Recht sicher?

Persönlichkeitsrechtsschutz im Netz

Thomas Fetzer

I. Einleitung

Das Thema "Datenschutz im Internet" hat in den vergangenen Wochen und Monaten auch in der öffentlichen Wahrnehmung an Bedeutung deutlich zugenommen. Im Vordergrund stehen dabei allerdings fast ausnahmslos Fälle, in denen der Staat beziehungsweise staatliche Einrichtungen auf personenbezogene Daten von Bürgern zugreifen wollen. Meist geht es darum, dass Gefahrenabwehr- oder Strafverfolgungsbehörden zum Zwecke der Terrorismusbekämpfung Zugriff auf Daten erhalten sollen. In diese Kategorie fällt die geplante Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten ebenso wie die intensiv diskutierte so genannte "Online-Durchsuchung" von PCs. Schließlich hat ein aktuelles Urteil des Landgerichts Berlin auch einer breiteren Öffentlichkeit offenbart, dass manche Behörden offensichtlich Daten von Besuchern der behördeneigenen Webseite speichern, um diese gegebenenfalls zu einem späteren Zeitpunkt zum Zwecke der Strafverfolgung oder Gefahrenabwehr einsetzen zu können.[1]

Angesichts dieser offenkundigen und schwerwiegenden Gefahren für die Privatsphäre der Bürger durch öffentliche Stellen darf allerdings nicht übersehen werden, dass der Privatsphäre des Einzelnen im Internet mindestens ebenso große Gefahren durch die kommerzielle Nutzung des Internet von der nicht-öffentlichen Seite drohen. Jeden Tag wird eine unvorstellbar große Menge von personenbezogenen Daten über das Internet verschickt. Bei jeder Be-

[1] LG Berlin, Urteil vom 06.09.2007, Az: 23 S 3/07.

stellung bei einem Internethändler, bei jedem Webseitenaufruf, ja bei jedem Zugang zum Internet fallen vielfältige Informationen über den jeweiligen Internetnutzer an. Eine besondere Gefährdungslage besteht dabei insbesondere im Verhältnis zwischen Internetnutzern und Internetprovidern. Internetprovider treten heute nur noch selten als reine Access Provider auf, die sich auf die rein technische Vermittlung eines Zugangs zum Internet beschränken. Sie sind vielmehr im Regelfall Internet Service Provider, die ihren Kunden in Form von Komplettpaketen neben der rein technischen Vermittlung eines Zugangs zum Internet auch die Nutzung des World Wide Web (www) und E-Mail sowie Nachrichtendienste anbieten. Bei einem solchen Angebot spielen eine ganze Reihe von personenbezogenen Daten eine Rolle: Neben den so genannten Bestandsdaten, die zur Abwicklung des Vertragsverhältnisses zwischen Internetprovider und Kunden erforderlich sind - also etwa Anschrift und Kontoverbindung des Kunden -, erhält der Provider nahezu zwangsläufig auch Kenntnis davon, welche Angebote seine Kunden nutzen, welche Webseiten sie besuchen, welche Produkte sie dort kaufen und mit wem sie E-Mails austauschen. Hierbei fallen regelmäßig als personenbezogene Daten neben der IP-Adresse, die eine Identifizierung eines Nutzers ermöglicht, unter anderem Datum, Uhrzeit, Dauer der Internetnutzung und auch die Adressen der dabei aufgerufenen Webseiten an.[2] Der Persönlichkeitsrechtsbezug dieser Daten ist erheblich: In der Hand einer einzigen Person - des Internetproviders - sind Daten vorhanden, die beispielsweise zur Erstellung von Nutzerprofilen verwendet werden können, die Rückschlüsse auf Einkaufsgewohnheiten, Freizeitverhalten und vieles mehr zulassen. Nicht umsonst konzentrieren sich auch die staatlichen Bemühungen um die Vorratsdatenspeicherung auf exakt diesen Datenpool. Auch für den Internetprovider haben diese Daten einen hohen - wenn auch kommerziellen - Wert, sofern er sie beispielsweise als Grundlage zielgruppenorientierten Marketings - des so genannten target marketing - nutzen kann.

Für das Datenschutzrecht ist die verfassungsrechtliche Ausgangslage auch in diesen Fällen einer Gefährdung des Persönlichkeitsrechts durch nicht-öffentliche Stellen klar: Ausgehend von den verfassungsrechtlichen Wurzeln in Art. 2 Abs. 1 Grundgesetz (GG) i. V. m. Art. 1 Abs. 1 GG ist Datenschutzrecht in Deutschland - an-

[2] Vgl. dazu Köhler/Arndt/Fetzer, Recht des Internet, 5. Aufl. 2006, S. 294.

ders etwa als in den USA[3] - vorrangig Persönlichkeitsrechtsschutz.[4] Das vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte Recht auf informationelle Selbstbestimmung,[5] das ein Aspekt des in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG verankerten allgemeinen Persönlichkeitsrechts ist, wirkt dabei zwar primär entsprechend der klassischen Funktion der Grundrechte als Abwehrrecht gegen staatliche Eingriffe.[6] Insofern müssen sich alle eingangs genannten aktuellen Beispiele für staatliche Datenerhebungen beziehungsweise Verarbeitungen an diesem Recht auf informationelle Selbstbestimmung messen lassen. Das Recht auf informationelle Selbstbestimmung verpflichtet den Gesetzgeber jedoch auch, einen umfassenden Schutz des Einzelnen gegenüber Gefahren für das Persönlichkeitsrecht, die von nicht-öffentlichen Stellen ausgehen, sicherzustellen.[7] Das Recht auf informationelle Selbstbestimmung hat hier nicht nur die Funktion eines Abwehrrechts gegen staatliche Eingriffe, sondern ist Ausdruck bestimmter Wertentscheidungen, die auch für den nicht-öffentlichen Bereich Geltung beanspruchen.[8]

Dies gilt angesichts der kurz skizzierten besonderen Gefährdungslage für das Persönlichkeitsrecht gerade auch für den Schutz personenbezogener Daten im Internet. Hier bedarf es ausgehend von den Vorgaben des Volkszählungsurteils bereichsspezifischer Regelungen, die den Einzelnen "gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" schützen.[9]

Dieser Beitrag setzt sich mit der Frage auseinander, ob das geltende Recht bereichsspezifische Regelungen bereithält, die einen wirksamen Schutz des Persönlichkeitsrechts auch gegen Gefahren durch nicht-öffentliche Stellen - also etwa Internetanbieter - gewährleisten. Eine der wesentlichen Voraussetzungen für einen solchen effektiven Schutz sind Regelungen, die dem Gebot der Norm-

---

[3] Hier tritt der Persönlichkeitsrechtsaspekt beim Schutz personenbezogener Daten deutlich hinter eine eigentumsrechtliche Perspektive zurück. Hierzu etwa Allen, Privacy Law, 2007, S. 27.

[4] Vgl. hierzu auch die einfachgesetzliche Regelung des § 1 Abs. 1 Bundesdatenschutzgesetz (BDSG).

[5] BVerfGE 65, 1.

[6] Vgl. hierzu statt aller Jarass, in: Jarass/Pieroth, GG Kommentar, 9. Aufl. 2007, Vorb. Vor Art. 1 Rn. 1.

[7] Vgl. Gola/Schomerus, BDSG Kommentar, 9. Aufl. 2007, Einleitung Rn. 6.

[8] Gola/Schomerus, BDSG Kommentar, 9. Aufl. 2007, Einleitung Rn. 6.

[9] BVerfGE 65, 1 (43).

klarheit entsprechen und hierdurch Rechtssicherheit schaffen.[10] In einem ersten Schritt soll daher der Frage nachgegangen werden, inwieweit die bestehenden gesetzlichen Vorschriften diese Vorgabe der Rechtsklarheit und Rechtssicherheit erfüllen können (dazu II.). Selbst klare und Rechtssicherheit schaffende Normen schützen aber das Persönlichkeitsrecht nicht ausreichend, wenn sie in der Praxis nicht oder jedenfalls nicht ausreichend befolgt werden. Das Datenschutzrecht setzt bei seiner Durchsetzung traditionell auf ordnungsrechtliche Ansätze. Eine zweite Frage, auf die daher eingegangen werden soll, ist, ob dieser primär ordnungsrechtlich ausgerichtete Ansatz des Datenschutzrechts ausreichend ist, um Persönlichkeitsrechtsschutz auch in Zeiten des Internet angemessen zu gewährleisten und welche alternativen Möglichkeiten gegebenenfalls hierzu bestehen (dazu III.). In einem abschließenden Teil werde ich mich schließlich der Frage zuwenden, welche Voraussetzungen bei den Trägern des allgemeinen Persönlichkeitsrechts - den einzelnen Personen - geschaffen werden müssen, um ihnen eine effektive Ausübung des Rechts auf informationelle Selbstbestimmung zu ermöglichen (dazu IV.).

II. Datenschutzrechtlicher status quo

Wendet man sich zunächst der Frage zu, ob es für den kommerziellen Umgang mit personenbezogenen Daten im Internet eine Rechtssicherheit schaffende bereichsspezifische Regelung gibt, so muss man feststellen, dass sich die Antwort hierauf leider nicht durch den Blick in ein einheitliches "Internetdatenschutzgesetz" ergibt. Vielmehr finden sich datenschutzrechtliche Regelungen zum Umgang mit personenbezogenen Daten durch Private im Internet in verschiedenen Gesetzen. Diese gesetzlichen Regelungen sind im Wesentlichen allerdings nicht das Ergebnis einer systematischen Analyse der datenschutzrechtlichen Gefährdungslage im Internet. Ihre Struktur ist meist schlicht historisch gewachsen:

Traditionell unterscheidet das Kommunikationsrecht nämlich unter anderem aufbauend auf ein so genanntes OSI-Schichtenmodell zwischen verschiedenen Ebenen eines Kommunikationsvorgangs.[11]

---

[10] Hierzu auch BVerfGE 65, 1 (44).

[11] Dabei ist das OSI-Schichtenmodell deutlich komplexer, was sich allein schon daran zeigt, dass es in einer einfachen Variante bereits von sieben Schichten ausgeht. Vgl. dazu Klußmann, Lexikon der Kommunikations- und Informationstechnik, Stichwort "OSI-Referenzmodell".

Die erste Ebene dieses Modells bildet die technische Übertragungsleistung. Sie betrifft ausschließlich den technischen Vorgang des Aussendens, Übermittelns und Empfangens von elektromagnetischen oder optischen Signalen. Die zweite Ebene ist die so genannte Diensteebene. Sie betrifft den Bereich des Angebots bestimmter Dienstleistungen auf elektronischem Wege. Die dritte Ebene erfasst schließlich die übertragenen Inhalte.

Diese traditionelle Unterteilung eines Kommunikationsvorgangs wird durch das Recht zumindest teilweise übernommen und dadurch verfestigt, dass für die Regelung der verschiedenen Ebenen die Gesetzgebungskompetenz zwischen Bund und Ländern aufgeteilt ist. Während für die Ebene der technischen Übertragungsleistung der Bund die ausschließliche Gesetzgebungskompetenz hat,[12] steht diese Kompetenz auf der Diensteebene zum Teil den Ländern zu, soweit es um Rundfunk geht,[13] zum Teil wohl aber dem Bund, soweit es um die wirtschaftliche Nutzung des Internet geht.[14] Nicht eingegangen werden soll an dieser Stelle auf rundfunkrechtliche Aspekte. Zwar spielen gerade diese in Zeiten von Livestreams und Video-on-demand beziehungsweise Video-near-demand Angeboten von Internetprovidern in der Praxis eine zunehmend größere Rolle. Ihre Behandlung würde jedoch den vorgegebenen Rahmen sprengen.

Auch bei Außerachtlassen rundfunkspezifischer Regelungen sind Internetprovider aber im Regelfall zumindest zwei Gesetzen unterworfen, die spezifisch das Internetangebot betreffen: dem Telekommunikationsgesetz (TKG), soweit auf der ersten Ebene eine technische Übertragungsleistung erbracht wird; dem Telemediengesetz (TMG), soweit auf der zweiten Ebene auch noch elektronische Informations- und Kommunikationsdienste angeboten werden.

Auf den ersten Blick scheint die datenschutzrechtliche Behandlung der verschiedenen Ebenen des Schichtenmodells durchaus einfach zu sein und damit die geforderte Rechtssicherheit zu bieten: Soweit ein Provider seinen Kunden den technischen Zugang zum Internet vermittelt, ist er Diensteanbieter im Sinne des § 3 Nr. 6 TKG und muss als solcher bei diesem Angebot die datenschutzrechtlichen Vorschriften der §§ 91 ff. TKG beachten. Soweit der Provider

[12] Art. 73 Nr. 7 GG "Telekommunikation".
[13] Art. 70 GG.
[14] Art. 74 Nr. 11 GG "Recht der Wirtschaft".

seinen Kunden www, E-Mail und Nachrichtendienste anbietet, ist er Telemediendiensteanbieter im Sinne des § 2 Nr. 1 TMG, mit der Folge, dass sich der Datenschutz bei diesem Angebot nach den §§ 11 ff. TMG richtet. So einfach sich diese Differenzierung in der Theorie anhört, so viele Schwierigkeiten bereitet sie aber im konkreten Einzelfall gerade bei Internetprovidern, die beide Leistungen in einem Komplettpaket anbieten.

Das Nebeneinander von TKG und TMG erfordert bei solchen Komplettangeboten nämlich die künstliche Aufspaltung eines einheitlichen Lebenssachverhaltes. Diese führt gerade in der Praxis immer wieder zu Abgrenzungsproblemen. Dies insbesondere auch deshalb, weil die gesetzlichen Regelungen zur Abgrenzung der Anwendungsbereiche von TKG und TMG teilweise unklar, teilweise sogar widersprüchlich sind.[15] Bei unbefangener Lektüre von § 1 Abs. 1 TMG, der den Anwendungsbereich des Gesetzes bestimmt, scheint es so, als ob eine Leistung entweder ein elektronischer Informations- und Kommunikationsdienst ist und damit dem Anwendungsbereich des TMG unterfällt, oder ein Telekommunikationsdienst beziehungsweise telekommunikationsgestützter Dienst, der in den Anwendungsbereich des Telekommunikationsgesetzes fällt. § 1 Abs. 1 TMG bestimmt nämlich unter anderem, dass das TMG für alle elektronischen Informations- und Kommunikationsdienste gilt, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, oder telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG sind.

Dieser erste Befund eines Ausschließlichkeitsverhältnisses der Anwendungsbereiche von TKG und TMG gerät allerdings gerade dann ins Wanken, wenn es um die datenschutzrechtliche Beurteilung einer Leistung geht, die sowohl Aspekte der technischen Übertragung als auch Aspekte eines elektronischen Kommunikationsdienstes in sich trägt. Nach § 11 Abs. 3 TMG gelten nämlich für solche Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen,[16] die datenschutzrechtlichen Vorschriften des TMG nur eingeschränkt, im Übrigen sollen für diese Dienste auch die datenschutzrechtlichen Vorschriften des TKG Anwendung finden.[17] Offensichtlich ging also der Gesetzgeber selbst davon aus, dass zwischen Telekommunikationsdienst einer-

[15] Dazu auch Fetzer, DRiZ 2007, 206.
[16] Dies entspricht der Definition von Telekommunikation in § 3 Nr. 23 TKG.
[17] BT-Drucks. 16/3078, S. 13.

seits und elektronischem Informations- und Kommunikationsdienst andererseits kein Ausschließlichkeitsverhältnis besteht. Entscheidend für die Frage, ob auf ein Angebot das TKG, das TMG oder beide Gesetze anwendbar sind, ist demnach, ob bei einer elektronischen Leistung nur eine technische Übertragungsleistung erbracht wird - dann findet nur das TKG Anwendung -, ob nur überwiegend eine technische Übertragungsleistung erbracht wird - dann finden TKG und TMG Anwendung -, oder ob die technische Übertragungsleistung nur eine untergeordnete Rolle spielt - dann findet nur das TMG Anwendung.

Diese Abgrenzung aufgrund des Überwiegens eines Leistungsaspekts ist unter zwei Gesichtspunkten problematisch: Zum einen stellt sich die praktische Frage, unter welchen Vorraussetzungen denn ein Dienst überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. In der juristischen Literatur wird hierzu teilweise die Auffassung vertreten, dass ein solches Überwiegen bei einer Quote von 50% anzunehmen sei.[18] Nach Maßstäben, wie diese Quote zu berechnen sein soll, sucht man allerdings - soweit ersichtlich - vergebens. Zum andern steht diese Abgrenzung nach dem Überwiegen eines Leistungsaspekts, wie sie durch das TMG vorgegeben wird, auch in einem gewissen Widerspruch zum Telekommunikationsgesetz: Nach § 3 Nr. 24 TKG gelten dort nämlich sowohl Dienste, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, als auch solche, die nur überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, als Telekommunikationsdienst. Auf diese wären demnach aber gemäß § 91 TKG ausschließlich die datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes anwendbar. Einen Verweis auf das TMG sucht man dort vergebens.

Die dargestellten Abgrenzungsschwierigkeiten zwischen Telekommunikationsgesetz einerseits und Telemediengesetz andererseits sind dabei nicht nur von rein akademischem Interesse. Sie wirken sich gerade im Datenschutzrecht auch praktisch aus. Ein erster bedeutsamer Unterschied liegt bereits in der Bestimmung der zuständigen Aufsichtsbehörde. Für Telekommunikationsdiensteanbieter ist gemäß § 115 Abs. 4 S. 1 TKG zuständige Aufsichtsbehörde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Für Telemediendiensteanbieter hingegen richtet sich in

[18] Vgl. hierzu die Nachweise bei Heckmann, Internetrecht, 2007, S. 8.

Ermangelung einer spezialgesetzlichen Regelung im TMG die zuständige Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz (BDSG).[19] Gemäß § 38 Abs. 6 BDSG bestimmen hier die jeweiligen Landesregierungen eine zuständige Aufsichtsbehörde für nichtöffentliche Stellen.

Daneben unterscheiden sich aber auch die materiellen Normen von TKG und TMG zumindest im Detail. Ein Beispiel hierfür, das in der Vergangenheit mehrfach die Gerichte beschäftigte, ist die Speicherung von Verbindungsdaten über das Ende einer Internetverbindung hinaus.[20] Verbindungsdaten sind solche personenbezogenen Daten, die für die Inanspruchnahme und Abrechnung von Telemedien beziehungsweise Telekommunikationsdiensten erforderlich sind.[21] Ein besonders wichtiges Verbindungsdatum bei Internetverbindungen sind dynamische IP-Adressen, die Internetnutzern von ihrem Provider für die Dauer einer Verbindung zugewiesen werden. Bereits vor Inkrafttreten des TMG war umstritten, ob diese IP-Adressen von Internetanbietern auch dann über das Verbindungsende hinaus gespeichert werden dürfen, wenn sie für die Abrechnung der Internetverbindung nicht relevant sind, weil der Kunde eine Flatrate, das heißt eine nutzungsunabhängige Tarifierung, mit seinem Anbieter vereinbart hatte. Die Rechtsprechung hatte überzeugend die Auffassung vertreten, dass eine Speicherung dieser Daten nicht erforderlich und damit grundsätzlich unzulässig sei.[22] An dieser Beurteilung ändert sich auch nichts, wenn man sie auf Grundlage des TMG vornimmt. Nach § 15 Abs. 4 TMG darf ein Diensteanbieter Nutzungsdaten über das Verbindungsende hinaus nur zu Abrechnungszwecken speichern. Anders sieht es freilich aus, wenn man die Speicherung von dynamischen IP-Adressen über das Verbindungsende hinaus nach dem TKG beurteilt, also als Teil einer technischen Übertragungsleistung an-

---

[19] Heckmann, Internetrecht, 2007, S. 174.

[20] LG Darmstadt, K&R 2006, 291 (292). Das Urteil ist rechtskräftig, nachdem der BGH die Beschwerde gegen die Nichtzulassung der Revision zurückgewiesen hat, MMR 2007, 37.

[21] Im Telekommunikationsgesetz werden diese Daten als Verkehrsdaten bezeichnet, § 3 Nr. 30 TKG. Das Telemediengesetz fasst diese Daten unter den Begriff der Nutzungsdaten, vgl. § 15 Abs. 1 S. 2 Nr. 2 und 3 TMG.

[22] LG Darmstadt, K&R 2006, 291 (292) s. FN 8. Während das LG Darmstadt die Zulässigkeit der Speicherung allein auf Grundlage des TKG beurteilt hat, hatte die Vorinstanz zumindest "hilfsweise" auf die Zulässigkeit des Speicherns auf Grundlage des TDDG geprüft und verneint, AG Darmstadt, MMR 2005, 634.

sieht. Durch das jüngst verabschiedete TKG-Änderungsgesetz[23] wurde der insoweit einschlägige § 99 Abs. 1 S. 1 TKG dahingehend ergänzt, dass Diensteanbieter auch für pauschal abgerechnete Telekommunikationsdienste ihren Kunden einen Einzelverbindungsnachweis anbieten können und damit zwangsläufig auch die entsprechenden Verbindungsdaten über das Verbindungsende hinaus speichern können müssen.[24] Ordnet man nun also die Leistung eines Internetanbieters ausschließlich oder zumindest überwiegend als Übertragung von Signalen über Telekommunikationsnetze ein, ist eine Speicherung von Verbindungsdaten über das Verbindungsende hinaus nun auch bei pauschal abgerechneten Tarifen zulässig. Sieht man hingegen kein solches Überwiegen der technischen Übertragungskomponente bei der Leistung eines Internetanbieters, so richtet sich die datenschutzrechtliche Zulässigkeit der Speicherung von Verbindungsdaten über das Verbindungsende hinaus ausschließlich nach dem Telemediengesetz und ist bei pauschal abgerechneten Tarifen unzulässig.

Als erster Zwischenbefund soll hier festgehalten werden, dass sich der Datenschutz im Internet einer Regelungskomplexität ausgesetzt sieht, die es dem Rechtsanwender mitunter nicht leicht macht. Der Rechtsanwender ist nämlich gezwungen die Anwendungsbereiche verschiedener gesetzlicher Regelungen gegeneinander abzugrenzen, die in sich selbst widersprüchlich sind und zudem zu einer künstlichen Aufspaltung einheitlicher Lebenssachverhalte führen.

Die hierbei entstehende Rechtsunsicherheit ist Ergebnis eines konzeptionellen Grundproblems des öffentlichen Medienrechts, das sich am Beispiel des Datenschutzes bei elektronischen Medien besonders deutlich zeigt: Das öffentliche Medienrecht geht im Grundsatz nach wie vor von der trennscharfen Unterscheidbarkeit zwischen technischer Übertragungsleistung und Übertragungsdienst aus. Diese theoretische Unterscheidbarkeit ist jedoch zunehmend eine realitätsfremde Fiktion: Internetprovider bieten ihren Kunden heute integrierte Leistungspakete an, die sowohl Elemente von Telekommunikation, von Telemedien und vielfach auch von Rundfunk

[23] Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften vom 27.02.2007, BGBl. I 2007, S. 106.

[24] Eine Verpflichtung der Diensteanbieter einen solchen Einzelverbindungsnachweis anzubieten besteht nicht. Hierzu Fetzer, in: Arndt/Fetzer/Scherer, Telekommunikationsgesetz, § 99 Rn. 3 im Erscheinen.

enthalten. Schon die teilweise widersprüchlichen Regelungen im TKG und TMG zeigen, dass eine trennscharfe Unterscheidung zwischen Übertragungsleistung und Übertragungsdienst in Zeiten des Internet nicht mehr möglich ist. Die erste Frage, ob es für den Datenschutz ein Regelungssystem gibt, das Rechtssicherheit und Rechtsklarheit schafft und damit einen effektiven Persönlichkeitsrechtsschutz sicherstellt, muss daher verneint werden. Das Recht müsste - wenn es wieder Sicherheit schaffen will - die traditionelle Unterscheidung zwischen technischer Übertragungsleistung und Dienst zugunsten einer einheitlichen datenschutzrechtlichen Behandlung elektronischer Medien aufgeben.

III. Implementierung ökonomischer Anreizmechanismen

Die Schaffung eines solchen einheitlichen Rechtsrahmens wäre allerdings nur ein Schritt zu einer Stärkung des Datenschutzes und damit des Persönlichkeitsschutzes im Internet. In einem nächsten Schritt muss sichergestellt werden, dass das Datenschutzrecht tatsächlich in der Praxis beachtet wird. Bisher bedient sich das Datenschutzrecht hierbei eines primär ordnungsrechtlichen Instrumentariums.

Die Erhebung, Verarbeitung und Verwendung von personenbezogenen Daten ist grundsätzlich unzulässig, es sei denn, es gibt eine gesetzliche Regelung, die dies gestattet, oder aber der Betroffene hat eine Einwilligung erklärt. Dieses in § 4 Abs. 1 BDSG allgemein normierte "Verbot mit Erlaubnisvorbehalt" gilt auch für den Bereich der Telekommunikation und ist für den Bereich der Telemedien sogar nochmals ausdrücklich in § 12 Abs. 1 TMG niedergelegt. Eine Verletzung dieses Verbots ist mit einer staatlichen Sanktion bedroht. Ein Verstoß gegen bestimmte datenschutzrechtliche Vorschriften begründet nach § 16 Abs. 1 Nr. 2 TMG beziehungsweise § 149 Abs. 1 Nr. 16 - 18 TKG eine Ordnungswidrigkeit, die mit einem Bußgeld geahndet werden kann. Dieses Bußgeld beträgt im Falle eines Verstoßes gegen Vorschriften des TMG gemäß § 16 Abs. 3 TMG maximal € 50.000,-, im Falle eines Verstoßes gegen Vorschriften des TKG gemäß § 149 Abs. 2 S. 2 TKG maximal € 300.000,-. Hierbei handelt es sich jeweils um Maximalbeträge, die angesichts des in manchen Fällen erheblichen kommerziellen Werts personenbezogener Daten die Frage aufwerfen, ob sie ausreichen, um die Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten.

Die Befolgung datenschutzrechtlicher Vorschriften wird von Unternehmen nämlich vielfach einer Kosten-Nutzen-Analyse unterzogen. Unternehmen wägen die potenziellen Kosten eines Datenschutzverstoßes gegen dessen Nutzen, beziehungsweise die Kosten der Befolgung datenschutzrechtlicher Vorschriften gegen deren Nutzen ab. Eine bewusste Kalkulation eines Rechtsverstoßes mag in einem moralischen Sinne verwerflich sein und bei Aufdeckungen zudem einen Reputationsverlust bewirken. Angesichts der Tatsache jedoch, dass die Wahrscheinlichkeit der Aufdeckung eines datenschutzrechtlichen Verstoßes in Zeiten des globalen Netzwerkes Internet, das eine Verschiebung riesiger Datenmengen von Kontinent zu Kontinent in wenigen Sekunden ermöglicht, vielfach äußerst gering ist, ist die abschreckende Wirkung, die von den Bußgeldern und dem möglichen Reputationsverlust ausgeht, jedoch eher gering.

Eine nur scheinbare Lösung dieses Problems läge darin, die Bußgelder für Verstöße gegen datenschutzrechtliche Normen drastisch zu erhöhen. Dies würde die angesprochene Kosten-Nutzen-Analyse kaum verändern. Angesichts des angesprochenen oftmals geringen Aufdeckungsrisikos spricht viel dafür, dass eine Erhöhung der Bußgelder keine signifikante Erhöhung der Bereitschaft zur Befolgung datenschutzrechtlicher Vorgaben bewirken würde.

Ist es demnach schwierig, die Kosten eines datenschutzrechtlichen Verstoßes - verstanden als Produkt von Sanktion und Sanktionswahrscheinlichkeit - zu erhöhen, bleibt als Alternative zur Effektivierung des Datenschutzes, den potenziellen Nutzen der Befolgung datenschutzrechtlicher Vorschriften zu steigern. Am ehesten kann dies gelingen, wenn man bei Unternehmen ein wirtschaftliches Eigeninteresse an der Einhaltung datenschutzrechtlicher Vorschriften weckt. Mit anderen Worten: Das bisherige Konzept des Datenschutzrechts, Verstöße zu sanktionieren, könnte ergänzt werden um Mechanismen, die besondere Anreize für die Einhaltung datenschutzrechtlicher Vorschriften schaffen. Datenschutzrecht muss insoweit zu einem Wettbewerbsfaktor werden.

Ein viel versprechender Ansatz sind staatliche Zertifizierungen, die es Online-Anbietern erlauben, mit einem besonders hohen Datenschutzniveau zu werben und damit einen Wettbewerbsvorteil gegenüber Konkurrenten, die dieses Niveau nicht erreichen, zu erzielen. Eine Form solcher staatlicher Zertifizierungen sind die so genannten Datenschutzaudits, bei denen Unternehmen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen durch unab-

hängige Stellen begutachten und bewerten lassen und dann mit den Ergebnissen dieser Bewertung werben können. Während § 21 Mediendienstestaatsvertrag (MDStV) für Mediendienste eine spezielle Regelung über Datenschutzaudits für den Bereich der neuen Medien enthielt, fehlt eine solche Regelung im TMG. Zurückzugreifen ist insoweit auf die in § 9a BDSG enthaltene Regelung zu Datenschutzaudits. Datenschutzaudits im nicht-öffentlichen Bereich haben bisher allerdings deshalb noch keine Bedeutung erlangt, weil nach § 9a S. 2 BDSG die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter für Datenschutzaudits der Regelung in einem besonderen Gesetz bedürfen. Solche Regelungen sind erforderlich, um Anbietern, die sich einem Audit unterziehen wollen, aber auch den Nutzern die Sicherheit zu bieten, dass das vergebene Zertifikat tatsächlich die Einhaltung eines bestimmten Datenschutzstandards gewährleistet. Nach wie vor allerdings gibt es eine solche bundesweite Regelung für den nicht-öffentlichen Sektor allerdings leider immer noch nicht. Immerhin liegt nun aber seit dem 7. September 2007 ein Referentenentwurf für ein Bundesdatenschutzauditgesetz vor.[25] Es bleibt zu hoffen, dass die gesetzliche Implementierung möglichst bald abgeschlossen wird, um diese sinnvolle Ergänzung des Datenschutzrechts durch wettbewerbliche Elemente nicht weiter zu verzögern.

IV. Information als Voraussetzung der informationellen Selbstbestimmung

Ein letzter Aspekt des Persönlichkeitsrechtsschutzes im Internet, auf den hier noch kurz eingegangen werden soll, betrifft die Personen, deren Persönlichkeit durch das Datenschutzrecht geschützt werden soll. Eine effektive Ausübung des in Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG verankerten Rechts auf informationelle Selbstbestimmung durch den Einzelnen setzt zwingend voraus, dass der Einzelne weiß, welche Daten über ihn erhoben, verarbeitet und genutzt werden.[26] Es ist immer wieder erstaunlich, wie wenig Internetnutzer im Hinblick auf den Schutz ihrer personenbezogenen Daten im Internet sensibilisiert sind. Während inzwischen die Mehrzahl der Internetnutzer durch eine stetige Berichterstattung in den Medien zwar ein Bewusstsein dafür entwickelt zu haben scheint,

[25] Entwurf eines Bundesdatenschutzauditgesetzes, Entwurf vom 07.09.2007, abrufbar unter http://www.datenschutzzentrum.de/
[26] BVerfGE 65, 1 (41).

dass die Übermittlung von Kreditkarten- oder sonstigen Bankdaten über das Internet zumindest zu finanziellen Risiken führen kann, scheint einem Großteil der Internetnutzer darüber hinaus kaum bewusst zu sein, in welchem Umfang bereits beim alltäglichen Surfen im Internet auf systemimmanenten Wegen personenbezogene Daten anfallen, die im Extremfall die Erstellung von Persönlichkeitsprofilen zulassen. Von den zahlreichen zusätzlichen Möglichkeiten, mittels Cookies, Webbugs oder Viren personenbezogene Daten von Internetnutzern zu erheben, soll an dieser Stelle überhaupt nicht die Rede sein.

Eine wichtige Aufgabe gerade auch für die Datenschutzbeauftragten wird es daher in Zukunft sein, Internetnutzer noch mehr als bisher auf all diese Möglichkeiten hinzuweisen und ihnen bewusst zu machen, welche Gefahren für ihr Persönlichkeitsrecht im Internet bestehen. Nur wer ausreichend informiert ist über diese Gefahren und die ihm zur Verfügung stehenden Möglichkeiten, diesen Gefahren tatsächlich - etwa durch den Einsatz von entsprechender Software - oder rechtlich - etwa durch die Anrufung von Datenschutzbeauftragten - zu begegnen, kann sein Recht auf informationelle Selbstbestimmung angemessen ausüben.

Das Recht auf informationelle Selbstbestimmung ist es allerdings auch, das dem Datenschutz Grenzen setzt. Das Recht auf informationelle Selbstbestimmung verpflichtet den Staat dann nicht mehr zum Schutz der Persönlichkeit des Einzelnen, wenn dieser in Ausübung dieses Rechts - und in Kenntnis aller relevanten Umstände - sich gleichwohl dazu entschließt, im Schutz der scheinbaren Anonymität des Internet über E-Mails oder Chatrooms persönliche Sachverhalte zu offenbaren, die man im realen Leben kaum einem Freund offenbaren würde. Insofern gilt auch im Internet, dass die Persönlichkeit nur dann geschützt werden muss, wenn die dazugehörige Person auch schutzbedürftig ist.

V. Zusammenfassung

Zusammenfassend lässt sich daher im Hinblick auf den Persönlichkeitsrechtsschutz im Internet Folgendes feststellen:

1. Die gesetzlichen Regelungen, die den Schutz des Persönlichkeitsrechts im Internet sicherstellen sollen, sind teilweise unklar, teilweise widersprüchlich. Dies trägt zu einer Rechtsunsicherheit bei, die einem effektiven

Datenschutz im Wege steht. Hier ist dringend eine einheitliche gesetzliche Regelung erforderlich, die nicht länger an die Unterscheidung zwischen technischer Übertragungsleistung und erbrachtem Dienst anknüpft.

2. Das Verlassen auf rein ordnungsrechtliche Ansätze zur Durchsetzung datenschutzrechtlicher Pflichten ist heute vielfach nicht mehr Erfolg versprechend. Die ordnungsrechtlichen Ansätze sollten durch Mechanismen ergänzt werden, die die Einhaltung datenschutzrechtlicher Vorschriften zu einem Wettbewerbsfaktor machen. Eine Möglichkeit hierzu bieten Datenschutzaudits.

3. Die effektive Ausübung des Rechts auf informationelle Selbstbestimmung setzt die Information des Einzelnen darüber voraus, welche Gefahren für sein Persönlichkeitsrecht im Internet bestehen und wie er diesen Gefahren tatsächlich und rechtlich begegnen kann.

Ausgehend vom Titel des Beitrags lässt sich die Frage: "Wie zuverlässig wird das Persönlichkeitsrecht im Internet insbesondere gegen Gefahren, die von nicht-öffentlichen Stellen drohen, geschützt?" derzeit nur mit einem "allenfalls recht sicher, aber nicht rechtssicher" beantworten.