchanfrage immer mehr Daten erhoben werden (Datenaggregation).⁶² Das Internet ist allgegenwärtig und beeinflusst die Art, wie wir arbeiten, wie wir Medien konsumieren und wie wir miteinander kommunizieren.⁶³ Im Laufe der Zeit wird die Notwendigkeit des Internets und den inbegriffenen Suchmaschinen für Wirtschaft, Universitäten, Schulen und viele weitere Lebensbereiche eine immer wichtigere Rolle spielen. Innerhalb von Sekunden ist es möglich für diverse Suchanfragen schier endlos viele Suchergebnisse zu finden, egal ob Videos zur Lieblingsband, Hotelanfragen für den nächsten Urlaub oder Rechercheanfragen. Das Internet bietet eine nahezu unbegrenzte Möglichkeit der Konnektivität. Allerdings sollte jeder sich vergegenwärtigen, dass der Großteil dieser Dienste nur durch das Erfassen, Auswerten und

⁵⁹ (klicksafe.de, 2016)

⁶⁰ Vgl.: (klicksafe.de, 2016)

⁶¹ (klicksafe.de, 2016)

⁶² Vgl.: (klicksafe.de, 2016)

⁶³ Vgl.: (klicksafe.de, 2016)

Bereitstellen von Daten ermöglicht wird. Andererseits stellt sich die Frage, welche Daten wie dauerhaft gesammelt werden und wie stark sie personalisiert sind.

II. Datenschutz = Persönlichkeitsrecht?

Das allgemeine Persönlichkeitsrecht ist die Grundlage des Datenschutzes. Ohne dieses Recht gäbe es den Datenschutz in der heutigen Form nicht.

Inhalt des allgemeinen Persönlichkeitsrechts ist die Achtung und Entfaltung der Persönlichkeit. 1954 wurde es vom Bundesgerichtshof entwickelt und stützt sich auf Art. 2 Abs. 1 GG (Freie Entfaltung der Persönlichkeit) in Verbindung mit Art. 1 Abs. 1 GG (Schutz der Menschenwürde).⁶⁴

Nach Auffassung des Bundesverfassungsgerichts ist Bestandteil des allgemeinen Persönlichkeitsrechts das Recht auf informationelle Selbstbestimmung, welches im Volkszählungsurteil des Bundesverfassungsgerichtes vom 15.12.1983 als Grundrecht anerkannt wurde. Danach hat der Einzelne das Recht, selbst über die Bekanntgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Wer das Grundgesetz liest, wird diesen Begriff darin vergeblich suchen. Der Begriffskomplex des Grundrechts auf informationelle Selbstbestimmung wird aus anderen Grundrechten abgeleitet, insbesondere aus der allerersten Regelung im Grundgesetz, „Die Würde des Menschen ist unantastbar“, und dem Grundrecht auf freie Entfaltung der Persönlichkeit in Artikel 2 GG.⁶⁵

Der Betroffene hat ein berechtigtes Interesse an der Vermeidung des Missbrauchs seiner persönlichen Daten. Daher ist die Beachtung der Gesetze und Vorschriften zum Datenschutz wichtig und auch notwendig.

„Auch in zehn Landesverfassungen finden sich ausdrückliche Regelungen zum Datenschutz. In den sechs Bundesländern Baden-Württemberg, Hamburg, Hessen, Niedersachsen, Schleswig-Holstein und Bayern gibt es keine. Aber auch dort existieren Landesdatenschutzgesetze.“⁶⁶

Der Datenschutz in allen ostdeutschen Ländern wird in ihren Verfassungen geregelt. „Bei der Verabschiedung dieser Verfassungen nach der politischen Wende 1989/1990 war der

⁶⁴ Vgl.: (DPN Datenschutz GmbH & Co. KG)

⁶⁵ Vgl.: (heise online)

⁶⁶ (heise online)

Datenschutz bereits gut entwickelt und seine überragende Bedeutung bekannt. Bei der Verabschiedung der Verfassungen der "alten Bundesländer" nach dem zweiten Weltkrieg war dies noch nicht der Fall. Nur in einzelnen Fällen gab es später Nachbesserungen.“⁶⁷

„In Österreich und der Schweiz existieren ebenfalls Datenschutzgesetze. Die Rechtslage insbesondere in der Schweiz ist in vielen Bereichen mit derjenigen in Deutschland vergleichbar. Auch dort wird auf Bundesebene der Datenschutz für die Bundesbehörden und der Umgang privater Unternehmen mit Daten geregelt. Alles andere legen die Datenschutzgesetze auf Kantonsebene fest. Auch in Österreich stößt man auf aus deutscher Sicht bekannte Regelungen. Dies hat damit zu tun, dass das Datenschutzrecht innerhalb der EU weitgehend harmonisiert ist.“⁶⁸

Nur wenige wissen, dass in Deutschland die staatlichen Datenschutzbestimmungen nicht im kirchlichen Bereich gelten. So haben die evangelische und die römisch-katholische Kirche ihre eigenen Datenschutzbestimmungen erlassen, was zum Beispiel beim Outsourcing im kirchlichen Bereich schon eine Rolle gespielt hat.⁶⁹ Sie sind mit denen des Bundesdatenschutzgesetzes weitgehend identisch. Hinzu kommen aber Regelungen zum umfassend geschützten Beichtgeheimnis.

Datenschutz ist ein relativ junges Rechtsgebiet. In Deutschland verabschiedete Hessen das erste Datenschutzgesetz im Jahr 1970. Sieben Jahre später folgte mit dem Bundesdatenschutzgesetz eine bundesweite Regelung. Und erst 1981 gab es in jedem Bundesland ein Gesetz für die Belange des Datenschutzes, die in die Kompetenz der Länder fallen und nicht bereits durch das BDSG geregelt waren, also etwa der Umgang mit Daten durch die Landesverwaltungen.⁷⁰

1. Im Spannungsfeld von Datenschutz und Persönlichkeitsrecht – Spickmich-Urteil

Eine richtungsweisende Entscheidung traf der BGH 2009 mit dem „Spickmich“-Urteil zur gleichnamigen Lehrerbewertungsplattform. „Im Rahmen der Frage, ob betroffene Lehrer ein Lösungsanspruch aus § 35 Abs. 2 S. 2 Nr. 1 BDSG zusteht, wägt der BGH das Recht auf informationelle Selbstbestimmung mit den Kommunikationsfreiheiten ab und kam zu dem

⁶⁷ (heise online)

⁶⁸ (heise online)

⁶⁹ Vgl.: (heise online)

⁷⁰ Vgl.: (heise online)

Entschluss, dass kein Anspruch auf Löschung bestehe.“⁷¹ Hierbei gab das Gericht zu bedenken, dass mit der Einführung der relevanten Normen im BDSG die Bewertung in Internet-Bewertungsportalen weder technisch möglich war, noch für denkbar gehalten wurde.⁷² Deshalb müsse das Gesetz verfassungskonform ausgelegt werden, sodass das Grundrecht der Meinungsfreiheit im Internetzeitalter ausreichend berücksichtigt wird. Der Einzelne habe dabei keine absolute, uneingeschränkte Herrschaft über seine Daten, denn er entfalte seine Persönlichkeit innerhalb der sozialen Gemeinschaft.⁷³ Eine Einschränkung des Rechts auf informationelle Selbstbestimmung müsse deshalb hingenommen werden, wenn und soweit solche Beschränkungen von hinreichenden Gründen des Gemeinwohls oder ein überwiegendes Rechtsinteressen Dritter besteht und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und die Grenze des Zumutbaren noch gewahrt ist.⁷⁴

2. Welche Informationen findet eine Suchmaschine über mich?

„Viele Nutzer sind erstaunt, wenn sie die Ergebnisse einer Suche nach ihrem eigenen Namen sehen. Für jeden auffindbar sind Informationen, wie das Alter, die besuchte Schule, die Adresse, Freunde aus Chatforen oder die Partybilder des letzten Wochenendes.“⁷⁵ Die gesamten auffindbaren Daten kommen nicht von nirgendwo, jeder Nutzer hat die Informationen irgendwo im Internet eingegeben, z.B. auf den Seiten von Sozialen Netzwerken. Die Daten sind dann oft lange Zeit über Suchmaschinen für jeden auffindbar. Jeder Einzelne sollte sich deshalb überlegen, welche Daten er eingibt bzw. welche Daten er von einer Suche ausschließt.⁷⁶

a) Daten im Netz

Eine Suchmaschine stellt Informationen über eine Person nicht selbst bereit, sondern findet und stellt lediglich solche Informationen zusammen, die auf Webseiten von Dritten veröffentlicht sind.⁷⁷ Sollte man Informationen über sich selbst finden, die entfernt werden sollen, muss man sich daher immer zuerst an denjenigen wenden, der diese Information veröffentlicht hat, also an den Webmaster der fraglichen Seite.⁷⁸

⁷¹ (Vogt, 2016)

⁷² Vgl.: (Vogt, 2016)

⁷³ Vgl.: (Vogt, 2016)

⁷⁴ Vgl.: (Vogt, 2016)

⁷⁵ (klicksafe.de, 2016)

⁷⁶ Vgl.: (klicksafe.de, 2016)

⁷⁷ Vgl.: (klicksafe.de, 2016)

⁷⁸ Vgl.: (klicksafe.de, 2016)

b) Was geschieht mit den Informationen, die eine Suchmaschine bei einer Suche erfasst?

Mit Hilfe von Protokolldaten und Cookies entwickeln sich Suchmaschinen permanent weiter. Sie führen zu der Verbesserung der Suchergebnisse, dienen der Entwicklung hilfreicher Dienste für den Nutzer, wie z.B. die Rechtschreibprüfung oder die Autocomplete-Funktion.

Abgesehen davon sind die erhobenen Daten nützlich, Suchmaschinen vor Betrug und anderem Missbrauch zu schützen, vor sogenanntem Suchmaschinen-Spam. Mit Protokolldaten und Cookies kann ein solcher Spam erkannt und gegebenenfalls zum Verursacher zurückverfolgt werden.

Des Weiteren dienen Protokolldaten und Cookies dazu, Werbeanzeigen zu personalisieren und zielgerichtet auf den Nutzer anzupassen.

c) Digitale Demenz

Das Internet vergisst nichts! So heißt es und so sprechen die meisten Menschen über das Internet, doch ist das eine Fehlinformation. In Wahrheit vergisst das Internet heute schneller, als die Daten damals hochgeladen wurden.⁷⁹ Nach einer Studie der US-Informatiker

Hany M. Salah-Eldeen und Michael L. Nelson vergisst das Netz nicht nur, es vergisst inzwischen schneller, als es seinerseits gedauert hat, Informationen einzustellen.⁸⁰

Salah-Edeen und Nelson stellten fest, dass nach einem Jahr rund elf Prozent der Quellen verschwunden waren und nach zweieinhalb Jahren bereits 27 Prozent des geprüften Materials nicht mehr auffindbar waren. Jason Henessy und Steven Xijin Gevon der Universität South Dakota ermittelten bei ihrer Analyse ähnliche Werte. Sie analysierten ca. 15.000 Links in wissenschaftlichen Arbeiten; dabei waren mehr als ein Drittel aller getesteten Links nicht auffindbar. Daraufhin berechneten die beiden Forscher die durchschnittliche Lebensdauer einer Internetseite mit der Ergebnis, sie würde weniger als 10 Jahren existieren.⁸¹

In der Wissenschaft sind „verrottende Daten“ ein Problem, privat ein Segen?

d) Was steckt hinter all dem?

Abgesehen davon, dass personenbezogen Daten erhoben werden, stellt sich die Frage, wie sicher sind diese Daten und wer hat bzw. kann Zugriff darauf nehmen.

⁷⁹ Vgl.: (Könau, 2017)

⁸⁰ Vgl.: (Könau, 2017)

⁸¹ Vgl.: (Könau, 2017)

Im August 2006 erregte der America Online (AOL) Privacy-Skandal die Gemüter der Online-Welt. AOL veröffentlichte zu diesem Zeitpunkt die Datenbankinhalte der letzten 3 Monate und damit die Suchdaten von 650.000 ihrer User. Die veröffentlichten Inhalte der Datenbank sind nach wie vor für jeden aufrufbar.

e) **America Online (AOL) Privacy-Skandal**

Der Internetanbieter AOL veröffentlichte im August 2006 eine Liste mit über 20 Millionen Suchbegriffen, die über 650.000 Nutzer in einem Zeitraum von drei Monaten eingegeben hatten.⁸² In der Liste waren eigentlich anonyme Nutzerdaten enthalten, die zu Forschungszwecken verwendet sollten. Stattdessen bestand die Liste aus zahlreichen, persönlichen Informationen, die man ohne weiteres konkreten Nutzern und deren Suchprotokoll zuordnen konnte.⁸³ Innerhalb von drei Tagen wurde die Liste von AOL von seiner Website entfernt. Allerdings waren zu diesem Zeitpunkt die Daten auf diversen anderen Seiten im Netz einsehbar. Maureen Govern, damaliger CTO von AOL, trat zwei Wochen nach diesem Vorfall zurück. Im September 2006 ging eine Sammelklage gegen AOL ein.

D) Das Recht auf Vergessenwerden

Das Recht auf Vergessenwerden bzw. verkürzt das Recht auf Vergessen soll sicherstellen, dass digitale personenbezogene Daten nicht dauerhaft zur Verfügung stehen. Der allgemeine Konsens besteht darin, dass der Verbraucher ein Recht haben sollte, seine Daten auf Verlangen löschen zu lassen und von der weiteren Verwendung und Verbreitung abgesehen wird.⁸⁴ Der Begriff des Rechts auf Vergessenwerden geht auf den Rechts- und Politikwissenschaftler Viktor Mayer-Schönberger zurück, der vorschlägt, digitale Daten mit einem Ablauf- bzw. Verfallsdatum zu versehen, so dass die Daten nach Ablauf des Datums durch ein Programm oder das Betriebssystem des Computers automatisch gelöscht werden. Da für das Recht auf Vergessen keine einheitliche Definition gegeben ist, ist das im Art. 17 der Datenschutz-Grundverordnung erwähnte Recht auf Vergessenwerden inhaltlich von den Ausführungen Viktor Mayer-Schönbergers zu unterscheiden. Wie bereits beschrieben, ähneln sich die Aussagen des Art. 17 der Datenschutz-Grundverordnung mit den Aussagen Viktor Mayer-Schönbergers, allerdings besteht der Unterschied darin, dass Viktor Mayer-Schönberger von der Möglichkeit ausgeht, Daten mit einem Verfallsdatum zu kodieren und somit eine ganze Ausgangssituation schafft.

⁸² Vgl.: (Fiutak, 2006)

⁸³ Vgl.: (Spiegel Online, 2006)

⁸⁴ Vgl.: (Schulze, 2013)

I. Löschpflichten und Löschantrag Art. 17 EU-DSGVO

Die Datenschutz-Grundverordnung nimmt sich der Frage nach dem Recht auf Vergessenwerden an. Im Gegensatz zur Richtlinie 95/46/EG und zum BDSG wird es hier explizit als solches erwähnt. Das in der Datenschutz-Grundverordnung aufgeführte Recht auf Vergessenwerden und auf Löschung ist wie folgt in Art. 17 definiert:

1. *Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:*
 - a) *Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.*
 - b) *Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.*
 - c) *Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.*
 - d) *Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.*
 - e) *Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.*
 - f) *Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.*

Zusammengefasst bedeutet Absatz 1, dass die betroffene Person das Recht besitzt, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten.

In Absatz 2 erläutert die Verordnung dem Verbraucher die Möglichkeit, die Verbreitung sowie den Handel mit seinen Daten zu unterbinden oder wenigstens zu beschränken.

2. *Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.*

Abgesehen davon beschreibt der Absatz 3, dass Daten aufgrund der Erfüllung gesetzlicher Pflichten, des öffentlichen Interesse oder aus Gründen wissenschaftlicher Forschung die Speicherung personenbezogener Daten notwendig machen.

3. *Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist*
- a) *zur Ausübung des Rechts auf freie Meinungsäußerung und Information;*
 - b) *zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;*
 - c) *aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;*
 - d) *für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder*
 - e) *zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.*

1. Wie ist der Löschantrag geltend zu machen?

Zu Beginn muss die betroffene Person Kenntnis über die gespeicherten Daten haben. Dazu besteht nach Art. 15 DSGVO das Auskunftsrecht.⁸⁵

Dem folgend, sollte die betroffene Person einen Antrag auf Löschung bei dem Verantwortlichen stellen; dazu wird empfohlen, einen Antrag zusätzlich schriftlich oder per E-Mail zu stellen.⁸⁶

In diesem Zusammenhang ist es erforderlich, die Identität der betroffenen Person nachzuweisen, da anderenfalls nach Art. 12 Abs. 6 DSGVO erst noch zusätzliche Informationen vom Verantwortlichen angefordert werden können oder die Löschung nach Art. 12 Abs. 2 Satz 2 DSGVO verweigert werden kann.⁸⁷

Wird die Löschung abgelehnt, ist dies vom Verantwortlichen zu begründen. Auf die Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde und auf einen gerichtlichen Rechtsbehelf ist hinzuweisen.

2. Wann ist zu löschen?

Nachdem die oben genannten Voraussetzungen erfüllt sind, sind die Daten unverzüglich zu löschen. Nach Antrag des Betroffenen oder nach Vorliegen des Löschantrags darf die Löschung nicht länger als unbedingt nötig hinausgezögert werden.⁸⁸

⁸⁵ Vgl.: (Dr. Datenschutz (Pseudonym), 2017)

⁸⁶ Vgl.: (Dr. Datenschutz (Pseudonym), 2017)

⁸⁷ Vgl.: (Dr. Datenschutz (Pseudonym), 2017)

⁸⁸ Vgl.: (Dr. Datenschutz (Pseudonym), 2017)

„Bei einem Löschungsantrag des Betroffenen ist allerdings in jedem Fall zu beachten, dass spätestens innerhalb eines Monats nach Eingang des Löschungsantrags die betroffene Person über die ergriffenen Maßnahmen bzw. über die Gründe der Ablehnung informiert werden muss. Gegebenenfalls müssen Verlängerungsmöglichkeiten ausgeschöpft werden.

Unabhängig von einem Löschungsantrag ist zukünftig aber auch zu beachten, dass zwischen der Kenntnisnahme vom Löschungsgrund und dem Tätig werden des Verantwortlichen kein schuldhaftes Zögern vorliegen darf. Der Verantwortliche hat deshalb regelmäßig zu prüfen, ob ein Löschungsgrund vorliegt.“⁸⁹

3. Mitteilungs- und Informationspflichten

Laut Art. 19 DSGVO gilt mit Bestehen der Löschungspflicht eine umfassende Mitteilungspflicht. So sind alle Empfänger von Daten über die Löschung zu informieren. Insofern der Verantwortliche die personenbezogenen Daten veröffentlicht hat und zur Löschung verpflichtet ist, sind zukünftig auch Informationspflichten zu beachten, damit die Rechte der betroffenen Person umfassend und effektiv gewahrt werden.⁹⁰ Der Verantwortliche ist somit verpflichtet, durch angemessene Maßnahmen alle Adressaten zu informieren, dies kann durchaus auch Adressaten außerhalb der EU betreffen. Eine Umsetzung ist insbesondere möglich⁹¹:

- durch Veröffentlichung der Löschung auf der Webseite des Verantwortlichen bzw. an der Stelle, an der die Daten zunächst veröffentlicht wurden
- technisch, beispielsweise durch Meta-Tags
- Techniken, die dem „Digital Rights Management“ (DRM) ähnlich sind (allerdings strittig)

„Eine Konkretisierung wird gemäß Art. 70 Abs. 1 lit d) DSGVO durch den Europäischen Datenschutzausschuss erfolgen, der Leitlinien, Empfehlungen und bewährte Verfahren „für die Löschung gemäß Art. 17 Abs. 2 DSGVO von Links zu personenbezogenen Daten oder Kopien oder Replikationen dieser Daten aus öffentlich zugänglichen Kommunikationsdiensten“ zur Verfügung stellen soll.“⁹² Insofern werden Anhaltspunkte

⁸⁹ (Dr. Datenschutz (Pseudonym), 2017)

⁹⁰ Vgl.: (Dr. Datenschutz (Pseudonym), 2017)

⁹¹ (Dr. Datenschutz (Pseudonym), 2017)

⁹² (Dr. Datenschutz (Pseudonym), 2017)

gegeben, die helfen, zu erkennen, welche Maßnahmen für die Umsetzung der Pflichten aus Art. 17 Abs. 2 DSGVO zur Verfügung stehen.

4. Ausnahmen von der Löschpflicht⁹³

Von der Löschungspflicht gibt es Ausnahmen. Eine Löschungspflicht besteht nicht,

- soweit die Verarbeitung erforderlich ist
- bei Ausübung des Rechts auf freie Meinungsäußerung und Information
- zur Erfüllung einer Rechtspflicht oder öffentlicher Aufgaben
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- bei im öffentlichen Interesse liegenden Archivzwecken, Forschungszwecken und statistischen Zwecken
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

5. Irrtümer des Rechts auf Vergessen

a) Inhalte werden nicht gelöscht. Die betroffenen Seiten bleiben weiterhin online.

Der europäische Gerichtshof erklärte in seinem Urteil, dass Links entfernt werden müssen, „auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden“.⁹⁴

Beispiel:

Für den Wikipedia-Eintrag zu Gerry Hutch (angeblich Irlands erfolgreichster Bankräuber) würde dies bedeuten, dass dieser Eintrag dort nicht verschwinden wird, wohl aber das Suchergebnis.⁹⁵

b) Die betroffene Seite wird nicht aus den Suchergebnissen „gelöscht“

In dem Urteil des europäischen Gerichtshofs wurde nicht die Löschung von Links erwähnt. Allein Suchergebnisse, die anhand der Suche des Namens angezeigt werden, sind zu

⁹³ Vgl.: (Dr. Datenschutz (Pseudonym), 2017)

⁹⁴ Vgl.: (Fiedler, 2014)

⁹⁵ Vgl.: (Fiedler, 2014)

entfernen, nicht zu löschen. Die betroffenen Seiten bleiben weiterhin in Googles Cache und Index.⁹⁶

c) Die betroffene Seite bleibt weiterhin auffindbar

„Sobald eine Suche nicht anhand des Namens der Person, wohl aber über die Eingabe anderer Suchbegriffe durchgeführt wird, wird die betroffene Seite weiterhin in den Ergebnissen aufgelistet. In einer Pressemitteilung erklärte der Europäische Gerichtshof, dass Suchergebnisse, die anhand eines Namens angezeigt werden, entfernt werden können, solange die Daten nicht länger für den Zweck erheblich sind oder darüber hinausgehen, nicht auf den neuesten Stand gebracht sind oder länger als erforderlich aufbewahrt werden.“⁹⁷

Beispiel:

Bei einer Suche des Namens Gerry Hutch würde nun die Wikipedia-Seite nicht mehr angezeigt werden. Allerdings mit dem Suchbegriff “Wikipedia Irish bank robberies” würde die Webseite weiterhin in den Ergebnissen auftauchen.⁹⁸

d) Die Suchergebnisse werden allein in den europäischen Versionen der Suchmaschinen entfernt

Alle Suchergebnisse, die von Google, Bing oder anderen Suchmaschinen in Europa entfernt werden müssen (bsp. auf google.de), sind bei „google.com“ oder „bing.com“ weiterhin zu finden.

Beispiel:

Wenn Gerry Hutch in google.co.uk eingegeben wird, soll die Wikipedia-Seite aus den Suchresultaten entfernt werden. Für eine identische Suche bei google.com wird die Wikipedia-Seite aber weiterhin in der Liste der Suchergebnisse angezeigt.⁹⁹

e) Das „Recht auf Vergessenwerden“ ist keine neue Erfindung

Das Recht auf Löschung gibt es schon seit der Datenschutzrichtlinie von 1995. Neu ist, dass der Europäische Gerichtshof nun eine Suchmaschine als Verantwortlichen ansieht. Im Fall

⁹⁶ Vgl.: (Fiedler, 2014)

⁹⁷ (Fiedler, 2014)

⁹⁸ Vgl.: (Fiedler, 2014)

⁹⁹ Vgl.: (Fiedler, 2014)

Google-Spanien versuchte Google zunächst zu argumentieren, dass die Firma nicht verantwortlich sein kann, da sie keine Kenntnis von den personenbezogenen Daten und keine Kontrolle über sie habe¹⁰⁰. Der Gerichtshof erkannte, dass es sich hier nicht um ein reines Hosting handelt, sondern darum, dass Google personenbezogene Daten sekundenschnell aus verschiedenen Quellen zusammenführt, neue Profile bildet und so viel tiefer in Persönlichkeitsrechte eingreift, als dies durch eine normale Veröffentlichung der Fall wäre und in der Verbindung personenbezogene Urteile trotz Unkenntnis gezogen werden.

„Die neue Wikimedia-Geschäftsführerin Lila Tretikov bemängelte, dass es nun keine öffentliche Erklärung, keine Beweiserbringung, keine richterliche Überprüfung und kein Beschwerdeverfahren für die Manipulation der Suchergebnisse gibt.“¹⁰¹ Der EuGH überlässt es einem privaten Unternehmen, intransparente Entscheidungen darüber zu treffen und abzuwägen, welche Suchergebnisse wie beeinflusst werden sollen.

Gleichzeitig werden Suchergebnisse per Definition manipuliert; es gibt keinen natürlichen Zustand.

Google wendet seit mehr als zehn Jahren US-amerikanisches Urheberrecht an und lässt Suchergebnisse bei mutmaßlichen Urheberrechtsverletzungen verschwinden.

6. Verfallsdatum für digitale Daten

Viktor Mayer-Schönberger sieht die Gefahren, die vom Datensammeln im Netz ausgehen, „quite literally, Google knows more about us than we can remember ourselves“¹⁰². In diesem Zusammenhang erklärt er, wie wichtig das Vergessen für das menschliche Zusammenleben ist.¹⁰³ „So begegnen wir einem alten Bekannten nach Jahren anders, da wir zwar viele der guten Erinnerungen behalten, aber die negativen Ereignisse verdrängt hätten.“¹⁰⁴ Angenommen, wir würden als sogenannte digitale Gedächtnisstütze alte Nachrichten lesen und in diesem Zusammenhang auf negative Informationen stoßen, würden wir voreingenommen sein, wenn wir nun auf diesen alten Bekannten treffen. Das Vergessen dient zum Selbstschutz, aber auch als Neustartfunktion, sowohl für zwischenmenschliche Beziehungen, als auch für das gesellschaftliche Zusammenleben.¹⁰⁵ Für jedes Individuum ist

¹⁰⁰ Vgl.: (Fiedler, 2014)

¹⁰¹ (Fiedler, 2014)

¹⁰² (Mayer-Schönberger, 2009) S. 7

¹⁰³ Vgl.: (Schulze, 2013)

¹⁰⁴ (Schulze, 2013)

¹⁰⁵ Vgl.: (Schulze, 2013)

es bedeutsam, dass die Gesellschaft vergisst, z.B. bei Straftaten oder auch nur bei unbedachten Äußerungen, „often such social forgetting gives individuals who have failed a second chance.“¹⁰⁶ Vergessen bedeutet sich geistig auf die Gegenwart zu konzentrieren. „Through perfect memory we may lose a fundamental human capacity – to live and act firmly in the present“¹⁰⁷. Er sieht zwar auch das, was das BVerfGE in seiner Urteilsbegründung zum Volkszählungsurteil 26 Jahre zur ebenfalls als Bedrohung für das Persönlichkeitsrecht wertete: „If we had to worry that any information about us would be remembered for longer than we live, would we still express our views [...] share personal experiences, make various political comments, or would we self-censor?“¹⁰⁸. „I act s I am watched even if I am not“¹⁰⁹. Während die Datenschutz-Grundverordnung eine Löschung personenbezogener Daten auf Verlangen des Betroffenen vorsieht, schlägt Mayer-Schönberger ein Verfallsdatum für Daten im Netz vor. „Er sieht als notwendigen Schritt die Wiederetablierung des Vergessens im digitalen Zeitalter.“¹¹⁰

„One possible way we can mimic human forgetting in the digital realm is by associating information we store in digital memory with expiration dates that users set. Our digital storage devices would be made to automatically delete information that has reached or exceeded its expiry date.“¹¹¹

In der Realität wird wohl kaum ein Unternehmen absichtlich Geräte entwickeln bzw. verwenden, die Daten löschen. Denn letzten Endes genießt auch jeder Konsument die omnipräsente Verfügbarkeit von Informationen jedweder Art. Die derzeitige Haltung einer Mehrheit der Gesellschaft lässt sich am treffendsten mit den Worten des italienischen Semiotikers Umberto Eco beschreiben: „Kultur ist nicht, zu wissen, wann Napoleon gestorben ist. Kultur bedeutet zu wissen, wie ich es in zwei Minuten herausfinden kann.“^{112, 113}

II. Vereinbarkeit mit dem Grundrecht

Als gesellschaftsrelevante Frage stellt sich nun, ob das Recht auf Vergessenwerden als Grundrecht deklariert werden kann. Um dem eine Antwort geben zu können, besteht die Notwendigkeit darin, nationale wie europäische Gesetze zu betrachten. Zum

¹⁰⁶ (Mayer-Schönberger, 2009) S. 13

¹⁰⁷ (Mayer-Schönberger, 2009) S. 12

¹⁰⁸ (Mayer-Schönberger, 2009) S. 5

¹⁰⁹ (Mayer-Schönberger, 2009) S. 11

¹¹⁰ (Schulze, 2013)

¹¹¹ (Mayer-Schönberger, 2009) S. 171

¹¹² (Beyer & Gorris, 2009)

¹¹³ Vgl.: (Schulze, 2013)

Grundverständnis wird im ersten Schritt geklärt, was unter einem Grundrecht zu verstehen ist. In der von der Bundeszentrale für politische Bildung (bpb) herausgegebenen Zeitung „Informationen zur politischen Bildung“ (Heft 305) schrieb Gudula Geuther (rechts- und innenpolitische Korrespondentin des Deutschlandfunks und Deutschlandradios Kultur) „Unter Grundrechten verstehen [wir], verbriefte Rechte für jeden Menschen oder jeden Staatsbürger bzw. jede Staatsbürgerin“¹¹⁴, „sie [bilden] die Weltordnung der Bundesrepublik Deutschland, an die sich nicht nur Privatpersonen, sondern ebenfalls Behörden und der Gesetzgeber selbst halten müssen.“¹¹⁵ Im Grundgesetz der Bundesrepublik Deutschland (GG) sind die Artikel 1 bis 19 unter der Überschrift „Die Grundrechte“ aufgeführt. Ebenfalls sind die Grundrechte in der Charta der Grundrechte der Europäischen Union sowie in Artikel 6 des Vertrages über die Europäische Union verankert.

III. Datenschutz als Grundrecht im europäischen Recht

Neben dem deutschen Grundgesetz ist der Datenschutz auch in der Charta der Grundrechte der Europäischen Union niedergeschrieben. In Artikel 8 Absatz 1 lautet es: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“ Gleich wie in der Datenschutzgrundverordnung der Europäischen Union diesen Status, in der geschrieben steht: „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht.“

IV. Urteile zum Recht auf Vergessen

1. Volkszählungsurteil von 1983

Anfang der 1980er Jahre sollte im Rahmen einer Vollerhebung eine Volkszählung in der BRD stattfinden. Nicht allein durch das Zurückgreifen von Daten von Ämtern, sondern durch Haustürbefragungen sollten neue Daten ermittelt werden. Dabei handelte es sich nicht nur um eine Kopfzählung, viel mehr auf das Erfassen von persönlichen Angaben, wie Beruf oder Wohnsituation.¹¹⁶ Das Ziel war es, durch die detaillierteren Einwohnerdaten staatliche Leistungen, vor allem in den Bereichen Verkehr, Finanzen und Soziales besser kalkulieren zu können. „Viele Bürger hegten indes Ängste, die vom Verlust der Privatsphäre bis hin zu Entpersonalisierung des Einzelnen und Ersetzung durch Datenpakete reichten.“¹¹⁷ Dies hätte sich vornehmlich durch die Vermischung administrativer und statistischer Daten ergeben. Es

¹¹⁴ (Geuther, 2013) S. 5

¹¹⁵ (Geuther, Grundrechte im Alltag, 2013) S. 4

¹¹⁶ Vgl.: (Schulze, 2013)

¹¹⁷ (Schulze, 2013)

erstreckte sich eine Protestbewegung gegen die Volkszählung über nahezu alle Schichten der Bevölkerung. Eine Verfassungsbeschwerde mehrerer Juristen hatte zur Folge, dass der Erste Senat des Bundesverfassungsgerichts (BVerfGE) die Zählung per Einstweiliger Anordnung bis zur abschließenden Klärung aussetzte. Besonders große Bedenken waren dem Paragraph 9 gewidmet. Dieser hätte es ermöglicht, Melderegisterdaten abzugleichen.¹¹⁸ Das abschließende Urteil vom 15. Dezember 1983 wird als Etablierung des Datenschutzes als Grundrecht angesehen. Selten zuvor sprach das BVerfGE einem Gesetz so weitreichend die Verfassungskonformität ab, wie in diesem Fall.

„Tatsächlich blieb vom Volkszählungsgesetz 1983 so gut wie nichts übrig. Die am meisten umstrittene Vorschrift, wonach Daten ans Melderegister, an Bundes- und Landesbehörden, an Gemeinden und deren Verbände hätten weitergegeben werden dürfen, wurde ohne Wenn und Aber für verfassungswidrig erklärt.“¹¹⁹

In Folge dessen wurde der BDSG angepasst. Dieses hat die Aufgabe, das Persönlichkeitsrecht des Einzelnen beim Umgang Anderer mit seinen personenbezogenen Daten zu schützen. Häufig wird diese Aufgabe als Datenschutz bezeichnet, tatsächlich ist diese Bezeichnung irreführend, da nicht die Daten sondern das Persönlichkeitsrecht geschützt werden soll.¹²⁰ Das Persönlichkeitsrecht kann durch mangelnde Datensicherheit gefährdet sein. Das Gericht erklärt in seinem Urteil:

„Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient [...] das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht [...]. Es umfasst [...] auch aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden [...]. Diese Befugnis darf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes.“¹²¹

Das Bundesverfassungsgericht stellt ausdrücklich die informationelle Selbstbestimmung als Teil des Persönlichkeitsrechts in Art. 2 Abs. 1 GG dar. Somit wurde durch den Richterspruch

¹¹⁸ Vgl.: (Schulze, 2013)

¹¹⁹ (o.V., 1983)

¹²⁰ Vgl.: (Schulze, 2013)

¹²¹ BVerfGE, Entscheidung vom 15.12.1983

der Datenschutz zu einem Grundrecht eines Jeden erklärt, womit seither eine besondere Schützenswürdigkeit besteht. Bleibt zu beantworten, weshalb der Datenschutz eine so zentrale Rolle einnimmt. Dazu heißt es in der Urteilsbegründung weiter:¹²²

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihm betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, [...] kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“¹²³

Das Bundesverfassungsgericht erklärte damit deutlich, dass zur freien Entfaltung der Persönlichkeit und zur Fähigkeit, freie Entscheidungen zu treffen, die informationelle Selbstbestimmung essentiell ist.

2. Der Fall Amanda Todd

Welche gesellschaftliche Relevanz das Recht auf Vergessenwerden hat, beschreibt am besten der Fall Amanda Todd, in dem es darum geht, welche Auswirkung das unbedachte Handeln eines Jugendlichen im Internet hat und inwieweit sich die Gesellschaft solchen Handelns entgegenstellen könnte.

Die Mobbingattacke(n) auf die 15-jährige kanadische Schülerin Amanda Todd aus British Columbia (BC) ist wohl der weltweit bekannteste Mobbingfall mit Todesfolge. Besonders an dem Sachverhalt ist, dass Amanda Todd nicht nur Opfer herkömmlichen Mobbingangriffen wurde, sondern auch vom sogenannten „cyber-bullying“, das heißt Verleumdung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen mit Hilfe elektronischer Kommunikationsmittel über das Internet, in Chatrooms, beim Instant Messaging und/oder auch mittels Mobiltelefonen. Dazu gehört auch der Diebstahl von (virtuellen) Identitäten, um in fremden Namen Beleidigungen auszustößen oder Geschäfte zu tätigen usw. Cybermobbing gehört zu einer der zentralen Gefahren im Umgang mit Internet

¹²² Vgl.: (Schulze, 2013)

¹²³ BVerfGE, Entscheidung vom 15.12.1983

und neuen Medien.¹²⁴ 2009 war Amanda Todd Schülerin der 7. Klasse, als sie wie viele Kinder ihres Alters, im Internet auf verschiedenen Chatrooms neue Bekanntschaften schließen wollte. Wie es im Chatrooms üblich ist, schrieb sie mit einem für sie Fremden, mit dem sie sich anscheinend gut verstanden hatte. Dieser für sie Unbekannte überzeugte sie, sich für ihn vor der Kamera oberkörperfrei zu präsentieren; dabei wurden Bilder von ihr erzeugt. Mit der Drohung, die Bilder im Netz zu veröffentlichen, erpresste er das Mädchen später und zwang sie, sich weitere Male nackt vor der Kamera zu zeigen. Als Amanda Todd nach 2 Jahren das Chatten einstellte, realisierte der Erpresser seine Drohung und veröffentlichte die Bilder des nun 14-jährigen Mädchens im Internet. Mit gefälschten Facebook-Accounts kontaktierte der Erpresser gezielt Amandas vermeintliche Schulfreunde, um die Bilder und Gerüchte zu verbreiten. Trotz mehrerer Orts- und Schulwechsel schaffte es Todd nicht, den Nachreden zu entkommen. Folge dessen waren diverse Mobbingattacken sowie physische Übergriffe ihrer Mitschüler auf sie. Am 10. Oktober 2012 nahm sich Amanda Todd das Leben. Unmittelbar vor ihrem Suizid stellte sie ein Video auf der Internetplattform YouTube ein, in dem sie mit Hilfe von Flash Cards ihre Geschichte erzählte.¹²⁵ Innerhalb kürzester Zeit erreichte dieses Video über 1.000.000 Klicks. Der tragische Fall wurde weltweit bekannt. Die Internetaktivistengruppe Anonymus kündigte nach dem Tod des Mädchens Vergeltung an und drohte, den Erpresser zu entlarven. Nach kurzer Zeit präsentierte Anonymus einen Mann als Täter, der daraufhin massiv bedroht und verfolgt wurde.¹²⁶ Dieser gab zu, mit Amanda Todd gehattet zu haben, bestritt aber der Erpresser gewesen zu sein. Nach intensiven Ermittlungen der Behörden, unter Einbeziehung der Royal Canadian Mounted Police (RCMP), wurde allerdings ein Anderer vor Gericht gestellt.

Der tragische Fall von Amanda Todd zeigt gleich mehrerer Aspekte, die die Datensicherheit und den Datenschutz heute wichtiger denn je erscheinen lassen.

1. Welche Relevanz die Aufklärung Jugendlicher im Umgang mit sensiblen personenbezogenen Daten hat.
2. Wie wichtig es ist, Daten löschen und die Verbreitung solcher sensibler Daten verhindern zu können.
3. Welche Bedeutung hinter der Ermittlung durch zuständige Behörden ist und welche Folgen Ermittlungen durch nicht Zuständige haben.

¹²⁴ Vgl.: (Stangl)

¹²⁵ Vgl.: (Schulze, 2013)

¹²⁶ Vgl.: (Schulze, 2013)

3. Google-Urteil des EuGH vom 13.05.2014 (C-131/12)

a) Sachverhalt

Dem Urteil des EuGH zugrunde lag eine Beschwerde des spanischen Staatsbürgers Mario Costeja González bei der Agencia Española de Protección de Datos (AEPD) gegen die LA Vanguardia Ediciones SL, die Herausgeberin der spanischen Tageszeitung La Vanguardia, sowie gegen Google Spain und dessen Mutterkonzern Google Inc.

Auslöser dieser Beschwerde waren zwei Artikel im Online-Archive der Zeitung La Vanguardia aus dem Jahr 1998, in denen unter Nennung des Namens von Herrn Costeja González über die Zwangsversteigerung seines Hauses berichtet wurde.¹²⁷ Bei Eingabe seines Namens als Suchanfrage in die Suchmaschine Google erschienen Links zu den Artikeln unter den ersten Suchergebnissen.

Auf Antrag von Herrn Costeja González sollte La Vanguardia angewiesen werden, die besagten Artikel zu löschen, zu anonymisieren oder mittels einer technischen Lösung vor Suchmaschinen zu verbergen.¹²⁸ Weiterhin sollte Google Spain bzw. Google Inc. angewiesen werden, die betreffenden Einträge aus dem Suchindex von Google Search zu löschen.

Die AEPD erklärte die Beschwerde im Juli 2010, soweit sie sich auf die Veröffentlichungen im Online-Archive von La Vanguardia bezog, als nicht berechtigt. Begründung hierfür war, dass die Berichterstattung seinerseits rechtmäßig war, da sie auf Anordnung des Arbeits- und Sozialministeriums erfolgt sei.¹²⁹ Gleichzeitig wies sie Google Spain und Google Inc. an, die entsprechenden Einträge zu löschen.

Google Spain und Google Inc. klagten daraufhin vor dem spanischen Gerichtshof Audiencia Nacional, der beide Verfahren zusammenfasste und dem EuGH im Vorabentscheidungsverfahren gem. Art. 267 AEUV mehrere auf den Fall bezogene Auslegungsfragen zur EU-Datenschutzrichtlinie 95/46/EG (DS-RL) vorlegte.

b) Vorlagefragen und Entscheidung des EuGH

„Insgesamt wollte der spanische Gerichtshof Audiencia Nacional mit seiner Vorlage wissen, ob aus der DS-RL ein Löschanpruch gegen Google folgt. Die Vorlagefragen gliedern sich dabei anhand der Prüfung eines solchen Löschanpruchs in drei Oberpunkte: Die

¹²⁷ Vgl.: (Vogt, 2016)

¹²⁸ Vgl.: (Vogt, 2016)

¹²⁹ Vgl.: (Vogt, 2016)

Anwendbarkeit europäischen Datenschutzrechts auf Google (sachlicher und räumlicher Anwendungsbereich) und die Frage, ob auch materiell ein Löschanpruch besteht.“¹³⁰

aa) Verantwortlichkeit des Suchindex

Entgegen der Reihenfolge der vorgelegten Fragen beantwortet der EuGH in seinem Urteil zuerst die Frage des sachlichen Anwendungsbereichs der DS-RL und der Verantwortlichkeit von Google für die Datenverarbeitung.

(1) Sachlicher Anwendungsbereich

Der Gerichtshof stellt zunächst fest, dass ein Suchmaschinenbetreiber personenbezogene Daten i.S.v. Art. 2 lit. b DS-RL verarbeitet. Der Suchmaschinenbetreiber erhebt die Daten, indem er das Internet automatisch, kontinuierlich und systematisch nach veröffentlichten Informationen durchsucht. Die aufgefundenen Daten werden dann mit Hilfe eines Indexierungsprogramms ausgelesen, gespeichert und organisiert und auf den Servern des Betreibers aufbewahrt.¹³¹ Anschließend werden die Daten in Form der Ergebnislisten den Nutzern weitergegeben bzw. bereitgestellt. Die Tatsache, dass die auf den Webseiten im Internet bereits vorhandenen Daten nicht verändert werden, ändert hieran nichts.¹³²

(2) Verantwortliche Stelle

Für die erhobenen Daten und der inbegriffenen Datenverarbeitung ist Google auch i.S.d. Art 2 lit. d DS-RL verantwortlich, da der Suchmaschinenbetreiber über die Zwecke und Mittel der Datenverarbeitung entscheidet.¹³³ Diese Verantwortung kann er nicht auf die Betreiber der originären Webseiten abwälzen. Der Umgang der Verarbeitung personenbezogener Daten durch eine Suchmaschine unterscheidet sich grundlegend von der Datenverarbeitung durch die Betreiber der Webseiten und steht damit selbstständig neben den übrigen Datenverarbeitungen im Zusammenhang mit den originären Webseiten.¹³⁴ Das spiegelt sich darin wieder, dass die Datenverarbeitung der Suchmaschine durch die Organisation und Aggregation der auf Webseiten veröffentlichten Informationen zu einem mehr oder weniger

¹³⁰ (Vogt, 2016)

¹³¹ Vgl.: (Vogt, 2016)

¹³² Vgl.: (Vogt, 2016)

¹³³ Vgl.: (Vogt, 2016)

¹³⁴ Vgl.: (Vogt, 2016)

detaillierten Profil der Betroffenen führt, das ohne die Suchmaschine nicht zur Verfügung stünde.¹³⁵

bb) Räumlicher Anwendungsbereich

Google müsste sich erst dann für seinen Suchindex verantworten, wenn die Richtlinie auch in räumlicher Hinsicht auf das Unternehmen anwendbar wäre. Der Gerichtshof geht dabei von der Situation aus, dass Google Inc. seinen Hauptsitz in den USA hat. Auf dortigen Servern findet auch die eigentliche Datenverarbeitung in Form der Ermittlung, Organisation und Indexierung statt.¹³⁶ Gleichzeitig unterhält der Konzern mit Google Spain eine Tochtergesellschaft zur Förderung des Verkaufs von Werbeflächen in einem Mitgliedstaat der EU.

„Bei der Beantwortung der Vorlagefrage bezieht sich der EuGH auf Art. 4 Abs. 1 lit. a DS-RL, nach dem der räumliche Anwendungsbereich eröffnet ist, wenn die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung erfolgt, die ihren Sitz im Hoheitsgebiet eines Mitgliedstaats hat.“¹³⁷ Der Gerichtshof argumentiert bei der Auslegung des Begriffs Niederlassung mit Hilfe des 19. Erwägungsgrundes der Richtlinie. Demnach ist eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung. Dies ist im Fall Google Spain unzweifelhaft gegeben.

Neu ist die Auslegung des EuGH hinsichtlich der Anforderungen an die Datenverarbeitung im Rahmen der Tätigkeiten der Niederlassung. Bisher galt die Auffassung, die Niederlassung selbst müsse wesentlichen Einfluss auf die relevanten Datenverarbeitungsvorgänge nehmen. Der EuGH erklärt, dass diese Auslegung zu eng sein, was einerseits aus dem Wortlaut von Art. 4 Abs. 1 lit. a DS-RL, andererseits aber auch aus den Erwägungsgründen und dem allgemeine Ziel der DS-RL folgt.¹³⁸ Der Wortlaut verlangt nicht, dass die Datenverarbeitung von der Niederlassung selbst ausgeführt wird, sondern nur im Rahmen der Tätigkeiten der Niederlassung erfolgen müsse. Abgesehen davon darf der Wortlaut aufgrund des allgemeinen Richtlinienziels, einen wirksamen und umfassenden Grundschutz der EU-Bürger zu gewährleisten, nicht zu eng ausgelegt werden. Hierfür sprechen auch die Erwägungsgründe 18 bis 20 der DS-RL, nach denen der Richtliniengeber mit einem weiten Anwendungsbereich die

¹³⁵ Vgl.: (Vogt, 2016)

¹³⁶ Vgl.: (Vogt, 2016)

¹³⁷ (Vogt, 2016)

¹³⁸ Vgl.: (Vogt, 2016)

Umgebung der Schutzmaßnahmen aus der DS-RL durch gezielte Standortpolitik verhindern wollte.¹³⁹

Angewendet auf den vorliegenden Fall führt diese weite Auslegung von Art. 4 Abs. 1 lit. a DS-RL dazu, dass auch die wirtschaftlichen Verflechtungen von Mutter- und Tochterunternehmen mit ins Blickfeld geraten. „Für den Fall Google stellt der Gerichtshof fest, dass Google Search nur durch den Verkauf von Werbeflächen überhaupt rentabel betrieben werden kann, Google Spain gleichzeitig ohne die Suchmaschine aber auch keine Plattform zum Verkauf der Werbung hätte. Die Tätigkeit des Suchmaschinenbetreibers und seiner Niederlassung sind deshalb untrennbar miteinander verbunden.“¹⁴⁰ Aus dieser engen wirtschaftlichen Verbindung folgt, dass in Hinblick auf Art. 4 Abs. 1 lit. a DS-RL eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit der Niederlassung von Google Spain bejaht werden kann.

Insgesamt sind die Regelungen der DS-RL deshalb auf die Tätigkeit von Google Spain und damit auch Google Inc. anwendbar.

c) Löschanspruch des Betroffenen

aa) Das Recht auf Vergessenwerden

Im Mittelpunkt des EuGH-Urteils steht das Recht auf Vergessenwerden (right to be forgotten). Der noch jungen Diskussion darüber liegt die Erkenntnis zu Grunde, dass es ein berechtigtes Interesse Einzelner gibt, im Internet über sie veröffentlichte Informationen zu einem bestimmten Zeitpunkt wieder aus dem Internet zu entfernen.¹⁴¹ Eine besondere Rolle spielen dabei Suchmaschinen, die das Internet erst als Informationsquelle nutzbar machen.

Der Forderung nach einem Recht auf Vergessenwerden wird regelmäßig die resignative Behauptung entgegengehalten, das Internet vergesse nichts.¹⁴² Das Internet besteht aus einer Vielzahl miteinander vernetzter Rechner. Daten darauf können naturgemäß wieder gelöscht werden; die komplexen Netzstrukturen stellen einen umfassenden Löschanspruch vor besondere Herausforderungen.¹⁴³ Allerdings kann ein wesentlicher Schritt zur Durchsetzung des Rechts auf Vergessenwerden darin liegen, die Auffindbarkeit der zu löschenden

¹³⁹ Vgl.: (Vogt, 2016)

¹⁴⁰ (Vogt, 2016)

¹⁴¹ Vgl.: (Schneider & Härting, 2014)

¹⁴² Vgl.: (Könau, 2017)

¹⁴³ Vgl.: (Könau, 2017)

Information mit Hilfe von Suchmaschinen zu verhindern oder jedenfalls wesentlich zu erschweren.

bb) Die Entscheidung des Gerichtshofs

Der Gerichtshof spricht selbst nicht von einem Recht auf Vergessenwerden. Er bezieht sich vielmehr auf den im EU-Recht verankerten Anspruch auf Löschung von Daten, an deren (fortgesetzter) Speicherung kein überwiegendes öffentliches Interesse bzw. Interesse der verantwortlichen Stelle besteht. Letztlich geht es ihm nicht ums Vergessenwerden, setzt jedoch voraus, dass bestimmte Informationen überhaupt nicht mehr im Internet auffindbar wären.¹⁴⁴ Der Gerichtshof stellte im Gegenteil dar, dass auch dann, wenn die originäre Information auffindbar bleibt, ihre Aufnahme (Indexierung) in ein Suchmaschinenprogramm und damit in eine Ergebnisliste unzulässig sein kann.¹⁴⁵

Der Gerichtshof stellt die besonderen Gefahren, die von (marktstarken) Suchmaschinen für die Persönlichkeitsrechte der Betroffenen ausgehen, in den Vordergrund. Eine Suchmaschine erleichtert durch die Aufführung der Webseiten, die personenbezogenen Daten einer bestimmten Person zu enthalten, erheblich den Zugang zu diesen Daten und trägt entscheidend zu ihrer Verbreitung bei. Mit Hilfe dessen und aus der Ergebnisliste resultiert ein Profil des Betroffenen, welches so ohne weiteres nicht getroffen würde.¹⁴⁶ Die Suchmaschine kann einen stärkeren Eingriff in das Grundrecht auf Achtung des Privatlebens des Betroffenen darstellen, als die Veröffentlichung auf der originären Webseite.

Das Ergebnis der Abwägung der Interessen des Betroffenen einerseits mit den Interessen der an Informationen interessierten Nutzer andererseits kann daher für den Suchmaschinenbetreiber und den Betreiber der originären Webseite durchaus unterschiedlich ausfallen.¹⁴⁷ Zudem kann die Datenverarbeitung auf der originären Webseite allein zu journalistischen Zwecken erfolgen und ist dann im Gegensatz zur Datenverarbeitung des Suchmaschinenbetreibers nach Art. 9 DS-RL privilegiert.

Der Gerichtshof erklärt, im Rahmen des Abwägungsergebnisses, dass die durch Art. 7, 8 GRCh geschützten Rechte des Betroffenen im Allgemeinen dem Interesse der Internetnutzer vorgestellt sind.¹⁴⁸ Nur in Ausnahmefällen ist ein anderes Ergebnis denkbar. Kriterien für

¹⁴⁴ Vgl.: (Hürlimann, 2014)

¹⁴⁵ Vgl.: (Piltz, 2014)

¹⁴⁶ Vgl.: (Schneider & Härting, 2014)

¹⁴⁷ Vgl.: (Hürlimann, 2014)

¹⁴⁸ Vgl.: (Hürlimann, 2014)

solche Ausnahmefälle sind insbesondere die Art der betreffenden Information, die Schwere der Beeinträchtigung des Privatlebens und das Gewicht des Informationsinteresses der Öffentlichkeit, etwa weil der Betroffene im öffentlichen Leben eine besondere Rolle spielt.

d) Folgen des Urteils

aa) Antragformular

Google war nun nach dem Urteil in der Situation, als Verantwortlicher reagieren zu müssen, und stellte dazu ein Antragsformular für Löschanträge bereit.¹⁴⁹ Die anfänglichen Anforderungen, eine Kopie des Personalausweises oder Reisepasses beizufügen, sind mittlerweile entfallen. Stattdessen genügt es, die Kopie eines anderen gültigen Lichtbildausweises dem Löschantrag anzuhängen.¹⁵⁰

bb) Vorschläge des Löschbeirats

Zur Unterstützung der eigenen Löschungs-Praxis richtete Google einen prominent besetzten Lösch-Beirat ein, dessen Aufgabe es war, Richtlinien für die Umsetzung des Urteils zu erarbeiten. „Der Beirat legte am 06.02.2015 einen Abschlussbericht vor, in dem vier materiell-rechtliche Hauptkriterien für den Abwägungsprozess genannt werden. Dazu zählen: Die Rolle des Antragstellers im öffentlichen Leben, die Natur der Information („Ist die Intimsphäre betroffen?“), die Art der Quelle (Social-Media-Webseite oder journalistisch-mediale Website) und letztlich die seit der Äußerung vergangene Zeit.“¹⁵¹

Des Weiteren formulierte der Expertenbeirat fünf prozessuale Anforderungen. Das Antragsformular für Löschungen solle leicht zugänglich und verständlich sein. Die Webmaster sollten über Löschungen aus dem Index informiert werden, wenn möglich, sogar schon im Voraus. Entscheidungen über Löschungen müssten von beiden Seiten, das heißt von dem Antragsteller oder der betroffenen Webseite anfechtbar sein. Löschungen sollten von Google begründet werden. Eine Löschung aus den nationalen Angeboten erachtet der Beirat als ausreichend. Letzten Endes sollen Statistiken über die Löschungen nur anonymisiert veröffentlicht werden.¹⁵²

¹⁴⁹ Vgl.: (Vogt, 2016)

¹⁵⁰ Vgl.: (Vogt, 2016)

¹⁵¹ (Vogt, 2016)

¹⁵² Vgl.: (Vogt, 2016)

cc) Ablauf einer Löschung

Google berichtet nicht sonderlich viel über den Ablauf des Löschprozesses, allerdings steht fest, dass die über das Antragsformular gesendeten Lösch-Anfragen in einer Einzelfallprüfung bei Google von einem Team im irischen Dublin geprüft und entschieden werden.¹⁵³ Eine vorherige Anhörung der Betreiber der Quellenwebseiten findet nicht statt. Des Weiteren ist unklar, nach welchen Kriterien bei der Löschung genau entschieden wird, da Google den eigenen Kriterien-Katalog bislang nicht veröffentlichte.¹⁵⁴

Vorerst löschte Google, wie vom Lösch-Beirat vorgeschlagen, die Suchergebnisse nur in den nationalen Versionen der Suchmaschine (z.B. „google.de“, „google.fr“).¹⁵⁵ Anfang 2016 reagierte das Unternehmen auf die Kritik der Datenschützer und führte außerdem ein Geo-Blocking für den europäischen Raum ein, durch das auch die Suchergebnisse in außereuropäischen Versionen der Suchmaschine (Bsp.: „google.com“) bei einem Aufruf aus Europa die Löschungen enthalten.¹⁵⁶

„Beschwerden von Antragstellern über Entscheidungen von Google in Bezug auf Löschanträge werden an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) Johannes Casper als zuständige Datenschutzbehörde für die Google Inc. gerichtet.“¹⁵⁷

dd) Statistik über Löschung

Die Befürchtung, Google könnte als privates Unternehmen aufgrund von wirtschaftlichen Interessen dazu übergehen, ähnlich der Personensuchmaschine „Yasni“, einfach allen an sie herangetretenen Löschanträgen stattzugeben, scheint unbegründet. Wie sich aus dem Transparenzbericht von Google ergibt, wurden nur knapp die Hälfte der Löschanträge aus Deutschland stattgegeben.¹⁵⁸

4. Daten im Gesellschaftsregister – EuGH-Urteil vom 09.03.2017 (C-398/15)

Der EuGH hat im Mai 2014 für Bürger ein Recht auf Vergessen-Werden gegen Suchmaschinenbetreiber und die Löschung von gespeicherten Links bejaht. In der nun

¹⁵³ Vgl.: (Vogt, 2016)

¹⁵⁴ Vgl.: (Vogt, 2016)

¹⁵⁵ Vgl.: (Tomik, 2016)

¹⁵⁶ Vgl.: (Tomik, 2016)

¹⁵⁷ (Vogt, 2016)

¹⁵⁸ Vgl.: (Vogt, 2016)

vorliegenden Entscheidung des EuGH vom 09.03.2017 verneinte dieser ein derartiges Recht für Personen, die in einem Unternehmensregister eingetragen sind.

Alle EU-Mitgliedsstaaten sind verpflichtet, in einem zentralen Register, z. B. bei einem Handels- und Gesellschaftsregister, Daten zu Bestellung und Ausscheiden der Gesellschaftsorgane sowie die Personalien der Mitglieder der Gesellschaftsorgane zu erfassen.¹⁵⁹ „Neben der (außer-)gerichtlichen Vertretungsbefugnis der Organe sind auch die Auflösung, Bestellung und Personalien der Liquidatoren sowie der Abschluss der Liquidation im Register zu verzeichnen.“¹⁶⁰ Dieses Register ist öffentlich zugänglich, dabei handelt es sich in Deutschland um das Handelsregister und das Unternehmensregister.

a) Sachverhalt

„Der Geschäftsführer einer Gesellschaft klagte gegen die italienische Handelskammer Lecce auf Löschung seiner Eintragung als Geschäftsführer einer 1992 insolvent gewordenen und 2005 liquidierten Gesellschaft.“¹⁶¹ Er argumentierte, dass die Verbindung seiner Person mit der Insolvenz dieser Gesellschaft einen nachteiligen Einfluss auf seine heute bestehende Geschäftstätigkeit habe.¹⁶² „Der von der Handelskammer Lecce angerufene Kassationsgerichtshof hatte dem EuGH nach erstinstanzlicher Verurteilung der Handelskammer zur Löschung der personenbezogenen Daten die Fragen zur Vorabentscheidung vorgelegt, ob es die Richtlinie zum Schutz der Daten natürlicher Personen und die Richtlinie über die Offenlegung von Gesellschaftsurkunden verbieten, dass jede Person ohne zeitliche Beschränkung Zugang zu natürliche Personen betreffende Daten im Gesellschaftsregister haben kann.“¹⁶³ Der EuGH sollte die Frage klären, ob die zeitlich unbegrenzte Speicherung personenbezogener Daten im öffentlich zugänglichen Unternehmensregister zulässig sei.¹⁶⁴

b) Ist ein unbefristeter Zugang zum Unternehmensregister zulässig?

„Der EuGH führte aus, dass die Offenlegung im Unternehmensregister grundsätzlich der Information aller interessierten Dritten diene. Eines besonderen Nachweises eines

¹⁵⁹ Vgl.: (Brenner, 2017)

¹⁶⁰ (Dr. Garbe, 2017)

¹⁶¹ (NOER, 2017)

¹⁶² Vgl.: (NOER, 2017)

¹⁶³ (NOER, 2017)

¹⁶⁴ Vgl.: (Dr. Garbe, 2017)

schutzbedürftigen Rechts oder Interesses bedürfe es nicht, insbesondere sei die Einsicht nicht auf Gläubiger der betroffenen Gesellschaft beschränkt.“¹⁶⁵

Selbst nach Auflösung der Gesellschaft könnten Rechte und Rechtsbeziehungen fortbestehen, die sich somit auf das eingetragene Unternehmen beziehen könnten. Für die Prüfung der Rechtmäßigkeit einer Handlung der Gesellschaft, sowie zur Geltendmachung von Ansprüchen Dritter gegen Mitglieder von Organen oder gegen Liquidatoren der Gesellschaft sei dies von besonderer Relevanz.¹⁶⁶

Offenzulegen seien nur wenige personenbezogene Daten, nämlich die Personalien und Aufgaben der Personen, welche die Gesellschaft gerichtlich und außergerichtlich vertreten und Aufsichts-, Verwaltungs- und Kontrollfunktion ausüben oder als Liquidator der Gesellschaft bestimmt sind.¹⁶⁷

„Dritte trügen generell aufgrund der Rechtsform der Gesellschaft (beschränkte Haftung) ein höheres wirtschaftliches Risiko. Daher sei es gerechtfertigt, dass am Wirtschaftsleben beteiligte Personen Daten über Personalien und Aufgaben innerhalb der Gesellschaft offenlegen. Dies geschehe zudem bewusst bei der Übernahme derartiger Tätigkeiten.“¹⁶⁸

Vor diesem Hintergrund verneinte der EuGH ein generelles Recht auf Vergessen-Werden im Unternehmensregister.

c) Ausnahme zur Einschränkung des Zugangs

Der EuGH schließt nicht aus, dass es besondere Situationen gibt, die eine Löschung zulassen, indem es aus überwiegenden, schutzwürdigen, sich aus dem konkreten Fall der betroffenen Person ergebenden Gründen ausnahmsweise gerechtfertigt ist, den Zugang zu den im Register eingetragenen personenbezogenen Daten nach Ablauf einer hinreichend langen Frist nach der Auflösung der fraglichen Gesellschaft auf Dritte zu beschränken, die ein besonderes Interesse an der Einsichtnahme in diese Daten nachweisen.¹⁶⁹ Es sei Sache des vorlegenden Gerichts, den Stand seines nationalen Rechts in dieser Hinsicht zu überprüfen. Aufgrund der

¹⁶⁵ (Dr. Garbe, 2017)

¹⁶⁶ Vgl.: (Dr. Garbe, 2017)

¹⁶⁷ Vgl.: (EuGH zum Recht auf Vergessen im Handelsregister- Wer mitmacht, muss offen legen , 2017)

¹⁶⁸ (Dr. Garbe, 2017)

¹⁶⁹ Vgl.: (NOER, 2017)

unterschiedlichen Verjährungsfristen der jeweiligen EU-Mitgliedstaaten ist es nicht möglich eine einheitliche Verjährungsfrist zu bestimmen.¹⁷⁰

V. Fazit

Das „Recht auf Vergessenwerden“ ist schon heute von enormer Bedeutung und wird mit jeder technischen Weiterentwicklung immer wichtiger für die Gesellschaft, vor allem aber für den Einzelnen.

Keine Spuren im Internet zu hinterlassen, ist schier unmöglich, es sei denn, man nutzt keinen Internetdienst. Das Internet ist omnipräsent und wird in dieser Rolle mit jeder Sekunde seines Bestehens verstärkt. Wie in der Arbeit erklärt wird, greift das Internet permanent in unser Leben ein. Es erfasst Daten über uns, ob durch Suchverhalten oder durch eigene Eintragungen, und es bestimmt zu einem Großteil unser Denken und Handeln. Wichtig ist, das Internet nicht nur negativ zu betrachten, sondern auch zu erörtern, wie nachhaltig das Internet unsere Gesellschaft positiv geprägt hat.

Der Fall Amanda Todd zeigt auf tragische Weise nicht nur, welche dramatischen Folgen die Nutzung des Internets speziell auf Kinder und Jugendlichen haben kann und welche Relevanz besteht, Kinder und Jugendliche über den Umgang des Internets aufzuklären, auch welche Folgen der falsche Umgang haben kann.

Das Internet ist für uns sowohl heute, wie in der Zukunft, unumgänglich, damit der Nutzer seine informationelle Selbstbestimmung nicht aus den Augen verliert.

Zu bedenken ist, dass das „Recht auf Vergessenwerden“ Grenzen besitzt, zur Strafverfolgung aber Eingriffe in das Grundrecht zu erwarten sind.

Letztlich bietet das „Recht auf Vergessenwerden“ uns die Möglichkeit unsere informationelle Selbstbestimmung aufrecht zu erhalten. Dennoch sind wir es, die entscheiden, wer was über uns erfährt und was wir von uns in der Öffentlichkeit preisgeben.

>>It is not technology that forces us to remember. Technology facilitates the demise of forgetting – but only if we humans so want. The Truth is we are causing the demise of forgetting, and it is up to us to reverse the change.<<

Viktor Mayer-Schönberger

¹⁷⁰ Vgl.: (Dr. Garbe, 2017)

Selbständigkeitserklärung

Hiermit versichere ich, dass die vor liegende Arbeit von mir selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen oder anderen Quellen entnommen wurden, sind als solche eindeutig kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form noch nicht veröffentlicht und noch keiner Prüfungsbehörde vorgelegt worden.

Maximilian Vorwerk

Bernburg, den 26.09.2017

Literaturverzeichnis

Aigner, I. (5. April 2010). *Spiegel Online*. Abgerufen am 20. August 2017 von <http://www.spiegel.de/politik/deutschland/offener-brief-an-zuckerberg-privates-muss-privat-bleiben-a-687280.html>

Auer-Reinsdorf, A., Jakobs, J., & Lepperhoff, N. (2011). *Vom Datum zum Dossier. Wie der Mensch mit seinen schutzlosen Daten in der Informationsgesellschaft ferngesteuert werden kann*. (1. Auflage Ausg.). Hannover: Heise Zeitschriftenverlag GmbH und Co. KG.

Baumgärtel, T. (kein Datum). *Reise ohne Karte :wie funktionieren Suchmaschinen?* Berlin, Berlin, Deutschland.

Beyer, S., & Gorris, L. (2009). Unwiderstehlicher Zauber. Der italienische Romancier und Semiotiker Umberto Eco über Listen als Ursprung der Kultur, die Leidenschaft des Sammelns und Aufzählens und die Tragik des Internets. *Der Spiegel* (45/2009), 165.

Breithut, J. (15. September 2016). *Spiegel Online*. Abgerufen am 20. August 2017 von <http://www.spiegel.de/netzwelt/web/so-findet-facebook-ihre-freunde-a-1111698.html>

Brenner, A. (Mai 2017). *IHK Ulm*. Abgerufen am 15. September 2017 von https://www.ulm.ihk24.de/recht_und_fair_play/handelsrecht/Aktuelles/Europaeischer-Gerichtshof--Kein-Recht-auf-Vergessen/3704640

Brössler, D. (15. Juni 2015). *SZ.de*. Abgerufen am 8. September 2017 von Süddeutsche Zeitung: <http://www.sueddeutsche.de/politik/recht-auf-vergessen-schutz-vor-google-und-facebook-1.2522321>

datenkraken.de. (kein Datum). *datenkraken.de*. Abgerufen am 23. August 2017 von <http://www.datenkraken.de/>

Demuth, N. (15. Juli 2015). *LTO*. Abgerufen am 12. September 2017 von LTO Legal Tribune Online: <https://www.lto.de/recht/hintergruende/h/recht-auf-vergessen-werden-theorie-eugh-praxis-google/>

DPN Datenschutz GmbH & Co. KG. (kein Datum). *DPN-Datenschutz*. Abgerufen am 12. September 2017 von DPN Datenschutz & Informationsfreiheit: <http://www.dpn-datenschutz.de/datenschutz/allgemeines-personlichkeitsrecht/>

Dr. Datenschutz (Pseudonym). (27. März 2017). *Datenschutzbeauftragter INFO*. Abgerufen am 7. September 2017 von Datenschutzbeauftragter INFO - Informationen zum Datenschutz: <https://www.datenschutzbeauftragter-info.de/das-recht-auf-vergessenwerden-bzw-die-loeschungspflicht-nach-dsgvo/>

Dr. Garbe, S. (14. März 2017). *ESCHE SCHÜMANN COMMICHAU*. Abgerufen am 14. September 2017 von blog.esche.de: <https://blog.esche.de/artikel/kein-generelles-recht-auf-vergessen-werden-im-handelsregister/>

Dr. Kraska, S. (2. Juni 2014). *iiTR Datenschutz*. Abgerufen am 11. September 2017 von Das Datenschutz-Blog: <https://www.datenschutzbeauftragter-online.de/google-urteil-eugh-datenschutz-informationsfreiheit/8011/>

Fiedler, K. (11. August 2014). *Netzpolitik.org*. Abgerufen am 11. September 2017 von <https://netzpolitik.org/2014/die-5-irrtuemer-zum-recht-auf-vergessenwerden/>

- Fiutak, M. (26. September 2006). *ZDNet*. Abgerufen am 6. September 2017 von http://www.zdnet.de/39147498/aol-skandal-milliardenklage-gegen-onlinedienst/?inf_by=59afe720681db87e118b48fc
- Funk, H. (18. Juli 2017). *puls*. Abgerufen am 5. September 2017 von <http://www.br.de/puls/themen/netz/anonyme-suchmaschinen-110.html>
- Geuther, G. (4. März 2013). Geschichte der Grundrechte. (B. f. Bildung/bpb, Hrsg.) *Informationen zur politischen Bildung* (überarbeitete Ausgabe), S. 5.
- Geuther, G. (4. März 2013). Grundrechte im Alltag. (B. f. Bildung/bpb, Hrsg.) *Informationen zur politischen Bildung* (überarbeitete Ausgabe), S. 4.
- heise online. (kein Datum). *heise online*. Abgerufen am 12. September 2017 von <https://www.heise.de/resale/artikel/Datenschutz-ein-grundlegendes-Persoentlichkeitsrecht-274418.html>
- Herr, A.-C. (13. Mai 2015). *LTO*. Abgerufen am 5. September 2017 von LTO Legal Tribune Online: <https://www.lto.de/recht/hintergruende/h/recht-auf-vergessenwerden-ein-jahr-bilanz/>
- Hürlimann, D. (2014). Das Google-Urteil des EuGH und die Entfernungspflicht von Suchmaschinen nach schweizerischem Recht. Schweiz.
- klicksafe.de - Die EU-Initiative für mehr sicherheit im Netz*. (kein Datum). Abgerufen am 03. Juli 2017 von <http://www.klicksafe.de/themen/suchen-recherchieren/suchmaschinen/wie-funktioniert-eine-suchmaschine/>
- klicksafe.de. (7. Juni 2016). *klicksafe.de*. Abgerufen am 5. September 2017 von <http://www.klicksafe.de/themen/suchen-recherchieren/suchmaschinen/datenschutz-und-suchmaschinen/>
- Könau, S. (15./16. Juli 2017). Die digitale Demenz. *Mitteldeutsche Zeitung*, 24.
- Lackes, R. P., Siepermann, M. D., & Sjurts, I. P. (kein Datum). *Gabler Wirtschaftslexikon*, 12. (S. G. Verlag, Herausgeber) Abgerufen am 03. Juli 2017 von <http://wirtschaftslexikon.gabler.de/Archiv/77388/suchmaschine-v12.html>
- Lochmann, C., Gewehr, J. E., & Szugat, M. (2010). *Soziale Netzwerke und Dienste. schnell + kompakt*. (1. Auflage Ausg.). Frankfurt a. M.: Software & Support Media GmbH.
- LTO*. (9. März 2017). Abgerufen am 15. September 2017 von LTO Legal Tribune Online: <https://www.lto.de/recht/nachrichten/n/eugh-urteil-c-398-15-publizitaet-handesregister-loeschung-personenbezogene-daten-frist/>
- Mayer-Schönberger, V. (2009). *Delete. The Virtue of Forgetting in the Digital Age* (Bd. 4. Auflage). Princeton, New Jersey, USA: Princeton University Press.
- NOER. (12. April 2017). *NOER*. Abgerufen am 13. September 2017 von NOER - Starke Persönlichkeiten sind starke Partner: <https://www.noerr.com/de/newsroom/News/ueberblick-rechtsprechung-im-gesellschaftsrecht-04-2017.aspx>
- nwb Datenbank. (9. März 2017). *nwb Datenbank*. Abgerufen am 12. September 2017 von <http://datenbank.nwb.de/Dokument/Anzeigen/692450/>

o.V. (13. Mai 2014). *Frankfurter Allgemeine*. Abgerufen am 10. September 2017 von Frankfurter Allgemeine - Wirtschaft: <http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/eugh-raeumt-recht-auf-vergessen-gegenueber-google-ein-12936895.html>

o.V. (1983). Schwere Schlappe. *Der Spiegel* (51/1983), S. 19.

o.V. (kein Datum). *Selbstdatenschutz*. Abgerufen am 17. September 2017 von [Selbstdatenschutz.info](https://www.selbstdatenschutz.info/): <https://www.selbstdatenschutz.info/datenkraken/>

Otto, P. (3. Juli 2017). *iRights info*. Abgerufen am 9. September 2017 von [iRights info](https://irights.info/) - Urheberrecht und kreatives Schaffen in der digitalen Welt: <https://irights.info/artikel/urheber-und-persnlichkeitsrechte-in-sozialen-netzwerken/5793>

Özbicerler, B. (26. Januar 2016). *FOCUS*. Abgerufen am 9. September 2017 von FOCUS-Online: http://www.focus.de/digital/handy/schluss-mit-datenkraken-so-verhindern-sie-dass-ihr-smartphone-sie-ausspaecht_id_5228212.html

Piltz, C. (13. Mai 2014). *DE LEGE DATA*. Abgerufen am 14. September 2017 von <https://www.delegedata.de/2014/05/das-google-urteil-des-eugh-uebers-ziel-hinaus-geschossen/>

Schneider, J., & Härting, N. (11. April 2014). *CRonline*. Abgerufen am 11. September 2017 von CRonline Portal zum IT-Recht: <https://www.cr-online.de/blog/2014/04/11/eugh-zu-grundrechten-der-charta-vorrang-fuer-das-materielle-schutzgut-am-beispiel-der-vorratsdatenspeicherung/>

Schonschek, O. (28. Juli 2014). *Datenschutz Praxis*. Abgerufen am 10. September 2017 von <https://www.datenschutz-praxis.de/fachartike/loeschantraege-bei-google-und-bing-bringen-sie-wirklich/>

Schonschek, O. (25. Januar 2016). *Datenschutz Praxis*. Abgerufen am 17. September 2017 von <https://www.datenschutz-praxis.de/fachartike/loeschpflichten-recht-auf-vergessenwerden/>

Schulze, S. F. (2013). *Das Recht auf Vergessenwerden - Essentielles Grundrecht im Netz?* Stuttgart: GRIN Verlag GmbH.

SEO-Summary.com. (März 2017). *SEO-Summary.com*. Abgerufen am 22. August 2017 von <https://seo-summary.de/suchmaschinen/>

Spehr, M. (29. Dezember 2016). *Frankfurter Allgemeine*. Abgerufen am 23. August 2017 von <http://www.faz.net/aktuell/technik-motor/digital/datenkrake-abgefischt-von-facebook-14590869.html>

Spiegel Online. (22. August 2006). *SPIEGEL ONLINE*. Abgerufen am 6. September 2017 von <http://www.spiegel.de/wirtschaft/nutzerdaten-skandal-aol-technologiechefin-muss-gehen-a-432813.html>

Stangl, W. (kein Datum). *Lexikon online*. Abgerufen am 11. September 2017 von Lexikon online - Online-Enzyklopädie für Psychologie und Pädagogik: <http://lexikon.stangl.eu/694/cyberbullying/>

Tippmann, U., Hemken, H., Rehberg, C., & Wienströer, S. (kein Datum). *seo-united.de*. Abgerufen am 03. 07 2017 von [seo-united.de](https://www.seo-united.de/glossar/suchmaschine/): <https://www.seo-united.de/glossar/suchmaschine/>

Tomik, S. (10. Februar 2016). *Frankfurter Allgemeine*. Abgerufen am 15. September 2017 von Frankfurter Allgemeine Politik: <http://www.faz.net/aktuell/politik/recht-auf-vergessenwerden-google-fuehrt-geoblocking-ein-14061531.html>

Verbraucherzentrale. (19. Juni 2017). *verbraucherzentrale.de*. Abgerufen am 12. September 2017 von <https://www.verbraucherzentrale.de/recht-auf-vergessen>

Vogt, N. (2016). *Das Recht auf Vergessenwerden nach dem Google-Urteil des EuGH vom 13.05.2014 und die Folgen*. Hamburg: GRIN Verlag, Open Publishing GmbH.

Weiß, F. (6. April 2017). *W&P Anwaltskanzlei Weiß & Partner*. Abgerufen am 1. September 2017 von <https://www.ratgeberrecht.eu/datenschutz-aktuell/personenbezogene-daten-im-gesellschaftsregister.html>

Wendt, J. (13. Mai 2014). *Zeit Online*. Abgerufen am 15. September 2017 von ZEIT ONLINE: <http://www.zeit.de/digital/datenschutz/2014-05/eugh-urteilt-ueber-recht-auf-vergessenwerden/komplettansicht>

Wirtschaft.com. (7. Februar 2017). *Wirtschaft.com*. Abgerufen am 22. August 2017 von <http://www.wirtschaft.com/anonyme-suchmaschinen-suchen-ohne-schnueffler-und-datenkraken/>

Wolling, J. (kein Datum). *researchgate.net*. Abgerufen am 03. Juli 2017 von [researchgate.net: https://www.researchgate.net/profile/Jens_Wolling/publication/267832138_Suchmaschinen_-_Selektiermaschinen/links/5561d3d208ae6f4dcc9525b2/Suchmaschinen-Selektiermaschinen.pdf](https://www.researchgate.net/profile/Jens_Wolling/publication/267832138_Suchmaschinen_-_Selektiermaschinen/links/5561d3d208ae6f4dcc9525b2/Suchmaschinen-Selektiermaschinen.pdf)

Abbildungsverzeichnis

Abbildung 1 Marktanteile Suchmaschinen	7
https://seo-summary.de/suchmaschinen/ ; Aufgerufen am 20. August 2017	
Abbildung 2 Statistische Marktanteile in Prozent.....	7
https://seo-summary.de/suchmaschinen/ ; Aufgerufen am 20. August 2017	
Abbildung 3 ixquick Logo	15
http://www.br.de/puls/themen/netz/anonyme-suchmaschinen-110.html ; Aufgerufen am 22. August 2017	
Abbildung 4 DuckDuckGo Logo.....	15
http://www.br.de/puls/themen/netz/anonyme-suchmaschinen-110.html ; Aufgerufen am 22. August 2017	
Abbildung 5 YaCy Logo.....	15
http://www.br.de/puls/themen/netz/anonyme-suchmaschinen-110.html ; Aufgerufen am 22. August 2017	