Institut für Rechtsinformatik

KURzStellungnahme zum ULD-Entwurf einer BDSG-Novelle – (KURS)

vorgelegt von
Prof. Dr. Nikolaus Forgó

25. November 2010

Leibniz Universität Hannover

Autoren

Univ.-Prof. Dr. Nikolaus Forgó, Dipl.-Jur. Christian Hawellek, RA'in Dr. Tina Krügel, LL.M., RA'in Kathrin Müllenbach, LL.M.

Dieses Gutachten wurde auf Grundlage einer Drittmittelvereinbarung zwischen der Leibniz Universität Hannover und der infas Geodaten GmbH erstellt.

Gliederung

1. Executive Summary

Regelungsvorschlag Nr. 1 ist aus systematischen, dogmatischen und logischen Gründen abzulehnen. Die durch das ULD konstatierten Defizite in der Rechtsdurchsetzung lassen sich durch ihn nicht bekämpfen. Spezifische Auswirkungen auf die Geoinformationsbranche sind insoweit zu erwarten, als es nichteuropäischen Anbietern, die in der Geoinformation schon jetzt stark sind, zumindest nicht erschwert, vermutlich sogar erleichtert würde, europäische Datenschutzstandards (weiterhin) nicht zu beachten.

Regelungsvorschlag Nr. 2 kann in der vorgelegten Form nicht überzeugen. Zunächst definiert er „Sachdaten", die gerade nicht Gegenstand des BDSG sind, was bereits aus systematischen Gründen abzulehnen, letztlich aber auch überflüssig ist, da das Sachdatum die Kehrseite des personenbezogenen Datums und damit bereits definiert ist. Zudem deckt die vorgeschlagene Definition, da allein auf das Vorliegen eines persönlichen oder sachlichen Verhältnisses abgestellt wird, nicht alle Bereiche ab, in denen Sachdaten vorliegen können. Sie ist folglich zu kurz geraten und daher eher hinderlich als hilfreich. Die Wiederholung des sachlichen Verhältnisses ist darüber hinaus redundant. Es bestehen auch sprachliche Einwände gegen die gewählte Formulierung.

Der Vorstoß, die Intention der verarbeitenden Stelle im Rahmen der Eröffnung des Anwendungsbereiches des Datenschutzrechts zu berücksichtigen, ist zu begrüßen. Jedoch sieht der Vorschlag die Berücksichtigung der Intention der verantwortlichen Stelle am falschen Merkmal vor, weshalb das Regelungsziel nicht erreicht werden kann.

Änderungen an der Definition des personenbezogenen Datums haben für die Geoinformationsbranche sehr erhebliche Relevanz.

Regelungsvorschlag Nr. 3 wäre zu unterstützen, soweit eine Einführung des vorgeschlagenen § 29a BDSG (Regelungsvorschlages Nr. 8) zu befürworten wäre. Eine Einführung des § 29 a BDSG ist jedoch abzulehnen, weshalb auch die hier geforderte Einführung einer Legaldefinition der Veröffentlichung obsolet wird. Für die Geoinformationsbrache hätte die Einführung einer Legaldefinition der Veröffentlichung keine Auswirkungen. Diese könnten sich erst aus einem für die Veröffentlichung zu schaffenden gesetzlichen Regime ergeben.

Regelungsvorschlag Nr. 4 stellt lediglich die bereits existierende Rechtslage klar, ist aber aus systematischen Gründen abzulehnen, da die Haftungsprivilegierung von Telemedien nichts mit der Definition der datenschutzrechtlich verantwortlichen Stelle zu tun hat. Im Gegenteil, eine Verortung dieses Verweises in der Definition führt ohne Not zu einer Reihe von Unklarheiten. Für die Geoinformationswirtschaft hat dieser Regelungsvorschlag keine weiteren Auswirkungen.

Regelungsvorschlag Nr. 5 ist grundsätzlich zu begrüßen, um einen genügenden Schutz des Nutzers vor Preisgabe seiner personenbezogenen Daten zu gewährleisten, begegnet aber erheblichen Schwierigkeiten im Detail. Auch wenn sich die Entwurfsvorschrift einzig an Betreiber von Diensten mit nutzergenerierter Datenverarbeitung richtet, könnte sie für Geoinformationsdienste relevant sein, nämlich dann, wenn diese Inhalte von Nutzern beinhalten.

Regelungsvorschlag Nr. 6 ist aus gesetzessystematischen Erwägungen und wegen der Verringerung des Schutzniveaus des Bürgers in Fällen „traditioneller Datenverarbeitung" nicht sinnvoll.

Eine Streichung des Satzes 2 und Integrierung des § 13 Abs. 2 TMG ist abzulehnen. Relevanz für die Geoinformationsbranche dürfte kaum gegeben sein.

Regelungsvorschlag Nr. 7 ist wegen daraus entstehenden dogmatischen Unsicherheiten abzulehnen. Die Relevanz für die Geoinformationsbranche ist gering.

Regelungsvorschlag Nr. 8 sieht die Einführung eines § 29a BDSG vor. Dies ist insgesamt abzulehnen, da der in Abs. 1 konstituierte Erlaubnistatbestand europarechtswidrig sein kann und jedenfalls mangels Berücksichtigung des Grundrechts auf Informationsfreiheit nach hier vertretener Ansicht verfassungswidrig ist. Die anderen Absätze bauen auf dieser Regelung auf. § 29a BDSG-E hat für die Geoinformationswirtschaft eine hohe Relevanz, wenn man ihn auf Tatsachenmitteilungen wie Geoinformationen mit dem ULD anwenden will. Tatsächlich ist die Norm allerdings nicht anwendbar, weil der klare Wortlaut nur Meinungsäußerungen, gerade aber keine Tatsachenmitteilungen umfasst.

Regelungsvorschlag Nr. 9 ist zu begrüßen, denn eine beschleunigte und vereinfachte Behördenkommunikation ist im Interesse aller Beteiligten und in der Telemedienbranche auch naheliegend. Allerdings sieht die Regelung keine Sanktionen für eventuelle Verstöße vor, also etwa, wenn eine Reaktion des Telemediendiensteanbieters ausbleibt. Die Relevanz für die Geoinformationswirtschaft beschränkt sich auf eventuelle Kommunikation mit der Aufsichtsbehörde, wenn Geodaten online gestellt werden, die Personenbezug aufweisen, und ist damit eher gering.

Regelungsvorschlag Nr. 10 setzt die dem BDSG schon bisher immanente Bußgeldbewehrung von Tatbeständen fort und erweitert diese auf zwei Anwendungsfälle des § 29a BDSG-E. Allerdings ist die Auswahl dieser Tatbestände ohne weitere Begründung selektiv und schon deswegen zu hinterfragen. Nennenswerte Auswirkungen auf die Geoinformationsbranche sind nicht zu erwarten.

Regelungsvorschlag Nr. 11 begegnet als Folgeregelung zu Regelungsvorschlag Nr. 6 den dort präsentierten Bedenken. Eine Relevanz für die Geoinformationsbranche ist kaum anzunehmen.

Tabellarisch dargestellt ergibt sich damit folgende Bewertung:

Regelungsvorschlag	Rechtliche Bewertung	Relevanz für die Geoinformations-wirtschaft
Nr. 1		
Nr. 2		
Nr. 3		
Nr. 4		
Nr. 5		
Nr. 6		
Nr. 7		
Nr. 8		*
Nr. 9		
Nr. 10		
Nr. 11		

* Keine Relevanz, soweit man mit hier vertretener Ansicht Tatsachenmitteilungen von dem Regelungsvorschlag nicht umfasst sieht.

Legende

Rechtliche Bewertung	zuzustimmen	teilweise bedenklich	abzulehnen
Relevanz für die Geoinformationswirtschaft	hoch	mittel	gering/keine

2. Einleitung

2.1.1 Hintergrund

Seit Monaten sind datenschutzrechtliche Fragen des Geoinformationswesens Gegenstand rechtspolitischer Auseinandersetzungen. Diese haben unter anderem zu einem Entwurf des Bundesrates vom 18.08.2010 (BR-Drs. 17/2765) geführt, der sich mit datenschutzrechtlichen Fragen der Verarbeitung von Geodaten befasst.

Vor diesem Hintergrund präsentierte das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) einen Gesetzesvorschlag zum 27. 10. 2010, der „personenbezogene Internetdatenveröffentlichungen" regulieren soll[1] (im Folgenden: Gesetzesvorschlag, Vorschlag oder BDSG-E). Grundlage der Bemühungen ist die Prämisse, dass „das Internet eine Überarbeitung des Datenschutzrechtes erforderlich macht."[2]

Als Faktor, der zur Präsentation des Vorschlags geführt habe, wird die intensive Diskussion rund um Geoinformationsdienste am Beispiel Google Street View angeführt. Jedoch will der Entwurf ersichtlich über eine geoinformationsbezogene Spezialregelung hinausgehen, sodass die Vorschläge, würden sie Gesetz werden, für zahlreiche weitere Branchen und Geschäftsmodelle, insbesondere für Betreiber von „Social Networks" und ähnlichen Web 2.0 Applikationen (zB Facebook, Twitter, Youtube, Xing, Myspace, Spickmich.de, Lokalisten, StudiVZ, De.licio.us etc.) aber auch für ältere Angebote, sofern sie zB eine Forenfunktion anbieten (zB amazon.de, ebay.de, heise.de, spiegel.de) entwickeln würde.

Diese vermutlich sehr erheblichen Implikationen für die Internetwirtschaft in Deutschland insgesamt können in diesem Kurzgutachten nicht im Detail beleuchtet werden. Deswegen erfolgt hier eine Fokussierung auf Fragen, die unseres Erachtens für die datenschutzrechtliche Bewertung des Geoinformationswesens relevant sind. Die weiterführenden Aspekte wären im Zuge einer breiteren Debatte mitzudenken, zu der dieses Kurzgutachten beitragen möchte, falls der Entwurf tatsächlich rechtspolitische Wirkkraft entfalten sollte.

[1] Abrufbar unter: https://www.datenschutzzentrum.de/internet/20101027-gesetzentwurf-internetveroeffentlichungen.html .
[2] Ebd.

2.1.2 Wortlaut des Vorschlags

Der präsentierte Vorschlag hat den folgenden Wortlaut:

Gesetz zur Regulierung von Internetveröffentlichungen im Bundesdatenschutzgesetz
(Stand 27.10.2010)[3]

1. ***§ 1 Abs. 5 S. 3 erhält folgende Fassung:***

   "Soweit eine verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, gilt als verantwortliche Stelle diejenige, die für die verantwortliche Stelle in diesem Gebiet wirtschaftlich tätig ist."

2. ***In § 3 Abs. 1 wird folgender Satz 2 angefügt:***

   "Keine personenbezogene Angaben sind Sachangaben, die zu einem Betroffenen nicht hinsichtlich Zweck, Ergebnisorientierung oder Inhalt in einem Bezug stehen oder gestellt werden sollen."

3. ***In § 3 Abs. 4 wird eine Nr. 2a eingefügt:***

   "2a. Veröffentlichen das Bereitstellen für eine unbestimmte Zahl von Empfängern zum elektronischen Abruf,"

4. ***In § 3 Abs. 7 wird folgender Satz 2 angefügt:***

   "§ 7 bis § 10 Telemediengesetz sind anwendbar."

5. ***Es wird folgender § 3b eingefügt:***

   "§ 3b Nutzergenerierte Datenverarbeitung

   Erfolgt eine Erhebung oder Verarbeitung durch Aktivitäten einer natürlichen Person, so sind die Grundeinstellungen des Dienstes so zu gestalten, dass so wenig wie möglich personenbezogene Daten erhoben oder verarbeitet werden. Eine Änderung der Einstellungen setzt die Berücksichtigung der Voraussetzungen des § 4a voraus."

6. ***In § 4a Abs. 1 wird Satz 2 gestrichen. Satz 3 wird Satz 2. Es wird folgender Abs. 1a eingefügt:***

   "Die Einwilligung bedarf der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Die Einwilligung kann elektronisch erklärt werden, wenn die verantwortliche Stelle sicherstellt, dass

   1. *der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat,*
   2. *die Einwilligung protokolliert wird,*
   3. *der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und*
   4. *der Nutzer die Einwilligung jederzeit mit der Wirkung für die Zukunft widerrufen kann."*

7. ***§ 29 Abs. 3 wird gestrichen. Die Absätze 4 bis 7 werden die Absätze 2 bis 6.***

8. ***Es wird folgender § 29a eingefügt:***

   "Veröffentlichung

   (1) Das Veröffentlichen personenbezogener Daten in Telemedien ist zulässig, wenn dies dem Zweck dient, eine Meinung frei zu äußern und zu verbreiten und kein Grund zu der Annahme besteht, dass das überwiegende schutzwürdige Interesse der Betroffene am Ausschluss der Veröffentlichung überwiegt.

   (2) Ein schutzwürdiges Interesse besteht bei besonderen Arten personenbezogener Daten nach § 3 Abs. 9, wenn nicht im Einzelfall das Interesse an der Veröffentlichung offensichtlich überwiegt.

   (3) Ein schutzwürdiges Interesse besteht, wenn der Betroffene gegenüber der verantwortlichen Stelle widerspricht, es sei denn, die verantwortliche Stelle legt dem Betroffenen gegenüber das überwiegende Interesse an einer Veröffentlichung dar. Die Darlegung nach Satz 1 kann in der Form des vom Betroffenen erklärten Widerspruchs oder schriftlich erfolgen.

[3] Abrufbar unter: https://www.datenschutzzentrum.de/internet/20101027-gesetzentwurf-internetveroeffentlichungen.html .

(4) Betroffene können ihre Datenschutzrechte gegenüber dem verantwortlichen Telemedien-Diensteanbieter elektronisch an die nach § 5 Absatz 1 Nr. 2 Telemediengesetz zu nennende Stelle richten. Wird die Beschwerde nicht unverzüglich beantwortet, so verletzt die weitere Veröffentlichung schutzwürdige Betroffeneninteressen. Kann die verantwortliche Stelle nicht die Richtigkeit der Daten nachweisen, so tritt neben die Löschungs- und Sperransprüche nach § 35 ein Anspruch auf Hinzufügung einer eigenen Darstellung von angemessenem Umfang. § 57 Abs. 3 Rundfunkstaatsvertrag zu Gegendarstellungen ist sinngemäß anzuwenden.

(5) Die Veröffentlichung von personenbezogenen Daten aus allgemein zugänglichen Quellen hat zu unterbleiben, wenn der entgegen stehende Wille des Betroffenen aus dieser Quelle oder auf andere Weise eindeutig erkennbar ist. Der Empfänger von veröffentlichten Daten hat sicherzustellen, dass Kennzeichnungen bei der Übernahme übernommen werden.

(6) Beabsichtigt ein Telemedien-Diensteanbieter die Veröffentlichung von personenbezogenen Daten zu mehr als 1000 oder von einer unbestimmten Zahl von Personen, so hat er dies auf einer beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingerichteten Internetseite vorher unter Nennung der Datenart und der Quelle bekanntzugeben.

(7) Verantwortliche Stellen, die personenbezogene Daten veröffentlichen, können diese mit einem Löschdatum versehen. Werden diese Daten von einer anderen verantwortlichen Stelle übernommen, so ist bei der weiteren Veröffentlichung und der sonstigen Verarbeitung das jeweilige Löschdatum zu berücksichtigen."

9. Es wird in § 38 folgender Absatz 1a eingefügt:

"Kontrolliert die Aufsichtsbehörde einen Telemediendienst nach § 1 Abs. 1 Telemediengesetz, so kann die Kommunikation über die nach § 5 Absatz 1 Nr. 2 genannte Adresse erfolgen. Der Telemediendienst hat auf eine elektronische Anfrage der Aufsichtsbehörde unverzüglich, spätestens innerhalb von 14 Tagen zu antworten. Bei Datenschutzverstößen in Telemedien kann die zuständige Datenschutzaufsichtsbehörde zu Warnzwecken einen öffentlichen Hinweis hierauf sowie auf die Schutzmöglichkeiten für Nutzer geben."

10. In § 43 Abs. 1 wird eingefügt:

"7c. entgegen § 29a Abs. 4 S. 2 eine Beschwerde nicht unverzüglich beantwortet,

7d. entgegen § 29a Abs. 6 bei einer Veröffentlichung umfangreicher Datenbestände eine Benachrichtigung unterlässt,"

Änderung des Telemediengesetzes (TMG)

11. § 13 Abs. 2 wird gestrichen. Die Absätze 3 bis 7 werden die Absätze 2 bis 6.

2.1.3 Aufbau dieser Kurzstellungnahme

Im Interesse bestmöglicher Parallelität der Kommentierung mit dem Vorschlag verzichtet diese Studie auf eine eigene Strukturierung der durch den Vorschlag aufgeworfenen Fragestellungen. Stattdessen werden die gemachten Regelungsvorschläge in ihrer Originalreihenfolge präsentiert und kommentiert.

3. Stellungnahme zum Regelungsvorschlag

3.1 Zu Regelungsvorschlag 1

Der Vorschlag zielt auf die Einführung eines „begrenzten Weltrechtsprinzips" „im Interesse einer minimalen Wahrung der Persönlichkeitsrechte". [4] Deutsches Recht soll, wie in den den Gesetzesentwurf begleitenden Thesen ausgeführt wird,[5] immer dann zur Anwendung gelangen, wenn ein Internetangebot auf den deutschen Markt zielt, egal, wo die Datenverarbeitung tatsächlich erfolgt. Zu diesem Zwecke soll § 1 Abs. 5 Satz 3 BDSG folgende Fassung erhalten: „Soweit eine verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, gilt als verantwortliche Stelle diejenige, die für die verantwortliche Stelle in diesem Gebiet wirtschaftlich tätig ist." Im Entwurf selbst wird dies damit begründet, dass häufig „die bisher verantwortliche Stelle im Sinne des § 3 Abs. 7 eine Stelle außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR) ist. Dies hat zur Folge, dass der Adressat von datenschutzrechtlichen Ansprüchen oder Aufsichtsmaßnahmen für Betroffene oder Aufsichtsbehörden nicht erreichbar ist, dass aber der wirtschaftliche Nutzen einem Unternehmen oder einer Unternehmensgruppe, das bzw. die in der EU oder im EWR wirtschaftlich agiert, zufließt."

Schon auf den ersten Blick wird deutlich, dass hier Fragen des anwendbaren Rechts („Weltrechtsprinzip") mit Fragen der Durchsetzbarkeit von Ansprüchen gegenüber Unternehmen, die in Deutschland keine Niederlassung betreiben (und daher „der Adressat von datenschutzrechtlichen Ansprüchen oder Aufsichtsmaßnahmen für Betroffene oder Aufsichtsbehörden nicht erreichbar ist"), vermengt werden. Diese Vermengung ist zT auch im geltenden Recht angelegt, hat doch § 1 Abs. 5 Satz 3 BDSG derzeit folgenden Wortlaut: „Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen."

Deswegen soll hier in einem ersten Schritt die geltende Rechtslage hinsichtlich des anwendbaren Rechts gezeigt werden.

3.1.1 Derzeitige Rechtslage

§ 1 Abs. 5 lautet derzeit wie folgt:

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen

[4] ULD, DAV-Forum Datenschutz am 27. Oktober 2010 in Berlin, Privatsphäre in der globalen Informationsgesellschaft – Ist der Datenschutz noch zu retten?, Podiumsdiskussion: Datenschutz 2020 – Thesen, https://www.datenschutzzentrum.de/vortraege/20101027-weichert-meinungsfreiheit-thesen.html.

[5] ULD, DAV-Forum Datenschutz am 27. Oktober 2010 in Berlin, Privatsphäre in der globalen Informationsgesellschaft – Ist der Datenschutz noch zu retten?, Podiumsdiskussion: Datenschutz 2020 – Thesen, https://www.datenschutzzentrum.de/vortraege/20101027-weichert-meinungsfreiheit-thesen.html.

Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

In vielen Fällen beruht das BDSG auf dem Territorialitätsprinzip. Regelmäßig soll dem Anwendungsbereich des BDSG jede verantwortliche Stelle, die personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt, unterliegen.[6]

§ 1 Abs. 5 S. 1 legt fest, wann bei grenzüberschreitenden Sachverhalten innerhalb der EU das BDSG anwendbar ist. § 1 Abs. 5 S. 2 bestimmt, wann das BDSG zu beachten ist, wenn die verantwortliche Stelle außerhalb der EU belegen ist. Bei richtlinienkonformer Auslegung ist § 1 Abs. 5 eine spezialgesetzliche Kollisionsnorm, welche in ihrem Anwendungsbereich dem allgemeinen Kollisionsrecht vorgeht.[7]

Es ergeben sich die folgenden Konstellationen:

3.1.1.1 Niederlassung des Anbieters in Deutschland

Das BDSG ist anwendbar, wenn verantwortliche Stellen personenbezogene Daten in Deutschland erheben, verarbeiten oder nutzen. Jedoch gelten innereuropäisch Besonderheiten, insbesondere für Fälle des grenzüberschreitenden Datenverkehrs. Gem. Art. 4 Abs. 1 lit. a) DSRL haben die EU-Mitgliedsstaaten ihre nationalen Datenschutzgesetze anzuwenden, wenn eine verantwortliche Stelle datenschutzrelevante Handlungen im Hoheitsgebiet des jeweiligen Staates durch eine Niederlassung ausführen lässt. Hier weicht die RL damit vom Territorialitätsprinzip ab und statuiert stattdessen das Niederlassungsprinzip; d.h. das anwendbare Recht hängt vom Ort der Niederlassung ab.[8] Diese Regelung dient der Stärkung des grenzüberschreitenden Handels im europäischen Binnenmarkt, denn Unternehmen, die ihre Leistungen EU weit anbieten wollen, können dies weiterhin auf der Grundlage ihrer nationalen Datenschutzgesetze tun, ohne unbekannte, ausländische Vorschriften beachten zu müssen.[9] Ein EU weit vergleichbares Schutzniveau wird dabei durch die DSRL selbst hergestellt.

Der Begriff der Niederlassung ist weit gefasst und im Einklang mit der Niederlassungsfreiheit gemäß §§ 52 ff. EG Vertrag als „die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung" zu interpretieren.[10] Vom Begriff der Niederlassung sollen ausgeschlossen sein eine Briefkastenfirma, Messestände und die Tätigkeit eines Handlungsreisenden, auch wenn er zum Abschluss von Verträgen im jeweiligen Mitgliedsstaat umherreist.[11]

---

[6] Florian Jotzo „Gilt deutsche Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?" MMR 2009, 232 [233].

[7] Dammann in Simitis, BDSG, § 1 Rz 216.

[8] Florian Jotzo „Gilt deutsche Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?" MMR 2009, 232 [234].

[9] Florian Jotzo „Gilt deutsche Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?" MMR 2009, 232 [233]; RL 95/46/EG, Erwägungen 1, 7, 8 .

[10] Dammann in Simitis, BDSG, § 1 Rz 202.

[11] Ebenda.

3.1.1.2 Niederlassung des Anbieters in einem anderen EU-Mitgliedsstaat

Ein Unternehmen, welches datenschutzrechtlich relevante Tätigkeiten von seiner Niederlassung in einem anderen EU Mitgliedsstaat aus vornimmt, unterliegt damit nicht den Regelungen des BDSG. Der Anwendungsbereich des BDSG ist erst dann eröffnet, wenn die Datenverarbeitung zumindest auch über eine in Deutschland befindliche Niederlassung erfolgt.[12]

3.1.1.3 Niederlassung des Anbieters außerhalb der EU

Anwendbar ist das BDSG gemäß § 1 Abs. 5 S.2 BDSG, wenn eine verantwortliche Stelle, die weder in einem Mitgliedstaat der Europäischen Union noch in einem anderen Vertragsstaat des EWR–Vertrages ansässig ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Gegenüber Drittstaaten gilt damit, anders als gegenüber den in Satz 1 privilegierten EU/EWR Vertragsstaaten, das Schutzniveau des BDSG, da ein vergleichbarer Schutzstandard im Verhältnis zu Drittstaaten nicht garantiert werden kann.[13] Auf ein im Einzelfall tatsächlich vermindertes Schutzniveau kommt es für die Anwendbarkeit des BDSG nicht an.[14] Laut Gesetzesbegründung zum BDSG ist Satz 2 in Hinblick auf das im Übrigen geltende Territorialitätsprinzip lediglich deklaratorisch zu verstehen. Die Regelung des Satz 2 bewirkt als Spezialregelung in Bezug auf den Regelungsgegenstand des BDSG – den Umgang mit personenbezogenen Daten -, dass die allgemeinen Vorschriften des EGBGB (Erster Teil/Zweites Kapitel) zum internationalen Privatrecht verdrängt werden.[15] Werden Daten in Deutschland erhoben, verarbeitet und genutzt, ist der territoriale Anwendungsbereich des BDSG eröffnet.

§ 1 Abs. 5 S. 2 BDSG stellt darauf ab, ob Daten im Deutschland erhoben, verarbeitet oder genutzt werden. Damit sind alle dem BDSG inhärenten Umgangsweisen mit personenbezogenen Daten erfasst und der Anwendungsbereich des BDSG hinsichtlich aller in Deutschland stattfindender relevanter Vorgänge ohnehin eröffnet, sofern nicht Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden (§ 1 Abs. 5 S. 4 BDSG).

Damit bleibt entscheidend, unter welchen Voraussetzungen davon auszugehen ist, dass personenbezogene Daten im Inland von einem Anbieter, der hier über keine Niederlassung verfügt, erhoben werden. Dies mag insbesondere in Fällen zweifelhaft sein, in denen Nutzer Informationen in Webformular im Inland eingeben, die dann auf Maschinen im Ausland übertragen und (ausschließlich) dort verarbeitet werden. Auf diese Frage werden in der Literatur bekanntlich unterschiedliche Antworten gegeben.[16]

---

[12] Florian Jotzo „Gilt deutsche Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?" MMR 2009, 232 [235].

[13] Dammann in Simitis, BDSG, § 1 Rz 210.

[14] Ebenda.

[15] Dammann in Simitis, BDSG, §1 Rz 216, m.w.N.

[16] Vgl. zum Ganzen Florian Jotzo „Gilt deutsche Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?" MMR 2009, 232 [235 - 237] mwN.

3.1.2 Änderung durch den Entwurf

§ 5 Abs. 3 Satz 3 soll nunmehr lauten: "Soweit eine verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, gilt als verantwortliche Stelle diejenige, die für die verantwortliche Stelle in diesem Gebiet wirtschaftlich tätig ist."

Damit erhielte § 5 Abs. 3 insgesamt die folgende Fassung:

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit eine verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, gilt als verantwortliche Stelle diejenige, die für die verantwortliche Stelle in diesem Gebiet wirtschaftlich tätig ist. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

Der bisherige § 1 Abs. 5 Satz 3 sagt weder etwas über die Bestimmung der verantwortlichen Stelle noch über das anwendbare Recht aus. Hingegen sieht die Norm bisher nur vor, dass eine (nicht in einem EWR-Mitgliedsstaat niedergelassene) ausländische verantwortliche Stelle, die im Inland personenbezogene Daten erhebt, verarbeitet oder nutzt, einen im Inland ansässigen Vertreter zu benennen hat. Dadurch soll sichergestellt werden, dass im Inland – bei vorauszusetzender Anwendbarkeit deutschen Rechts ! – ein Ansprechpartner zur Verfügung steht.[17]

Dem Entwurf lieg nun der vom ULD festgestellte Missstand zugrunde, dass „der Adressat von datenschutzrechtlichen Ansprüchen oder Aufsichtsmaßnahmen für Betroffene oder Aufsichtsbehörden nicht erreichbar ist, dass aber der wirtschaftliche Nutzen einem Unternehmen oder einer Unternehmensgruppe, das bzw. die in der EU oder im EWR wirtschaftlich agiert, zufließt.". Es soll also verhindert werden, dass eine datenverarbeitende Stelle bei vorausgesetzter Anwendbarkeit deutschen Rechts sich dessen Durchsetzung entzieht, indem die verantwortliche Stelle vom EWR-Ausland operiert, während im Inland ein (Tochter-)unternehmen nur als Vertreter auftritt.

Dieses Problem ist jedoch gerade keine Frage der Anwendbarkeit deutschen Rechts, sonder eine Frage der Durchsetzbarkeit der vorausgesetzten Anwendbarkeit deutschen Rechts im Ausland. Damit ist die vorgeschlagene Norm schon systematisch falsch verortet, da § 1 BDSG bekanntlich (im hier interessierenden Teil) lautet: „Anwendungsbereich des Gesetzes". Auch sind Probleme der Normdurchsetzung dem Internet inhärent und daher nicht auf der Ebene der Bestimmung des Anwendungsbereichs eines Gesetzes zu erfassen, sondern vielmehr im Wege internationaler Vereinbarungen.

[17] Vgl. nur Gola/Schomerus, Bundesdatenschutzgesetz, 10. Aufl. 2010, § 1 Rn. 29.

Der Vorschlag geht aus einem weiteren Grund fehlt: Stimmt man dem vom ULD erhobenen Befund, eine „Umgehung" datenschutzrechtlicher Standards durch die „Degradierung" von wirtschaftlich in Wahrheit operierenden Töchtern, die als bloße Vertreter agieren, finde derzeit statt, zu[18], so wäre auf diesen Umstand etwa durch die Übernahme von Verantwortlichkeitsregeln aus anderen Bereichen des IT-Rechts in das Datenschutzrecht möglicherweise zu reagieren. Es wäre also, würde man einen derartigen Ansatz schon begrüßen, insbesondere zu prüfen, ob das von der Rechtsprechung entwickelte Institut der Störerhaftung bzw. der Verantwortlichkeit für das Verhalten Dritter auf das Datenschutzrecht sinnvoll übertragen werden kann, ob also – und gegebenenfalls unter welchen Bedingungen - Verantwortlichkeiten für Fehlverhalten Dritter zu begründen wären.[19]

Stattdessen führt der Entwurf jedoch dazu, dass der „Störer" als verantwortliche Stelle „gilt".

Die verantwortliche Stelle ist gesetzlich definiert als „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt." (§ 3 Abs. 7 BDSG). Der Umstand, dass die verantwortliche Stelle *für sich selbst* agiert, ist das entscheidende Abgrenzungskriterium vom Auftragsdatenverarbeiter. Wenn nun aber in Fällen, in denen die verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, etwas Anderes, nämlich der/die wirtschaftlich Tätige als verantwortliche Stelle „gilt", wird durch diese Fiktion die zentrale Eigenschaft, für sich selbst zu agieren, in ihr Gegenteil verkehrt und damit verwässert. Die ohnehin schon komplexe Abgrenzung zwischen verantwortlicher Stelle und Auftragsdatenverarbeiter würde ohne Not weiter erschwert.

Die Begriffsbestimmung ist auch zirkulär oder sprachlich unklar und damit rechtlich unbestimmt. Es heißt: „Soweit eine verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, gilt als verantwortliche Stelle ***diejenige***, die für die verantwortliche Stelle in diesem Gebiet wirtschaftlich tätig ist." Das Demonstrativpronomen „diejenige" ist hier unbestimmt. Es ist zu vermuten, dass es die Wortfolge „die verantwortliche Stelle" substituieren soll, sodass der Satz zu lesen ist wie folgt: „Soweit eine verantwortliche Stelle ihren Sitz nicht im Gebiet nach Satz 2 hat, gilt als verantwortliche Stelle **diejenige verantwortliche Stelle**, die für die verantwortliche Stelle in diesem Gebiet wirtschaftlich tätig ist." Das ist zirkulär, weil dann die verantwortliche Stelle vor dem Greifen der Fiktion eine solche wäre, sodass es der Fiktion nicht bedürfte.

Soll sich das „diejenige" aber auf etwas/jemanden beziehen, was erst durch die Fiktion zur verantwortlichen Stelle wird, bleibt unbestimmt, welche Eigenschaften diese Entität zu erfüllen (juristische Person? Tochter im Konzern? gesellschaftsrechtliche Verflechtung? etc.) hat, um sich für die Fiktion zu qualifizieren.

Darüber hinaus müsste diese dann durch Fiktion zu einer solchen gemachten Vertreterin im Inland datenschutzrechtlich für Verhalten einzustehen haben, das sie nicht zu vertreten und daher auch nicht zu beeinflussen hat. Dies mag bei Tochterunternehmen im Konzern noch denkbar

[18] Dies wird hier nicht weiter geprüft. Der Vorschlag enthält keine weiterführenden Belege.

[19] Damit wird einem derartigen Ansatz hier ausdrücklich nicht das Wort geredet, insbesondere vor dem Hintergrund, dass die genannte Judikatur zu zahlreichen unerwünschten Effekten führt, die hier nicht vertieft werden können und vor dem Hintergrund der Haftungsprivilegierungen der E-Commerce-Richtlinie problematisch ist.

sein, wird aber in Fällen, in denen das nicht in Deutschland ansässige Unternehmen durch einen gesellschaftsrechtlich mit ihm nicht verbundenen Vertreter – etwa einen Rechtsanwalt - vertreten wird, nicht zu halten sein.

Und schließlich würde der Vorschlag aus folgenden Gründen voraussichtlich zum Gegenteil des Intendierten führen: Entfällt die Verpflichtung, im Inland einen Vertreter zu benennen, müssen sich Datenschutzbehörde und Betroffener im Streitfall erst auf die Suche begeben, wer im Inland „in diesem Gebiet wirtschaftlich tätig ist" statt direkt den zu benennenden Vertreter zu belangen. Weiter ist zu erwarten, dass häufig strittig sein wird, wer für die verantwortliche Stelle wirtschaftlich tätig ist und dies erhebliche Beweisprobleme aufwerfen wird. Es werden Fälle auftreten, in denen mehrere Stellen für die verantwortliche Stelle wirtschaftlich tätig sind, sodass der Betroffene zwischen unterschiedlichen Stellen hin und her verwiesen wird. Und schließlich wird es, gerade für verantwortliche Stellen, die sich des Internet bedienen, ein Leichtes sein, die Einrichtung, die „in diesem Gebiet wirtschaftlich tätig ist" ins (europäische) Ausland zu verlagern, sodass der Betroffene keinen Ansprechpartner im Inland mehr vorfände. Insgesamt würde dies nicht zu einer Verbesserung sondern vielmehr zu einer Verschlechterung der datenschutzrechtlichen Situation (zumindest) der Betroffenen führen.

Der Vorschlag ist daher aus systematischen, dogmatischen und logischen Gründen abzulehnen. Die durch das ULD konstatierten Defizite in der Rechtsdurchsetzung lassen sich durch ihn nicht bekämpfen. Spezifische Auswirkungen auf die Geoinformationsbranche sind insoweit zu erwarten, als es nichteuropäischen Anbietern zumindest nicht erschwert, vermutlich sogar erleichtert würde, europäische Datenschutzstandards nicht zu beachten.

3.2 Zu Regelungsvorschlag 2

3.2.1 Bedeutung

Nr. 2 des Regelungsvorschlages sieht eine Ergänzung des § 3 Abs. 1 BDSG (derzeitiger Wortlaut: *„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)."*) vor. Dem Vorschlag nach soll die in diesem Absatz verortete Definition des personenbezogenen Datums um folgenden Satz 2 ergänzt werden:

"Keine personenbezogene Angaben sind Sachangaben, die zu einem Betroffenen nicht hinsichtlich Zweck, Ergebnisorientierung oder Inhalt in einem Bezug stehen oder gestellt werden sollen."

Die Bedeutung einer wie auch immer gearteten Änderung des § 3 Abs. 1 BDSG ist nicht zu unterschätzen. § 3 Abs. 1 BDSG liefert das entscheidende Eingangstor zur Eröffnung des Anwendungsbereichs des datenschutzrechtlichen Regimes insgesamt. Das BDSG ist nur auf personenbezogene Daten anwendbar und folgt hier dem Vorbild der Richtlinie 1995/46/EG. Wie die europäische Kommission in einer aktuellen Mitteilung[20] und der ihr zugrunde liegenden Zusammen-

[20] Communication from the European Commission, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final vom 4. 11. 2010.

fassung einer Konsultation[21] deutlich macht, werde der „Alles-oder-Nichts"-Zugang dies derzeitigen Regimes zwar von manchen kritisiert,[22] gleichwohl stelle das Konzept des personenbezogenen Datums eines der Schlüsselkonzepte des Schutzes von Personen durch das europäische Normwerk dar.[23]

Gerade vor diesem Hintergrund sollte mit Änderungen der Definition bei derzeit noch gleich gebliebener europarechtlicher Rechtslage schon deswegen restriktiv umgegangen werden, weil nicht ausgeschlossen werden kann, dass demnächst wegen veränderter europarechtlicher Rahmenbedingungen eine weitere Reform ansteht. Jedweder Formulierungsänderung oder Ergänzung wird auch deswegen und auch in Brüssel zu Recht besondere Aufmerksamkeit entgegengebracht werden.

Nichtsdestotrotz muss das Datenschutzrecht im Hinblick auf die praktischen und rechtlichen Herausforderungen einer global vernetzten Welt selbstverständlich ständig angepasst werden, insbesondere wenn das geltende Recht neue Sachverhalte nicht angemessen zu regeln vermag. Allerdings ist die Begründungslast für einen Vorschlag, der die nationale Situation vor einer bereits begonnen habenden und für 2011 weiter zu erwartenden flächendeckenden Diskussion auf europarechtlicher Ebene an zentraler Stelle ändern will, sehr hoch, sodass nur zwingende Gründe zu einem nationalen Vorpreschen führen sollten. Dies gilt umso mehr, weil das BDSG bekanntlich bereits 2009 nicht weniger als drei Mal novelliert wurde, was der Übersichtlichkeit des Normwerks insgesamt geschadet hat.[24]

Da es sich bei § 3 Abs. 1 BDSG also um eine, wenn nicht *die Kernvorschrift* des deutschen Datenschutzrechts handelt und folglich Unklarheiten, seien sie sprachlicher oder inhaltlicher Natur, geeignet sind, zu erheblicher Rechtsunsicherheit zu führen, sind an entsprechende Anpassungen besonders hohe Anforderungen zu stellen. Sie müssen aus sich heraus verständlich und eindeutig formuliert sein, sollten Redundanzen vermeiden und so wenig Interpretationsspielraum wie möglich lassen.

Der vorliegende Änderungsvorschlag Nr. 2 wird diesem Anspruch nicht gerecht:

3.2.2 Sprachliche und systematische Einordnung

So weist der Satz bereits eine sprachliche Ungenauigkeit auf: Zu etwas in **einem** Bezug stehen verlangt im Deutschen den Dativ aber etwas ist zu etwas in **einen** Bezug zu stellen (Akkusativ). Die Wortfolge „Keine personenbezogene Angaben sind Sachangaben, die zu ***einem Betroffenen*** nicht hinsichtlich Zweck, Ergebnisorientierung oder Inhalt in einem Bezug stehen ***oder gestellt***

[21] Summary of replies to the public consultation about the future legal framework for protecting personal data, Brussels, 4 November 2010, http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf .
[22] Summary of replies to the public consultation about the future legal framework for protecting personal data, Brussels, 4 November 2010, http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf, 5.
[23] Communication from the European Commission, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final vom 4. 11. 2010, 5.
[24] Vgl. etwa die Synopse unter https://www.gdd.de/nachrichten/arbeitshilfen/BDSG-Gesetzestext%20mit%20Novelle%20I-III.pdf .

werden sollen" vermengt diese beiden Fälle. Dies ließe sich wohl durch Streichung des Wortes „einem" berichtigen.

Sprachlich fällt weiter auf, dass der Satz eine doppelte Verneinung aufweist („Keine .... nicht"). Eine doppelte Verneinung kann im Hochdeutschen die Funktion einer vorsichtigen, abgeschwächten Bejahung haben[25], sodass die Aussage „Keine personenbezogenen Angaben sind Sachangaben, die nicht in einem Bezug stehen" schwächer bejaht als die Aussage „Personenbezogene Angaben stehen in einem Bezug zu einem Betroffenen" und vermutlich auch schwächer als „Keine personenbezogene Angaben sind Sachangaben, die in keinem Bezug zum Betroffenen stehen". Darüber hinaus erschweren doppelte Verneinungen das Verständnis.[26] Schließlich ist auch rätselhaft, warum in Satz 1 von *Einzel*angaben, in Satz 2 hingegen von Angaben insgesamt die Rede ist, ob also Satz 2 (gewollt?) auch Sammelangaben mit umfassen soll.

Vermutlich ließen sich diese sprachlichen Einwände durch eine Reformulierung beheben.

Der vorgeschlagene Satz 2 wirft aber auch inhaltlich eine Reihe von Fragen auf.

Insgesamt ist bereits ungewöhnlich, dass in einen Gesetz, das ausschließlich auf personenbezogene Daten Anwendung findet, nunmehr eine Definition des Sachdatums aufgenommen werden soll. Zwar wird der negative Anwendungsbereich eines Gesetzes in Ausnahmefällen definiert, dies, soweit ersichtlich, in der Regel aber nur, wenn er unmittelbar zur Anwendung eines anderen Gesetzes führt, wo er ebenfalls definiert ist.[27] Die vorliegende Situation ist jedoch eine andere: Sachdaten unterliegen gerade keiner mit dem datenschutzrechtlichen Regime korrespondierenden gesetzlichen Regelung. Eine Definition des Sachdatums im BDSG ist daher bereits aus logisch-systematischen Gründen problematisch, weil Heranziehung einer Bestimmung, wann ein Gesetz nicht anwendbar sein soll, dessen Anwendung bereits logisch voraussetzt.

Aber auch die Definition an sich erscheint nicht gelungen. Zu unterscheiden sind zwei Aspekte des vorgeschlagenen Satz 2.

Einerseits findet der Kontext der Verarbeitung Berücksichtigung („Keine personenbezogene Angaben sind Sachangaben, die zu einem Betroffenen nicht hinsichtlich Zweck, Ergebnisorientierung oder Inhalt in einem Bezug stehen"), andererseits wird mit den Worten „oder gestellt werden sollen" eine Art Zukunftsprognose eingeführt.

3.2.3 Kontext der Verarbeitung

Der Begründung des Regelungsvorschlages nach greift Satz 2 den Ansatz der Art.29-Datenschutzgruppe auf, die in ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" v. 20.06.2007[28] zu der Frage, wann Informationen *über* eine Person vorliegen (das europä-

[25] Vgl. http://www.canoo.net/services/OnlineGrammar/Satz/Negation/Doppelte.html.

[26] Vgl. etwa http://www.spiegel.de/kultur/zwiebelfisch/0,1518,394969,00.html.

[27] Etwa die Abgrenzung des Anwendungsbereiches TMG und TKG (§ 1 Abs. 1 Nr. 1 TMG:„Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, *soweit sie nicht Telekommunikationsdienste nach **§ 3 Nr. 24 des Telekommunikationsgesetzes**, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen*, ...")

[28] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf .

ische Pendant zum „persönlichen oder sachlichen Verhältnis" im deutschen Recht), auf den Kontext der Verarbeitung abgestellt hat. Konkret sei, dieser Stellungnahme folgend, eine Information ***über*** eine Person anzunehmen, wenn die Information ein Inhalts-, Zweck- oder Ergebniselement aufweist, wobei die Beziehung zwischen Information und Betroffenen bei diesen drei Elementen absteigend offensichtlich ist. Eben diese drei Elemente finden sich - nun allerdings aus unerfindlichen Gründen in einer anderen Reihenfolge - in dem vorliegenden Regelungsvorschlag wieder. Es handele sich um Sachdaten und eben nicht um personenbezogene Daten, wenn keines dieser Elemente vorläge.

Dieser Feststellung ist auch nach hier vertretener Ansicht zuzustimmen, sie dürfte sich jedenfalls in Deutschland inzwischen auch umfänglich durchgesetzt haben.

Allerdings wiederholt Satz 2 damit nur, dass ein personenbezogenes Datum eben nicht vorliegt, wenn kein persönliches oder sachliches Verhältnis gegeben ist. Diese ist allerdings kaum als Fortentwicklung zu begreifen, denn dass ein solches Verhältnis erforderlich ist, steht bereits in dem zurzeit gültigen § 3 Abs. 1 BDSG.

Auch hat diese Redundanz keineswegs klarstellenden Charakter. Gerade das Gegenteil ist der Fall, denn sie reduziert die Abgrenzung zwischen personenbezogenen Daten und Sachdaten künstlich auf das persönliche oder sachliche Verhältnis.

Damit wird impliziert, dass allein dieses eine Merkmal für die Abgrenzung entscheidend sei. Das ist aber entsprechend der Definition des personenbezogenen Datums gerade nicht der Fall. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten ***Einzelangaben*** *über* ***persönliche oder sachliche Verhältnisse*** *einer* ***bestimmten oder bestimmbaren natürlichen Person*** *(Betroffener).* Die Definition hält also folglich 3 weitere Merkmale zur Abgrenzung bereit, nämlich Einzelangaben (1), einer bestimmten oder bestimmbaren (2) natürlichen (3) Person. Im Umkehrschluss liegen Sachdaten folglich immer vor, wenn eines dieser Merkmale nicht erfüllt ist. Sie sind damit bereits definiert, denn sie bilden die Kehrseite des personenbezogenen Datums und umfassen damit alle Daten, die, aus welchem Grund auch immer, nicht personenbezogen sind. Nicht mehr aber vor allem auch nicht weniger.[29] Dass das in dem persönlichen oder sachlichen Verhältnis enthaltene Erfordernis eines Kontextbezuges durch einen ergänzenden Satz 2 derart plakativ in den Vordergrund gezogen wird, führt erneut zu einer Reduzierung auf einzelne Merkmale der Definition des personenbezogenen Datums wie wir dies aus den Jahren zuvor bereits im Hinblick auf die „Bestimmbarkeit" der Person kennen.

Es ist zudem kein Zufall, dass die Art. 29-Datenschutzgruppe, den Kontextbezug unter der Unterüberschrift *Zweites Element: „über"*[30] entwickelt hat, nachdem zuvor das *Erste Element: „alle*

[29] Vgl. auch Summary of replies to the public consultation about the future legal framework for protecting personal data, Brussels, 4 November 2010, http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf, 5.

[30] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf S. 10.

Informationen"[31] und danach das *Dritte Element: eine bestimmte oder bestimmbare natürliche Person"*[32] erläutert worden ist.

Das erneute Aufgreifen des ohnehin bereits in der Definition enthaltenen Merkmales „persönliches oder sachliches Verhältnis" ist folglich redundant und führt zu einer auch europarechtlich nicht gebotene Herausstellung dieses Merkmales gegenüber den anderen.

3.2.4 Einführung einer Zukunftsprognose

Im Gegensatz dazu führt der vorgeschlagene Satz 2 mit den Worten „oder gestellt werden ***soll***" etwas Neues, nämlich eine Art Zukunftsprognose ein, aus der abgeleitet werden können soll, ob Sachangaben als personenbezogene Angaben zu verstehen sind.

Etwas in dieser Art sieht das BDSG bislang grundsätzlich nicht vor. Dies ist auch stringent, eröffnet sich der Anwendungsbereich des BDSG doch erst mit Vorliegen eines personenbezogenen Datums. Allenfalls dem § 34 Abs. 3 S. 2 Nr. 1 BDSG im Rahmen der Auskunftsrechte ist eine ähnliche Tendenz zu entnehmen, dort freilich vor dem Hintergrund einer zwangsläufigen, weil erforderlichen, wenn auch zukünftigen, Herstellung des Personenbezuges, um Auskunft erteilen zu können.

Auch hier fällt zunächst eine gewisse Ungenauigkeit des Entwurfs auf, denn der Regelungsvorschlag versäumt es, deutlich zu machen, wessen Intention hier zu berücksichtigen ist. Dies hat aber erhebliche Auswirkungen: Wollte man hier auch Intentionen Dritter berücksichtigen, würde das Merkmal „persönliches oder sachliches Verhältnis" gerade vor dem Hintergrund der Internetveröffentlichung, gar keinen begrenzenden Charakter mehr haben, denn dann stünde dieses Merkmal vor dem gleichen Dilemma, wie derzeit schon das Merkmal der Bestimmbarkeit: Da man nie wissen kann, wo welches Zusatzwissen vorhanden ist, bzw. nunmehr, was Dritte möglicherweise für Intentionen haben, wäre dieses Merkmal immer erfüllt. Dies kann aber gerade nicht Sinn und Zweck eines Abgrenzungsmerkmales sein. Zudem wäre es insoweit systemfremd, als man der verarbeitenden Stelle die Intention von Dritten zurechnen würde, die die verarbeitende Stelle nicht kennen und daher auch nicht beeinflussen kann.

Insoweit unterscheidet sich dieser Fall auch von dem der Zurechnung von Drittwissen im Rahmen der Bestimmbarkeit. In letzterem Fall geht es nämlich um ein rein objektives Kriterium: Ist Zusatzwissen vorhanden oder nicht. Im ersten Fall geht es um einen Verarbeitungskontext, der höchst subjektiv ist.[33] Würde man der verarbeitenden Stelle die Intentionen Dritter zurechnen, müsste beispielsweise auch die Erhebung von statistischen Angaben bereits dem Datenschutzrecht unterfallen, weil es selbstverständlich auch hier Geschäftszweck sein kann, diese Daten - zum Zwecke der Verknüpfung und der daraus folgenden Entstehung eines Personenbezugs durch Aktivitäten Dritter - zu veräußern.

---

[31] Ebenda, S. 7.

[32] Ebenda, S. 14.

[33] Im Fall des Dienstes Google StreetView ist eine solche Intention seitens Google nicht erkennbar. Zur Zeit bietet der Dienst Straßenansichten, Google StreetView hält zumindest in der jetzigen Ausgestaltung keine Funktion zur Verknüpfung mit natürlichen Personen bereit.

Es ist daher wohl nicht davon auszugehen, dass der vorgeschlagene Satz 2 auch die Intentionen Dritter berücksichtigen will, insoweit wäre folglich dringend eine Klarstellung geboten.

Die Einbeziehung der Intentionen der verarbeitenden Stelle ist hingegen nicht von vornherein abzulehnen, im Gegenteil. Die Verfasser vertreten seit Längerem einen ähnlichen Ansatz in Bezug auf Geodaten, allerdings anders als hier, festgemacht am Merkmal der Einzelangabe und nicht am persönlichen oder sachlichen Verhältnis. Danach sollten Geodaten auch dann als Einzelangaben i.S.d. Datenschutzrechts bewertet werden, wenn die verarbeitende Stelle diese Daten gerade erhebt oder verarbeitet, um sie mit natürlichen Personen zu verknüpfen.[34]

Anders als *Weichert*[35] diesen Ansatz damals offenbar verstand, sollte dadurch gerade keine Reduzierung des Anwendungsbereichs des BDSG allein mit Blick auf die Interessen und Absichten der verarbeitenden Stelle betrieben werden. Die Ursache für das damalige Missverständnis lag vermutlich in einer Vermengung der unterschiedlichen Merkmale der Definition des personenbezogenen Datums. Die von *Weichert* vorgebrachte Kritik, es dürfe nicht auf die Intention der verarbeitenden Stelle ankommen, wann Personenbezogenheit zu bejahen ist und wann nicht, ist eine Voraussetzung, die entsprechend der Datenschutzrichtline nach herrschender Meinung für das Merkmal der *Bestimmbarkeit* verlangt wird. Die Verfasser suchten jedoch nach einer Definition des Merkmals *Einzelangabe*. Nach der Art. 29 Datenschutzgruppe kommen hierfür nur solche Geoinformationen in Betracht, die objektiv Informationen *über eine Person* beinhalten. Die Verfasser wollten über diesen Ansatz jedoch hinausgehen und den Anwendungsbereich – anders als *Weichert* annahm – nicht einschränken, sondern vielmehr ausweiten und zwar auch auf solche Geoinformationen, die von der verarbeitenden Stelle gerade zum Zwecke der eigenen Verknüpfung gesammelt worden sind, aber noch nicht verknüpft worden sind.

Rechtlicher Anknüpfungspunkt dieser Überlegung war die Semantik des Begriffs „Einzelangabe". Legt der Begriff ein aktives Tun nahe, ist Ausgangspunkt hierfür immer auch eine entsprechende Intention der verarbeitenden Stelle, gerichtet auf das Sammeln von Informationen über eine Person. Diese Intention liegt aber bereits vor, wenn Informationen eben zu dem Zweck gesammelt werden, sie sodann zu verknüpfen. Das Gefährdungspotential für das Recht auf informationelle Selbstbestimmung ist daher bereits vor der intendierten Verknüpfung gegeben.

Der vorliegende Vorschlag scheint das gleiche Ziel zu verfolgen und will die Intention der Verknüpfung in das Gesetz aufnehmen, was zu begrüßen ist.

Allerdings ist der Anknüpfungspunkt falsch. Da der neue Satz 2 nämlich das Merkmal persönliches oder sachliches Verhältnis wiederholt, wird die Intention erst bei diesem zweiten Merkmal berücksichtigt. Systematisch richtig wäre es hingegen, die Intention bereits im Rahmen der Prüfung des Tatbestandsmerkmals der Einzelangabe zu berücksichtigen. Denn liegt schon keine Einzelangabe vor, was der Fall ist, wenn es sich um ein Sachdatum handelt, das (noch) keine Infor-

[34] Etwa in Forgó/Krügel, Der Personenbezug von Geodaten - Cui bono, wenn alles bestimmbar ist?, in MMR 2010, 17 (22).

[35] Weichert, Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, in DuD 2009, 351.

mation über eine Person ist[36], scheitert der Anwendungsbereich des Datenschutzrechts bereits mit dem ersten Merkmal, zur Prüfung eines persönlichen oder sachlichen Verhältnisses käme man unter diesen Umständen gar nicht. Das Regelungsziel wird mithin verfehlt, wenn man, wie hier vorgeschlagen, die Intention der verarbeitenden Stelle an die Prüfung des persönlichen oder sachlichen Verhältnisses koppelt.

3.2.5 Ergebnis

Zusammenfassend ist der vorliegende Regelungsvorschlag Nr. 2 wegen des Vorstoßes, die Intention der verarbeitenden Stelle im Rahmen der Eröffnung des Anwendungsbereiches des Datenschutzrechts zu berücksichtigen, zu begrüßen.

Trotzdem muss seine Aufnahme in das BDSG abgelehnt werden. Zunächst definiert er „Sachdaten", die gerade nicht Gegenstand des BDSG sind, was bereits aus systematischen Gründen abzulehnen, letztlich aber auch überflüssig ist, da das Sachdatum die Kehrseite des personenbezogenen Datums und damit bereits definiert ist. Zudem deckt die vorgeschlagene Definition, da allein auf das Vorliegen eines persönlichen oder sachlichen Verhältnisses abgestellt wird, nicht alle Bereiche ab, in denen Sachdaten vorliegen können. Sie ist folglich zu kurz geraten und daher eher hinderlich als hilfreich. Die Wiederholung des sachlichen Verhältnisses ist darüber hinaus redundant, Letztlich sieht der Vorschlag die Berücksichtigung der Intention der verantwortlichen Stelle am falschen Merkmal vor, weshalb das Regelungsziel nicht erreicht werden kann.

Änderungen an der Definition des personenbezogenen Datums haben für die Geoinformationsbranche sehr erhebliche Relevanz.

3.3 Zu Regelungsvorschlag 3

Regelungsvorschlag Nr. 3 fügt eine Definition des Veröffentlichens in § 3 Abs. 4 BDSG ein. Er sieht folgende Formulierung vor:

"2a. Veröffentlichen das Bereitstellen für eine unbestimmte Zahl von Empfängern zum elektronischen Abruf,"

Die Veröffentlichung von personenbezogenen Daten zum elektronischen Abruf ist bisher weder auf europäischer noch auf deutscher Ebene speziell geregelt. Sie unterfällt nach deutschem Verständnis dem Begriff der Übermittlung von personenbezogenen Daten § 3 Abs. 4 Nr. 3 BDSG[37] und stellt deren „intensivste Form" dar.[38]

Diese Einordnung ist jedoch nicht unproblematisch, seit der Lindqvist-Entscheidung[39] des EuGH ist sie sogar, wie sich auch der Begründung des Entwurfs entnehmen lässt, höchst fragwürdig.

[36] Vgl. die Art. 29 Datenschutzgruppe, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf , S. 7.
[37] Für das BDSG etwa Dammann in Simitis, § 3 Rn. 157.
[38] OVG Lüneburg, NJW 1992, 192 (195); zustimmend Gola/Schomerus, Bundesdatenschutzgesetz, 10. Aufl. 2010, § 3 Rn. 33.
[39] Urteil des EuGH, Urteil vom 06.11.2003, abrufbar unter: http://www.jurpc.de/rechtspr/20040030.htm .

Sie führt nämlich, nachdem der Abruf durch eine unbegrenzte Zahl von Empfängern auf der ganzen Welt erfolgen kann, zu der Problematik, dass möglicherweise nach nationalem Recht auch eine Übermittlung in Drittländer vorliäge, mit der Folge, dass die verantwortliche Stelle gem. § 4b Abs. 2 BDSG ein angemessenes Schutzniveau des jeweiligen Drittlandes gewährleisten müsste und dies eine entsprechende Veröffentlichung von Daten im Internet faktisch unmöglich machen würde. In seiner Entscheidung stellte der EuGH folglich zur korrespondierenden europarechtlichen Frage fest, dass das Veröffentlichen von Daten im Internet keine Übermittlung in ein Drittland darstelle.[40] Diese europarechtliche Interpretation ist bei Auslegung des nationalen Rechts wegen des Grundsatzes der richtlinienkonformen Auslegung bindend.

Unstreitig ist jedenfalls, dass die Veröffentlichung dem Oberbegriff der Verarbeitung personenbezogener Daten unterfällt.[41] Der EuGH beschreibt die Veröffentlichung im Internet als eine Verarbeitung, bei der die Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden.[42]

Der vorliegende Entwurf nimmt diese Judikatur insoweit auf, als der Begriff Übermittlung vermieden und stattdessen auf den Begriff der Bereitstellung zurückgegriffen wird. Darüber hinaus deckt sich die Definition des BDSG-E weitestgehen mit der Formulierung des EuGH.

Grundsätzlich ist gegen die Legaldefinition der Veröffentlichung mithin nichts einzuwenden. Ob eine solche allerdings sinnvoll ist, hängt jedoch vor allem davon ab, ob das BDSG für die Veröffentlichung von personenbezogenen Daten eigenständige Regelungen vorsieht, ob dieser Begriff also in der weiteren Gesetzesformulierung überhaupt wieder aufgegriffen wird. Dies ist nach geltender Rechtslage nicht der Fall. Gleichzeitig ist der Definition jedoch zugute zu halten, dass sie die mit der Lindqvist-Entscheidung entstandene Forderung aufgreift, den Veröffentlichungsbegriff vom Übermittlungsbegriff zu trennen.[43] Hierfür ist allerdings keine Definition im Gesetz erforderlich, weil sich dies ohnehin bereits aus der insoweit bindenden Entscheidung des EuGH ergibt.

Regelungsvorschlag Nr. 8 des Gesetzesentwurfs sieht mit einem neu einzufügenden § 29 a BDSG vor, die Veröffentlichung personenbezogener Daten gesondert zu regeln. Der vorliegende Regelungsvorschlag Nr. 3 wäre mithin vertretbar, soweit eine Einführung des vorgeschlagenen § 29a BDSG (Regelungsvorschlages Nr. 8) und damit eine spezielle rechtliche Einhegung der Veröffentlichung zu befürworten wäre. Aus unter 3.8 benannten Gründen ist eine Einführung des § 29 a BDSG jedoch abzulehnen, weshalb auch die hier geforderte Einführung einer Legaldefinition der Veröffentlichung obsolet wird.

Für die Geoinformationsbrache hätte die Einführung einer Legaldefinition der Veröffentlichung keine Auswirkungen. Diese könnten sich erst aus einem für die Veröffentlichung zu schaffenden gesetzlichen Regime ergeben.

---

[40] Ebenda, Ziff. 71.

[41] Ebenda, Ziff. 25 und 47.

[42] Ebenda, Ziff. 47.

[43] Ob und wenn ja inwiefern die Abspaltung der Veröffentlichung von der Übermittlung Auswirkungen auf die an die Übermittlung geknüpften erweiterten Zulässigkeitsvoraussetzungen hat, wurde vorliegend nicht geprüft.

3.4 Zu Regelungsvorschlag 4

Regelungsvorschlag Nr. 4 sieht eine Ergänzung des § 3 Abs. 7 BDSG vor. § 3 Abs. 7 BDSG lautet: „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.". Nach dem Entwurf soll folgender Satz 2 eingefügt werden:

"§ 7 bis § 10 Telemediengesetz sind anwendbar."

Zur Begründung wird angeführt, dass Telemedien zur Zeit wegen der §§ 7-10 TMG nicht für die Einstellung fremder Inhalte verantwortlich, trotzdem aber durch die technische Verfügungsmacht über die Daten datenschutzrechtlich verantwortlich seien. Dies führe *„praktisch zu großen Problemen bei Suchmaschinen, Sozialen Netzwerken, Blogs und Foren, wo die Verantwortlichkeit für personenbezogene Inhalte faktisch nicht oder nur schwer durchsetzbar"* sei. Der Verweis würde dazu führen, dass eine Verantwortlichkeit für fremde personenbezogene Inhalte erst dann begründet würde, wenn die verarbeitende Stelle Kenntnis erlange. Dies wiederum führe dazu, dass der Dienstleister verantwortlich gemacht werden (könne), wenn die Daten von einem Dienstleister übernommen werden bzw. wenn der Betroffene technisch die Hoheit über seine Daten verliere.

Sowohl der Änderungsvorschlag an sich als auch seine Begründung werfen Fragen auf.

§ 3 Abs. 7 BDSG definiert die verantwortliche Stelle. Bei Verortung des Haftungsprivilegs, wie es die §§ 7-10 TMG vorsehen, als Satz 2 der Definition stellt sich nun die Frage, ob verantwortliche Stellen, auf die das Haftungsprivileg zutrifft, aus diesem Grund nicht mehr verantwortliche Stelle im Sinne des Datenschutzes seien sollen (wer ist denn dann verantwortliche Stelle?) oder ob die verantwortlichen Stellen eben nur für mögliche Datenschutzverstöße Dritter nicht haften soll. Vermutlich ist letzteres gemeint. Dann ist die Verortung in der Definition jedoch höchst missverständlich und muss als systematisch verunglückt bezeichnet werden.

Überdies greift das Haftungsprivileg der §§ 7 – 10 TMG bei Telemedien auch nach geltender Rechtslage wohl schon für datenschutzrechtliche Verstöße im Rahmen fremder Inhalte.[44] Satz 2 regelt folglich, anders als die Begründung des Regelungsvorschlages vermuten lässt, auf den ersten Blick nichts Neues, sondern soll vermutlich allenfalls klarstellenden Charakter haben.

Auch dies ließe sich jedoch anders interpretieren, da sich nämlich in der Begründung nichts zu der Art des Verweises finden lässt, stellt sich die Frage, ob das Haftungsprivileg der §§ 7 – 10 TMG durch Satz 2 nun für alle verantwortlichen Stellen gelten soll, also auch für solche, die keine Telemedien sind.

Letztlich verwirrt dann auch der letzte Satz der Begründung, der wiederum auf die tatsächliche Hoheit über die Daten abstellen will und nicht auf die Kenntnis der verantwortlichen Stelle, die mit der Anwendbarkeit der §§ 7 – 10 TMG eben gerade entscheidendes Abgrenzungskriterium ist.

[44] Dies wäre allerdings vor dem Hintergrund insbesondere des Art. 5 lit. b) der Richtlinie 2000/31/EG, auf den die §§ 7-10 TMG bekanntlich zurückgehen, detaillierter zu prüfen.

Soll im Rahmen der Novelle folglich nochmals klargestellt werden, dass Telemedien (und nur diese!) (auch) nicht für datenschutzrechtliche Verstöße haften, soweit die §§ 7 – 10 TMG erfüllt sind, ist hiergegen nichts einzuwenden. In der Definition der verantwortlichen Stelle ist ein Haftungsprivileg jedoch fehlplatziert.

Regelungsvorschlag Nr. 4 ist daher aus systematischen Gründen problematisch, da die Haftungsprivilegierung von Telemedien nichts mit der Definition der datenschutzrechtlich verantwortlichen Stelle zu tun hat. Im Gegenteil, eine Verortung dieses Verweises in der Definition führt ohne Not zu einer Reihe von Unklarheiten. Für die Geoinformationsbranche hat dieser Regelungsvorschlag keine weiteren Auswirkungen.

3.5 Zu Regelungsvorschlag 5

Regelungsvorschlag 5 sieht die Einfügung eines § 3b BDSG-E vor uns lautet: „Erfolgt eine Erhebung oder Verarbeitung durch Aktivitäten einer natürlichen Person, so sind die Grundeinstellungen des Dienstes so zu gestalten, dass so wenig wie möglich personenbezogene Daten erhoben oder verarbeitet werden.

Eine Änderung der Einstellungen setzt die Berücksichtigung der Voraussetzungen des § 4a voraus."

3.5.1 Zu Satz 1

In diesem Punkt sieht der Entwurf eine Erweiterung des Datenschutzes insbesondere auf die Freigabe personenbezogener Daten durch die Nutzer in sog. Soziale Netzwerke vor.[45] Darunter fallen Dienste mit nutzergenerierten Inhalten wie beispielsweise Facebook, MySpace oder YouTube.

Normiert werden soll der Grundsatz des „Privacy by default". Dieser wurde bereits im Spitzengespräch „Digitalisierung Stadt und Land" vom 20. September 2010 diskutiert, hier allerdings im Zusammenhang mit Geodatendiensten.[46] Das Prinzip „Privacy by default" ist eine Ausprägung des Grundsatzes „Privacy by design", der datenschutzfreundliche Voreinstellungen bereits im Design eines Geräts verankert sehen will. Auch in Europa gibt es verstärkt Bestrebungen, diesen

[45] Vgl. zur Problematik auch Bonneau/Preibusch: The Privacy Jungle: On the Market for Date Protection in Social Networks", http://www.preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf; Privatsphärenschutz in Soziale-Netzwerke-Plattformen, Fraunhofer SIT, http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm501-35966.pdf ; Gross/Acquisti, Information Revelation and Privacy in Online Social Networks (The Facebook case), http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

[46] Die Eckpunkte des Bundesministerium des Innern unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/eckpunkte_geodienste.pdf?__blob=publicationFile ; vgl. auch die Rede von Bundesminister Dr. Thomas de Maizière, MdB „Grundlage für eine gemeinsame Netzpolitik der Zukunft" am 22. Juni 2010, I. 1. hier statt „Privacy by default" „Respect by default": http://carta.info/29493/de-maizieres-redemanuskript-grundlagen-fuer-eine-gemeinsame-netzpolitik-der-zukunft/ .

Grundsatz zu normieren.[47] Ebenso hat die Fraktion Bündnis 90/ Die Grünen im Oktober die Bundesregierung zur Einbringung eines Gesetzesentwurfs zur Verbesserung des Datenschutzes in sozialen Netzwerken aufgefordert.[48,49]

Die Datenfreigabe durch die Nutzer wird bei Sozialen Netzwerken in der Regel durch Voreinstellungen kanalisiert. Dies wird bislang relativ unterschiedlich gehandhabt: Teilweise sind die Voreinstellung relativ eng, so dass ein hohes Datenschutzniveau Standard ist[50], welche vom Nutzer dann gesenkt werden kann, wenn er mehr Inhalte mit mehr Nutzern teilen möchte. Dann wiederum gibt es Dienste, die zunächst ein relativ geringes Datenschutzniveau voreingestellt bereitstellen[51], das der Nutzer dann erhöhen kann. Die Übergänge sind fließend.

Möchte der Nutzer nicht so viele personenbezogene Daten von sich preisgeben wie vom Dienst vorgesehen, muss er den Einstellungen explizit widersprechen. Über die aufgrund der Voreinstellungen bereits einmal freigegebenen Daten kann der Nutzer unter Umständen nicht mehr verfügen, weil diese an anderen Stellen im Internet abrufbar bleiben, er verliert also die Herrschaft über seine Daten trotz Widerrufs.

Das ULD will deswegen das Vorhalten datenschutzfreundlicher Voreinstellungen für die Betreiber von Diensten mit nutzergenerierten Inhalten in seinem Entwurf verpflichtend gestalten.

Statt eines Opt-Out soll jetzt ein Opt-In bezüglich der Freigabe der personenbezogenen Daten durch die Nutzer normiert werden. Zweck der geplanten Regelung ist, dass der Nutzer Sozialer Netzwerke, der in diese seine personenbezogenen Daten einstellt, davor geschützt werden soll, ungewollt zu viele Daten der Öffentlichkeit zugänglich zu machen. Man kann wohl davon ausgehen, dass das ULD mit den „Aktivitäten", durch die die Erhebung oder Verarbeitung der Daten geschehen soll, in erster Linie das Einstellen personenbezogener Daten meint.

Die am Institut der Verfasser durchführten Forschungen im Bereich sozialer Netzwerke im Rahmen eines FP7-Projektes[52] sind zum Zeitpunkt der Erstellung dieses Gutachtens noch nicht abgeschlossen und veröffentlicht. Es zeichnet sich allerdings ab, dass insgesamt der Umgang mit

---

[47] So etwa: Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, European Data Protection Supervisor Peter Hustinx vom 18. März 2010: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf ; auch die Rede des Vice- President of the European Commission Viviane Reding, „Unleashing the digital single market Conference auf einer Konferenz in Lissabon am 16. September 2010: http://webcache.googleusercontent.com/search?q=cache:KV9TEn2y02UJ:europa.eu/rapid/pressReleasesAction.do%3Freference%3DEDPS/10/6+eu+kommission+privacy+be+default&cd=3&hl=de&ct=clnk&gl=de&client=firefox-a; vgl. auch das Rom Memorandum, Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten von der International Working Group on Data Protection in Telecommunications vom 4.3.2008, www.datenschutz-berlin.de/attachments/470/675.36.13.pdf .

[48] BT-Drs. 17/1589.

[49] Hingegen kritisch zu „Privacy by default"-Bestrebungen etwa Jeff Jarvis, der auf der re:public 2010 in Berlin zu „Privacy to public" aufgefordert hatte.; http://www.youtube.com/watch?v=pSqyEXLkrZ0 .

[50] Etwa bei „SchuelerVZ".

[51] Etwa „Spick mich", wo quasi sämtliche vom User bereitgestellten Daten sowie weitere vom Dienst erhobene Daten grundsätzlich für jedermann sichtbar sind.

[52] Vgl. http://www.consent.law.muni.cz/ .

personenbezogenen Daten innerhalb der großen in Deutschland verfügbaren sozialen Netzwerke wenn überhaupt nur in Teilbereichen für den Nutzer nachvollziehbar und insgesamt nicht besonders transparent ist. So bedarf es auch relativ zur typischen Nutzergruppe deutlich überdurchschnittlicher Kenntnisse, um die Vorgänge – soweit sie überhaupt in Datenschutzerklärungen erläutert sind – nachzuvollziehen. Insbesondere sind die entsprechenden Informationen häufig nur schwer aufzufinden, auf verschiedene Dokumente verteilt und nicht selten widersprüchlich. Vor allem was die Weitergabe von Daten an Dritte angeht, sind die Erläuterungen – sofern überhaupt existent – nicht selten unklar. Auch die Zwecke der Datenerhebung sind im Allgemeinen jenseits der Vertragserfüllung obskur. Des Weiteren ist selten bekannt, wie Daten verknüpft werden und welche weiteren Daten erhoben und abgeglichen werden – dies betrifft insbesondere das Nutzerverhalten, Datenabgleiche mit anderen, insbesondere befreundeten Nutzern sowie Verknüpfungen von Nutzern, die ähnliche Daten speichern (z.B. eMail-Adressen), und so weiter.

Ein von der Stiftung Warentest im März dieses Jahres durchgeführter Test hat ergeben, dass die Organisation und Transparenz der Daten bei kaum einem Netzwerk als gut beurteilt wurde, und sogar bei den Marktführern wie MySpace, LinkedIn oder Facebook zu wünschen übrig lassen.[53] Der Verbraucherzentrale Bundesverband e.V. leitete kürzlich gegen die Netzwerke MySpace, Facebook, lokalisten.de, wer-kennt-wen.de und Xing wegen nutzerfeindlicher Geschäftsbedingungen Unterlassungsverfahren ein.[54] Angesichts solcher Fakten ist eine Pflicht der Diensteanbieter zu datenschutzfreundlichen Voreinstellungen sicher begrüßenswert.

Gegen eine solche Regelung könnte allerdings sprechen, dass hierdurch Rechte der Betreiber Sozialer Netzwerke beschnitten würde. Würde die Veröffentlichung der personenbezogenen Daten verringert, könnte auch eine Schmälerung der Verbreitungs- und Streuungseffekte zu befürchten sein. In Betracht kommt das Recht der Betreiber Sozialer Netzwerke auf die Freiheit unternehmerischer Betätigung gemäß Art. 12 Abs. 1 GG sowie das Auffanggrundrecht des Art. 2 Abs. 1 GG, die allgemeine Handlungsfreiheit. Welches dieser beiden Grundrechte als Rechtfertigung für einen Eingriff in das informationelle Selbstbestimmungsrecht angenommen werden kann, ist umstritten,[55] kann aber hier dahinstehen. Denn es ist zweifelhaft, inwieweit ein Geschäftsmodell überhaupt Schutz verdient, das darauf abzielt, den - unerfahrenen oder gedankenlosen - Nutzer Sozialer Netzwerke durch Voreinstellungen dazu zu bringen, möglichst viele personenbezogene Daten preiszugeben. Der Dienst als solcher wird durch „privacy by default" nicht tangiert, dessen Zweck ist nach wie vor gegeben, nämlich dem Nutzer zu ermöglichen, seine Daten und seine Inhalte einzustellen und sich so mit anderen in dieser Netzgemeinschaft auszutauschen. Die Verpflichtung zu datenschutzfreundlichen Voreinstellungen wäre lediglich als eine Art Übereilungsschutz, nicht zu viele Daten freizugeben oder zu veröffentlichen, zu be-

[53] http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1854999/.

[54] https://www.vzbv.de/go/presse/1180/8/97/index.html .

[55] Jarass nimmt an, dass die Freiheit wirtschaftlicher Betätigung und die unternehmerische Handlungsfreiheit dem Schutz von Art. 2 Abs. 1 GG unterliege und nur in bei Maßnahmen mit direktem Berufsbezug bzw. mit berufsregelnder Tendenz Art. 12 Abs. 1 GG unterfalle; Jarass/Pieroth, Art. 2 Rz 4a. Dagegen hält Murswiek, Art. 12 Abs. 1 GG Art. 12 Abs. 1 GG für das speziellere Grundrecht, dass Art. 2 Abs. 1 GG verdränge; Sachs, Art. 2 Rz 54.

greifen. Dies dürfte gerade für Minderjährige, die die Konsequenzen eines sorglosen Umgangs mit ihren Daten vielleicht nicht in Gänze überblicken, sinnvoll sein.

Eine „Entmündigung" des Nutzers ist nicht zu befürchten. Denn auch bei datenschutzfreundlichen Voreinstellungen ist es dem Nutzer nach wie vor freigestellt, nach seinem Belieben personenbezogene Daten zu veröffentlichen.

Allerdings könnte angezweifelt werden, inwieweit die Pflicht zu datenschutzfreundlichen Voreinstellungen überhaupt noch im BDSG geregelt werden muss.[56] Denn § 3a BDSG normiert bereits ausdrücklich den Grundsatz der Datenvermeidung und Datensparsamkeit. Laut Gesetzgeber sollte die Regelung dazu führen, dass durch den gezielten Einsatz datenschutzfreundlicher Technik die Gefahren für das informationelle Selbstbestimmungsrecht reduziert werden.[57] Dadurch soll die verantwortliche Stelle dazu verpflichtet werden, sich schon vor Erhebung der Daten über die Erforderlichkeit und Gebotenheit der Erhebung klar zu werden.[58] Aus § 3a BDSG, der auch für Soziale Netzwerke gilt, ergibt sich bereits die allgemeine Maxime, dass möglichst wenig Daten der Nutzer verarbeitet werden sollen. Allerdings ist dieser Grundsatz nur als Zielvorgabe zu verstehen.[59] Zumindest stellt er keine zwingende Handlungsanweisung dar, wie es die vom ULD vorgesehene Pflicht zu Voreinstellungen, die den Nutzer vor allzu großer Freigiebigkeit hinsichtlich seiner personenbezogenen Daten bewahrt, täte.

Um einen ausreichenden Schutz des Nutzers vor Preisgabe seiner personenbezogenen Daten zu gewährleisten, wäre eine wie vom ULD vorgesehene Regelung grundsätzlich zu begrüßen. Auch wenn sich die Entwurfsvorschrift an Betreiber von Diensten mit nutzergenerierter Datenverarbeitung richtet, so könnte sie für Geoinformationsdienste gleichwohl relevant sein, nämlich insbesondere dann, wenn diese nutzergenerierte Inhalte bereithalten.

3.5.2 Zu Satz 2

Des Weiteren will das ULD eine etwaige Änderung der datenschutzrechtlichen Grundeinstellungen von einer Einwilligung, die den Voraussetzungen des § 4a BDSG genügen soll, abhängig machen, wörtlich lautet der Vorschlag: „Eine Änderung der Einstellungen setzt die Berücksichtigung der Voraussetzungen des § 4a voraus." Auch hier bestehen wiederum sprachliche Unklarheiten, weil sich nicht exakt bestimmen lässt, welche Voraussetzungen hier zu berücksichtigen sind, da § 4a die Einwilligung bekanntlich insgesamt regelt. Gemeint sind vermutlich die Voraussetzungen für die *Wirksamkeit* einer Einwilligung.[60]

---

[56] So u.a. Stephan Hansen-Oest, http://www.datenschutz-guru.de/2010/09/privacy-by-design-privacy-by-default-die-neuen-buzzwords-im-datenschutz/ , der im Grundsatz „Privacy by default" das neue „Buzz-Word" für den modernen Datenschutz sieht.

[57] BT-Drs. 14/4329, S. 30.

[58] Vgl. Taeger/Gabel (Hrsg.)/Zscherpe, Kommentar zum BDSG , 2010, § 3a BDSG, Rn. 2.

[59] Vgl. Taeger/Gabel (Hrsg.)/Zscherpe, Kommentar zum BDSG , 2010, § 3a BDSG, Rn. 20.; BT-Drs. 16/13657, S. 17.

[60] So auch die Erläuterung, vgl. dort zu 5.: „Erfolgt eine darüber hinausgehende Erhebung oder Verarbeitung, so sind die Anforderungen an die Wirksamkeit einer Einwilligung zu stellen (Freiwilligkeit, Bestimmtheit bzgl. Art der Daten, verarbeitende Stellen und Zweck, Warnfunktion, Hervorhebung)." Auch diese ist freilich wiederum ungenau, weil es sich zB bei der Warnfunktion nicht um eine Wirksamkeitsanforderung handelt, sondern um einen Grund, dessenthalben an die Einwilligung bestimmte Voraussetzungen genüpft werden.

Der Telos der Norm liegt wohl darin, sicherzustellen, dass eine über die Grundeinstellung hinausgehende Erhebung oder Verarbeitung der personenbezogenen Daten einwilligungsbasiert so zu erfolgen hat, dass an diese hohe Anforderungen zu stellen sind. Ausweislich des vorgeschlagenen Normtextes geht es also eindeutig allein um Anforderungen an die Einwilligung, sodass Erhebungen und Verarbeitungen, deren Rechtmäßigkeit nicht auf einer Einwilligung, sondern auf einer gesetzlichen Grundlage beruhen (insb. §§ 28 und 29 BDSG), von der Bestimmung nicht erfasst sind.

Jedoch liest man in der Begründung des Entwurfs: „Um zu gewährleisten, dass die Nutzenden insofern ihr Selbstbestimmungsrecht wahrnehmen können, werden die Diensteanbieter verpflichtet, ihren Dienst so zu gestalten, dass nicht mehr Daten erhoben und verarbeitet werden, als für die Nutzung des Dienstes unbedingt erforderlich ist. *Erfolgt eine darüber hinausgehende Erhebung oder Verarbeitung, so sind die Anforderungen an die Wirksamkeit einer Einwilligung zu stellen (Freiwilligkeit, Bestimmtheit bzgl. Art der Daten, verarbeitende Stellen und Zweck, Warnfunktion, Hervorhebung).*" Daraus ergibt sich, dass der Entwurf offenbar davon ausgeht, dass eine (allenfalls auch nachträgliche) Abkehr von der maximal restriktiven Grundeinstellung nur mit Zustimmung des Betroffenen erfolgen dürfe. Dieses Erfordernis ergibt sich jedoch weder aus dem Normtext (insb. nicht aus § 3b Satz 1, der ja auf ein relationales Element „so wenig wie möglich" abstellt) noch ist ein derart ausschließliches Abstellen auf die Zustimmung (zulasten sonstiger Rechtsgrundlagen, insb. §§ 28, 29 BDSG) der bisherigen Systematik des BDSG inhärent. Ob und inwieweit diese Stärkung der Einwilligung mit konfligierenden, grundrechtlich geschützten Interessen des Plattformbetreibers, der Plattformnutzer und der Öffentlichkeit kompatibel ist, kann hier nicht im Detail (ansatzweise aber immerhin zu § 29a BDSG-E) untersucht werden, jedoch wäre eine solche Prüfung, insbesondere im Lichte des Verhältnismäßigkeitsgrundsatzes, durch das BVerfG bald nach Inkrafttreten zu erwarten.

§ 4a Abs. 1 Satz 3 BDSG normiert in der derzeit geltenden Fassung, dass die Einwilligung der Schriftform bedürfen soll, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist. Es ist unklar, ob in den hier interessierenden Fällen eine andere Form angemessen sein könnte.

Eine Einwilligung die so aussähe, dass der Nutzer einen Brief oder eine Postkarte an den Betreiber Sozialer Netzwerke zu schreiben hat, worin er um eine Änderung der Grundeinstellungen bittet, wird wohl kein realistisches Szenario darstellen Daher erscheint Satz 2 des § 3a BDSG-E als überflüssig vor dem Hintergrund geltenden Rechts.

Jedoch ist der Vorschlag gemeinsam mit Regelungsvorschlag 6 zu lesen. Dessenthalben soll nämlich die Einwilligung auch elektronisch erklärt werden können, sofern die Anforderungen an die elektronische Einwilligung, wie sie derzeit im TMG gestaltet sind und nun in das BDSG übertragen werden sollen, eingehalten werden. Damit betreffen die zu Regelungsvorschlag 6 vorgebrachten Einwände auch Regelungsvorschlag 5.

Aufgrund mangelnder Praxisrelevanz erscheint Satz 2 des § 3a BDSG-E als überflüssig, wenn nicht sogleich Änderungsvorschlag 6 umgesetzt wird. Wird sogleich Änderungsvorschlag 6 ebenfalls umgesetzt, so sind die dort zu erhebenden Einwände auch gegen Regelungsvorschlag 5, Satz 2, zu erheben. Eine Relevanz für die Geoinformationsbranche ist nicht auszuschließen, sofern Geoinformationsdiensten mit nutzergenerierten Inhalten arbeiten.

3.6 Zu Regelungsvorschlag 6

Regelungsvorschlag 6 sieht eine Reform des § 4a BDSG vor und lautet: „In § 4a Abs. 1 wird Satz 2 gestrichen. Satz 3 wird Satz 2. Es wird folgender Abs. 1a eingefügt:

"Die Einwilligung bedarf der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Die Einwilligung kann elektronisch erklärt werden, wenn die verantwortliche Stelle sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat,
2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit der Wirkung für die Zukunft widerrufen kann."

Der Regelungsvorschlag 6 sieht also vor, die elektronische Einwilligung des § 13 Abs. 2 TMG mitsamt ihren Voraussetzungen durch die Schaffung eines Abs. 1a in § 4a BDSG zu integrieren. Der Grund dafür sei, dass in der Praxis diese Form der Einwilligung oft neben die schriftliche Einwilligung trete.[61] Unter einer elektronischen Einwilligung iSd § 13 TMG versteht man eine elektronische Willenserklärung, wozu eine eindeutige und bewusste Handlung des Nutzers erforderlich ist, ohne Voraussetzung einer besonderen Form.[62] § 13 TMG setzt keine qualifizierte elektronische Signatur (und damit keine elektronische Form im Sinne des § 126a BGB) voraus, sondern sie soll technikoffen gestaltet werden können.[63] Es genügt, wenn die Einwilligungserklärung beispielsweise durch das Setzen eines Häkchens bestätigend wiederholt wird.[64] Zwar ist bereits normiert, dass auch eine elektronische Form der Einwilligung möglich ist - Abs. 1 Satz 3 (... soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.), aber der Verweis auf die Möglichkeit einer elektronischen Einwilligung scheint aufgrund seiner klarstellenden Funktion auf den ersten Blick sinnvoll zu sein.

Allerdings ist es zum einen fraglich, ob das Schriftlichkeitsgebot der Einwilligung und der der Schriftform und ihrer Warnfunktion inhärente Betroffenenschutz nicht verwässert werden. Bislang findet sich die Möglichkeit der elektronischen Einwilligung im TMG, die dortige Verortung ist auch aufgrund des Sachzusammenhangs sinnvoll. Mit der vom ULD vorgesehenen Regelung wird jedoch unklar, in welchen Fällen „klassischer Datenverarbeitung" überhaupt die Schriftform noch gewahrt werden muss, auch wenn das ULD an dem Grundsatz der Schriftform nichts geändert sehen will.[65]. Die bisherige Regelung normiert die Schriftform als Regel, da die Warnfunktion am besten durch diese Form erreicht werden könne.[66] Von der Schriftform kann es jedoch bei Vorliegen besonderer Umstände eine Ausnahme geben, so insbesondere, wenn für die Kommunikation ein elektronisches Medium genutzt wird.[67] § 4a BDSG-E normiert die Schriftform (von der

[61] Begründung des BDSG-E, Vorschlag Nr. 6, S. 6 unten.
[62] Vgl. Spindler/Schuster/Nink: Recht der elektronischen Medien, 1. Aufl. 2008, § 13 Rn. 6.
[63] Schaar, MMR 2001, 644, 646.
[64] OLG Brandenburg, MMR 2006, 405, 406.
[65] Begründung des BDSG-E, Vorschlag Nr. 6, S. 6 unten.
[66] Taeger/Gabel (Hrsg.)/Zscherpe, Kommentar zum BDSG , 2010, § 4a BDSG, Rn. 32.
[67] Taeger/Gabel (Hrsg.)/Zscherpe, Kommentar zum BDSG , 2010, § 4a BDSG, Rn. 32.

Ausnahmen möglich sind) UND die elektronische Einwilligung als Regel. Danach soll eine elektronische Einwilligung IMMER möglich sein (sofern die verantwortliche Stelle die nachfolgenden Punkte beachtet). Wenn das gewollt ist, kann die Erwähnung der Schriftform weggelassen werden. Wenn das nicht gewollt ist, sollte der Satz so formuliert werden, dass die elektronische Einwilligung im Zusammenhang mit elektronischen Medien genutzt werden kann, andernfalls aber die Schriftform zu verwenden ist.

Auch entstehen durch die gewählte Zusammenführung des TMG mit dem BDSG systematische Probleme, weil unklar bleibt, ob der Vorschlag drei Formen der Einwilligungserklärung kennen will (nämlich Schriftform [welche durch die elektronische Form im Sinne des § 126a BGB substituiert werden kann[68]], andere Form, die aufgrund der Umstände angemessen zu sein hat und elektronische Form) oder nur zwei (nämlich Schriftform, andere Form, die aufgrund der Umstände angemessen zu sein hat, und als Unterfall der anderen Form die elektronische Form). Sollte letzteres gemeint sein, würde dies dazu führen, dass erst recht in jedem Fall zu prüfen wäre, ob die elektronische Form aufgrund der Umstände im Einzelfall angemessen ist oder nicht, was bei der ersten Lesart nicht der Fall wäre. Die Frage kann erhebliche Relevanz entfalten, weil eine Prüfung des Einzelfalls die Einsetzung der elektronischen Form aus Sicht der datenverarbeitenden Stelle erst recht riskant erscheinen ließe.

Schließlich ist es auch systemwidrig, den Regelungsgehalt eines Spezialgesetzes in ein Auffanggesetz zu integrieren. Vorliegend handelt es sich bei § 13 TMG um eine spezielle datenschutzrechtliche Regelung, die auf Telemediendienstebetreiber Anwendung findet. Das BDSG legt als Auffangregelung die allgemeinen datenschutzrechtlichen Prinzipien fest. Würde man einfach die speziellen Regelungen in ein allgemeines überführen, läuft das der Gesetzessystematik zuwider.

Auffällig ist zudem, dass aufgrund der geplanten Streichung des Satzes 2 nun die umfassenden Aufklärungspflichten wegfallen. Darin wird die verantwortliche Stelle verpflichtet, den Betroffenen auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die etwaigen Folgen der Verweigerung der Einwilligung hinzuweisen. Ob diese Pflicht absichtlich nicht mehr in dem Entwurf vorhanden ist, ist unklar, die Begründung des BDSG-E gibt darüber keinen Aufschluss. Möglicherweise soll die Aufklärungspflicht in Nr. 1 des Abs. 1a hineinzulesen sein, wonach die verantwortliche Stelle sicherzustellen hat, dass "der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat". Jedoch kann dieser Formulierung nicht eindeutig entnommen werden, dass der Nutzer über Zweck und Folgen der Verweigerung der Einwilligung aufzuklären ist. Diese Aufklärungspflicht sollte definitiv und klar formuliert im BDSG vorhanden sein.

Vielleicht wurde es auch versäumt, ebenfalls den Satz 1 (am Anfang) des § 13 Abs. 1 TMG zu übernehmen, wonach die Pflicht des Anbieters zur Aufklärung des Nutzers über den Zweck der Erhebung seiner Daten geregelt ist. Das ULD will laut seiner Begründung die bisherige Regelung des § 3 Abs. 2 TMG auf § 4a BDSG übertragen.[69] Ein Blick in das TMG zeigt jedoch, dass es in § 3

[68] Zutreffend Gola/Schomerus, Bundesdatenschutzgesetz, 10. Aufl. 2010, § 4a, Rn. 13.
[69] So in der Begründung zum BDSG-E, zu Vorschlag 6, S. 6 f.

Abs. 2 TMG nicht um Einwilligung geht. Diese findet sich vielmehr in § 13 Abs. 2 TMG (offensichtlich handelt es sich um einen Schreibfehler [70]) und wurde wörtlich übernommen.

Aus gesetzessystematischen Erwägungen und der Verringerung des Schutzniveaus des Bürgers ist die Streichung des Satzes 2 und Integrierung des § 13 Abs. 2 TMG nicht sinnvoll. Eine Relevanz für die Geoinformationsbranche ist kaum gegeben.

3.7 Zu Regelungsvorschlag 7

Laut Begründung des Entwurfs soll der § 29 Abs. 3 BDSG gestrichen und durch einen neuen § 29a Abs. 5 ersetzt werden, im Wortlaut: „§ 29 Abs. 3 wird gestrichen. Die Absätze 4 bis 7 werden die Absätze 2 bis 6."

Inwieweit § 29a Abs. 5 des Entwurfs problematisch sein kann, wird in Punkt 3.8 geklärt. Hier ist ergänzend darauf hinzuweisen, dass die in § 29a Abs. 5 gewählte Formulierung, dass der entgegenstehende Wille auch außerhalb der Ursprungsquelle „auf andere Weise eindeutig erkennbar" sein kann, erneut Unklarheiten aufwirft, weil nicht deutlich wird, welche anderen Weisen hier gemeint sein können und wie sich die datenverarbeitende Stelle darum zu kümmern hat, diese Informationen zu erlangen. Ist eine derartige Ausweitung des Betroffenenschutzes gewollt, dann sollte uE auch eine klare gesetzgeberische Anleitung gegeben werden, wie der Betroffene diesen Willen auf andere Weise kommunizieren kann, sodass ihn die verantwortliche Stelle zur Kenntnis zu nehmen hat. Eine Möglichkeit, dies zu realisieren wäre etwa das Führen einer „Robinson-Liste" an einer zentralen Stelle, etwa beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.[71]

Allerdings ist nicht recht ersichtlich, warum dies zu einem verstärkten Betroffenenschutz sinnvoll beitragen kann, wenn man vom Betroffenen die Eintragung in einer weiteren Liste verlangt, um die verantwortliche Stelle auf andere Weise eindeutig zu informieren. Verzichtet man jedoch auf ein derartiges Erfordernis, schafft man für die verantwortliche Stelle kaum kontrollierbare Risiken hinsichtlich anderer, „auf eindeutige Weise erkennbarer" Willenserklärungen. Schließlich steht zu vermuten, dass diese Bestimmung Auswirkungen auf die Dogmatik der Einwilligungserklärung insgesamt entwickeln kann, welche ja aus zivilrechtlich-dogmatischen Gründen den Empfänger der Einwilligung bzw. ihres Widerrufs, an die man eine Erklärung richtet, als Adressaten kennt[72] - und nicht die Allgemeinheit, der gegenüber man sich „eindeutig" äußert.

Der Vorschlag erscheint daher aus praktischen wie aus dogmatischen Gründen problematisch. Die Relevanz für die Geoinformationsbranche könnte dann erheblich sein, wenn auf Dauer un-

[70] Begründung des BDSG-E, Vorschlag 6, S. 7 oben.

[71] Ein entsprechendes Beispiel lässt sich etwa in § 7 As. 2 Satz 1 des österreichischen E-Commerce-Gesetzes finden: „Die Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) hat eine Liste zu führen, in die sich diejenigen Personen und Unternehmen kostenlos eintragen können, die für sich die Zusendung kommerzieller Kommunikation im Weg der elektronischen Post ausgeschlossen haben." Die Anwendung dieser Bestimmung führt freilich zu erheblichen Folgeproblemen, die hier nicht angerissen werden und Konstruktionen, bei denen Betroffene ihren Willen „auf andere Weise" erklären können, insgesamt zweifelhaft erscheinen lassen.

[72] Vgl. dazu vertiefend Ansgar Ohly, „Volenti non fit iniuria": Die Einwilligung im Privatrecht, Tübingen 2002, 341 f. et passim.

klar bleibt, wie ein entgegenstehender Wille „auf andere Weise eindeutig erkennbar" gemacht und zur Kenntnis genommen werden kann.

3.8 Zu Regelungsvorschlag 8

Die Einfügung eines § 29a BDSG wird einem zentralen Anliegen des ULD in seinem Entwurf gerecht: der Konstitution eines rechtlichen Rahmens für die **Veröffentlichung von personenbezogenen Daten im Internet**. Die Regelung soll dem Umstand Rechnung tragen, dass entsprechende Veröffentlichungen von Daten legitimen Interessen dienen und insoweit eine wichtige gesellschaftliche Funktion erfüllen können[73]. Gleichzeitig soll damit auf Gesetzesebene der Ausgleich vorgenommen werden bezüglich des gegenläufigen Persönlichkeitsrechts des Betroffenen[74].

Die vorgeschlagene Norm ist zunächst dahingehend zu untersuchen, ob sie Regelungen im Anwendungsbereich der Richtlinie 95/46/EG trifft. Ist dies der Fall, ist sie an den Vorschriften dieser Richtlinie und deren Ziel, ein einheitliches Datenschutzniveau in Europa zu schaffen, zu messen. Ansonsten sieht sich § 29a BDSG-E systematisch im Bereich der Datenverarbeitung durch private Stellen verankert. Sie steht damit in Zusammenhang insbesondere mit den dort anzutreffenden **Erlaubnistatbeständen** für die Datenverarbeitung, die die Erforderlichkeit der Einwilligung durch den Betroffenen entfallen lassen. § 29a BDSG-E stellt also eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten mit generell-abstrakter Wirkung dar, die dem Betroffenen die Kontrolle über seine Daten insoweit entzieht, als die Verarbeitung nicht an dessen explizites Einverständnis gebunden ist. § 29a regelt insoweit als speziellere Norm, was bisher den §§ 28 und 29 BDSG unterfällt. Insoweit steht die Norm in der Tradition der §§ 28a, 28b und 30a BDSG, die ebenfalls Sonderfälle der Datenverarbeitung spezialgesetzlich regeln und erst vor wenigen Monaten geschaffen wurden.

Der Umstand, dass eine generell-abstrakte Norm dem Betroffenen die individuelle Kontrolle über seine Daten entzieht und damit in der Ausübung seines Rechts auf informationelle Selbstbestimmung stark limitiert, erfordert eine kritische Auseinandersetzung mit dem Entwurf. Unzweifelhaft haben gesetzliche Erlaubnistatbestände ihre Berechtigung, auch wenn das individuelle Recht der Herrschaft über die eigenen Daten dadurch beschnitten wird. Denn der Grundannahme, dass es eine Verarbeitung von personenbezogenen Daten im Allgemeininteresse geben kann, hinsichtlich der es einen Interessenausgleich geben muss, der nur durch eine gesetzliche Regelung bewirkt werden kann, ist nichts entgegenzusetzen. Dessen ungeachtet bedeutet der Verlust individueller Einflussnahme auf Seiten des Betroffenen allerdings auch, dass eine solche **Regelung** nur dort Raum finden kann, wo sie **geeignet, erforderlich** und angemessen ist, den erstrebten **Zweck** zu erreichen, dieser also nicht durch eine weniger belastende Maßnahme zu erreichen ist.

[73] Begründung zum BDSGE-Weichert, zu Nr. 8.
[74] Weichert, a.a.O.

3.8.1 Zu Absatz 1

Die tatsächliche Kodifizierung des Erlaubnistatbestandes findet sich im prüfungsgegenständlichen Vorschlag in Absatz 1 des § 29a BDSG-E.

„Das Veröffentlichen personenbezogener Daten in Telemedien ist zulässig, wenn dies dem Zweck dient, eine Meinung frei zu äußern und zu verbreiten und kein Grund zu der Annahme besteht, dass das überwiegende schutzwürdige Interesse der Betroffene am Ausschluss der Veröffentlichung überwiegt."

3.8.1.1 Europarechtliche Zulässigkeit

Zu klären ist zunächst, inwiefern es dem nationalen Gesetzgeber überhaupt offensteht, eine entsprechende Regelung zu treffen.

Der EuGH hat in der **Lindqvist-Entscheidung**[75] festgestellt, dass die „von den Mitgliedstaaten zur Gewährleistung des Schutzes personenbezogener Daten getroffenen Maßnahmen [...] sowohl mit den Bestimmungen der Richtlinie 95/46 als auch mit deren Ziel im Einklang stehen [müssen], ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre zu wahren. Dagegen sind die Mitgliedstaaten durch nichts daran gehindert, den Geltungsbereich der die Richtlinie 95/64 umsetzenden innerstaatlichen Rechtsvorschriften auf vom Anwendungsbereich dieser Richtlinie nicht erfasste Bereiche auszudehnen, soweit dem keine andere Bestimmung des Gemeinschaftsrechts entgegensteht" (6. Tenor). Das bedeutet, dass jede nationalstaatliche Regelung, die den Umgang mit personenbezogenen Daten bestimmt, zunächst dahingehend zu untersuchen ist, ob die in den **Anwendungsbereich der Richtlinie** fällt. Ist dies der Fall, ist sodann zu prüfen, ob die nationalstaatliche Regelung mit der Richtlinie und ihren Zielen **konform** ist. Fällt sie hingegen schon gar nicht in den Anwendungsbereich der Richtlinie, ist sie jedenfalls europarechtlich zulässig.

Absatz 1 des vorgeschlagenen § 29a BDSG-E regelt die Veröffentlichung von personenbezogenen Daten. Art. 95/64/EG regelt: „Diese Richtlinie gilt für die ganz oder teilweise automatisierte **Verarbeitung** personenbezogener Daten [...]". Der Regelungsgegenstand des § 29a BDSG-E fällt also genau dann in den Anwendungsbereich der Richtlinie, wenn das Veröffentlichen von Daten eine Verarbeitung darstellt.

Der Begriff der „**Veröffentlichung**" von personenbezogenen Daten ist, wie oben unter 3.2.1 ausgeführt, nach derzeitiger Rechtslage nicht legaldefiniert. Demgegenüber ergibt sich aus Art. 2 b) 95/46/EG, dass „Verarbeiten" (u.a.) „die Weitergabe durch **Übermittlung**, **Verbreitung** oder jede andere Form der **Bereitstellung**" ist. Der EuGH führt hierzu aus: „Der Vorgang, der darin besteht, personenbezogene Daten auf eine Internetseite zu stellen, ist somit als eine solche Verarbeitung anzusehen"[76]. Insbesondere spricht das Urteil von „der Verarbeitung personenbezogener Daten, die in deren Veröffentlichung im Internet besteht"[77].

---

[75] EuGH, Urteil vom 6. November 2003, C-101/01.
[76] EuGH, a.a.O., Rn. 25.
[77] EuGH, a.a.O., Rn. 47.

Damit fällt die Regelung des **§ 29a I BDSG-E** in den Anwendungsbereich der **RL 95/46/EG**.

§ 29a I BDSG-E darf folglich keine Regelungen treffen, die mit den Regelungen der Richtlinie und ihrem Zweck, einen Ausgleich zwischen dem freien Verkehr personenbezogener Daten in der Gemeinschaft und dem Schutz der Privatsphäre des Einzelnen zu erzielen, unvereinbar sind.

Erwägungsgrund (EG) 22 der Richtlinie führt hinsichtlich **mitgliedstaatlicher Normen**, die die Zulässigkeit der Datenverarbeitung regeln, aus: „Die Mitgliedstaaten können in ihren Rechtsvorschriften oder bei der Durchführung der Vorschriften zur Umsetzung dieser Richtlinie die allgemeinen Bedingungen präzisieren, unter denen die Verarbeitungen rechtmäßig sind. Insbesondere nach Artikel 5 in Verbindung mit den Artikeln 7 und 8 können die Mitgliedstaaten neben den allgemeinen Regeln besondere Bedingungen für die Datenverarbeitung in spezifischen Bereichen und für die verschiedenen Datenkategorien gemäß Artikel 8 vorsehen".

Art. 5 RL 95/46/EG lautet: „Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die **Voraussetzungen** näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist."

§ 29a BDSG-E ist daher als Norm, die Zulässigkeit der Datenverarbeitung regelt, insbesondere an den Art. 6 bis 9 95/46/EG zu messen.

Danach könnte die Einführung einer solchen Norm zunächst wegen **Art. 9** zulässig sein. Dort heißt es „Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu **journalistischen**, **künstlerischen** oder **literarischen Zwecken** erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen".

Diese Regelung scheint auf den ersten Blick eben jenen Ausgleich zwischen Schutz der Privatsphäre und Meinungsfreiheit dem nationalen Gesetzgeber zu übertragen, den § 29a I BDSG-E bewirken soll. Tatsächlich bezieht sich die Norm allerdings **nur** auf (**redaktionell**-)**journalistische** Beiträge der Meinungsäußerung, also solche, die dem Bereich der ***Pressefreiheit*** unterliegen. Gewöhnliche Meinungsäußerungen oder gar einfache Auflistungen von Daten, wie das ULD sie in seinem Entwurf in den Regelungsbereich einbeziehen will[78], sind gerade nicht erfasst. Art. 9 der Richtlinie hat im Übrigen bereits eine Umsetzung in § 41 BDSG erfahren[79].

Eine Regelung wie die des § 29a BDSG-E könnte allerdings wegen Art. 7 f) 95/46/EG zulässig sein. In dieser Bestimmung wird festgelegt, dass die Mitgliedstaaten eine Verarbeitung erlauben können, unter der Bedingung, dass „die Verarbeitung [...] erforderlich [ist] zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen".

[78] ULD, a.a.O.

[79] Zu den Voraussetzungen an die journalistische Qualität von § 41 BDSG umfasster Äußerungen siehe: BGH, Urteil vom 23. 6. 2009 - VI ZR 196/08, NJW 2009, 2888, 2890, Rn. 20 f.

Die freie Meinungsäußerung stellt ein berechtigtes Interesse des Äußernden dar. Dieser ist, insoweit es das Hochladen von Informationen in einen selbst kontrollierten Webspace betrifft, Verantwortlicher, ansonsten - etwa bei Nutzung bestimmter Dienste – kann dieses Interesse auch durch Dritte wahrgenommen werden, denen die Daten übermittelt werden.

Weiter dürfen weder das Interesse des Betroffenen daran, dass die Daten nicht verarbeitet werden, noch dessen Grundrechte überwiegen.

§ 29a BDSG-E sieht grundsätzlich eine Interessensabwägung vor, ohne dass allerdings die zu berücksichtigenden Grundrechte explizit genannt werden. Letzterer Umstand für sich lässt die Norm in ihrem Entwurf allerdings noch nicht europarechtswidrig werden, da die Norm im Licht der Grundrechte insgesamt auszulegen ist, so dass überwiegende grundrechtliche Positionen jedenfalls auch ein überwiegendes Interesse am Ausschluss der Veröffentlichung, wie es § 29a BDSG-E benennt, begründen.

Sodann stellt § 29a BDSG-E eine Vermutung dahingehend auf, dass die Verarbeitung zulässig ist, indem er die Tatsache, dass lediglich keine Gründe für die Annahme eine überwiegenden Interesses bestehen, ausreichen lässt. Damit ist nicht klar, ob durch die Regelung eine tatsächliche Interessensabwägung geboten ist oder nicht, es scheint nach dem Wortlaut der Norm ausreichend, wenn nicht ersichtlich ist, dass eine solche zugunsten des Betroffenen ausgehen könnte. Die europarechtliche Konformität erscheint daher unter Bedachtnahme auf EG 22 und Art. 7f 95/46/EG zumindest zweifelhaft[80].

3.8.1.2 Verhältnismäßigkeit der Norm

Ungeachtet der europarechtlichen Problematik muss sich § 29a BDSG-E, indem er in das Grundrecht des Betroffenen auf **informationelle Selbstbestimmung** eingreift, auch am **Grundsatz der Verhältnismäßigkeit** messen lassen. Verhältnismäßig ist die Regelung, wenn sie zur Erreichung des mit ihr erstrebten Zwecks geeignet, erforderlich und angemessen ist.

3.8.1.2.1 Zweck des § 29a BDSG-E

Um diese Frage zu klären, ist zunächst der Zweck des § 29a I BDSG zu bestimmten. Der **Wortlaut** lässt allerdings insoweit **keine Rückschlüsse** darüber zu, zu welchem Zweck die Veröffentlichung personenbezogener Daten *im Einzelnen* zulässig sein soll. Vielmehr wird lediglich allge-

[80] Die Regelung des § 29a BDSG-E erscheint nämlich insoweit weiter, als es der Ausnahmetatbestand des Art. 7 f) vorsieht, welcher eine tatsächliche Interessenabwägung gebietet, als in ersterem nur keine Gründe zur Annahme, dass eine solche Interessenabwägung zu Gunsten des Betroffen ausgehen könnte, vorliegen dürfen. Damit können solche Gründe bestehen, der Stelle aber nicht bekannt sein. Eine Nachforschung muss nicht erfolgen. Dieselbe Formulierung findet sich allerdings auch in § 28 I 1 Nr. 2 BDSG. Zwar sieht § 29a III BDSG-E ein Widerspruchsrecht vor, wie es Art. 14 I 95/46/EG für Fälle des Art. 7 f) bestimmt, allerdings ändert das nichts an dem genannten Umstand, dass die Richtlinie eine vermutete Zulässigkeit nicht kennt. Art. 14 selbst lässt sich nämlich gerade nicht entnehmen, dass das Widerspruchsrecht im Falle einer fälschlich vermuteten Zulässigkeit der Verarbeitung bestehen soll, sondern – wenn man die Norm in direktem Zusammenhang mit Art. 7 f) liest – in dem Fall, dass sich die Umstände des Betroffenen ändern.

meinen darauf verwiesen, dass die Veröffentlichung der **freien Äußerung** und **Verbreitung einer Meinung** dient.

Damit allein ist allerdings wenig an Erkenntnis gewonnen, denn innerhalb dieser Meinungsäußerungen können je nach **Zweck der Meinungsäußerung** – die ja im Allgemeinen gerade keinen reinen Selbstzweck aufweisen wird – wiederum völlig **unterschiedliche Bewertungen** geboten sein. Insoweit sei an dieser Stelle auf die beiden vertrauten juristischen Schlagworte „Berichterstattung über Personen des öffentlichen Lebens" und „Schmähkritik" als gegensätzliche *Extrema* verwiesen, die das Spektrum möglicher Intentionen bei der Meinungsäußerung veranschaulichen dürften. Je nach dem unterscheidet sich das Allgemeininteresse an Veröffentlichung, das wiederum in Relation zu setzen ist mit dem Schutzinteresse des Individuums. Daran zeigt sich, dass ein allgemeiner Zweck, einen Ausgleich zwischen Meinungsfreiheit und Schutz personenbezogener Daten zu schaffen, als Wertmaßstab kaum geeignet ist, die Geeignetheit und Erforderlichkeit einer entsprechenden Norm zu überprüfen. Vielmehr wird es darauf ankommen, welchen Zwecken die Meinungsäußerung ihrerseits dient. Diese vorgelagerte Problematik des aus den verschiedenen Zwecken der Meinungsäußerung resultierenden, völlig unterschiedlichen Allgemeininteresses an Veröffentlichungen von bestimmten Meinungen, versucht die Norm nachgeschaltet dadurch zu lösen, dass eine **Interessenabwägung** geboten wird. Diese Interessenabwägung wird allerdings in die Sphäre der verarbeitenden Stelle verlagert, zudem ist es nach dem Entwurf auch ausreichend, dass „**kein Grund zu der Annahme**" eines überwiegenden Interesses des Betroffenen besteht. Damit wird die eigentliche Abwägung durch eine Vermutungsregelung ersetzt, die insoweit in praxi einen Abwägungsausfall bewirken dürfte.

Auch an dieser Stelle ist im Übrigen keine Erkenntnis darüber zu gewinnen, zu welchen Zwecken genau die Veröffentlichung generell-abstrakt zulässig sein soll.

Vor allem fällt aber auf, dass die Norm Tatsachenmitteilungen und das damit verbundene Grundrecht auf Informationsfreiheit, das Art. 5 I GG neben der Meinungsfreiheit als solcher kennt, überhaupt nicht berücksichtigt. Zwar ist die Informationsfreiheit gerade Voraussetzung für die Meinungsfreiheit und hat deshalb für den Diskurs einer demokratischen Öffentlichkeit vergleichbare Bedeutung[81], es handelt sich jedoch um ein eigenständiges Grundrecht mit einem eigenen Schutzbereich[82]. Damit ist der Schutz der Informationsfreiheit nach dem insoweit eindeutigen Wortlaut des § 29a BDSG-E nicht Zweck der Norm[83].

Für das ULD selbst scheint der Zweck des von ihm vorgeschlagenen Erlaubnistatbestandes auch nicht bis in letzter Konsequenz ausdifferenziert. Zunächst verweist er auf die Tatsache, dass die Veröffentlichung von personenbezogenen Daten zum Zweck der Meinungsäußerung im Lichte des Art. 5 GG verfassungsrechtlich legitimiert sein kann.[84] Dies ist kaum zu bestreiten, gleichzeitig scheint es aber nicht nur um den Fall der individuellen Meinungsäußerung zu gehen, sondern

[81] BVerfG, Urteil v. 3. 10. 1969, BVerfGE 27, 71, 83 ff.
[82] Dietrich/Schmidt, Erfurter Kommentar zum Arbeitsrecht, Art. 5 GG, Rn. 13.
[83] A.A. offenbar ULD, a.a.O., wenn Suchmaschinen und Straßenansichten von der Regelung erfasst sein sollen, die ganz offensichtlich nicht geeignet sind, Meinungen kundzutun.
[84] Weichert, a.a.O.

auch um Datenauflistungen, die wie individuelle Medienbeiträge der öffentlichen Meinungsbildung dienen, aber mangels individuell-redaktioneller Gestaltung nicht unter das Privileg des § 41 BDSG fallen.[85] Dann wieder heißt es: „Dienste wie Suchmaschinen, auch Personensuchmaschinen, oder Internet-Straßenansichten unterfallen der neuen Regelung des § 29a."[86]

Wenn nun also „Suchmaschinen" bzw. Internetstraßenansichten erfasst sein sollen, dann können diese eigentlich nur noch in der Weise der Äußerung oder Verbreitung einer Meinung dienen, als diese als Informationsquellen herangezogen werden und daher der Meinungsbildung im Vorfeld der Meinungsäußerung zumindest dienlich sind. Dies ist dann aber, wie soeben dargestellt, gerade kein Fall des Grundrechts auf freie Meinungsäußerung, sondern fällt in den originären Schutzbereich des Grundrechts auf Informationsfreiheit, das nach dem klaren Wortlaut des § 29a BDSG-E gerade nicht erfasst ist. § 29a BDSG-E ist damit, entgegen der in der Begründung geäußerten Ansicht, gerade *nicht* auf Suchmaschinen, Straßendarstellungen und Geodaten – soweit überhaupt personenbezogen - anwendbar.

Es bleibt festzuhalten, dass sich der Zweck der Regelung nicht bis ins letzte Detail bestimmen lässt. Wenn also die Frage zu klären ist, ob die vorgeschlagene Regelung als Erlaubnistatbestand einen Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen generell-abstrakt ermöglichen darf, weil sie zu Erreichung des bestrebten Zwecks erforderlich, geboten und angemessen ist, dieser Zweck aber aus Norm und Begründung nicht ohne weiteres im Einzelnen ersichtlich bzw. widersprüchlich ist, lässt schon dies Zweifel an deren Verhältnismäßigkeit aufkeimen.

3.8.1.2.2 Geeignetheit des § 29a BDSG-E, die freie Meinungsäußerung zu fördern

Geht es also nur allgemein um einen Ausgleich zwischen dem Grundrecht auf freie Meinungsäußerung und dem allgemeinen Persönlichkeitsrecht, so erscheint bereits deren **Geeignetheit** zur Erreichung diesen Zwecks fraglich, weil die Regelung hierfür keine Rahmenbedingungen aufstellt. Die für die Interessenabwägung wesentliche Frage des Zwecks der Meinungsäußerung (Berichterstattung, Schmähkritik, etc.) bleibt unberücksichtigt, ist aber entscheidend für die Frage, wann ein entsprechendes Allgemeininteresse besteht. Dazu kommt, dass allein das Fehlen eines Grundes zur Annahme eines überwiegenden Interesses des Betroffenen ausreichend sein soll, die Veröffentlichung zunächst als zulässig anzusehen. Dies lässt entsprechende Irrtümer zu – nämlich dann, wenn solche (berechtigten) Interessen des Betroffenen tatsächlich bestehen, es aber zunächst auf Seiten der verarbeitenden Stelle keinen Grund gibt, sie anzunehmen. Gleichzeitig vermutet die Norm das Nicht-Bestehen solcher Interessen, wie sich aus der Negation in der Formulierung („wenn [...] kein Grund zu der Annahme besteht") ergibt.

Dies ist wohl auch durchaus gewollt, denn daraus ergibt sich die vermutete Zulässigkeit der Veröffentlichung, welcher der Betroffene dann im Nachhinein mit dem Instrumentarium des Absatzes 3 entgegentreten kann, wodurch der Betroffene durch Widerspruch die Darlegungspflicht eines überwiegenden Interesses an der Veröffentlichung auf die verarbeitende Stelle überträgt.

[85] A.a.O.
[86] A.a.O.

Damit sind die Daten dann aber noch lange nicht wieder aus dem Internet gelöscht. Im Gegenteil erscheint die Regelung zwar pragmatisch, dies allerdings ausschließlich auf Kosten des Betroffenen. Denn dieser muss von der Rechtsverletzung zunächst erfahren, sich dann erfolgreich dagegen wehren und hat dann immer noch keine Sicherheit, dass es keine Kopien der Daten irgendwo gibt (ganz zu schweigen von dem Umstand, dass es keinen Anspruch auf „menschliches Vergessen" gibt, diejenigen, denen die Daten bekannt geworden sind, also von diesem Wissen profitieren oder neue Daten gleichen Inhalts erstellen können).

All dies lässt Zweifel aufkommen, was die Geeignetheit der Regelung angeht, dem bekundeten Zweck zu dienen, gerade einen Ausgleich zwischen Veröffentlichungsinteresse und Schutzinteresse des Betroffenen zu erreichen.

3.8.1.2.3 Erforderlichkeit der Einführung des § 29a BDSG

Selbst wenn man die Regelung als geeignet sehen wollen würde, einen solchen Ausgleich herbeizuführen, wäre aber an der **Erforderlichkeit** zu zweifeln. Denn zumindest der Wortlaut der Regelung gibt nicht mehr her, als sich aus den ihr zugrundeliegenden Grundrechten und deren dogmatischer Verankerung bei einfachrechtlicher Auslegung sowieso ergibt. Die Rechte aus Artikel 5 GG kollidieren vielfach mit dem allgemeinen Persönlichkeitsrecht desjenigen, auf den sich eine Meinungsäußerung bezieht. Dieser Konflikt ist im Rahmen der einfachen Rechtsauslegung ohnehin zu lösen. Wenn also etwa eine Meinung über eine natürliche Person in einem Forum publiziert wird, ist hinsichtlich der Frage der Zulässigkeit einer solchen Äußerung ebenfalls nach bestehender Gesetzeslage eine Interessenabwägung vorzunehmen. Dies hat der BGH beispielsweise hinsichtlich des § 29 BDSG im Rahmen des sog. „Spick-mich"-Urteils getan[87].

Anders wäre es, wenn, wie eingangs dargestellt, die neue Regelung **Fallgruppen** kennte, welche als Anhaltspunkte herangezogen werden könnten. In einem solche Fall würde hierdurch eine gesetzgeberische Wertung erreicht, die der Rechtsanwendung insoweit dienlich wäre, als einerseits **häufige Konstellation geregelt** wären und diese damit in der Praxis stets gleich behandelt würden, und andererseits **neue Konstellationen** auf **Wertmaßstäbe** treffen würden, welche zu deren Beurteilung herangezogen werden könnten. Der Gesetzgeber würde also die Interessenabwägung insoweit objektiviert vorwegnehmen und könnte damit in diesem Fall tatsächlich zu einem gerechten Ausgleich zwischen Veröffentlichungsinteressen und Schutzinteresse des Einzelnen beitragen. Letztlich erlaubte eine geschickte Gestaltung der Fallgruppen zudem eine **Abstufung**, die angemessen auf die eingangs angedeuteten unterschiedlich hohen Veröffentlichungsinteressen der Allgemeinheit abzustimmen wäre. Damit könnte insoweit tatsächlich ein besserer Ausgleich zwischen den widerstreitenden Rechten aus den Art. 5 GG und Art. 2 I i.V.m. 1 I GG erzielt werden.

Dem vorliegenden Regelungsvorschlag des § 29a I BDSG-E hingegen wird man dies nicht attestieren können. Die Regelung erscheint damit als Neueinfügung nicht geboten.

[87] BGH, Urteil vom 23. 6. 2009 - VI ZR 196/08, NJW 2009, 2888, 2891, Rn. 26 ff.

3.8.1.3 Grundrecht auf Informationsfreiheit

Neben der im vorigen Abschnitt behandelten Abwägung des Grundrechts auf informationelle Selbstbestimmung und desjenigen auf freie Meinungsäußerung, steht § 29a BDSG-E ebenfalls innerhalb des Spannungsfeldes zwischen dem Grundrecht auf Informationsfreiheit und demjenigen auf informationelle Selbstbestimmung. Wie schon im vorigen Abschnitt festgestellt, berücksichtigt die Norm das Grundrecht auf Informationsfreiheit überhaupt nicht, da der klare Wortlaut nur die Meinungsäußerung erfasst.

Während im vorigen Abschnitt festgestellt wurde, dass die Norm kein ausgewogenes Verhältnis zwischen Meinungsfreiheit und informationeller Selbstbestimmung erzielt, weil stets vermutet wird, dass die Meinungsfreiheit überwiege hinsichtlich aller Daten (die nicht unter § 3 IX BDSG fallen) in allen Situationen und insoweit ein zu niedriges Datenschutzniveau anstrebt, verhält es sich hinsichtlich des Grundrechts auf Informationsfreiheit gerade anders herum.

Die anderen Erlaubnistatbestände des BDSG für die Datenverarbeitung, die nicht für die Sonderfälle des Übermitteln von Daten an Auskunfteien und des Scorings gelten, kennen stets einen Erlaubnistatbestand für die Verarbeitung von Daten aus öffentlich zugänglichen Quellen (§ 28 I Nr. 3 BDSG, § 28 VI Nr. 2 BDSG, § 29 I Nr. 2 BDSG, § 30 II Nr. 2 BDSG, § 30a I Nr. 2 BDSG). Damit wird ein angemessener Ausgleich zwischen informationeller Selbstbestimmung und Informationsfreiheit erzielt.

§ 29a BDSG-E kennt einen solchen Erlaubnistatbestand hingegen nicht. Vielmehr wird lediglich umgekehrt negativ festgestellt, dass das Veröffentlichen von Daten aus allgemein zugänglichen Quellen unzulässig ist, wenn der Betroffene einen entsprechenden Willen erkennbar gemacht hat. Abgesehen davon, dass insoweit an Absatz 5 Zweifel bestehen müssen hinsichtlich seiner Verfassungskonformität, fehlt es jedenfalls an einem positiven Erlaubnistatbestand für das (ggf. sonstige) Verarbeiten von personenbezogenen Daten aus allgemein zugänglichen Quellen. So könnte man § 29a I BDSG-E dergestalt lesen, dass es auf die Frage der Quelle hinsichtlich der Veröffentlichungserlaubnis nicht ankommt.

Allerdings gebietet die Grundrechtsabwägung jedenfalls eine Interessenabwägung, die auch die anderen Erlaubnistatbestände des BDSG für Daten aus allgemein zugänglichen Quellen kennen. Insofern unterscheidet sich § 29a BDSG-E zunächst grundsätzlich im Ergebnis was die Interessenabwägung angeht nicht von dem Ergebnis, das erzielt würde, wenn man den Wortlaut beispielsweise des § 29 I Nr. 2 BDSG übernähme, denn die Voraussetzungen für die Veröffentlichung wären dann nicht geringer. Allerdings balancieren die anderen Erlaubnistatbestände die Interessenabwägung anders aus: bei diesen muss bei allgemein zugänglichen Daten stets das Interesse des Betroffenen *offensichtlich* überwiegen, damit die Verarbeitung unzulässig wird. So lässt sich ein gerechter Ausgleich zwischen den widerstreitenden Grundrechten erzielen, da das Recht auf informationelle Selbstbestimmung bei (zulässigerweise) frei zugänglichen Daten ohnehin ein geringeres Gewicht hat, also insoweit das Gefahrenpotential geringer ist.

Indem § 29a BDSG-E kein offensichtliches Überwiegen der Interessen des Betroffenen für die „Veröffentlichung" von allgemein zugänglichen Daten voraussetzt, verkennt er die Bedeutung des Grundrechts auf Informationsfreiheit und ist insoweit nicht verfassungskonform. Daran ändert auch die Tatsache nichts, dass bereits allgemein zugängliche Daten als solche nicht (erneut) veröffentlicht werden können und man daher erwägen könnte, dass deren Bereitstellung im

Internet tatbestandlich schon gar nicht erfasst sei. Denn aus Absatz 5 ergibt sich klar, dass – trotz einer gewissen begrifflichen Widersprüchlichkeit – auch die „Veröffentlichung" von veröffentlichten Daten gemeint sein soll.

Die Regelung ist daher insgesamt abzulehnen, da ihre Konformität mit der Datenschutzrichtlinie, in deren Anwendungsbereich sie fällt, zweifelhaft ist und die Regelung verfassungswidrig ist, weil sie das Recht auf Informationsfreiheit nicht in angemessenem Maß berücksichtigt. Sie ist auch verfassungswidrig, weil sie das Recht auf informationeller Selbstbestimmung im ungeeigneter, jedenfalls aber in nicht erforderlicher Weise einschränkt. Die Auswirkungen auf die Geoinformationsbranche wären hoch, würde am mit dem ULD Tatsachenmitteilungen wie Geodaten von der Norm erfasst sehen. Tatsächlich sind diese allerdings nach dem klaren Wortlaut der Norm nicht erfasst, eine andere Auslegung ist aufgrund der Wortlautgrenze unzulässig. Eine Einbeziehung von Tatsachenmitteilungen in den Anwendungsbereich wäre dann nur contra legem im Wege der Analogie möglich, wobei es jedoch vermutlich schon an einer Regelungslücke, erst recht aber an deren Planwidrigkeit mangeln würde.

3.8.2 Absatz 2

„Ein schutzwürdiges Interesse besteht bei besonderen Arten personenbezogener Daten nach § 3 Abs. 9, wenn nicht im Einzelfall das Interesse an der Veröffentlichung offensichtlich überwiegt."

Absatz 2 der vorgeschlagenen Regelung soll vorschreiben, dass hinsichtlich **besonders schutzwürdiger Daten** im Sinne des § 3 IX BDSG (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben), die **Frage der Zulässigkeit der Veröffentlichung** – anders als im Regelfall des Absatzes 1 des Entwurfs – sofort **zugunsten des Betroffenen** vermutet werden soll. Dies ist im Grundsatz zu begrüßen, vielfach wird eine entsprechende Regelung auch im Lichte der hiermit verbundenen verschiedenen Grundrechte geboten sein.

Eine Ausnahme soll bestehen, wenn das **Veröffentlichungsinteresse „offensichtlich" überwiegt**. Dies ist insoweit kritisch, als an einer entscheidenden Stelle ein unbestimmter Rechtsbegriff darüber entscheidet, ob beispielsweise Informationen über sexuelle Neigungen einer Person im Internet veröffentlich werden dürfen oder nicht. Wann genau das allgemeine Interesse an solchen Informationen das Schutzinteresse des Einzelnen offensichtlich überwiegt, wird sich schwer ausmachen lassen. Unabhängig davon ist die Regelung an Art. 8 95/46/EG zu messen. Danach ist die Verarbeitung solcher Daten durch die Mitgliedstaaten grundsätzlich zu verbieten. Die in Absatz 2 genannten Ausnahmen lassen eine anderweitige Regelung nicht zu. Allerdings können gem. Absatz 4 auch sonstige Ausnahmeregelugen durch die Mitgliedstaaten getroffen werden, wenn dies aus wichtigem öffentlichen Interesse vorbehaltlich angemessener Garantieren erfolgt. § 29a II BDSG-E kennt derartige Garantien allerdings nicht.

Die Regelung ist insoweit bedenklich, als die von Art. 8 95/46/EG verlangten Garantien unklar bleiben. Auswirkungen auf die Geoinformationswirtschaft sind nicht zu erwarten.

3.8.3 Zu Absatz 3

Absatz 3 stellt eine Ausgleichsregelung zur vermuteten Zulässigkeit der Veröffentlichung nach Absatz 1 dar.

„Ein schutzwürdiges Interesse besteht, wenn der Betroffene gegenüber der verantwortlichen Stelle widerspricht, es sei denn, die verantwortliche Stelle legt dem Betroffenen gegenüber das überwiegende Interesse an einer Veröffentlichung dar. Die Darlegung nach Satz 1 kann in der Form des vom Betroffenen erklärten Widerspruchs oder schriftlich erfolgen."

Damit ist die Veröffentlichung solange zulässig, bis der Betroffene **widerspricht**. Ab diesem Punkt muss die **verarbeitende Stelle** darlegen, dass tatsächlich ein überwiegendes **Interesse an Veröffentlichung** besteht.

Die Regelung versucht einen Ausgleich zu finden zwischen dem Umstand, dass häufig der Betroffene der verarbeitenden Stelle im Internet gar nicht bekannt ist, und der Tatsache, dass er auf den Umgang mit seinen Daten reagieren können muss.

Der Gedanke ist an sich begrüßenswert, denn generell ist angesichts der extrem hohen Zahl an Verarbeitungen personenbezogener Daten im Internet, die jedoch **vielfach marginale Informationen** betreffen, gegen deren Verarbeitung viele Betroffenen gar nichts einzuwenden haben, eine Zulässigkeitsvermutung ein guter Weg, entsprechende Services überhaupt zu ermöglichen, ohne dabei allzu stark in die Rechte der Betroffenen einzugreifen. Die **Erlaubnisvermutung mit Widerspruchsrecht** ist letztlich ein Modell, das Google bei **StreetView** – ungeachtet der Frage, ob dort überhaupt personenbezogene Daten verarbeitet werden und ungeachtet einer bestehenden oder nicht bestehenden rechtlichen Verpflichtung hierzu – eingeführt hat.

Die **Problematik** dieses Modells an dieser Stelle ist wiederum die **generell-abstrakte Regelung** insoweit, als dass es auch jenseits der sensiblen Daten im Sinne des § 3 IV BDSG Daten geben wird, deren Veröffentlichungsinteresse im Allgemeinen nicht ohne weiteres als überwiegend vermutet werden kann – etwa Informationen über die berufliche Qualifikation wie Arbeitszeugnisse. Dem kann zwar grundsätzlich wiederum mit der Regelung des Absatz 1 begegnet werden, wonach die verarbeitende Stelle sich zu fragen hat, ob Gründe für ein Interesse des Betroffenen an der Nicht-Veröffentlichung bestehen, dies kann im Einzelfall aber ohne weiteres zuungunsten des Betroffenen durch diese Stelle entschieden werden.

Eine endgültige Entscheidung erfolgt dann erst nach dessen Aufmerksamwerden und Widerspruch. Zu diesem Zeitpunkt sind die Daten dann allerdings bereits im Netz veröffentlicht und damit kaum wieder zu entfernen, weil sie unter Umständen bereits verbreitet wurden und nicht mehr ohne weiteres nachvollziehbar ist, wer alles beispielsweise Kopien gespeichert oder gespiegelt hat. Ein Beispiel mögen private Aufnahmen von Prominenten sein, die – einmal online gestellt – kaum wieder aus dem Netz zu entfernen sind.

Eine Alternative zur vorgeschlagenen Regelung wäre möglicherweise, spiegelbildlich zu § 3 IX BDSG **Kategorien von Daten** zu bilden, für die die **Vermutung des überwiegenden Veröffentlichungsinteresses** aufrecht zu halten wäre. Dies müssten Datenkategorien sein, hinsichtlich derer generell-abstrakt ein geringer Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kategorisch vermutet werden kann, während gleichzeitig ein hohes Veröffentlichungsinteresse besteht. Würde man Luftbilder als (eventuell) personenbezogene Daten interpretieren wollen, dann wären derartige Daten ein Beispiel für eine solche Kategorie. Die Kategorisierung hätte den Vorteil, einer Positivbestimmung der Daten, für die ein überwiegendes Veröffentlichungsinteresse vermutet würde, so dass die Negativdefinition (alle personenbezogenen Daten, die nicht unter

§ 3 IX BDSG fallen) mit den aufgezeigten Gefahren der Gleichbehandlung von Ungleichem entfiele. Insoweit könnte ein besserer Ausgleich zwischen den widerstreitenden Interessen und gleichzeitig in erhöhte Rechtssicherheit geschaffen werden.

Die Regelung ist, wenn man die Grundregelung des Absatzes 1 entgegen hier vertretener Ansicht für zulässig erachtet oder sie durch eine zulässige Regelung ersetzte, grundsätzlich sinnvoll und insoweit zu begrüßen. Auswirkungen auf die Geoinformationswirtschaft sind insoweit zu erwarten, als Geodaten veröffentlich werden. Hier wäre die Veröffentlichung zunächst zulässig, bis der Betroffene widerspricht.

3.8.4 Zu Absatz IV

„Betroffene können ihre Datenschutzrechte gegenüber dem verantwortlichen Telemedien-Diensteanbieter elektronisch an die nach § 5 Absatz 1 Nr. 2 Telemediengesetz zu nennende Stelle richten. Wird die Beschwerde nicht unverzüglich beantwortet, so verletzt die weitere Veröffentlichung schutzwürdige Betroffeneninteressen. Kann die verantwortliche Stelle nicht die Richtigkeit der Daten nachweisen, so tritt neben die Löschungs- und Sperransprüche nach § 35 ein Anspruch auf Hinzufügung einer eigenen Darstellung von angemessenem Umfang. § 57 Abs. 3 Rundfunkstaatsvertrag zu Gegendarstellungen ist sinngemäß anzuwenden."

Absatz IV enthält zunächst eine Regelung, die wegen Unklarheit problematisch in Bezug auf den **Bestimmtheitsgrundsatz** ist. So heißt es dort in Satz 1: "Betroffene können ihre Datenschutzrechte gegenüber dem verantwortlichen Telemedien-Diensteanbieter elektronisch an die nach § 5 Absatz 1 Nr. 2 Telemediengesetz zu nennende Stelle richten". Was darunter zu verstehen ist, dass man Rechte „gegenüber jemand" „an eine Stelle" „richtet" bleibt unklar. Aus Satz 2 ergibt sich, dass wohl Beschwerden über Rechtsverletzungen gemeint sein müssen. Danach können diese gegenüber dem **Telemediendiensteanbieter** geltend gemacht werden und erfordern von diesem eine **unverzügliche Reaktion**.

Dies ist ein interessantes Modell. Wenn sich entgegen der soeben vorgebrachten Kritik eine Regelung finden lässt, aufgrund derer ***bestimmte* Datenarten** tatsächlich aufgrund vermuteten Rechts zur Veröffentlichung unproblematisch publizieren lassen, so erscheint es sinnvoll, wider Erwarten dennoch bestehende Beschwerden der Betroffenen hiergegen über den Telemediensteanbieter abzuwickeln und von diesem auch ein unverzügliches Handeln einzufordern. Der in der Begründung angegebene Umstand, „elektronische Informationsanbieter müssen personell, technisch und organisatorisch gewährleisten, dass sie grds. in der Lage sind, die Betroffenenbegehren derart zeitnah zu bearbeiten" erscheint ein probates Mittel, Datenschutz in der Praxis zu erhöhen, ohne demgegenüber Services so zu bürokratisieren, dass sie praktisch undenkbar werden (etwa durch zwingende Vorabanfragen bei den Betroffenen).

Insbesondere regelt Absatz 4 in Folge der Regelung des Absatz 3 die Konstellation, dass nach erfolgtem Widerspruch des Betroffenen die verarbeitende Stelle die **Richtigkeit der Daten** nicht **nachweisen** kann. Für diesen Fall soll zu den bestehenden Betroffenenrechten ein **Gegendarstellungsrecht** hinzutreten. Inwiefern dieses neben einem Löschungsrecht eine praktische Relevanz hat, erscheint nicht ohne weiteres klar, denn auch eine Gegendarstellung trägt ein Stück weit zur Perpetuierung bei. Wenn allerdings die Veröffentlichung der (vermeintlich) falschen Darstellung an einer sehr prominenten Stelle erfolgt ist, dennoch aber die presserechtlichen Gegendars-

tellungsrechte nicht greifen, weil es sich nicht um eine Veröffentlichung in der Presse handelt, kann jenseits neben der einfachen Löschung der (falschen) Daten auch ein zusätzlicher Gegendarstellungsanspruch sinnvoll sein.

Die Regelung ist, wenn man die Grundregelung des Absatzes 1 entgegen hier vertretener Ansicht für zulässig erachtet oder sie durch eine zulässige Regelung ersetzte, grundsätzlich sinnvoll und insoweit zu begrüßen. Auswirkungen auf die Geoinformationswirtschaft sind nur in geringem Maße zu erwarten.

3.8.5 Zu Absatz V

Absatz V sieht vor, dass auch aus **allgemein zugänglichen Quellen** verfügbare Daten **nicht veröffentlicht** werden dürfen.

„Die Veröffentlichung von personenbezogenen Daten aus allgemein zugänglichen Quellen hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dieser Quelle oder auf andere Weise eindeutig erkennbar ist. Der Empfänger von veröffentlichten Daten hat sicherzustellen, dass Kennzeichnungen bei der Übernahme übernommen werden."

Diese Regelung erscheint zunächst widersinnig, weil eine Veröffentlichung in diesem Fall eigentlich bereits erfolgt ist. Es geht also um die weitere bzw. anderweitige Veröffentlichung solcher Daten. Der Vorschlag wird verständlicher, wenn man die Begründung hierzu betrachtet, in der es heißt:

„Die Regelung ist z. B. auch auf Straßenansichten anwendbar: Ist der einer Veröffentlichung entgegen stehende Wille aus der Informationsquelle oder anderweitig eindeutig erkennbar, so muss dieser berücksichtigt werden". Es geht hierbei also insbesondere um die Widerspruchsschilder an Grundstücken.

Die Regelung ist schon deswegen problematisch, weil sich nicht einsehen lässt, warum Daten, die an anderer Stelle (rechtmäßig) öffentlich sind, dies hinsichtlich einer bestimmten verarbeitenden Stelle nicht sein sollten. Insofern würde es hier innerhalb der Regelung erheblicher Einschränkungen bedürfen. Insbesondere verkennt die Regelung den Bedeutungsgehalt des Grundrechts auf Informationsfreiheit (s.o.). Schon deshalb ist Absatz 5 abzulehnen. Im übrigen ist die Regelung deshalb widersprüchlich, weil sie – zumindest bei Auslegung anhand der Materialien – Tatsachenmitteilungen betreffen soll, nach dem klaren Wortlaut des Absatzes 1 aber ausschließlich Meinungsäußerungen erfasst sind. Die genannten Straßenansichten sind somit gerade nicht Gegenstand der Regelung.

Die Regelung ist mangels Verfassungskonformität abzulehnen, da sie das Grundrecht auf Informationsfreiheit nicht angemessen berücksichtigt. Sie ist zudem widersprüchlich. Auswirkungen auf die Geoinformationswirtschaft sind hoch, wenn man Geodaten von dieser Regelung mit dem ULD erfasst sehen wollen würde. Tatsächlich sind die nach dem klaren Wortlaut der Norm nicht erfasst, so dass eine andere Auslegung nicht zulässig ist (Überschreitung der Wortlautgrenze).

3.8.6 Zu Absatz VI

Absatz VI sieht vor, dass bei einer großen Zahl Betroffener die Benachrichtigung nicht mehr individuell nach § 33 BDSG erfolgt, sondern zentral über eine Webseite beim Bundesdaten-

schutzbeauftragten. Sie lautet: „Beabsichtigt ein Telemedien-Diensteanbieter die Veröffentlichung von personenbezogenen Daten zu mehr als 1000 oder von einer unbestimmten Zahl von Personen, so hat er dies auf einer beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingerichteten Internetseite vorher unter Nennung der Datenart und der Quelle bekanntzugeben."

Die Regelung erscheint im Grundsatz als eine sinnvolle Vereinfachung, ist doch die Veröffentlichung von Informationen, die der Transparenz und Kontrolle dienen sollen und sich an eine unbestimmte Zahl von Empfängern richten, an einer zentralen, prominenten Stelle, eine im Bereich anderer Publizitätspflichten, etwa hinsichtlich der Pflichten nach § 325 HGB, bewährte Regelung. Jedoch fehlen Klarstellungen dahingehend, wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Übermittlung der Daten an ihn möglichst bürokratiearm zu gestalten hat – insbesondere, ob und wie hier elektronische Mittel eingesetzt werden können. Auch ist § 29a Abs. 6 nicht die Verpflichtung zu entnehmen, Kontaktdaten der verarbeitenden Stelle vorzuhalten, sodass der Betroffene diese erst recht wieder mühsam suchen müssen würde. Und schließlich sind die Wertungsgesichtspunkte, die eine Bekanntgabepflicht erst ab 1000 Personen begründet erscheinen lassen, zu hinterfragen, lässt sich doch aus der Quantität allein eine Beurteilung der Eingriffsqualität nicht bestimmen.

Die Regelung ist im Ansatz verständlich, jedoch im Detail weiter zu diskutieren. Auswirkungen auf die Geoinformationswirtschaft sind zu erwarten, da hier spürbare Bürokratiekosten entstehen können.

3.8.7 Zu Absatz VII

„Verantwortliche Stellen, die personenbezogene Daten veröffentlichen, können diese mit einem Löschdatum versehen. Werden diese Daten von einer anderen verantwortlichen Stelle übernommen, so ist bei der weiteren Veröffentlichung und der sonstigen Verarbeitung das jeweilige Löschdatum zu berücksichtigen."

Absatz VII zieht schließlich die Möglichkeit der Verwendung eines **Löschdatums** vor, die den Bestand eines Datums zumindest theoretisch zeitlich limitiert, nämlich dann, wenn dieses Datum nur in Systemen verarbeitet wird, die zum gegebenen Zeitpunkt eine Löschung tatsächlich vornehmen und sonst keine weiteren Kopien bestehen.

Die Idee eines digitalen Verfallsdatums hat interessante Aspekte, was dem Versuch angeht, dass Daten aus der Öffentlichkeit des Internets quasi nicht wieder zu entfernen sind. Sie wird allerdings letztlich zumindest nicht an dieser Stelle von normativen Gegebenheiten abhängen, die Verbreitung solcher Systeme also nicht durch Einführung der Option, solche „Verfallsdaten" zu Daten hinzuzufügen, beschleunigt werden. Vielmehr sind vorgelagert die **technischen Rahmenbedingungen entscheidend** dafür, wie effektiv ein solches Vorgehen ist. Diese können zwar im Sinne des „Systemdatenschutzes" bzw. des Prinzips von „privacy by design" entsprechend durch gesetzliche Regelungen bestimmt werden, dies wäre dann aber auch der Ansatzpunkt, an dem ein normatives Eingreifen effizient wäre. Abgesehen davon bräuchte es hierfür wohl einer europäischen Initiative.

Die schlichte Option, solche Verfallsdaten zu Daten zu speichern, wie sie im Entwurf vorgesehen ist, würde für sich genommen wenig bewirken, da weder sichergestellt wäre, dass die Option

genutzt wird, noch dass die Daten nur auf Systeme gelangen, die entsprechende Löschmaßnahmen automatisch durchführen. Effektiv könnte das gewünschte Ergebnis nur dann erzielt werden, wenn (zumindest europaweit) vorgeschrieben wäre, dass Betriebssysteme Daten bei Erreichen deren Löschdatums zu löschen haben. Selbst dann wäre allerdings zu bezweifeln, ob ein solcher Umstand wünschenswert ist. Zum einen können Daten ab einem gewissen Alter auch einen archivarischen Wert haben, selbst wenn sie sich auf Triviales beziehen. Zum anderen widerspricht die Idee dem Grundsatz der Datensicherheit, die gerade den Bestand von Daten garantieren sollen. Insbesondere kann eine solche Funktion Sicherheitslecks schaffen, weil sich entsprechende Attribute manipulieren lassen.

Die Regelung stellt einen grundsätzlich richtigen Ansatz dar, die Beständigkeit von Daten zu überdenken. Sie dürfte in der Praxis allerdings ungeeignet sein, die gewünschten Veränderungen zu bewirken. Daneben bedenkt die Regelung Aspekte der Informationssicherheit nicht, so wie den Umstand, dass es archivarisches Interesse an bestimmten Daten lange nach ihrer Verwendung geben kann. Auswirkungen auf die Geoinformationswirtschaft sind eher nicht zu erwarten.

3.8.8 Ergebnis

§ 29a BDSG-E ist insgesamt abzulehnen, da der in Abs. 1 konstituierte Erlaubnistatbestand europarechtswidrig sein kann und jedenfalls mangels Berücksichtigung des Grundrechts auf Informationsfreiheit verfassungswidrig ist. Die anderen Absätze bauen auf dieser Regelung auf. § 29a BDSG-E hat für die Geoinformationswirtschaft eine hohe Relevanz, wenn man ihn auf Tatsachenmitteilungen wie Geoinformationen mit dem ULD anwenden will. Tatsächlich ist die Norm allerdings nicht anwendbar, weil der klare Wortlaut nur Meinungsäußerungen, gerade aber keine Tatsachenmitteilungen umfasst.

3.9 Zu Regelungsvorschlag 9

Regelungsvorschlag Nr. 9 sieht die Einführung eines Absatzes 1a in den bestehenden § 38 BDSG, der die Aufsicht über nicht-öffentliche Stelle regelt, vor. Er soll lauten: „Kontrolliert die Aufsichtsbehörde einen Telemediendienst nach § 1 Abs. 1 Telemediengesetz, so kann die Kommunikation über die nach § 5 Absatz 1 Nr. 2 genannte Adresse erfolgen. Der Telemediendienst hat auf eine elektronische Anfrage der Aufsichtsbehörde unverzüglich, spätestens innerhalb von 14 Tagen zu antworten. Bei Datenschutzverstößen in Telemedien kann die zuständige Datenschutzaufsichtsbehörde zu Warnzwecken einen öffentlichen Hinweis hierauf sowie auf die Schutzmöglichkeiten für Nutzer geben."

Danach soll die Aufsichtsbehörde mit Telemediendienstbetreibern über die gemäß § 5 I Nr. 2 TMG im Impressum anzugebende Möglichkeit der schnellen Kontaktaufnahme – im Allgemeinen also eMail – kommunizieren können. Die Regelung soll der Schnelllebigkeit insbesondere im Internet gerecht werden, welche eine entsprechend schnelle Kommunikation erfordert[88].

Die Möglichkeit des einfachen und schnellen Kontakts zwischen Aufsichtsbehörde und Telemediendienstbetreiber ist für sich genommen sinnvoll. Grundsätzlich hat der Gesetzgeber mit dem

[88] Begründung zum BDSGE-ULD, zu Nr. 9.

§ 3a VwVfG bereits 2003 explizit die Möglichkeit eröffnet, Verwaltungskommunikation auch elektronisch abzuwickeln. Ungeachtet dieser Norm ist dies grundsätzlich wegen § 10 S. 1 VwVfG, der – vorbehaltlich spezieller Regelungen – das Verwaltungsverfahren als nicht-formgebunden festschreibt, auch zuvor generell möglich gewesen.

Generell ist es staatliches Anliegen, dem Bürger eine moderne Verwaltung, die über die für ihn üblichen Kommunikationsmittel verfügt, zu Seite zu stellen, und insbesondere das sog. eGovernment voranzutreiben[89]. In diesem Kontext ist die Einführung des § 3a VwVfG zu sehen[90]. Gleichzeitig hat der Gesetzgeber bei Einführung der Norm (zu einem Zeitpunkt, als die flächendeckende Versorgung in Deutschland mit Internetzugängen überhaupt erst weniger als ein halbes Jahrzehnt gegeben war) erkannt, dass ein solcher elektronischer Weg zwanglos sein müsse, weil die entsprechenden Voraussetzungen weder auf Behörden- noch auf Bürgerseite zum damaligen Zeitpunkt zwingend erwartet werden konnten[91]. Aus diesem Grund enthält der zweite Halbsatz des § 3a I VwVfG die Einschränkung, dass der (jeweilige) Empfänger für die elektronische Kommunikation einen Zugang eröffnen müsse. Es bedarf insoweit also einer expliziten Bekundung des Willens, am elektronischen Verkehr teilzunehmen. Dies kann – wie sich im Umkehrschluss aus Absatz 2 ergibt – sowohl förmlich (elektronische Form, § 126a BGB) – als auch formlos geschehen (eMail, Webformulare, etc.).

Insoweit könnte die vorgeschlagene Regelung vor diesem Hintergrund bedenklich sein, da sie Telemediendiensteanbieter und Behörden nun mehr verpflichtete, entsprechende Kommunikationswege zu nutzen und insoweit jedenfalls der gesetzgeberischen Intention bei Einführung des § 3a VwVfG ein Stück weit zuwider liefe.

Tatsächlich sprechen allerdings gleich mehrere Argumente gegen derartige Bedenken. Zunächst ist zu beachten, dass sich die Situation seit Verabschiedung des Gesetzentwurfes 2002 verändert hat: insbesondere eMail-Kommunikation ist bei Privaten, Unternehmen und Behörden heute wesentlich weiter verbreitet als dies noch vor fast zehn Jahren der Fall war. Sie mag in vielen Bereichen, soweit es nicht gerade auf bestimmte Formeinhaltung ankommt oder Dokumentation und Archivierung eine besondere Rolle spielen, die postalische Kommunikation weitgehend verdrängt haben (ohne dass dies an dieser Stelle abschließend festgestellt werden könnte). Jedenfalls hat sich die Gefahr, die seinerzeit abwartende Zurückhaltung des Gesetzgebers gebot – nämlich, dass Bürger oder Verwaltung durch die technische Innovation überfordert sein könnten -, nicht intensiviert, sondern ist im Gegenteil geringer worden.

Zum anderen – und dies mag das wesentlichere Argument sein – ist zu bedenken, dass § 3a VwVfG (vorbehaltlich spezieller Normen) für *alle* Verwaltungsverfahren aller Behörden gilt, und insoweit auf beiden Seiten des Verfahrens sehr unterschiedliche Personen auftreten können. Dementsprechende Zurückhaltung war bei der Konstitution von Nutzungspflichten hinsichtlich bestimmter Kommunikationswege geboten. Diese Argument ist allerdings gerade nicht valide hinsichtlich Telemediendiensteanbietern, denn dieser werden naturgemäß im Umgang mit mo-

[89] Entschließung des Bundesrats vom 9. 6. 2000 – BR-Dr. 231/00, S. 2 ff.
[90] Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, § 3a Rn. 1 f.
[91] Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, § 3a Rn. 10 f.

dernen Kommunikationsmitteln bestens ausgestattet und vertraut sein. Umgekehrt steht es dem Gesetzgeber frei, die Verwaltung – die gerade an die Gesetze gebunden ist – dazu zu verpflichten, bestimmte moderne Formen der Kommunikation zu nutzen, wenn dafür Sorge getragen ist, dass die entsprechenden Voraussetzungen bei der Behörde geschaffen werden, um dies zu ermöglichen[92].

Der verpflichtenden Einführung der Nutzung bestimmter (elektronischer) Kommunikationswegen über die nach § 5 I Nr. 2 TMG im Impressum des Diensteanbieters angegeben Kanäle, stünden daher grundsätzlich keine Bedenken entgegen. Sie könnte vielmehr als fortschrittliche Entwicklung im Verwaltungsverfahren zu begrüßen sein. In einem derartigen Fall wären im Gesetz jedoch Mindeststandards festzuschreiben, die die Behörde ihrer Kommunikation mit dem Nutzer einzuhalten hat – etwa hinsichtlich der Protokollierung, der Authentifizierung und Identifizierung, der Plattformneutralität etc. An derartigen Bestimmungen mangelt es hier.

Darüber hinaus handelt es sich beim Vorschlag jedoch gerade nicht um die verpflichtende Einführung der Nutzung bestimmter Kommunikationswege, sondern um die bloße Eröffnung einer Möglichkeit zugunsten allein der Behörde („so kann die Kommunikation über die nach § 5 Absatz 1 Nr. 2 genannte Adresse erfolgen") – weil insbesondere nicht normiert wird, dass sich die Behörde dieser Adresse zu bedienen hat und weil auch nicht klar ist, welche Behördenadresse zu verwenden ist, sodass die Bestimmung die Position des Bürgers insgesamt nicht verbessert, sondern einseitig verschlechtert.

Weiter ist aus systematischen (und rechtsvergleichenden) Gründen darauf hinzuweisen, dass die Bezugnahme auf eine „Adresse der elektronischen Post" andernorts aus Gründen der Technologieneutralität vermieden wird. So spricht etwa § 8b Abs. 4 Satz 2 VwVfG in der Fassung nach Umsetzung der Dienstleistungsrichtlinie davon, dass Informationen „elektronisch übermittelt werden sollen" – also gerade ohne Bezugnahme auf eine „Adresse der elektronischen Post". Damit werden im ersten Fall auch sonstige Formen der elektronischen Kommunikation (insbesondere Webformular, aber wenigstens im Grundsatz auch Facebook- oder Twitteraccounts) nicht ausgeschlossen.

Daneben wird eine Pflicht der Anbieter konstituiert, auf Anfragen durch die Aufsichtsbehörde spätestens innerhalb von 14 Tagen zu reagieren. Eine solche Pflicht kann zur Beschleunigung und Vereinfachung von entsprechenden Verfahren beitragen, was aufgrund der schnellen Verbreitung von Informationen im Internet ohne Zweifel begrüßenswert ist.

Ob dies bei Ausnutzen der maximalen Frist von 14 Tagen auch noch gelten kann, erscheint allerdings fraglich. Hinzu kommt, dass die Regelung keine Sanktion für Verstöße vorsieht, denn die vorgesehene Einfügung eines § 43 I Nr. 7c BDSG-E betrifft nur Verstöße aus dem vorgesehenen § 29a IV 2 BDSG-E, nicht aber § 38 1a BDSG-E.

Schließlich wird der Aufsichtsbehörde die Möglichkeit eingeräumt, zu Warnzwecken öffentliche Hinweise auszusprechen. Gerade im Bereich eines durch Verbraucher nicht ständig beobachte-

[92] Letzteres ist an dieser Stelle nicht zu beurteilen, es handelt sich auch nicht um eine normative Frage, sondern eine solche der exekutiven Organisation.

ten Felds wie dem des Datenschutzes, der zudem mitunter vertiefte technische Kenntnisse im Internet erfordert, erscheint es – nicht zuletzt angesichts der Skandale der letzten Jahre – zweckdienlich, wenn die Aufsichtsbehörde Warnhinweise und Möglichkeiten des Selbstschutzes publiziert.

Die vorgeschlagene Regelung ist im Grundsatz zu begrüßen, denn eine beschleunigte und vereinfachte Behördenkommunikation ist im Interesse aller Beteiligten und in der Telemedienbranche auch naheliegend. Allerdings sieht die Regelung keine Sanktionen für eventuelle Verstöße vor, also etwa, wenn eine Reaktion des Telemediendiensteanbieters ausbleibt. Daneben bestehen die oben geschilderten Bedenken hinsichtlich fehlender Parität und Technologieneutralität. Die Relevanz für die Geoinformationswirtschaft beschränkt sich auf eventuelle Kommunikation mit der Aufsichtsbehörde, wenn Geodaten online gestellt werden, die Personenbezug aufweisen, und damit eher gering.

3.10 Zu Regelungsvorschlag 10

Dieser Regelungsvorschlag erweitert den Bußgeldkatalog des § 43 Abs. 1 auf Verstöße gegen den neu zu schaffenden § 29a Abs. 4 S. 2 und § 29a Abs. 6 BDSG. Diese sollen als Ordnungswidrigkeit qualifiziert werden (§ 43 Abs. 1 BDSG) und mit einer Geldbuße bis zu fünfzigtausend Euro bedroht werden, die im Einzelfall auch überschritten werden darf (§ 43 Abs. 3 Satz 2, Satz 3 BDSG).

Bußgeldbewehrt wird damit erstens, dass eine verantwortliche Stelle, die die Richtigkeit der Daten nach Beschwerde nicht nachweisen kann, eine eigene Darstellung in angemessenem Umfang nicht hinzufügt.

Damit fällt auch hier auf,[93] dass eine Sanktion für einen Verstoß gegen die aus § 29 Abs. 4 Satz 2 entstammende Verpflichtung, eine Beschwerde, die an die Adresse der elektronischen Post gerichtet war, unverzüglich zu beantworten, nicht vorgesehen ist. Damit bleibt auch hier ein im Netz immer wieder zu beobachtender Missstand, dass eine Adresse elektronischer Post schlicht nicht angeboten wird (sondern stattdessen nur Mehrwerttelefonnummern oder Webformulare, vgl. zB www.lufthansa.com) unsanktioniert, ohne dass sich dem Entwurf eine Begründung für diese Wertungsdifferenzierung entnehmen ließe.

Bußgeldbwehrt wird zweitens die Nichtbekanntgabe der Absicht eines Telemedien-Diensteanbieters, personenbezogenen Daten zu mehr als 1000 oder von einer unbestimmten Zahl von Personen zu veröffentlichen (§ 29a Abs. 6 BDSG). *Nicht* bußgeldbewehrt bleibt daher – wiederum ohne Nennung sachlicher Gründe – ein Verstoß gegen § 29 Abs. 5 („Die Veröffentlichung von personenbezogenen Daten aus allgemein zugänglichen Quellen hat zu unterbleiben, wenn der entgegen stehende Wille des Betroffenen aus dieser Quelle oder auf andere Weise eindeutig erkennbar ist. Der Empfänger von veröffentlichten Daten hat sicherzustellen, dass Kennzeichnungen bei der Übernahme übernommen werden."). Auch hier zeigt sich daher eine dem Entwurf immanente Stärkung der Position von Datenschutzbehörden. Auch aus diesem Grunde wäre eine grundsätzliche Diskussion der Effizienz von Bußgeldkatalogen als Instrument

[93] Vgl. zur korrespondierenden Problematik hinsichtlich § 38 Abs. 1a BDSG-E oben bei 3.9.

der Sicherung des Datenschutzniveaus durch Datenschutzbehörden in Deutschland angezeigt, die hier freilich aus Platzgründen nicht geleistet werden kann.[94]

Die vorgeschlagene Regelung setzt die dem BDSG schon bisher immanente Bußgeldbewehrung von Tatbeständen fort. Allerdings ist die Auswahl der Tatbestände ohne weitere Begründung selektiv und schon deswegen zu hinterfragen. Daneben treten grundsätzliche Erwägungen zur Effektivität des § 43 als Instrument zur Sicherung der datenschutzrechtlichen Normen. Nennenswerte Auswirkungen auf die Geoinformationsbranche sind nicht zu erwarten.

3.11 Zu Regelungsvorschlag 11

Dieser Vorschlag sieht die Streichung des § 13 Abs. 2 TMG vor und lautet wörtlich: „§ 13 Abs. 2 wird gestrichen. Die Absätze 3 bis 7 werden die Absätze 2 bis 6". Gesetzessystematisch ist daher anzumerken, dass diese Änderung in einem eigenen Artikel zu erfolgen hätte, da sie das TMG und nicht wie die anderen zehn Vorschläge das BDSG betrifft.

§ 13 Abs. 2 TMG soll laut Regelungsvorschlag 6 des ULD in § 4a BDSG integriert werden und damit in § 13 TMG wegfallen. Der Vorschlag begegnet daher den bereits oben bei 3.6 präsentierten Bedenken. Thematisch gehört die elektronische Einwilligung in das TMG, da dort die Rechte und Pflichten der Betreiber von Telemediendiensten speziell geregelt werden. Wie oben bereits erläutert, ist die Übernahme einer spezialgesetzlichen Vorschrift in ein Auffanggesetz systemwidrig und führt zu Verwerfungen hinsichtlich des Verhältnisses zwischen Schriftform elektronischer Form unter Verwendung einer qualifizierten elektronischen Signatur, „einfacher" elektronischer Form und sonstiger Form.

Daher ist dieser Regelungsvorschlag abzulehnen. Eine Relevanz für die Geoinformationsbranche ist kaum anzunehmen.

[94] Hingewiesen sei allein auf den Umstand, dass eine Judikaturrecherche nach § 43 BDSG in Juris insgesamt 14 Treffer verzeichnet, deren jüngster aus dem April 2007 stammt.

4. Fazit

Der Vorschlag des ULD erweitert die Geoinformationsdiskussion um eine weitere Facette und ist daher im Interesse einer breiten und sachlichen Diskussion zu begrüßen. Die politische Auseinandersetzung der folgenden Wochen wird zeigen, inwiefern die ihn tragenden Ideen Realisierungschancen haben. Vermutlich sind diese, insbesondere vor dem Hintergrund der vom sachlich (mit-)zuständigen BM de Maizière getätigten Äußerungen[95] als eher gering einzustufen. Sollten sie gleichwohl bestehen, wären die hier aufgebrachten Fragestellungen und Kritikpunkte in den weiteren Diskussionsprozess einzubringen.

[95] Vgl. etwa http://carta.info/29493/de-maizieres-redemanuskript-grundlagen-fuer-eine-gemeinsame-netzpolitik-der-zukunft/: „Open Government ist v.a. für wirtschaftliche Nutzungen sinnvoll und innovativ. In diesem Zusammenhang ist auch der Aufbau der Geodateninfrastruktur in Deutschland zu nennen, der mir besonders am Herzen liegt."; „Selbstregulierung hat Vorrang vor neuer Rechtsetzung. Bevor wir an neue gesetzliche Regelungen denken, sollten wir in einer freiheitlichen Ordnung die Selbstregulierungskräfte von Gesellschaft und Wirtschaft nutzen und einfordern. Erst wo dies nicht zu gesellschaftsverträglichen Lösungen führt oder starke Partikularinteressen das Gemeinwohl überlagern, muss der Staat aktiv werden."; Manchmal ist der Gesetzgeber auch gut beraten, Einzelfragen zu technischen Entwicklungen zunächst durch die Rechtsprechung anhand konkreter Fälle klären zu lassen. Wo der Staat im Internet gesetzgeberisch handelt, muss er den damit verbundenen Anspruch tatsächlich erfüllen können. Er sollte sich daher auf Maßnahmen konzentrieren, die in der digitalen Welt wirklich halbwegs umgesetzt werden können." etc.