RAINER STENTZEL

# Privatsphäre und Datenschutz – zwei Seiten einer Medaille?

## I. Rechtliche Ausgangslage

Privatsphäre und Datenschutz sind zwei Ausprägungen einer Medaille, nämlich des Persönlichkeitsrechts. Beide Seiten zeigen jedoch ein unterschiedliches Bild bzw. einen anderen Wert, wenn es um Abwägungen mit der Öffentlichkeit geht.

Das einfache Recht zum Schutz der Privatsphäre einerseits und zum Schutz personenbezogener Daten andererseits ist höchst unterschiedlich.

### 1. Zivilrechtlicher Privatsphärenschutz

Beim Privatsphärenschutz geht es um eine Abgrenzung und Grenzziehung zur Öffentlichkeit. Sein Ziel ist es, der Öffentlichkeit eine private Information vorzuenthalten. Dabei ist der Anwendungsbereich relativ eng begrenzt auf Dinge, die als privat oder vertraulich gelten. Das bereits öffentlich Sichtbare gehört nicht dazu. Das auf Schadensersatz und Unterlassen gerichtete Recht zum Schutz der Privatsphäre kann allenfalls der punktuellen Rückeroberung privater Räume gegenüber der Öffentlichkeit dienen.

Der Privatsphärenschutz ist neben einigen strafrechtlichen Normen zivilrechtlich ausgestaltet. Das Zivilrecht bezieht sich klassischerweise auf das Verhältnis Privater untereinander. Die Geltendmachung und Durchsetzung erfolgt individuell durch den Betroffenen. Der Privatsphärenschutz steht damit unter der Einschätzungsprärogative und zur Disposition des Betroffenen. Hinzu kommt eine Darlegungs- und Beweislast. Bei der Verletzung des allgemeinen Persönlichkeitsrechts nach §§ 823, 1004 BGB handelt es sich um einen „offenen Tatbestand". Die Widerrechtlichkeit ist nicht indiziert, sondern muss positiv festgestellt werden.[1] Der gerichtlichen Interessensabwägung geht damit eine individuelle Abwägung voraus. Der Betroffene muss entscheiden, ob ihm erstens der Schutz der Privatsphäre einen Rechtsstreit wert ist, und er zweitens eine Chance hat zu obsiegen. Antragserfordernis und Prozessrisiko tragen dazu bei, dass der zivilrechtliche Privatsphärenschutz lediglich punktuell zum Tragen kommt. In der Regel greift er nur bei gravierenden Eingriffen in die Privatsphäre, etwa

[1] S. hierzu BGHZ 45, 296, 307 f.; BGHZ 73, 120, 124; zur Verfassungskonformität dieser Sichtweise BVerfGE 114, 339, 348; vgl. ferner MüKO-BGB/*Wagner*, 5. Auflage 2009, § 823 Rn. 179.

durch eine Presseberichterstattung, die private Lebensumstände gegenüber einer breiten medialen Öffentlichkeit offenlegt.[2]

## 2. Datenschutz

Der Datenschutz folgt einer gänzlich anderen Systematik. Er greift nicht individuell-konkret auf Initiative des Betroffenen ein und unterliegt nicht den allgemeinen Spielregeln des Zivilrechts. Der Datenschutz ist – auch im Verhältnis der Privaten untereinander – öffentlich-rechtlich ausgestaltet. Das Datenschutzrecht erhebt den Anspruch, dass der Persönlichkeitsschutz unabhängig vom Willen des Betroffenen flächendeckend durch staatliche Datenschutzaufsichtsbehörden durchgesetzt wird.

Materiell setzt das Datenschutzrecht nicht erst beim konkreten Eingriff in das Persönlichkeitsrecht oder gar die Privatsphäre des Betroffenen an. Das Datenschutzrecht statuiert einen vorgelagerten Schutz im Sinne eines präventiven Ordnungsrechts. Es regelt eine abstrakte Gefährdung durch *Technik*.

Im Datenschutzrecht impliziert der Einsatz einer bestimmten Technik – nämlich automatisierter Datenverarbeitung – die Widerrechtlichkeit bzw. Unzulässigkeit einer Handlung. Wer personenbezogene Daten automatisiert verarbeitet, braucht hierfür eine Rechtfertigung, und zwar klassischerweise eine datenschutzrechtliche Erlaubnisnorm oder die Einwilligung des Betroffenen. Die Regelungstechnik des Datenschutzrechts folgt damit dem klassischen Staat-Bürger-Verhältnis.

In diesem Verhältnis ist auch der Begriff des informationellen Selbstbestimmungsrechts verortet.[3] Dabei ist die Selbstbestimmung demokratisch zu verstehen. Was der Staat über seine Bürger wissen darf, legen nicht seine handelnden Exekutivorgane, sondern der demokratisch unmittelbar legitimierte Gesetzgeber fest, und zwar beschränkt auf das für die Aufgabenerfüllung notwendige Mindestmaß. Es gilt das rechtsstaatliche Übermaßverbot. In den Worten von *Dieter Grimm* geht es bei der informationellen Selbstbestimmung weniger um das Handeln des individuellen Grundrechtsträgers als vielmehr um das Behandeltwerden durch den Staat.[4] Dieser muss sich für sein Handeln gegenüber dem Grundrechtsträger rechtfertigen.

Die Rechtfertigungspflicht für das eigene Handeln wurde beim Datenschutz vom klassischen Staat-Bürger-Verhältnis auf das Verhältnis Privater untereinander übertragen. Erklären lässt sich dies historisch. Das Datenschutzrecht ist ein technikbezogenes Recht. Es regelt die automatisierte Datenverarbeitung. Als es entstand, verfügten nur der Staat und einige Großunternehmen über diese Technik. Angesichts des noch

---

[2] So betreffen wichtige Leitentscheidungen zum zivilrechtlichen Privatsphärenschutz den Konflikt zwischen Pressefreiheit und Persönlichkeitsrechten, s. etwa BGHZ 13, 334 (Leserbrief); BVerfGE 7, 198 (Lüth); BVerfGE 34, 269 (Soraya); BVerfGE 101, 361 (Caroline von Monaco II).

[3] Vgl. grundlegend BVerfGE 65, 1 (Volkszählung); ferner BVerfGE 100, 313 (Telekommunikationsüberwachung); BVerfGE 109, 279 (Großer Lauschangriff); vgl. aktueller auch BVerfGE 124, 43 (Beschlagnahme von E-Mails); BVerfGE 120, 274 (Online-Durchsuchungen).

[4] Vgl. *Grimm*, Verfassungsrechtliche Vorgaben für einen modernen Datenschutz, Rede auf der Berliner Datenschutzkonferenz am 17. 10. 2012, abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Datenschutz/rede_grimm.pdf?__blob=publicationFile.

punktuellen Einsatzes von elektronischer Datenverarbeitung, die sich im Wesentlichen in der Nutzung klassischer Dateien erschöpfte, schien eine Übertragung des staatlichen Rechtfertigungsmodells vertretbar. Allerdings war die Frage, ob der öffentliche Bereich und der private Bereich datenschutzrechtlich einheitlich geregelt werden sollen, von Beginn an umstritten.

## II. Technische Entwicklung in der modernen Informationsgesellschaft

Seit den ersten großen Kodifikationen des Datenschutzrechts[5] hat sich die Welt in technischer Hinsicht grundlegend verändert. Die IT-technische Entwicklung hin zu einer modernen, digital vernetzten Kommunikationsgesellschaft hat weitreichende Folgen für das Verhältnis von Privatheit und Öffentlichkeit. Wie wir diesen Wandel beurteilen, hängt von der Perspektive ab. Es lohnt sich ein kurzer Blick in die Vergangenheit.

Meine spanische Freundin hat mir berichtet, dass man sich in dem kleinen Dorf, in dem sie aufgewachsen ist, Geschichten über alles und jeden erzählt hat. Ein Beispiel betraf ihren Großvater. Dieser hatte mit 12 Jahren auf einem Dorffest seine ersten Erfahrungen mit Alkohol gemacht. Die daraus resultierenden Unpässlichkeiten wurden zum allgemeinen Amüsement der Dorfbewohner augenzwinkernd tradiert. Weil man einander kannte, hat man versucht, Geheimnisse zu schützen. Unterwäsche hing man auf eine separate Leine, die man von außen nicht einsehen konnte. Wohl jeder hat diese Erfahrung bereits machen müssen: Je enger die Gemeinschaft, desto schwieriger wird es mit der Privatsphäre.

In einer engen Gemeinschaft zu leben, in der Erfahrungen, Geschichten und Schicksale geteilt werden, muss nicht von vornherein ein Nachteil sein. Die Anonymität einer Großstadt ist für manchen eine mindestens ebenso große Last wie für den anderen die Enge eines kleinen Dorfes, in dem jeder über jeden fast alles weiß. Wir haben uns indessen auf das Leben in der relativen Anonymität einer dynamischen Massengesellschaft eingestellt. Sowohl die Sozialsphären als auch die Öffentlichkeit sind gewachsen. Unsere „Öffentlichkeit" hat einen größeren Radius. Innerhalb dieses größeren Radius wird die Aufmerksamkeit auf Bereiche der Privatheit reduziert.

Bringt das Internet nun den Wandel zurück in die Vergangenheit? Die digitale Welt ist – mal mehr, mal weniger – eine öffentliche. Und die digitale Welt ist ein Dorf. Wie die Dorfgemeinschaft vergisst auch das Internet nicht. Wer es geschickt anstellt, kann über andere einiges erfahren. Ich kann meine neuen Nachbarn, Kollegen und Bekanntschaften googeln und einen ersten Eindruck gewinnen. Wer sich mit *Google Analytics* auskennt, kann umgekehrt herausfinden, durch wen er in letzter Zeit gegoogelt wurde.

---

[5] So datiert etwa das Bundesdatenschutzgesetz vom 27. Januar 1977. Als weltweit erstes Datenschutzgesetz gilt das erste Hessische Datenschutzgesetz aus dem Jahre 1970. Auf europäischer Ebene wurde durch die Richtlinie 95/46/EG eine erste Kodifikation des Datenschutzrechts geschaffen. Vgl. ausführlich zur Geschichte des Datenschutzrechts Simitis/*Simitis*, BDSG, 6. Aufl. 2006, Einl. Rn. 1 f.; ferner *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, 2013, S. 51 f.

Die Folge der technischen Entwicklung ist zum einen eine Stärkung der Öffentlichkeit und zum anderen eine Ausweitung des Anwendungsbereichs des Datenschutzrechts.

## 1. Stärkung der Öffentlichkeit

Das Internet hat eine neue, vielschichtige digitale Öffentlichkeit konstituiert. Die Summe der Informationen, die für die Öffentlichkeit zugänglich sind, hat sich vervielfacht. Quellen der Öffentlichkeit sind nicht mehr nur Presse und Rundfunk. Jeder hat die Möglichkeit, über eine Homepage, einen Blog, *Twitter* oder ein soziales Netzwerk Informationen potentiell allen Menschen zur Verfügung zu stellen. Gleichzeitig wurde der Zugang zu bereits öffentlich vorhandenen Informationen radikal vereinfacht. Straßenzüge und Häuserfassaden waren seit jeher für jeden sichtbar, der sich in der Straße befand. *Google Street View* überwindet die Ortsgebundenheit des Betrachters.

Die Stärkung der Öffentlichkeit muss aus grundrechtlicher Sicht in erster Linie als Mehrwert begriffen werden. Sie dient der Grundrechtsausübung in vielfältiger Weise. Gefördert werden insbesondere die Meinungsfreiheit und andere Kommunikationsgrundrechte, die Berufsfreiheit sowie die freie Entfaltung der Persönlichkeit. Die Bedeutung für eine freie demokratische Gesellschaft lässt sich am Arabischen Frühling 2011 ermessen. Blogs, *Youtube*, *Facebook* und *Twitter* haben sich als technische Infrastrukturen zur Ausübung von (verfassungsrechtlich noch gar nicht abgesicherten) Grundrechten erwiesen.

## 2. Ausweitung des Anwendungsbereichs des Datenschutzrechts

Neben den zusätzlichen Möglichkeiten der Grundrechtsausübung birgt die Expansion öffentlicher Räume freilich auch Risiken. Chancen der Beeinträchtigung der Privatsphäre und der allgemeinen Persönlichkeitsrechte nehmen zu. Hierauf scheint das Datenschutzrecht automatisch zu reagieren. Die expandierende digitale Öffentlichkeit bedient sich eben jener Technik der automatisierten Datenverarbeitung, die den Anwendungsbereich des Datenschutzrechts eröffnet.[6] Mit der Anwendung des Datenschutzrechts steht die erweiterte digitale Öffentlichkeit jedoch unter einem Rechtfertigungszwang. Gleiches gilt für nach wie vor nicht-öffentliche Lebensbereiche, in denen die Datenverarbeitung bereits Einzug gehalten hat. Als Beispiele seien nur die digitale Fotografie, der digitale Notizblock im Smartphone oder das vernetzte Navigationssystem genannt.

[6] Das eingrenzende Merkmal des personenbezogenen Datums (legaldefiniert in § 3 Abs. 1 BDSG) verliert zunehmend an Bedeutung; vgl. zur sehr weiten Auslegung dieses Begriffs *Gola/Schomerus*, Bundesdatenschutzgesetz, 11. Auflage 2012, § 3 Rn. 2 ff.

## III. Rechtspolitische Implikationen dieser Entwicklung

Nimmt man die durch die digitale Vernetzung gesteigerten Gefahren für das Persönlichkeitsrecht in den Blick, erscheint der gewachsene Anwendungsbereich des Datenschutzrechts folgerichtig. Allerdings müsste das Datenschutzrecht auch in der Lage sein, auf diese Gefahren zu reagieren. Zugleich müsste sichergestellt sein, dass die neuen Chancen und Möglichkeiten der Grundrechtsausübung, welche die neuen digitalen Räume eröffnen, nicht über Gebühr beeinträchtigt werden.

Hieran bestehen zunehmend Zweifel: So scheint die Steuerungsfähigkeit des Datenschutzrechts gerade dort abzunehmen, wo die Gefahren am größten sind. Während sich einfache, bipolare Sachverhalte leicht nach dem Datenschutzrecht beurteilen lassen, verschwimmen datenschutzrechtliche Verantwortlichkeiten und Zuständigkeiten in mehrpolaren Fallgestaltungen mit unterschiedlichen Beteiligten.

Ein einfaches Beispiel: Sie besuchen eine Konferenz. Neben ihnen sitzen zwei Personen, die sich angeregt unterhalten. Ihr Sitznachbar erhält von seinem Gesprächspartner eine Visitenkarte. Offenbar ist er Fachanwalt für Medienrecht. Sie sind seit langem auf der Suche nach einem Medienrechtler und fragen ihren Nachbar, ob Sie mal einen Blick auf die Visitenkarte werfen können. Sie tippen den Namen und die Telefonnummer in ihr Smartphone, um später mit dem Anwalt Kontakt aufzunehmen. Mit dem Eintippen der Kontaktdaten erfolgt eine automatisierte Datenverarbeitung. Sie sind verantwortliche Stelle im Sinne des Datenschutzrechts. Wenn Sie geschäftlich Kontakt mit dem Anwalt aufnehmen wollen, greift auch die datenschutzrechtliche Ausnahme[7] für Privatpersonen nicht. Nach Art. 14 der gegenwärtig in Brüssel diskutierten Datenschutz-Grundverordnung[8] müssten Sie Ihren Nachbarn über die Datenverarbeitung informieren. Sie müssten eine Einwilligung verlangen oder sich auf einen datenschutzrechtlichen Erlaubnistatbestand berufen können.[9] Was das Recht Ihnen in dieser Situation an Informations- und Nachweispflichten, Zweckbestimmungen und Folgeabschätzungen aufbürdet, ist erheblich. Möglicherweise haben Sie auf Ihrem Smartphone Apps installiert, die Ihre Adressdaten automatisch zu Werbe- oder anderen Zwecken an Dritte weiterleiten. Möglicherweise befinden sich diese Dritten im Ausland. Wenn dem so ist: Welche datenschutzrechtliche Verantwortung tragen Sie und der App-Anbieter oder der Dritte? Hätte der App-Anbieter Sie fragen müssen, ob er Ihr Adress- oder Telefonverzeichnis verwenden darf? Wenn ja: Wären Sie überhaupt dispositionsbefugt oder müssten Sie die Inhaber des jeweiligen Telefonanschlusses ihrerseits um Einwilligung bitten? Was ist, wenn Sie soeben die Telefondaten des Anwalts gespeichert haben, der einen Partner in seiner Kanzlei hat?

---

[7] Vgl. Art. 3 Abs. 2 Richtlinie 95/46; § 1 Abs. 2 Nr. 3 BDSG; Art. 2 Abs. 2 Buchstabe d) Entwurf Datenschutz-Grundverordnung.

[8] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg.

[9] Art. 6 ff. Entwurf Datenschutz-Grundverordnung.

Mehrpolare Datenverarbeitungen mit parallelen Verantwortlichkeiten sind in einer vernetzten Welt außerhalb des öffentlichen Bereichs[10] eher die Regel als die Ausnahme. Die Rechtssicherheit und die Steuerungsfähigkeit des Rechts nehmen ab. Auch die Exekutive bietet im Datenschutzrecht aus strukturellen Gründen wenig Orientierung. Angesichts der Unabhängigkeit der Aufsichtsbehörden verbietet sich eine zentrale Verwaltungssteuerung durch die Ministerialverwaltung.

Die sinkende Steuerungsfähigkeit verhindert nicht die potentielle Allgegenwärtigkeit des Datenschutzrechts. Mit zunehmender Digitalisierung aller Lebensbereiche entsteht – zumindest abstrakt – ein Primat des öffentlich-rechtlichen Datenschutzrechts innerhalb der Rechtsordnung. Der konsequente Vollzug des Datenschutzrechts würde – überspitzt gesagt – andere Rechtsgebiete „kannibalisieren" und Wachstum und Konstituierung der digitalen Öffentlichkeit erschweren. Insbesondere im Verhältnis zum zivilrechtlichen Persönlichkeitsrechtsschutz ergeben sich zunehmend Wertungswidersprüche. Ein Beispiel ist der Fall einer bekannten Leichtathletin, die sich durch E-Mails sexuell belästigt fühlte und die Mails mitsamt dem Namen des Absenders auf *Facebook* veröffentlichte. Zivilrechtlich könnte sich der Absender zur Wehr setzen. Ihn träfe dann die Darlegungs- und Beweislast. Auch müsste er sich mit Blick auf die erforderliche Interessenabwägung zum Inhalt seiner E-Mails einlassen. Datenschutzrechtlich liegt die Darlegungs- und Beweislast allein bei der Leichtathletin. Da anzunehmen ist, dass sie keine Einwilligung des Absenders eingeholt hat, wäre die Veröffentlichung der E-Mail nach geltendem deutschen Datenschutzrecht an § 29 BDSG zu messen. Sie müsste prüfen und darlegen, dass „kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat". Ihre Bewertung unterliegt dabei der staatlichen Datenschutzaufsicht und ist bußgeldbewehrt. Man mag darüber streiten, ob es rechtens war, dass die Leichtathletin die E-Mail veröffentlicht und damit ihren Peiniger bloßgestellt hat. Einigkeit sollte jedoch darüber bestehen, dass die Rechtsordnung für ein und denselben Sachverhalt in Bezug auf das Persönlichkeitsrecht keine unterschiedlichen Maßstäbe errichten sollte.

Das Primat des Datenschutzrechts führt – wie das Beispiel *Google Street View* zeigt – zudem dazu, dass die Verfügungsbefugnis über allgemeine oder fremde Güter einseitig zugunsten desjenigen anerkannt wird, der seine Privatsphäre in den öffentlichen Raum ausweitet. Aktuell diskutierte Fortentwicklungen des Datenschutzrechts wie insbesondere das „Recht auf Vergessenwerden"[11] sind geradezu von dem Gedanken einer Re-Privatisierung des Öffentlichen geleitet.

---

[10] Im öffentlichen Bereich hat sich die Steuerungsfähigkeit des Datenschutzrechts grundsätzlich erhalten. Die zunehmende Vergesetzlichung der Informationserhebung und vor allem der Informations- oder Datenweiterverarbeitung birgt allerdings Gefahren der zunehmenden Undurchschaubarkeit gesetzlicher Detailregelungen; vgl. *Stentzel*, Sicherheit und Transparenz, in: Informationsfreiheit und Informationsrecht, Jahrbuch 2008, S. 47, 50 ff.

[11] Art. 17 KOM-Entwurf Datenschutz-Grundverordnung; hierzu *Koreng/Feldmann*, ZD 2012, 311; vgl. auch den Beitrag von Bundesinnenminister *Friedrich*, Das „Recht auf Vergessen" und die Netzfreiheit, in: SPIEGEL online v. 29. 2. 2012, abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/0,1518,817830,00.html; ferner *Nolte*, ZRP 2011, 236; ausführlich *Mayer-Schönberger*, Delete – The Virtue of Forgetting in the Digital Age, 2009, passim.

Die datenschutzrechtliche „Kannibalisierung" kann auch Zuständigkeiten betreffen. Mit Blick auf die von der Kommission vorgelegte EU-Datenschutz-Grundverordnung gilt dies insbesondere für den öffentlichen Bereich und das bereichsspezifische Datenschutzrecht im öffentlichen Fachrecht der Mitgliedstaaten, wie z. B. dem Sozialrecht, dem Schulrecht, dem Passrecht oder dem Recht nationaler Register wie dem Ausländerzentralregister.

Insgesamt müssen wir uns fragen, ob die Stärkung des Datenschutzes als eine Seite der Medaille des allgemeinen Persönlichkeitsrechts mit einem möglicherweise ungewollten Absolutheitsanspruch einhergeht und wie sich die Steuerungsfähigkeit des Datenschutzrechts verbessern lässt.

Nehmen wir hin, dass sich der Anwendungsbereich des öffentlich-rechtlichen Datenschutzrechts aufgrund der unaufhaltsamen digitalen Vernetzung auf nahezu alle private Lebensbereiche ausweitet, betreiben wir Rechtspolitik durch Unterlassen. Wir würden uns tendenziell gegen die neue digitale Öffentlichkeit und für ein Primat des Persönlichkeitsrechts entscheiden, wie wir es in dieser Form in anderen Rechtsbereichen mit kollidierenden Grundrechten nicht kennen. Dabei wäre eigentlich eine breite und offene gesellschaftliche Debatte darüber nötig, welche Folgen die Ausweitung des Datenschutzrechts in seiner bestehenden Systematik hat, wie sich die Steuerungsfähigkeit des Datenschutzrechts zurückgewinnen lässt und welchen Wert die neue digitale Öffentlichkeit für uns alle hat.

## IV. Lösungsansätze

Ein modernes Datenschutzrecht sollte sich auf den gemeinsamen Kern und Ursprung sowohl des Schutzes der Privatsphäre als auch des Datenschutzes zurückbesinnen: das allgemeine Persönlichkeitsrecht. In Brüssel wird im Zuge der EU-Datenschutzreform derzeit darüber beraten, wie sich das Datenschutzrecht besser an den Risiken und Gefahren für das Persönlichkeitsrecht ausrichten lässt. Das Ziel ist es, wirkungsvollere Regelungen dort zu schaffen, wo stärkere Beeinträchtigungen des Persönlichkeitsrechts drohen. Dabei wird unter anderem erwogen, konkrete Schutzziele zu benennen, die sich aus dem allgemeinen Persönlichkeitsrecht ableiten lassen und denen das Datenschutzrecht dienen sollte. Beispielhaft zu nennen sind der Schutz vor Diskriminierung, insbesondere finanzieller Benachteiligung, der Schutz vor Identitätsmissbrauch oder der Schutz der Ehre.

Ferner wird in der zuständigen Ratsarbeitsgruppe in Brüssel darüber nachgedacht, wie im Datenschutzrecht der Ausgleich mit kollidierenden Grundrechten, insbesondere der Meinungsfreiheit, besser sichergestellt werden kann und Wertungswidersprüche zu anderen Rechtsgebieten, z. B. zum Äußerungs- und Presserecht, vermieden werden können. Ein Lösungsansatz könnte darin bestehen, natürliche Personen, die nicht gewerblich oder freiberuflich bzw. nicht zu professionellen Zwecken Daten verarbeiten, vom Anwendungsbereich der Datenschutz-Grundverordnung auszunehmen. Meinungsäußerungen von Privatpersonen wären damit per se nicht erfasst.

Schließlich wird erwogen, die datenschutzrechtlichen Verantwortlichkeiten nach Verantwortungsbereichen näher zu spezifizieren und zu ordnen. Dies betrifft insbesondere die Verantwortlichkeiten von Anbietern und Nutzern. Die Unterscheidungen, die beispielsweise dem Telemediengesetz zugrunde liegen, sollten im allgemeinen Datenschutzrecht nicht außer Acht gelassen werden. Wenn eine an den Gefährdungen für das Persönlichkeitsrecht orientierte Neujustierung des Datenschutzrechts gelingt, die sowohl den Risiken als auch den Chancen der Informationsgesellschaft und der neuen digitalen Öffentlichkeit Rechnung trägt, stärken wir alle Seiten des Persönlichkeitsrechts.