Datenschutz bei Internetveröffentlichungen

Von Dr. Thilo Weichert*, Kiel

Die Beschwerden von Betroffenen über Datenschutzverstöße im Internet bei Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich haben in jüngster Zeit massiv zugenommen. Ihr Anteil am Gesamtbeschwerdeaufkommen nähert sich der 50 %-Marke. Dabei geht es um die Verarbeitung von Daten auf fremden Webseiten, um die distanzlose Veröffentlichung von – im übertragenen Sinn – blauäugigen Nutzenden von Social Communities, etwa von SchülerVZ oder Facebook, um die anonyme Anprangerung von Nachbarn, Lehrkräften in Schulen und Kollegen oder um die Zugänglichkeit von Kundendaten auf einer Unternehmens-Webseite. Behörden und Unternehmen veröffentlichen ungefragt Angaben zu ihren Mitarbeitern im weltweiten Netz. Sportvereine und -veranstalter publizieren ebenso ungefragt und selbstverständlich Teilnehmerlisten und Ergebnisse. Über Webcams mit hohem Auflösungsvermögen kann per Zufall festgestellt werden, dass ein Bekannter gerade in der Fußgängerzone des Ortes unterwegs ist. In Blogs, Foren und ähnlichen Diensten erfolgen oft Äußerungen, die über das Anständige und Erlaubte hinausgehen. Besonders beschwerdeträchtig ist die systematische Einstellung von Daten, etwa von Geodaten wie Google Street View, Google Earth oder Microsoft Virtual Earth, mit denen weltweit Informationen zu Wohnungen und Häusern und damit zum individuellen Lebensumfeld abgerufen werden können, sowie die systematische Erfassung unerwünscht im Internet veröffentlichter Daten mithilfe von Suchmaschinen.

Die Reaktionsmöglichkeiten von Kontrollstellen sind oft beschränkt: Bei ausländischen Webseitenbetreibern ist selten eine direkte Einflussnahme möglich. Die Verantwortlichkeit für die Datenveröffentlichung ist schwer festzustellen. Die anzuwendenden Regelungen sind regelmäßig wenig ergiebig und ermöglichen keine adäquate staatliche Intervention. Dennoch gilt: Das Internet ist kein rechtsfreier Raum. Es hat nichts mit Zensur zu tun, wenn Aufsichtsbehörden oder sonstige Kontrollstellen bei Persönlichkeitsrechtsverletzungen im Internet aktiv werden. Die Rechtslage ist aber angesichts der neuen Sachverhalte und der weitgehend fehlenden klaren Regelungen weder den Internet-Nutzenden noch den Betroffenen eindeutig erkennbar – Grund genug, die bestehenden gesetzlichen Rudimente darzustellen und auszufüllen und dadurch etwas mehr Rechtssicherheit zu schaffen.

A. Übergeordneter Rechtsrahmen

Bei der Darstellung von datenschutzrechtlichen Betroffenenrechten und Betreiberpflichten wird in der Regel mit den spezifischsten Normen begonnen. Da es im Hinblick auf Internetveröffentlichungen solche nur in beschränktem Maße gibt, sollen hier zunächst die *verfassungsrechtlichen Rahmenbedingungen* vorgestellt werden, bevor auf die Anwendung konkreter Regelungen eingegangen wird. Die Veröffentlichungen stehen jeweils im Spannungsverhältnis verschiedener Grundrechte, die für und gegen die Datenpreisgabe, für und gegen die Wahrung der Vertraulichkeit der Daten streiten. Dabei muss im Blick bleiben, dass die Grundrechte gegenüber privaten Personen und Stellen keine direkten Wirkungen entfalten. Wohl aber ergeben sich aus diesen Grundrechten, die in erster Linie Abwehrrechte gegen staatliches Handeln sind, Wertentscheidungen unserer Rechtsordnung, die bei der Anwendung einfachen Rechts, also auch des Privat- und Wirtschaftsrechts, berücksichtigt werden müssen. Zudem ergeben sich aus diesen Grundrechten staatliche Gewährleistungspflichten, also die Aufgabe für Gesetzgeber und Behörden, sich schützend vor betroffene Bürgerinnen und Bürger zu stellen.

Für die Veröffentlichung und gegen deren Beschränkung spricht zunächst *Art. 5 Grundgesetz* (GG), der drei für unser freiheitlich-demokratisches Gemeinwesen zentrale Internet-Freiheiten beinhaltet. Diese sind das Recht auf freie Meinungsäußerung für alle Menschen und die Freiheit der Presse, also das Recht, ohne Zensur am demokratischen Austausch und Meinungsbildungsprozess teilzunehmen. Damit korrespondiert das Recht aller Menschen,[1] sich aus allgemein zugänglichen Quellen – und hierfür ist das Internet geradezu das ideale Medium – zu informieren, also die Informationsfreiheit.

Die verfassungsrechtlichen *Grenzen dieser Informations- und Meinungsfreiheitsrechte* dienen im Allgemeinen dem Schutz der von der Internetveröffentlichung betroffenen Personen. Diese können in ihren unterschiedlichen Grundrechten beeinträchtigt werden, etwa dem Art. 14 GG, dem Schutz des Eigentums, durch die Verletzung von Urheberrechten oder von Betriebs- und Geschäftsgeheimnissen. Aus Datenschutzsicht steht das allgemeine Persönlichkeitsrecht im Vordergrund, das sich aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG ergibt.

Dieses *allgemeine Persönlichkeitsrecht* hat durch die Rechtsprechung des Bundesverfassungsgerichtes (BVerfG) eine Vielzahl von Konkretisierungen erfahren, die bei der Nutzung des Internets relevant sein können. Zuallererst ist das im Jahr 1983 begründete Recht auf informationelle Selbstbestimmung, also das Grundrecht auf Datenschutz, zu nennen.[2] Dieses begründet generell die Befugnis selbst zu bestimmen, wer was wann bei welcher Gelegenheit über einen weiß. Zwei Spezifizierungen des allgemeinen Persönlichkeitsrechts mit Internetrelevanz haben eine erheblich ältere Geschichte, nämlich das Recht am eigenen Bild und das Recht am gesprochenen Wort. Eine brandaktuelle Konkretisierung des allgemeinen Persönlichkeitsrechtes erfolgte durch das BVerfG anlässlich von Beschwerden gegen die Zulassung von heimlichen Online-Durchsuchungen für den nordrhein-westfälischen Verfassungsschutz, durch die Ableitung eines Grund-

* Der Verfasser ist Landesbeauftragter für Datenschutz Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz in Kiel.

1 BGH Urt.v. 23.06.2009, Az.: VI ZR 196/08.

2 BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

rechtes auf Gewährleistung der Vertraulichkeit und Integrität selbst genutzter informationstechnischer Systeme.[3] Damit schuf das BVerfG, ähnlich dem Schutz der räumlichen Privatsphäre Wohnung durch Art. 14 GG, eine vor allem technisch definierte digitale Privatsphäre.

Neben dem allgemeinen Persönlichkeitsrecht bestehen besondere *Lebensbereiche spezifisch schützende Grundrechte*, die durch die Datenverarbeitung im Internet verletzt werden können. An erster Stelle ist das Fernmeldegeheimnis des Art. 10 GG zu nennen, das heute Telekommunikationsgeheimnis genannt wird. Weitere relevante Grundrechte können sein: der Schutz von Kindern, Jugend und Familie (Art. 4 GG), politische Freiheitsrechte (Art. 8, 9 GG), die allgemeine Handlungsfreiheit (Art. 2 Abs. 2 GG).[4]

Nicht nur nationales Verfassungsrecht, auch internationales Recht, bindet die deutsche Gesetzgebung, Rechtsprechung und Verwaltung. Die *Europäische Menschenrechtskonvention* (EMRK) enthält analog zum Grundgesetz zwei bei Internetveröffentlichungen relevante Garantien und schafft zugleich einen gesamteuropäischen Ordnungsrahmen, der über Art. 6 Abs. 2 EU-Vertrag und die Rechtsprechung des Europäischen Gerichtshofes (EuGH) den Grundrechtsschutz in der EU mitprägt: Art. 10 EMRK gewährleistet die Meinungsfreiheit, nach der neuesten Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) auch bei der Nutzung des Internets. Art. 8 EMRK sichert das Recht auf Privatsphäre und schützt Kommunikation und Persönlichkeitsentfaltung nicht nur vor staatlichen Eingriffen, sondern bietet auch Schutz vor privaten Beeinträchtigungen. Nach Art. 34 EMRK kann sich jeder, der sich in seinen Konventionsrechten verletzt sieht, an den EGMR in Straßburg wenden, wenn innerstaatliche Rechtsbehelfe keinen Erfolg haben.[5]

Noch keine aktuelle, aber absehbar künftige Rechtsverbindlichkeit entwickelt die *Europäische Grundrechtecharta*. Art. 7 sichert die Achtung des Privat- und Familienlebens: „Jeder Mensch hat das Recht auf Achtung seines Privat- und Familienlebens, seiner Wohnung sowie seiner Kommunikation." Art. 8 Abs. 1 soll personenbezogene Daten schützen: „Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten." Art. 11 garantiert die Freiheit der Meinungsäußerung und Informationsfreiheit: „(1) Jeder Mensch hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. (2) Die Freiheit der Medien und ihre Pluralität werden geachtet."

Einen übergeordneten Rechtsrahmen für personenbezogene Internetveröffentlichungen bietet weiterhin die *Europäische Datenschutzrichtlinie* (EU-DSRL).[6] Diese EU-DSRL erging zu einer Zeit, in der das Internet noch nicht die praktische Relevanz hatte wie heute. Sie enthält hierzu auch keine spezifischen Regelungen. Wohl aber ist sie ein verbindlicher Rechtsrahmen, der bei der Auslegung des nationalen Rechts herangezogen werden muss. Zudem eröffnet sie eigenständige europäische Handlungsmöglichkeiten, insbesondere die Klage beim Europäischen Gerichtshof (EuGH). Von Bedeutung ist u. a. Art. 9 EU-DSRL, der für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen von den normativen Vorgaben der Richtlinie nur soweit erlaubt, "als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen". Nach Art. 29 EU-DSRL wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt, die aus Vertretern der nationalen Kontrollstellen besteht, die Prüfungen vornimmt sowie Stellungnahmen und Empfehlungen abgibt (Art. 29-Gruppe). Diese Art. 29-Gruppe hat eine Vielzahl von Arbeitspapieren zur Internet-Datenverarbeitung beschlossen. Diesen Arbeitspapieren kommt eine hohe Bedeutung wegen ihres nationenübergreifenden Ansatzes zu, der dem grenzüberschreitenden Charakter des Internets entspricht.[7]

B. Gesetzliche Regelungen

Nicht die Internet-Inhalte, sondern die dort anfallenden *Bestands-, Verkehrs- bzw. Nutzungsdaten* (einschließlich Standortdaten) betreffen die Regelungen des für Zugangsanbieter (Access-Provider) geltenden Telekommunikationsgesetzes (TKG). Die Verarbeitung solcher Daten durch Inhaltsanbieter (Content-Provider) ist im Telemediengesetz (TMG) geregelt.

Das Recht auf Pressefreiheit wird durch die Landespressegesetze sowie durch den Rundfunkstaatsvertrag (RStV) geschützt. Im 9. Rundfunkänderungsstaatsvertrag haben die Landesgesetzgeber mit dem § 57 RStV eine Norm über die journalistisch-redaktionelle Datenverarbeitung von Inhaltsdaten durch Anbieter von Telemedien, also für den Onlinebereich, verabschiedet.[8] § 57 RStV konkretisiert die Rahmenvorschrift des § 41 BDSG. Dem § 57 RStV für die Unternehmen oder Hilfsunternehmen der Telemedien entsprechen inhaltlich bzgl. der sonstigen Medien die Regelungen der Landespressegesetze für die Printmedien sowie § 41 Abs. 2, 3 BDSG für den Bundesrundfunk (Deutsche Welle). Die Gesamtheit dieser Regelungen wird als datenschutzrechtliches „*Medienprivileg*" bezeichnet. Privilegiert sind im Bereich des Internets nur Online-Verlage mit redaktionellen Strukturen. Presseabteilungen von Unternehmen, Verbänden, Parteien und anderen Organisationen, die Onlineausgaben produzieren, fallen nur dann unter den Schutzbereich, wenn sie von der übrigen Struktur eine abgetrennte Organisationseinheit bilden. Mit privilegiert als Hilfsorganisationen sind Betriebe mit dem Geschäftszweck der ständigen Unterstützung von Verlagen und Redaktionen. Nach § 57 Abs. 1 RStV gelten im journalistisch-redaktionellen Bereich nur die §§ 5, 7, 9, 38a BDSG. Die Ausnahmevorschrift setzt voraus, dass ausschließlich journalistisch-redaktionelle Zwecke verfolgt werden, erfasst dann aber den gesamten Vorgang beginnend bei der Recherche über die Herstellung und Verbreitung bzw. Sendung und Speicherung. Gleiches gilt bei literarischen Zwecken. Auf die Rechtmäßigkeit der Datenerhebung kommt es in diesem Bereich, also bei Beiträgen zum öffentlichen Meinungskampf, nicht an.

---

3 BVerfG NJW 2008, 822 = DÖV 2008, 459 = MMR 2008, 315= DVBl 2008, 582.

4 Vgl. den Überblick bei Däubler/Klebe/Wedde/Weichert-*Weichert*, Bundesdatenschutzgesetz - BDSG, 2. Aufl. 2007, Einl. Rz. 27 ff.

5 *Uerpmann-Wittzack/Jankowska-Gilberg*, MMR 2008, 83 ff.; *Siemen*, Datenschutz als europäisches Grundrecht, 2006; zum Verhältnis von Persönlichkeitsschutz und Pressefreiheit nach EMRK *Bruns*, JZ 2005, 428 ff.

6 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281/31 v. 23.11.1995.

7 Abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm.

8 Die Regelung ist bzgl. Bestands-, Nutzungs- und Abrechnungsdaten identisch mit den Vorgängerregelungen des § 20 MDStV.

Die Medienprivilegierung entfällt, wenn *weitere Zwecke* verfolgt werden, die nicht mehr von der Pressefreiheit des Art. 5 GG gedeckt sind, z. B. die Erstellung von Nutzer- bzw. Leseranalysen, die Werbung, die technische Optimierung der Datenbanken, das Verfolgen von privaten Motiven eines Journalisten oder die kommerzielle Verwertung von redaktionellen Datenbeständen. Über die Erwähnung des § 38a BDSG wird den Berufsverbänden die Möglichkeit eröffnet, datenschutzbezogene Verhaltensregeln für ihre Mitglieder im Rahmen von Onlineangeboten zu schaffen. Die bisher ausdrücklich nur für die gedruckte Presse geltenden publizistischen Grundsätze des Pressekodex des Deutschen Presserates sind nunmehr anwendbar für das journalistisch-redaktionelle Internetangebot der Presseverlage.[9] Bei Verstößen gegen das Datengeheimnis nach § 5 BDSG, technisch-organisatorisch geforderte Datensicherheitsmaßnahmen nach § 9 BDSG sowie bei Verletzungen der Verhaltensregeln nach § 38a BDSG besteht gem. § 7 BDSG ein Schadenersatzanspruch.[10]

Nichtredaktionelle Meinungsäußerungen im Internet – und dies ist der ganz große Anteil bei den Internetveröffentlichungen mit personenbezogenen Daten – genießen nicht den Schutz der Pressefreiheit, sondern allenfalls den allgemeinen Schutz des jedem Menschen nach Art. 5 GG zustehenden Rechts auf freie Meinungsäußerung. Die zentralen einfachgesetzlichen Regelungen zur Wahrung des Datenschutzes bei Internetveröffentlichungen finden sich im *Bundesdatenschutzgesetz* (BDSG) und dort insbesondere im 4. Abschnitt (§§ 27 ff.). Das BDSG stammt in seiner bis heute erhaltenen Struktur und den wesentlichen für Internetveröffentlichungen einschlägigen Normen aus dem Jahr 1990, also aus einer Zeit, in der das Internet für personenbezogene Datenverarbeitung noch keine Rolle gespielt hat.[11]

Zivilrechtliche Normen zum Verhältnis zwischen Webseiten- oder Inhaltsanbietern und den Betroffenen finden sich im Bürgerlichen Gesetzbuch (BGB), und zwar insbesondere im Recht der Allgemeinen Geschäftsbedingungen (AGB, §§ 305 ff. BGB). Die Nutzungs-AGB enthalten oft Aussagen zur Verarbeitung nicht nur von Bestands- und Nutzungsdaten, sondern auch von Inhaltsdaten, also z. B. von in Webformularen gemachten Angaben. Soweit es sich bei den Betroffenen um Verbraucher handelt, kann weiterhin das Verbraucherschutzrecht anwendbar sein,[12] handelt es sich bei diesen um Arbeitnehmer, das Arbeitnehmerdatenschutzrecht.

Auch können je nach Art der Daten weitere spezielle Regelungen anwendbar sein, so bei der Veröffentlichung von Bildern das Kunsturhebergesetz (§§ 22 ff. KUG) sowie bei Veröffentlichung spezifischer Daten, Bilder oder Tonaufnahmen das Strafgesetzbuch (§§ 201 ff. StGB). Von Relevanz sind schließlich die strafrechtlichen Verbote der Beleidigung, der Verleumdung sowie allgemein des strafrechtlichen Ehrschutzes (§§ 185 ff. StGB).

Schließlich gibt es eine Vielzahl von öffentlich-rechtlichen Normen, welche die Veröffentlichung von personenbezogenen Daten durch *Behörden und sonstige öffentliche Stellen* regeln.[13] Weitere rechtliche Fragen ergeben sich bei der Veröffentlichung von personenbezogenen Daten, die Private von öffentlichen Stellen erhalten haben.[14]

C. Der Personenbezug von Sachdaten

Voraussetzung für die Anwendung des Datenschutzrechtes bei Internetveröffentlichungen ist, dass hiervon personenbezogene Daten betroffen sind, d. h. Angaben zu den persönlichen oder sachlichen Verhältnissen einer identifizierbaren natürlichen Person (§ 3 Abs. 1 BDSG). *Personenbeziehbarkeit* genügt, d. h. es muss nicht ausdrücklich der Name genannt werden. Diese Personenbeziehbarkeit ist nicht mehr gegeben, wenn die Einzelangaben nicht mehr oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person zugeordnet werden können (Anonymisierung, § 3 Abs. 6 BDSG). Bei Internetveröffentlichungen ist zu berücksichtigen, dass diese grds. weltweit abrufbar sind, d. h. Daten werden dadurch personenbezogen, dass irgendwo auf der Welt jemand eine Zuordnung zu einer Person vornehmen kann. Dies hat zur Folge, dass z. B. die Übertragung von Bildern einer Webcam personenbezogen ist, wenn die dargestellten Personen beispielsweise anhand ihres Gesichts oder ihrer Kleidung eindeutig identifiziert werden können. Es ist nicht nötig, dass der Betreiber der Webcam die Zuordnung vornehmen kann oder dies einem großen Teil der Internet-Community möglich ist. Die Identifizierungsmöglichkeit durch wenige mögliche Nutzer genügt, z. B. durch nähere Bekannte dieser Person oder durch Behördenmitarbeiter oder einen Arbeitgeber, die über relevantes Zusatzwissen verfügen (etwa Kenntnis der Kleidung, des Kfzs, des konkreten Aufenthalts).

Personenbezogen sind auch Angaben über *sachliche Verhältnisse einer Person*, wie über das eigene Auto, das Handy, das eigene Haus oder Grundstück und die genutzte Wohnung. Daher kann es sich bei Veröffentlichungen von Straßenansichten im Internet, wie etwa durch den Dienst Google Street View, um personenbezogene Daten handeln, zumal die Bilder auf elektronischen Kartendiensten genau einer Geokoordinate zugewiesen werden können, welche wieder einer Adresse und diese wieder Bewohnern oder Eigentümern zugeordnet werden können.[15] Sachdaten ohne persönlichkeitsrechtliche Relevanz, die aber dennoch einer Person zugeordnet werden können, unterliegen nicht dem Datenschutzrecht. Nötig ist eine Angabe zur Identität, zu Merkmalen oder zum Verhalten einer Person. Informationen über eine Sache können sich auf die Rechte oder zumindest auf die Interessen einer natürlichen Person auswirken und entfalten dadurch Persönlichkeitsrelevanz. Zumindest einer der folgenden Kontexte muss bestehen:

1. Beim Ergebniskontext wirkt das Datum auf Rechte und Interessen einer Person ein. 2. Daten mit Zweckkontext zielen auf das Beschreiben oder Beeinflussen des sozialen, kulturellen, wirtschaftlichen oder sonstigen gesellschaftlichen Agierens einer natürlichen Person ab. 3. Der Inhaltskontext ist dann gegeben, wenn ein Datum eine inhaltliche Aussage über eine Person trifft.[16]

Kein Personenbezug besteht, wenn die Daten so verschleiert bzw. anonymisiert oder Daten in einer Gruppe so zusammengefasst, d. h. aggregiert wurden, dass eine genaue Zuordnung

9 Zum Datenschutz durch den Deutschen Presserat *Münch*, AfP 2002, 18 ff.; *Thomale*, Die Privilegierung der Medien im deutschen Datenschutzrecht, 2006, Ziff. 7.
10 So richtig *Thomale*, AfP 2009, 107.
11 *Weichert*, DuD 2009, 7 f.
12 Klumpp/Kubicek/Roßnagel/Schulz-*Weichert*, Informationelles Vertrauen für die Informationsgesellschaft, 2008, S. 317 ff; *ders.*, VuR 2006, 377 ff.
13 Z.B. aktuell Agrar- und Fischereifonds-Informationengesetz v. 26.11.2008, BGBl. I 2008, 2330.
14 Z.B. zur Veröffentlichung von identifizierenden Gerichtsurteilen *Flechsig*, AfP 2008, 284 ff.
15 *Weichert*, DuD 2007, 113 ff.
16 Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 v. 20.06.2007, WP 136.

zu einzelnen Personen nicht mehr möglich ist. Eine solche Anonymisierung ist möglich durch das Verschleiern bzw. Verpixeln von Gesichtern, Kfz-Kennzeichen oder Hausnummern.

Es kommt bei der Frage der Personenbeziehbarkeit nicht darauf an, welchen Zweck *die verarbeitende Stelle* mit den Daten verfolgt.[17] Relevant ist auch nicht, dass das zur Identifizierung nötige Zusatzwissen nur mit unzulässigen Methoden beschafft werden kann.[18] Da zumindest für Internet-Anbieter durch Anfrage bei den Zugangsanbietern bei Angabe des konkreten Zeitpunktes die Zuordnung einer dynamischen IP-Adresse zu einem Anschlussinhaber möglich ist, handelt es sich hierbei um ein personenbezogenes Datum.[19] Ist durch ein wirksames Identitätsmanagement des Betroffenen nur durch diesen ein verwendetes Pseudonym zuordenbar, so ist dieses für andere Personen und Stellen nicht personenbezogen.

D. Anwendbares Recht

Bevor eine weitere rechtliche Prüfung stattfindet, muss erst festgestellt werden, ob wegen des globalen Charakters des Internets überhaupt nationales deutsches Recht anwendbar ist. Für die Anwendbarkeit des Telemediengesetzes wird nach § 3 Abs. 1 TMG auf das Herkunftsland abgestellt. § 1 Abs.1 5 TMG stellt jedoch klar, dass damit keine Kollisionsregeln geschaffen werden, sodass die allgemeinen Kollisionsnormen gelten.[20] § 1 Abs. 5 BDSG knüpft an dem *Ort der Datenverarbeitung* der verantwortlichen Stelle an. Teilweise wird die Ansicht vertreten, dass es für die Anwendung des deutschen Datenschutzrechts auf den Serverstandort oder den Sitz des Unternehmens ankommt, da der Anbieter keine Vorstellung davon habe, wer von seinem Angebot Gebrauch macht. Es fehle ihm bzgl. der Verarbeitung von Nutzungsdaten und von Inhaltsdaten, z. B. aus Deutschland, ein konkretisierter Erhebungswille. Richtig ist aber, dass für die Anwendbarkeit des Datenschutzrechtes der Ort der Datenverarbeitung maßgeblich ist. Dies kann u. U. sogar der Standort des Clients sein, wenn dort etwa Cookies eines Betreibers verarbeitet werden.[21] Haben Internetunternehmen Töchter oder Filialen in Deutschland und zielt deren Angebot auf den deutschen Markt, etwa, indem sie ein deutschsprachiges Angebot bereithalten oder unter deutscher Länderkennung (xx.de) auftreten, so verfolgen sie gezielt die Erhebung und Verarbeitung von Nutzerdaten; sie können nicht behaupten, die bei ihnen verarbeiteten Daten seien aufgedrängt.

Es ist die Zielsetzung der EU-DSRL, eine möglichst einheitliche rechtliche Verantwortlichkeit für Unternehmen innerhalb der Europäischen Union (EU) zu gewährleisten, um den grenzüberschreitenden Datenverkehr nicht übermäßig zu beschränken. Insofern stellt § 1 Abs. 5 S. 1 BDSG auf das Sitzland ab, es sei denn, die Verarbeitung erfolgt durch eine Niederlassung im Inland.[22] Im letztgenannten Fall gilt auch das BDSG. Es war nicht Intention der EU-DSRL, bei einer *Verarbeitung außerhalb der EU*, also in einem sog. Drittland, das dortige Rechtsregime ausschließlich für anwendbar zu erklären und dadurch den Schutz des Rechts auf informationelle Selbstbestimmung möglicherweise vollständig auszuschließen. Das BDSG ist nach § 1 Abs. 5 S. 2 BDSG daher auch dann anwendbar, wenn die verantwortliche Stelle nicht im Bereich der EU bzw. des Europäischen Wirtschaftsraums (EWR) einen Sitz hat, in Deutschland aber die Daten erhebt, verarbeitet oder nutzt. Dies ist z. B. bei vielen Anbietern in den USA der Fall, die innerhalb der EU keine eigenen Niederlassungen haben. Nach § 1 Abs. 5 S. 3 können derartige Unternehmen außerhalb der EU einen im Ausland ansässigen Vertreter benennen, dem gegenüber die Datenschutzrechte geltend gemacht werden können und müssen.

Der Regelungsansatz der EU-DSRL und des BDSG führt dazu, dass in vielen, ja in den meisten Fällen einer Internetveröffentlichung mit einem deutschen Bezug deutsches oder zumindest sonstiges europäisches nationales Recht zur Anwendung kommt. Es gibt aber Fälle, in denen Webseiten in den USA gehostet werden und in Europa weder eine Niederlassung noch eine Vertretung existiert und hier auch keine Stelle ausgemacht werden kann, die für die Verarbeitung verantwortlich zu machen ist, obwohl das Angebot auch auf den deutschen Markt abzielt. In diesen Fällen gibt es u. U. *keine rechtlichen europäischen Ansatzpunkte* zum Tätigwerden. Ein solches Beispiel war die Prangerseite rottenneighbor.com in den USA, auf der deutsche Nutzer anonym (diffamierende) Daten über Nachbarn einstellen konnten. Im konkreten Fall konnte dennoch über aufsichtsbehördliche Aktivitäten erreicht werden, dass dieser Anbieter sein deutsches Angebot aus dem Netz nahm.[23]

E. Datenschutzrechtliche Verantwortlichkeit für Internetveröffentlichungen

Die Klärung der Verantwortlichkeit für Internetveröffentlichungen kann unterschiedliche Zielrichtungen verfolgen. Geht es um die Haftung für Veröffentlichungen, so gelten die Regelungen der §§ 7 ff. TMG.[24] Relevant sein kann die Frage der Verantwortlichkeit aus zivilrechtlicher Sicht, im Hinblick auf die Sanktionierbarkeit nach Ordnungswidrigkeiten- und nach Strafrecht, als Adressat von behördlichen Verfügungen, z. B. zur Gefahrenabwehr und natürlich aus Datenschutzsicht. Bei von einer Person *selbst ins Netz gestellten Inhalten* ist die Verantwortlichkeit in jeder rechtlichen Hinsicht selbstverständlich durch sie selbst gegeben.

Fraglich ist dagegen die Verantwortlichkeit, wenn der für ein Portal, einen Dienst oder eine Seite Verantwortliche nur die Plattform zur Verfügung stellt und andere, evtl. gar anonym, Informationen einstellen. Nach § 10 TMG ist der *Anbieter für fremde Informationen* nur insofern verantwortlich, als er Kenntnis von den rechtswidrigen Inhalten erlangt hat und nicht unverzüglich tätig geworden ist, um die Informationen zu entfernen oder den Zugang zu ihnen zu sperren. Diese Regelungen setzen im Grunde die Kenntnisnahme der jeweiligen Inhalte voraus. Dies gilt auch für die strafrechtliche Verantwortlichkeit, wobei neben der Kenntnis ein Willenselement des Veröffentlichers hinzukommen muss, also Absicht, Vorsatz oder zumindest Fahrlässigkeit.[25] Für die Verantwortlichkeit für zivilrechtliche Ansprüche auf Schadenersatz ist § 10 TMG nicht direkt anwendbar. Da ein Webseitenbetreiber die Möglichkeit hat, schnell rechtsverletzende Beiträge zu

17 *Weiche*rt, DuD 2009, 351; a.A. *Forgó/Krügel/Reiners*, Geoinformation und Datenschutz, Gutachten v. 20.12.2008.
18 Däubler/Klebe/Wedde/Weichert-*Weichert,* a.a.O. (s. Fn. 4), § 3 Rz. 3; a.A. *Marian/Forgó/Krügel,* DuD 2006, 704.
19 *Breyer,* MMR 2009, 16; Däubler/Klebe/Wedde/Weichert-*Weichert,* a.a.O. (s. Fn. 4), § 3 Rz. 4; a.A. *Meyerdierks*, MMR 2009, 8 ff.
20 *Jotzo*, MMR 2009, 234.
21 *Jotzo*, MMR 2009, 237; *Ott*, MMR 2009, 160.
22 *Jotzo*, MMR 2009, 234 f.
23 31. Tätigkeitsbericht - TB - des ULD, 2009, Kap. 7.4, S. 137 ff.
24 Schneider-*Hoeren*, FS Heussen, 2009, 215.
25 BGH MMR 2007, 518 f.

entfernen und evtl. bestimmte Nutzungsformen zu sperren, bestehen gegen ihn die zivilrechtlichen Beseitigungs- und Unterlassungsansprüche. Anwendbare Kollisionsnorm für zivilrechtlich geltend zu machende Persönlichkeitsverletzungen ist Art. 40 EGBGB.[26] Der Bundesgerichtshof hat diese Störerhaftung durch das Kriterium der "Zumutbarkeit" eingeschränkt. Nur wenn er zumutbare Prüfungspflichten im Hinblick auf mögliche rechtswidrige Inhalte verletzt hat, kann er wegen Unterlassung und Beseitigung in Anspruch genommen werden).[27] Es ist klar, dass der Betreiber ab dem Zeitpunkt der Kenntnis einer Rechtsverletzung tätig werden muss. Die Rechtsprechung nimmt umso mehr eine Prüfungspflicht an, je höher die Gefahr der Rechtsverletzung ist. Dies gilt besonders, wenn ein Rechtsverstoß provoziert wurde.[28] Dass ein Betreiber die von anderen auf seiner Webseite eingestellten Inhalte regelmäßig überprüfen müsste,[29] ohne zuvor von Verstößen in Kenntnis gesetzt worden zu sein, ist angesichts der verwendeten Internet-Technologie und dem sich daraus ergebenden Massengeschäft nicht zumutbar, ja oft nicht einmal objektiv möglich.[30]

Demgegenüber ist die *datenschutzrechtliche Verantwortung* nicht von einer Kenntnis der Daten abhängig. Die datenschutzrechtliche Verantwortlichkeit hat in vieler Hinsicht Bedeutung. Sie ist relevant bei Kontrollmaßnahmen nach § 38 BDSG sowie bei der Wahrnehmung von Betroffenenrechten nach § 33 ff. BDSG, also auch bei Ansprüchen auf Auskunft, Sperrung oder Löschung. Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle, wer personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt. In Art. 2d) EU-DSRL wird darauf abgestellt, wer "über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". D. h., im Datenschutzrecht wird unabhängig vom Wissen über die Daten darauf abgestellt, wer objektiv über die Daten bestimmen kann, wer die Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung hat.[31] Der Rückgriff auf eine Datenverarbeitung im Auftrag nach § 11 BDSG ist bei Internetveröffentlichungen schon deshalb nicht möglich, weil ein explizites vertragliches Auftragsverhältnis zwischen dem Seitenbetreiber und demjenigen, der einen Inhalt eingestellt hat, in der Regel nicht besteht. Auch die weiteren Anforderungen des § 11 BDSG liegen zumeist nicht vor. Dies hat zur Folge, dass jeder Inhaltsanbieter in datenschutzrechtlicher Hinsicht für sämtliche gehosteten Daten verantwortlich ist. Dies führt bei das ganze öffentliche Web umfassenden Suchmaschinen mit eigenem Cache dazu, dass rechtlich eine Verantwortlichkeit für alle erfassten Webinhalte besteht.[32]

Die Identität des *verantwortlichen Seitenbetreibers* lässt sich bei deutschen Anbietern relativ einfach über das Impressum feststellen (§ 5 TMG, § 55 RStV).

F. Einwilligung in die Veröffentlichung

Die Veröffentlichung von Daten im Internet ist zulässig, wenn die betroffene Person eingewilligt hat (§ 4 Abs. 1 BDSG). Gemäß § 4a Abs. 1 S. 2 BDSG setzt eine wirksame Einwilligung eine besonders hervorgehobene *schriftliche Erklärung* voraus, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist". Bei der digitalen Kommunikation, die der Internet-Veröffentlichung oft vorangeht, kann eine konventionelle schriftliche Einwilligung oft nicht mehr als angemessen angesehen werden, insbesondere wenn der Betroffene sich räumlich weit entfernt vom Inhaltsanbieter befindet. Etwas anderes gilt bei einem persönlichen Kontakt zwischen Anbieter und Betroffenen, etwa bei Veröffentlichungen auf der Seite einer Schule, eines Sportvereins, des Veranstalters eines Ereignisses oder des Arbeitgebers. Nach § 13 Abs. 2 TMG kann eine Einwilligung elektronisch erteilt werden. Diese explizit nur für Mediendienste geltende Regelung ist auch auf Internetveröffentlichungen anwendbar. Voraussetzung für die Wirksamkeit ist, dass die Einwilligung bewusst und eindeutig ist. Damit sollen versehentliche Mausclicks nicht mit Rechtsfolgen verknüpft sein. Dem Erfordernis genügt z. B. eine wiederholte Bestätigung und die zumindest das Wesentliche enthaltende Darstellung des Erklärungsinhaltes.[33] Nach § 13 Abs. 2 Nr. 2 TMG muss der Anbieter die Einwilligung protokollieren. Der Nutzer muss die Möglichkeit haben, die elektronische Einwilligung abzurufen, etwa indem sie ihm über einen Link im Volltext zur Verfügung gestellt wird (Abs. 2 Nr. 3). Nach Abs. 2 Nr. 4 muss der Betroffene jederzeit die Einwilligung für die Zukunft widerrufen können. Auf diese Möglichkeit ist er vor der Einwilligung hinzuweisen; auch dieser Hinweis muss so zugänglich gespeichert sein, dass er vom Betroffenen jederzeit abrufbar ist (§ 13 Abs. 3 TMG).

Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, so ist sie *besonders hervorzuheben* (§ 4a Abs. 1 S. 3 BDSG). Soll die Einwilligung in die Veröffentlichung im Rahmen von Allgemeinen Geschäftsbedingungen (AGB) erklärt werden, so muss die Einwilligungserklärung in direktem Zusammenhang zur Unterschrift stehen.

Die einwilligende Person muss eine hinreichende Vorstellung über die Art der Daten, deren Adressaten und die damit verfolgten Zwecke haben (*Bestimmtheitserfordernis*).[34] Da mit einer Internetveröffentlichung eine weltweite Verfügbarkeit gegeben ist und Zwecke nicht mehr eingegrenzt werden können, muss sich die Einwilligung hierauf ausdrücklich beziehen und die Art der Daten möglichst präzise beschrieben werden. Für eine Einwilligung genügt z. B. nicht die Teilnahme an einer Sportveranstaltung, auch wenn den Teilnehmenden in allgemeiner Form bekannt gemacht wurde, dass deren Namen und Ergebnisse im Web veröffentlicht werden. Vielmehr muss diese Bekanntmachung so erfolgen, dass jeder Teilnehmer diese tatsächlich zur Kenntnis nimmt und mit der Teilnahmeerklärung seine Zustimmung zur Veröffentlichung erklärt.

Eine Einwilligung ist nur wirksam, wenn sie freiwillig erfolgt (§ 4a Abs. 1 S. 1 BDSG). Wann dies der Fall ist, kann streitig sein. Wenn eine soziale Drucksituation gegeben ist, kann die nötige *Freiwilligkeit* ausgeschlossen sein, etwa, wenn in einem Klassenverbund einer Schule eine gemeinsame Teilnahme an einer mit einer Internetveröffentlichung verbundenen Sportveranstaltung erfolgt. Keine Freiwilligkeit ist mehr gegeben, wenn ein Sportverband in seiner Satzung zwangsweise und ohne Wahlmöglichkeit die Veröffentlichung der Namen von Teilnehmern an Sportveranstaltungen und deren Ergebnisse

26 *Jotzo*, MMR 2009, 233.
27 BGH NJW 2001, 3265 ff.
28 OLG Hamburg CR 2007, 44 ff.
29 So wohl LG Hamburg MMR 2007, 450 ff. u. 726 ff.
30 *Breyer*, MMR 2009, 14 ff. gegen OLG Hamburg MMR 2008, 823.
31 *Weichert*, DuD 2009, 10; *Jotzo*, MMR 2009, 233.
32 Lewandowski-*Weichert*, Handbuch Internet-Suchmaschinen, 2009, S. 293 f.; a.A. wohl *Ott* für reine Vermittlungsdienste ohne Cache-Speicherung und im Licht von Art. 5 GG, MMR 2009, 162.
33 Schneider-*Hoeren*, a.a.O. (s. Fn. 24), S. 213.
34 Däubler/Klebe/Wedde/Weichert-*Däubler,* a.a.O. (s. Fn. 4), § 4a Rz. 18.

vorsieht, da hierdurch alle ausgeschlossen werden, die ihre Daten unveröffentlicht sehen und dennoch einen bestimmten Sport gemeinsam mit anderen, d. h. organisiert, ausüben wollen. Die Freiwilligkeit kann auch dadurch eingeschränkt sein, dass die Einwilligung zur Verarbeitung von personenbezogenen Daten bis hin zur Internetveröffentlichung, zur Voraussetzung gemacht wird zur Erlangung von bestimmten Diensten und Leistungen. Dem versucht das Recht mit Koppelungsverboten entgegenzuwirken (§ 12 Abs. 1 TMG, künftig § 28 Abs. 3b BDSG).[35]

Für die Feststellung der Freiwilligkeit kann es von Bedeutung sein, ob den Betroffenen eine nichtpersonenbezogene Alternative angeboten wird. Diese kann in einer einfachen Form eines sog. *Identitätsmanagements* liegen, also darin, dass der Name durch ein Pseudonym (z. B. Spieler/Mitglied/Teilnehmer/Schüler 1, 2, 3 ... oder A, B, C ...) ersetzt wird und für den Betroffenen insofern eine Wahlmöglichkeit besteht.

G. Gesetzliche Verarbeitungsnormen

Die §§ 28 Abs. 1 Nr. 3, 29 Abs. 1 Nr. 2 BDSG erlauben die Verarbeitung von Daten, wenn diese "allgemein zugänglich sind". Nicht möglich ist aber der Zirkelschluss, dass unzulässig ins Netz gestellte Daten allgemein zugänglich sind und daher deren weitere Verarbeitung erlaubt wäre. Eine solche Auslegung würde sämtliche Inhalte im Web zulässig machen; Datenschutz gäbe es bei Internetveröffentlichung nicht mehr. Die gesetzlichen Regelungen enthalten daher auch die Beschränkung, dass das „schutzwürdige Interesse des Betroffenen" an der Verarbeitung nicht offensichtlich überwiegt. Das Gesetz verlangt damit etwas bei Internetinhalten objektiv fast Unmögliches: Die *Abwägung* zwischen dem schutzwürdigen Betroffeneninteresse und dem berechtigten Interesse nicht bekannter, möglicherweise millionenfacher Nutzender. Das Schutzinteresse ist für die meisten Verantwortlichkeiten kaum einschätzbar, da diese die Betroffenen zumeist nicht kennen, schon gar nicht deren individuelle Interessen.

Im Internet veröffentlichte Daten sind solche, die zum *Zweck der Übermittlung* verarbeitet werden, was in § 29 BDSG geregelt ist. Nach dieser Norm müssten hohe Anforderungen gestellt werden: Glaubhaftmachung eines berechtigten Interesses, Festlegung eines Zweckes, Abwägung der Interessen, Dokumentation und stichprobenhafte Prüfung der Abrufe. Nähme man das BDSG wörtlich, so wären Bewertungsportale, Blogs, Chatbeiträge über Dritte, Suchmaschinen und vieles mehr rechtswidrig.[36] Die Rechte aus Art. 5 GG werden in § 29 BDSG nicht ausdrücklich erwähnt. Einige der in § 29 genannten Anforderungen lassen sich selbst über eine verfassungskonforme Auslegung nicht erfüllen. Dies hat zur Folge, dass, solange für Internetveröffentlichung keine spezialgesetzlichen Regelungen bestehen,[37] von diesen Anforderungen Abstriche gemacht werden müssen, soweit anderenfalls Art. 5 GG unverhältnismäßig beschnitten würde. Bei der vorzunehmenden Abwägung spielen folgende Aspekte eine wichtige Rolle: vorherige individuelle oder allgemeine Benachrichtigung der Betroffenen, Möglichkeit des Widerspruchs der Betroffenen, keine Aufnahme auf Widerspruchslisten (vgl. § 29 Abs. 3 BDSG), relativ geringe Sensibilität, Erkennbarkeit des Wertungscharakters der Daten, Betroffenheit der Person als Funktionsträger, keine Schmähkritik.

Redaktionell-journalistische Tätigkeit unterliegt dem besonderen Schutz der Pressefreiheit des Art. 5 Abs. 1 S. 2, 3 GG. Absolute materiell-rechtliche Restriktionen bestehen nicht. Vielmehr unterliegen Veröffentlichungen der Abwägung zwischen dem Veröffentlichungs- und dem Schutzinteresse des Betroffenen. Ein präventiver Schutz ist nicht zulässig; nachträgliche Schutzvorkehrungen liegen insbesondere in den Betroffenenrechten. Es gilt Ziff. 8 des *Pressekodexes des Deutschen Presserats*: „Die Presse achtet das Privatleben und die Intimsphäre des Menschen. Berührt jedoch das private Verhalten öffentliche Interessen, so kann es im Einzelfall in der Presse erörtert werden. Dabei ist zu prüfen, ob durch eine Veröffentlichung Persönlichkeitsrechte Unbeteiligter verletzt werden. Die Presse achtet das Recht auf informationelle Selbstbestimmung und gewährleistet den redaktionellen Datenschutz." Damit wird die Veröffentlichung von personenbezogenen Daten immer von einer Abwägung abhängig gemacht, auch wenn nicht die Privat- oder Intimsphäre betroffen sind.

H. Betroffenenrechte

Wegen der oft schwer zu klärenden tatsächlichen Verantwortlichkeit und den Möglichkeiten des Kopierens und Umadressierens von Inhalten, ist es äußerst schwierig, die eigenen Betroffenenrechte im Internet durchzusetzen. Besonders problematisch ist es, wenn Betroffene selbst keinen Internetzugang haben und dadurch selbst praktisch überhaupt nicht ihre Betroffenheit feststellen können. Zumindest hinsichtlich der Auskunftserlangung über im Web zur eigenen Person gespeicherten Daten gibt es ein – technisches, nicht rechtlich fundiertes – Instrument: Mithilfe von Suchmaschinen kann festgestellt werden, auf welchen Seiten Daten über einen selbst wie über andere gespeichert sind. Erheblich schwieriger ist die *praktische Durchsetzung von Ansprüchen* auf Berichtigung, Löschung und Sperrung. Nur selten bieten Internetangebote eine Kommentar-Funktion an, über die abweichende Sichtsweisen dargestellt werden können. Dies hat dazu geführt, dass private Firmen als "Reputation Defender" ihre Dienste anbieten, um inkriminierende Inhalte aus dem Netz zu bekommen oder nicht zwangsläufig korrekte eigene positive Darstellungen vorzunehmen.[38]

Der *Anspruch auf Auskunft* über die zur eigenen Person gespeicherten Daten ergibt sich direkt aus dem Grundrecht auf informationelle Selbstbestimmung, es handelt sich beim Auskunftsanspruch sozusagen um die Magna Charta des Datenschutzes.[39] Im Hinblick auf gespeicherte Bestands- und Nutzungsdaten besteht der Anspruch auf Auskunft nach § 13 Abs. 7 TMG. Der Auskunftsanspruch zu Inhaltsdaten ergibt sich gegenüber der verantwortlichen Stelle aus § 34 BDSG. Als Einwand gegen eine Auskunftspflicht können bei Internetdatenspeicherungen regelmäßig keine Geschäftsgeheimnisse vorgetragen werden (vgl. § 34 Abs. 1 S. 3); auch eine Kostenerhebung ist regelmäßig ausgeschlossen, selbst bei Internet-Auskunfteien, da hier das ideelle Informationsinteresse das wirtschaftliche Eigeninteresse regelmäßig zurückdrängt (vgl. § 34 Abs. 5 S. 2 BDSG). Bzgl. geschützt gespeicherter Inhalte bieten Internet-Suchmaschinen keine Hilfe; hier muss der Anspruch über ein Auskunftsbegehren des

35 Dazu Schneider-*Hoeren,* a.a.O. (s. Fn. 24), S. 213.
36 *Weichert*, MR-Int 2007, 191.
37 Dies fordert *Weichert*, DuD 2009, 11 f.
38 *Weichert*, Online Reputation Management, 1/2009, abzurufen unter: https://www.datenschutzzentrum.de/vortraege/20090213-weichert-reputation-management.html; zu den praktischen Problemen und den rechtspolitischen Konsequenzen bei Betroffenenrechten *Weichert*, DuD 2009, 11 f.

Betroffenen geltend gemacht werden. Da der gesetzliche Auskunftsanspruch nicht von der technischen Kompetenz des Betroffenen abhängig gemacht wird, kann dieser auch schriftlich geltend gemacht werden. Er hat sich an die im Impressum genannte Adresse zu richten. Um eine schnelle und erfolgreiche Bearbeitung zu gewährleisten, sollte jeder Auskunftsanspruch an den betrieblichen Datenschutzbeauftragten gerichtet werden (vgl. §§ 4f, 4g BDSG). Ein Anspruch auf Löschung von selbst ins Netz gestellten Überzeugungen besteht in den engen Grenzen des § 42 UrhG. Danach muss ein Werk urheberrechtlich geschützt sein und der Inhalt muss von der inzwischen bestehenden Überzeugung des Urhebers abweichen.[40]

Weiterhin hat jeder Betroffene einen Anspruch auf Berichtigung unrichtiger Angaben im Internet (§ 35 Abs. 1 BDSG). Unzulässig gespeicherte Daten sind zu löschen (§ 35 Abs. 2 Nr. 1 BDSG). Dass die Lösch- bzw. Prüfpflicht am Ende des 4. Jahres nach der erstmaligen Speicherung besteht (§ 35 Abs. 2 Nr. 4 BDSG), lässt sich zwar aus dem Gesetz ableiten. Es ist aber fraglich, ob diese nicht auf das Internet ausgerichtete Regelung auf Webangebote übertragbar, d. h. eine solche Prüfpflicht zumutbar ist.

Bzgl. redaktionell-journalistischer Onlineangebote gewährt § 57 Abs. 2 RStV unter bestimmten Voraussetzungen einen Auskunfts- und Berichtigungsanspruch. Der Auskunftsanspruch besteht grds. bereits vor einer Berichterstattung. Teilweise oder gar völlig eingeschränkt ist der Auskunftsanspruch aber, wenn die journalistische Aufgabe des Veranstalters beeinträchtigt würde. Daher ist in der Praxis ein Auskunftsanspruch vor Berichterstattung i. d. R. ausgeschlossen. Es muss ein schutzwürdiges Auskunftsinteresse geltend gemacht werden. Es ist dabei eine Abwägung zwischen der durch Art. 5 Abs. 1 GG geschützten Tätigkeit und dem Persönlichkeitsschutz nach Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG vorzunehmen. Eine reine Interessenbehauptung oder ein subjektiver Vortrag genügt nicht. Nötig ist aber auch nicht eine erfolgte Rechtsbeeinträchtigung. Der Anspruch erstreckt sich nur auf die gespeicherten Daten, nicht auf die Quelle der Informationen.[41] Eine Auskunftsverweigerung ist möglich, wenn durch die Auskunft eine Ausforschung der journalistischen Tätigkeit erfolgen würde, also z. B. die Recherchemethode, die Herkunft, der Umfang und die Zusammensetzung der vorhandenen Informationen aufgedeckt würden. Geschützt werden die an der Veröffentlichung beteiligten Mitarbeiter, Einsender bzw. Auskunftspersonen und sonstige Quellen (§ 57 Abs. 2 Nr. 1, 2 RStV). In jedem Fall ist eine Interessenabwägung vorzunehmen. Auch gemäß dem Pressekodex hat das verantwortliche Publikationsorgan dem Betroffenen Auskunft über die der Berichterstattung zugrunde liegenden Daten zu erteilen. Verweigerungsgründe bestehen dann, wenn auf Informanten oder sonstige Quellen geschlossen werden kann oder wenn nur so das Recht auf Privatsphäre mit der Freiheit der Meinungsäußerung in Einklang gebracht werden kann.

§ 57 Abs. 2 S. 3 RStV legt zudem einen *Berichtigungsanspruch* fest, also auf die Korrektur von unrichtigen Daten. Der Betroffene trägt die Beweislast für die Unrichtigkeit. Alternativ kann der Betroffene auch verlangen, dass den Daten eine eigene Darstellung von angemessenem Umfang hinzugefügt wird. § 57 Abs. 3 RStV verpflichtet Telemedienanbieter zur Zuspeicherung von Gegendarstellungen bei den über den Betroffenen gespeicherten Daten – unverzüglich, ohne Kosten für den Betroffenen und ohne Abrufentgelt. Die Gegendarstellung ist über denselben Zeitraum aufzubewahren wie der Originaldatensatz. Dies zielt auf die kommunikative Chancengleichheit des Betroffenen mit dem Anbieter ab.[42] Der Anbieter ist verpflichtet, die Gegendarstellungen bei einer Übermittlung der Daten gemeinsam mit diesen weiterzugeben. Ergänzend enthält Ziff. 3 des Pressekodex eine Richtigstellungsverpflichtung unrichtiger Presseberichte. Gem. Ziff. 4 muss das Publikationsorgan die Richtigstellungen, Widerrufe, Gegendarstellungen oder Rügen des Presserates zu den gespeicherten Daten nehmen und für dieselbe Zeitdauer dokumentieren. Bei Verstößen gegen den Pressekodex besteht weiterhin die Pflicht zur Sperrung oder zur Löschung.

I. Anrufung der Aufsichtsbehörde

Bei der behördlichen *Aufsicht über das Internet* ist zwischen verschiedenen Zielsetzungen zu unterscheiden. Es gibt keine einheitliche Internetaufsicht; zu unterscheiden ist u. a. zwischen Jugendschutz, der wirtschaftsrechtlichen Aufsicht über Telemedien[43] und der Datenschutzaufsicht.

Bestehen Hinweise auf eine unzulässige Datenverarbeitung, so kann sich der Betroffene an die *zuständige Datenschutzkontrollinstanz* wenden. Dieser Anspruch ergibt sich aus dem Petitionsrecht des Art. 17 GG sowie aus einfachgesetzlichen Regelungen (z. B. § 21 BDSG, § 40 LDSG SH). Zuständig für die Datenschutzkontrolle von Internetveröffentlichungen durch private Stellen sind die Länderbehörden nach § 38 BDSG. Anknüpfungspunkt für die örtliche Zuständigkeit ist regelmäßig der Ort der Datenverarbeitung bzw. der Sitz der verantwortlichen Stelle. Liegt der Sitz im europäischen Ausland und gibt es keine nationale Niederlassung, so muss sich der Betroffene an die Aufsichtsbehörde des Sitzlandes wenden.[44] Die in Deutschland örtlich zuständigen Aufsichtsbehörden sind im Internet zu finden unter http:www.datenschutz.de (dort „Institutionen", dann „Deutschland (nichtöffentlicher Bereich)".[45]

Bei *redaktionell-journalistischen Beiträgen* im Internet tritt an die Stelle der Datenschutzaufsichtsbehörde nach § 38 BDSG der Deutsche Presserat (§ 57 Abs. 1 i. V. m. § 38 BDSG).[46] Dieser ist zunächst Standesorganisation und damit zur Wahrung der Interessen der Presse verpflichtet. Er sieht hierin die Legitimation zur Feststellung von Missständen im Pressewesen und fungiert damit auch als Beschwerdeinstanz. Anzuwenden sind die „publizistischen Grundsätze" des 1973 aufgestellten Pressekodex. Der Deutsche Presserat hat 2001 seine Beschwerdeordnung um rundfunkrechtliche Elemente erweitert. Hierzu gehören: Zuspeicherungspflicht von Gegendarstellungen, Auskunftsanspruch nach Berichterstattung, Sperrung und Löschung kodexwidriger Inhalte, Sicherung des Redaktionsgeheimnisses und ein Beschwerderecht bei der Annahme von Datenschutzverstößen.[47] Die Beschwerdeordnung des Deutschen Presserates ermöglicht nicht nur die

39 Hahn/Vesting-*Herb*, Rundfunkrecht, 2008, § 57 Rz. 20; zur verfassungsrechtlichen Verortung *Weichert*, NVwZ 2007, 1005 f.
40 *Ott*, MMR 2009, 163.
41 Simitis-*Walz*, BDSG, 6. Aufl. 2006, § 41 Rz. 39.
42 BVerfGE 63, 142 ff.
43 Dazu *Holznagel/Ricke*, MMR 2008, 18 ff.
44 Die aktuellen Adressen sind abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_de.htm.
45 Abzurufen unter der Internetadresse: http://www.bfdi.bund.de/cln_030/nn_531524/DE/AnschriftenUndLinks/AufsBehoerdFuerDenNichtOeffBereich/AufsBehoerdFuerDenNichtOeffBereich_node.html_nnn=true; zum Reformbedarf *Weichert*, DuD 2009, 13.
46 Vgl. http://www.presserat.de; *Münch*, AfP 2002, 18 ff.
47 *Thomale*, AfP 2009, 107 f.

Anrufung durch den Betroffenen, sondern auch – kostenlos und ohne bürokratische Einschränkungen – für jede dritte Person.[48] Ist eine Beschwerde begründet, so spricht der Presserat eine Sanktion in Form einer öffentlichen Rüge bzw. u. U. aus Gründen des Opferschutzes, eine nichtöffentliche Rüge, eine Missbilligung oder einen Hinweis aus. Wird eine öffentliche Rüge ausgesprochen, so liegen meistens Persönlichkeitsverletzungen vor, die nach der Rechtsprechung auch einen Schadenersatzanspruch auslösen.[49] Hat das Presseorgan eine entsprechende Selbstverpflichtungserklärung unterschrieben, so muss es im Fall einer Rüge diese abdrucken. Der Presserat hat einen entsprechenden einklagbaren Anspruch. Ein hieraus ableitbarer Anspruch für den Betroffenen selbst wird demgegenüber aber nicht angenommen.[50]

J. Perspektiven

Der Schutz vor unzulässigen Inhalten im Internet ist – technisch bedingt – nur unzureichend zu gewährleisten.[51] Dies darf keineswegs ein Grund für eine Kapitulation vor der Aufgabe des Staates sein, seiner Gewährleistungspflicht insbesondere im grundrechtlichen Bereich nachzukommen. Es besteht zweifellos schon heute ein normativer und organisatorischer Rahmen zum Schutz des Rechts auf informationelle Selbstbestimmung bei Internetveröffentlichungen. Diese können und sollten die Betroffenen in Anspruch nehmen. Nur dadurch erweisen sich die Unzulänglichkeiten und ergibt sich der notwendige politische Leidensdruck für die Umsetzung von Verbesserungen. Derartige Verbesserungen können auf allen Ebenen ansetzen: rechtlich, organisatorisch, technisch, pädagogisch, beim Betroffenen, bei Datenschutz- und Verbraucherschutz-Interessenvertretern, bei den Internetanbietern und bei der Politik, national, auf europäischer Ebene wie auch global.[52] Als Nadelöhr muss aber derzeit die nationale Gesetzgebung ausgemacht werden: Ohne Anpassung des nationalen Rechts kann es weder auf den untergeordneten noch auf den übergeordneten Ebenen nennenswerte Fortschritte geben. Alle Beteiligten sind gefordert, Beiträge zur Gewährleistung des Datenschutzes im Internet zu liefern; an erster Stelle kommt aber dem Bundesgesetzgeber eine solche Pflicht zu.[53]

48 *Münch*, AfP 2002, 18.
49 *Thomale*, AfP 2009, 109.
50 *Thomale*, AfP 2009, 109.
51 *Weichert*, RDV 2007, 54 ff.
52 *Hermann*, AfP 2003, 233 ff.
53 *Weichert*, DuD 2009, 7 ff.