Schleswig-Holsteinischer Landtag
Umdruck 18/553

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ULD • Postfach 71 16 • 24171 Kiel

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Vorsitzende Frau Barbara Ostmeier
Postfach 7121

24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200

Aktenzeichen:
LD -01.03/01.304

Kiel, 19. Dezember 2012

Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet - Antrag der Fraktion der PIRATEN - Drucksache 18/195
Ihr Schreiben vom 27.11.2012, L 215

Sehr geehrte Frau Vorsitzende Ostmeier,
sehr geehrte Frau Schönfelder,
sehr geehrte Damen und Herren Abgeordnete,

gerne komme ich Ihrer Bitte um Stellungnahme zu dem o. g. Antrag nach. Ergänzend weise ich auf die Stellungnahme des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 17.12.2012 (Umdruck 18/533) hin, der ich mich inhaltlich anschließe.

1. Rahmenbedingungen

Das in Deutschland geltende Datenschutzrecht, insbesondere das Bundesdatenschutzgesetz (BDSG), ist in mancher Hinsicht noch von der Großrechnertechnologie der 70er Jahre des 20. Jahrhunderts geprägt. Wir befinden uns inzwischen in einer Informationsgesellschaft, die vom stationär wie mobil nutzbaren interaktiven Internet geprägt ist. Dieses Netz weist vier technikspezifische Eigenschaften auf, die gravierende Konsequenzen für den Regelungsbedarf haben:

1. Die Virtualität des Netzes schafft neben der analogen eine digitale Realität, die mit der analogen in einem engen gestaltbaren Wechselspiel steht. Wegen der Auswirkungen dieser digitalen Realität auf das Persönlichkeitsrecht der Menschen kann und muss ordnend bzw. regulierend eingegriffen werden.

2. Das Netz ist universell und konvergent. Dadurch werden im analogen Raum bestehende Grenzziehungen zwischen Lebens- und Medienwelten, also etwa zwischen privat und öffentlich, Konsument und Produzent, Information und Einwirkung, eingeebnet.

3. Die Globalität des Netzes erschwert eine Lokalisierung informationstechnischer Sachverhalte, die Zuordnung von Verantwortung hierfür und staatliche Interventionen.

4. Das Netz ist gekennzeichnet durch den paradox erscheinenden Widerspruch von Intransparenz der Datenverarbeitung und Anonymität der Nutzenden einerseits und absoluter Kontrollierbarkeit andererseits.

2. Entwicklung der Diskussion

Im bestehenden nationalen Regelungsrahmen gilt für Internet-Inhaltsdaten das BDSG. Dessen Grundkonzept aus den 70er Jahren wurde in den 90er Jahren an die Rechtsprechung des Bundesverfassungsgerichtes und die neuen Anforderungen des Schutzes des Grundrechts auf informationelle Selbstbestimmung angepasst. Seitdem erfolgten mehrfach Nachbesserungen, aber keine umfassende Überarbeitung. Die o. g. Eigenschaften blieben unberücksichtigt. Für Telemedien bzw. Diensteanbieter bestehen im Telemediengesetz (TMG) und für Kommunikationsnetze bzw. Zugangsanbieter im Telekommunikationsgesetz (TKG) eher zeitgemäße Regelungen. Neben diesen aus Datenschutzsicht zentralen Gesetzen gibt es eine Vielzahl von flankierenden Normen mit Datenschutzrelevanz, etwa das Verbraucherrecht mit seinen Regelungen zu Allgemeinen Geschäftsbedingungen oder das Recht der immer stärker von Informationstechnik geprägten Arbeitsverhältnisse.

Seit Jahren ist unstreitig, dass eine Anpassung des Rechts an die neuen technischen, sozialen und ökonomischen Realitäten des Internet nötig ist. Dies veranlasste das Bundesministerium des Innern, hierzu ein Gutachten in Auftrag zu geben, das im Jahr 2001 nach einer intensiven öffentlichen Diskussionsphase von Roßnagel/Pfitzmann/Garstka mit dem Titel „Modernisierung des Datenschutzrechts“ vorgelegt wurde. Zu einer Umsetzung der Gutachtenvorschläge kam es nicht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschloss am 17./18.03.2010 einen ausführlichen Katalog von Vorschlägen („Ein modernes Datenschutzrecht für das 21. Jahrhundert“). Am 27.10.2010 legte das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) im Hinblick auf die im Antrag geforderte Stärkung der Freiheit und der Privatsphäre im Internet konkrete umfassende Gesetzesformulierungen vor („Gesetzesvorschlag zur Internet-Regulierung“). Diese Vorschläge aus der Aufsichtspraxis fanden bisher ebenfalls keinen Eingang in Gesetzesinitiativen. Am 01.12.2010 legte das Bundesministerium des Innern einen Gesetzentwurf „zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht“ vor, der unter dem Stichwort „rote Linien“ bekannt wurde und die Einführung eines § 38b in das BDSG vorsah. Dieser erwies sich wegen seiner inhaltlichen Begrenztheit für eine Weiterentwicklung des Internetdatenschutzrechts für ungeeignet.

Mit Datum vom 21.03.2011 unterbreitete das Bundesland Hessen im Bundesrat Vorschläge zur Änderung des Telemediengesetzes (BR-Drs. 156/11; BT-Drs. 17/6765). Neugeregelt werden sollen danach die Informationspflichten von Telemedienanbietern bei der Datenerhebung (auch über die Datenschutzaufsicht und Übermittlungen ins Drittausland), die technische Sicherstellung von Nutzerrechten (Ansprüche auf Korrektur und Löschung von Daten, Zweckbegrenzung), die Umsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie (s. u. Abschnitt 3.7), technische Sicherungen bzgl. bei Telemediendiensten durch die Nutzenden generierten Daten (Privacy by Default, s. u. Abschnitt 3.7, Informationspflichten, Wahlmöglichkeiten, das Vermeiden der Erfassung durch Suchmaschinen, Ju-

gendschutz) und u. a. auch der Anspruch auf Löschung von nutzergenerierten Inhalten. Leider wurde dieser in seiner Zielrichtung zu begrüßende Entwurf im Gesetzgebungsverfahren nicht weiter behandelt.

Auf adäquate Datenschutzregelungen im Internet zielt nun der Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung – EU-DSGVO)“ der EU-Kommission vom 25.01.2012 ab (KOM(2012) 11 endgültig).

In direkter Reaktion hierauf legte die Regierung der USA, wo der Internetdatenschutz bis heute weitgehend ungeregelt ist, im Februar 2012 eine Consumer Privacy Bill of Rights vor, die primär auf Selbstregulierung der Wirtschaft setzt (http://www.datenschutzzentrum.de/gesetze/Consumer-Privacy-Bill-of-Rights.html).

Dass dieser Ansatz der unregulierten Selbstregulierung keinen Erfolg verspricht, zeigen die bisherigen Erfahrungen. Eine Selbstregulierung des Wirtschaftsverbandes BITKOM zu Internet-Panoramadiensten blieb hinter den gesetzlichen Anforderungen zurück. Entsprechende Bestrebungen zu sozialen Netzwerken verlieren sich in der unterschiedlichen Perspektive von deutschen und US-amerikanischen Anbietern und einem völlig disparaten Verständnis der – zweifellos in vieler Hinsicht ungeklärten – aktuellen Rechtslage.

Der jüngste nationale Diskurs über den Schutz des Persönlichkeitsrechts im Internet erfolgte auf dem 69. Deutschen Juristentag am 19.09.2012 in München (Abteilung IT- und Kommunikationsrecht) mit dem grundlegenden und sehr umfassenden Gutachten von Prof. Gerald Spindler „Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung“.

3. Wesentliche Regelungsfragen

Der deutsche Gesetzgeber steht in der Pflicht. Er hat teilweise europäisches Recht noch nicht umgesetzt. Ein Inkrafttreten der EU-DSGVO vor 2016 ist unrealistisch. Schon deshalb muss national gehandelt werden. Dies wäre nicht nur eine Überbrückung der Zeit bis zur Geltung einheitlichen europäischen Rechts, sondern auch ein Beitrag zu dessen Gestaltung.

Die Eigenschaften des Internet führen zu Fragestellungen, die neuer Antworten bedürfen. Es geht um Neujustierungen in folgenden datenschutzrechtlich zentralen Bereichen:

- Verantwortlichkeit,
- Anwendbarkeit des Rechts und Aufsichtszuständigkeit,
- Verhältnis des Datenschutzes zu den Grundrechten auf Informations-, Presse- und Meinungsfreiheit,
- Zweckbindung in Hinblick auf Person, Lebensbereich und Rolle,
- Arbeitgeberkontrolle,
- Betroffenenrechte (Datenlöschung, Auskunft, Portabilität) und Transparenz,
- Einwilligung aus rechtlicher wie technischer Sicht,
- Beschwerdemanagement und Sanktionen.

Bevor die Vorschläge im Antrag der Fraktion der PIRATEN in Einzelnen kommentiert werden (unter Abschnitt 4.), soll der Regelungsbedarf in diesem größeren Zusammenhang dargestellt werden:

3.1 Verantwortlichkeit

Die Auflösung der klaren Rollentrennung zwischen verarbeitender Stelle und Betroffenem, welche die ersten zwei Generationen des Datenschutzrechts (1. Generation: Missbrauchsverhinderung beim Großrechnereinsatz, 2. Generation: Grundrechtsverwirklichung bei komplexer, aber einseitiger Datenverarbeitung) prägte, macht die Festlegung von Rechten und Pflichten aller Beteiligten komplizierter:

Die Netznutzenden werden zumindest im Hinblick auf die von ihnen selbst generierten Inhalte mit Personenbezug selbst verantwortlich. Zugleich entsteht der Bedarf an einem Recht auf Anonymität bzw. Pseudonymität oder auf Identitätenmanagement. Bei den informationstechnischen Dienstleistern erfolgen funktional unterscheidbare Aktivitäten. Es gibt Anbieter von 1. Inhalten 2. Diensten bzw. Applikationen, 3. Betriebssystemen, 4. Portalen und 5. Netzen sowie Netzkomponenten. Die Übergänge zwischen diesen Bereichen sind fließend; einzelne Akteure nehmen mehrere oder viele der Funktionen wahr. Webseitenbetreiber sind nicht nur für ihre eigenen Inhalte verantwortlich, sondern auch für ihre Auswahl von Software, Portaldiensten usw. und damit auch (jedenfalls indirekt) für die Generierung von Nutzungsdaten: Wer z. B. sein Webangebot über Facebook gestaltet, legt damit fest, dass Facebook den Besuch der eigenen Fanpage nachvollziehen und auswerten kann. Auch wer IFrames integriert, etwa in Form von Social Plugins, oder das Setzen von Cookies erlaubt, teilt mit den Anbietern dieser IFrames bzw. Cookies regelmäßig die Nutzungsdaten und evtl. sogar Inhaltsdaten der Betroffenen.

Intermediäre im Internet, also z. B. Suchmaschinen oder Blogbetreiber, erhalten die technische Souveränität über Inhalts- und Nutzungsdaten und werden dadurch u. U. ausschließlich hierfür verantwortlich, ohne dass eine bewusste Kenntnisnahme von den Daten erfolgt sein müsste. Dieser Umstand wurde in den §§ 7 ff. TMG adäquat rechtlich berücksichtigt. Rechtliche Konsequenzen werden dem gemäß aus der technischen Verantwortlichkeit erst gezogen, wenn der Betreiber einen konkreten Sachverhalt zur Kenntnis genommen und die Möglichkeit zu einem evtl. notwendigen Tätigwerden hatte. Bzgl. der zivilrechtlichen Verantwortlichkeit hat die Rechtsprechung entsprechende Lösungen entwickelt. Die derzeit geltende Datenschutzregelung des § 3 Abs. 7 BDSG enthält keine solche Beschränkung und ignoriert damit diese Problematik.

Zugangs- bzw. Netzanbieter haben grds. die technische Macht und Möglichkeit, sämtliche über ihr Netz vermittelten Daten und Informationen zu speichern und auszuwerten. Dies hat zwei paradox scheinende Folgen: Diese Datenverarbeitung muss im Interesse des Persönlichkeitsschutzes streng begrenzt werden. Andererseits werden die Anbieter zu umfassenden Datenspeicherungen im Interesse staatlicher Rechtsdurchsetzung gezwungen, z. B. durch die Pflicht zur Vorratsdatenspeicherung oder zur Identifizierung der Netznutzenden. Dieser Konflikt kann nur durch diese Schutzziele verfolgende, ausgewogene Regelungen gelöst werden.

Die Art. 4 Abs. 5, 24 Entwurf EU-DSGVO sehen zur Verantwortlichkeit Klarstellungen vor. Abgestellt wird darauf, dass die Stelle „über die Zwecke, Bedingungen und Mittel der Verarbeitung" bestimmt, wobei dies allein oder gemeinsam, arbeitsteilig oder in Kooperation erfolgen kann. Während bisher nur bei der klassischen Auftragsdatenverarbeitung eine vertragliche Klärung gefordert wird, soll künftig auch bei gemeinsamer Verarbeitung eine rechtlich belastbare Vereinbarung die Wahrung der Betroffenenrechte sicherstellen.

3.2 Anwendbarkeit des Rechts

Das Internet hat einerseits die Anwendbarkeit von nationalen Rechtsbereichen vervielfältigt, andererseits die faktische Anwendung des Rechts reduziert: Gemäß dem bisher geltenden Territorialitätsprinzip gibt es viele Anknüpfungspunkte: die Rechner der Nutzenden, die Weiterleitung im Netz, die Verarbeitung bei den Inhalts- und Diensteanbietern sowie die bei den Portal- und den Applikationsanbietern. Damit gibt es potenziell viele Adressaten des Datenschutzrechts und viele zuständige Aufsichtsbehörden.

Die Realität ist jedoch, dass bei internationalen Diensten regelmäßig entweder überhaupt kein Vollzug erfolgt, oder sich ein Verarbeiter das für ihn günstigste Rechtsregime herauspickt. Dies kann in einem Fall das Datenschutzrecht des Unternehmenssitzes sein, das, wie in den USA, nur geringe Anforderungen festlegt. In einem anderen Fall bietet sich ein Mitgliedstaat an, der möglicherweise national das EU-Recht nur unzureichend umsetzt und möglicherweise ein hohes Vollzugsdefizit aufweist. Letzteres kann an unzureichenden Ressourcen der Aufsichtsbehörde liegen oder daran, dass sich diese von steuerlichen oder arbeitsmarktpolitischen ökonomischen Interessen leiten lässt.

Diese praktischen Probleme werden teilweise durch die Aktivitäten der Artikel-29-Datenschutzgruppe angegangen, wenn in Arbeitspapieren eine Vereinheitlichung der aufsichtsbehördlichen Sichtweise angestrebt wird oder ein Informations- und Meinungsaustausch zwischen den potenziell zuständigen Behörden erfolgt. Bisher gibt es weder ein formalisiertes Verfahren noch eine realistische Aussicht auf einen flächendeckenden Datenschutzvollzug wegen der absolut unzureichenden Ausstattung der Behörden, ungenügender Kommunikationsstrukturen und des fehlenden rechtlichen Zwangs zur Abstimmung.

Der Entwurf einer EU-DSGVO will hierzu valide Antworten geben, indem in Art. 4 Abs. 13 der Ort der Grundsatzentscheidungen bzgl. Zweck, Bedingungen und Mittel der Datenverarbeitung zum primären Anknüpfungspunkt gemacht wird und nach Art. 3 über das Marktortprinzip gewährleistet werden soll, dass ein Herauswinden aus der Verantwortlichkeit nicht mehr möglich ist. Zugleich soll über die Umsetzung des One-Stop-Shop-Prinzips die Verlässlichkeit behördlicher Aufsichtsverfahren erhöht werden. Zwecks Vermeidung eines Zuständigkeits-Hoppings bzw. eines Race-to-the-bottom-Effekts ist ein kompliziertes Abstimmungs- bzw. Kohärenzverfahren in den Art. 55 ff. EU-DSGVO vorgesehen.

3.3 Informations-, Presse- und Meinungsfreiheit

Die Informations- und Kommunikations-Grundrechte aus Art. 5 Grundgesetz lebten seit 1983 mit dem damals geschaffenen Grundrecht auf informationelle Selbstbestimmung lange in friedlicher Koexistenz. Selbst das Aufkommen der Informationsfreiheitsgesetze in den 90er Jahren war in Deutschland kein Grund, das Datenschutzrecht zu überarbeiten. Die meinungsmachenden Datenverarbeiter mit ihren journalistisch-redaktionellen Zwecken blieben die nach § 41 BDSG privilegierte Ausnahme. Nachdem im Internet die Nutzenden selbst zu Meinungsmachern und Medienproduzenten werden konnten und das Netz Funktionen von Presse, Rundfunk und Fernsehen übernahm, hat sich die Realität gewandelt: Das Datenschutzrecht benötigt Instrumente zum Ausgleich des Meinungs- und des Persönlichkeitsschutzes. Die alten Grenzen zwischen privilegierter Presse und den nur rezipierenden Pressenutzenden lösen sich immer mehr auf.

Markant hierzu war die Spick-mich-Entscheidung des Bundesgerichtshofes aus dem Jahr 2009, als das Gericht – zu Recht – Regeln des § 29 BDSG für unanwendbar erklärte, weil diese im Rahmen von Lehrkräftebewertungen das Recht der Schüler nach Art. 5 GG beschränkte, anonym ihre Meinung im Internet zum Ausdruck zu bringen (BGH, NJW 2009, 2888 ff.). Generell gilt im Interesse eines umfassenden Grundrechtsschutzes im Internet, dass das Datenschutzrecht bei Meinungsveröffentlichungen eine Abwägung ermöglichen muss. Wie eine Regelung hierzu aussehen könnte, wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein am 27.10.2010 vorgeschlagen mit einer generellen Vermutung zugunsten des Art. 5, materiellen Ausnahmen bei sensiblen Daten und einem Konfliktlösungsverfahren. Die Vorschläge wurden jedoch von der Politik bis heute nicht aktiv aufgegriffen.

Der Entwurf einer EU-DSGVO ist insofern wenig wegweisend. In Art. 80 enthält er einen nationalen Regelungsvorbehalt für „journalistische Zwecke“ zum Ausgleich mit der „Freiheit der Meinungsäußerung“. Wenn es einen Bedarf an europäischer Regulierung und Vereinheitlichung im Datenschutzrecht gibt, dann hier beim Ausgleich der seit 2009 europäisierten Grundrechte auf Datenschutz und Meinungsäußerung (Art. 8 und 11 Europäische Grundrechtecharta).

3.4 Zweckbindung

Das Datenschutzprinzip der Zweckbindung wird durch das Internet im höchsten Maße herausgefordert. Dies gilt nicht nur wegen der Unmöglichkeit einer spezifischen Zweckzuweisung bei global veröffentlichten Daten. Eine faktisch größere Gefährdung des Zweckbindungsgrundsatzes liegt in der extensiven Auswertung von Nutzungsdaten für kommerzielle, insbesondere für Werbe-Zwecke, vor allem durch US-Anbieter, und vor allem in Big-Data-Bestrebungen auf allen Ebenen, also in der zweckfreien Auswertung der – nicht nur im Netz anfallenden – digitalen Datenmassen.

Unser TMG sieht hinsichtlich Bestandsdaten in § 14 eine strenge Zweckbindung vor. In § 15 TMG wird die Zweckbindung bei Nutzungsdaten festgelegt verbunden mit einer Ausnahme in Absatz 3 für Zwecke der „Werbung, Marktforschung oder bedarfsgerechten Gestaltung“. Diese Ausnahme setzt voraus, dass die Verarbeitung pseudonym erfolgt, die Betroffenen informiert wurden und ihnen ein Recht auf Widerspruch eingeräumt wurde. Art. 5 Abs. 3 der E-Privacy-Richtlinie engt die Anforderung im Hinblick auf das Setzen von Cookies, die für die Erbringung eines Dienstes nicht

erforderlich sind, weiter ein. Dass diese Regeln in der Praxis oft unbeachtet bleiben, liegt nicht an den technischen Gegebenheiten des Netzes, sondern an den Vollzugsproblemen nicht nur deutscher Aufsichtsbehörden im globalen Netz.

Die unzureichende Beachtung der Zweckbindung im gewillkürten Bereich der Internetnutzung, also bei Vertragsgestaltung und -vollzug, ist dem Umstand geschuldet, dass bisher der Grundsatz „Privacy by Default" nicht gilt, dass uferlose sog. „Privacy Policies" und Nutzungsbestimmungen Anbietern beliebige Zweckänderungen erlauben und dass die Nutzenden keine Informationen erhalten geschweige denn Wahlmöglichkeiten zugestanden bekommen. Dass einmal veröffentlichte Daten im globalen Internet allenfalls begrenzt wieder hinsichtlich Zweck und Lebensdauer eingefangen werden können, ist technisch zwangsläufig.

Dies zwingt aber nicht zur Aufgabe des Prinzips der Zweckbindung. Dieses Signal geht auch vom Entwurf der EU-DSGVO aus, der in Art. 6 Abs. 1 von einem oder mehreren genau festgelegten Zwecken spricht, die sich z. B. aus einem Vertrag oder einem Gesetz ergeben. Mit Absatz 4 soll die Rechtsprechung des deutschen Bundesverfassungsgerichtes erstmals allgemein in europäisches Recht umgesetzt werden, indem Zweckunverträglichkeiten verboten werden. Schließlich versucht Art. 20 das Problem von Tracking, Scoring und Profiling aus Big-Data-Beständen in den Griff zu bekommen. Ob dies mit der Entwurfsformulierung gut gelungen ist, kann bezweifelt werden.

3.5 Beschäftigtenüberwachung

Ein spezielles Problem der Zweckbindung besteht bei der Nutzung von Internetdaten durch Arbeitgeber für Überwachungs- und Kontrollzwecke. Diese stellen oft die Technik für den Zugang zum Netz zur Verfügung, und diese ist grds. zur vollständigen Überwachung aller informationstechnischer Vorgänge in der Lage. Das Problem wird verschärft bei der nicht getrennten Nutzung von Soft- und Hardware für private und dienstliche Zwecke, etwa durch die dienstliche Nutzung privater Geräte – „bring your own device" (BYOD). Insbesondere soziale Netzwerke haben die Tendenz der Verwischung der Grenzen zwischen privaten und dienstlichen Aktivitäten, etwa wenn der Arbeitgeber die Nutzung von solchen Communities erwartet oder gar verlangt. Das Risiko besteht darin, dass dem Arbeitgeber rein private Aktivitäten zur Kenntnis gelangen und diese Informationen dienstlich genutzt werden.

Es gibt keine technischen Zwänge, die eine Trennung von privaten und dienstlichen Aktivitäten verhindern, selbst bei gemeinsam genutzter Hard- und Software. Es gibt keinen gesetzlichen Zwang, dienstlich oder privat Echtnamen zu verwenden. Wohl gibt es aber einen solchen (ökonomisch getriebenen) Zwang durch Portalanbieter. Auch sonstige zweckübergreifende Identifikatoren (z. B. E-Mail-Adressen, Cookies) könnten vermieden werden.

Gesetzliche Regelungen wären insofern äußerst wünschenswert, sind aber – auch angesichts der Rechtsprechung der Arbeitsgerichtsbarkeit – nicht unbedingt nötig. Über technische, organisatorische und andere rechtliche Sicherungen (z. B. über Betriebsvereinbarungen mit dem Betriebsrat) können funktionelle und/oder Rollentrennungen, die Beschränkung der Arbeitgeberkontrolle bei dienstlicher und in stärkerem Maße bei privater Nutzung und weitere Sicherungen realisiert werden.

3.6 Betroffenenrechte

Der Kanon der Betroffenenrechte ist derzeit von den Art. 10 ff. der Europäischen Datenschutzrichtlinie vorgegeben und durch das BDSG umgesetzt (Benachrichtigung § 33; Auskunft § 34; Berichtigung, Sperrung, Löschung, Widerspruch § 35; Schadenersatz §§ 7, 8; Anrufung der Aufsichtsbehörde §§ 21, 38). Die geplanten Regelungen in der EU-DSGVO bilden diese Rechtslage erneut ab (Information Art. 14; Auskunft Art. 15; Berichtigung Art. 16; Löschung Art. 17; Widerspruch Art. 19). Die Bezeichnung des Löschanspruchs als „Recht auf Vergessenwerden" in Art. 17 ist weniger normativ als programmatisch zu verstehen.

Die EU-DSGVO greift in Art. 17 Abs. 2 die internetspezifische Problematik der Datenreplikation auf und verweist sie in den Verantwortungsbereich der verarbeitenden Stelle. Innovativ ist auch die Regelung der Datenübertragbarkeit (Portabilität Art. 18), womit die Möglichkeit der Mitnahme von Nutzerkonten von einem zu einem anderen Anbieter eröffnet werden soll. Eine Funktion dieser Regelung liegt darin, die Abhängigkeit der Nutzenden von einem Anbieter zu reduzieren und Anbieterwechsel zu erleichtern. Ein ebenfalls bedenkenswerter Ansatz bestünde darin, einen Anspruch für den Nutzer zu eröffnen, umfassende Dienste (z. B. soziale Netzwerke) von außen zu adressieren, um so unabhängig vom Bestehen faktischer Monopole in bestimmten Anwendungsbereichen den Zwang zum Verbleib in den „walled gardens" eines Anbieters oder einer Anbietergruppe zu reduzieren.

Zu begrüßen sind die sehr weitgehenden Rechtsschutzmöglichkeiten, die Betroffenen in den Art. 74, 75 des Entwurfs der EU-DSGVO erhalten – nicht nur gegenüber der verantwortlichen Stelle, sondern auch gegenüber der zuständigen Aufsichtsbehörde. Nicht weiter verfolgt werden offensichtlich weitere Ideen verbraucherrechtlicher Betroffenenrechte, etwa des pauschalisierten Schadenersatzes oder sonstiger zivilrechtlicher Instrumente.

Zu den Rechten der Betroffenen im weiteren Sinne gehören auch deren Transparenzansprüche, also die Informationspflichten der Anbieter und korrespondierende Ansprüche der Nutzenden. Während die Impressumspflichten der §§ 5, 6 TMG inzwischen weitgehend beachtet werden, besteht bei den spezifischen Informationspflichten zu verantwortlichen Stellen, Zwecken, Empfängern, Auslandsübermittlungen, Cookies und Auswertungsformen wie z. B. Profilbildung weiterhin ein großes Vollzugsdefizit (§§ 4 Abs. 2, 33 BDSG, 13 Abs. 1, 15 Abs. 3 S. 2 TMG). Entsprechendes gilt für gesetzliche Informationspflichten zu Betroffenenrechten, etwa hinsichtlich der bestehenden Widerspruchsmöglichkeiten (z. B. §§ 28 Abs. 4 S. 2 BDSG, 15 Abs. 3 S. 2 TMG). Informationen über Betroffenenrechte und darüber, wie diese gegenüber wem direkt ausgeübt werden können, werden in der Praxis fast nie gegeben, wenn dazu keine gesetzliche Pflicht besteht. Entsprechende zusätzliche Verpflichtungen sind im Sinne eines verbesserten Verbraucherdatenschutzes wünschenswert.

Ein bisher völlig vernachlässigter Aspekt der Nutzerinformationen ist neben der Frage des „Ob" die des „Wie". Das „Zutexten" von Nutzenden in Nutzungsbestimmungen (Terms of Use) oder Datenschutzhinweisen (Privacy Policies) führt dazu, dass diese regelmäßig weggeklickt und nicht zur Kenntnis genommen, geschweige denn beachtet werden. Das Problem lässt sich mit durchdachten technisch-organisatorischen Vorkehrungen bewältigen, indem Informationen anlassbezogen kurz und knapp zur Verfügung gestellt werden. Über Hilfefenster können hinter solchen Kurzinformatio-

nen ausführliche detaillierte Erläuterungen zugänglich gemacht werden. Einheitliche technische Standards würden es den Nutzenden ermöglichen, dienstbezogen oder browserseitig Präferenzen vorzugeben, die von Kommunikationspartnern automatisch berücksichtigt werden (müssen). Datenschutzfreundliche Grundeinstellungen können hierfür eine Grundlage sein. Auch eine verbesserte AGB-Kontrolle könnte insofern eine Beseitigung bestehender Missstände bewirken.

3.7 Einwilligung

Die bestehenden Regelungen mit Einwilligungserfordernissen sind vielfältig und betreffen z. B. die Verarbeitung sensibler Daten (§ 28 Abs. 6 BDSG), bestimmte Werbenutzungen (§ 28 Abs. 3 S. 1 BDSG) oder das Setzen nicht zur Diensterbringung nötiger Cookies (Art. 5 Abs. 3 E-Privacy-Richtlinie). Die mehr als berechtigten Versuche, die Einwilligungspflichtigkeit von Werbung zu erweitern (Permission Marketing), waren schon mehrfach wegen massiver Lobbyarbeit der Wirtschaft erfolglos, etwa anlässlich der BDSG-Novelle 2009 und nun auch anlässlich der Vorlage des Entwurfs der EU-DSGVO, wo in letzter Sekunde vor der Veröffentlichung des Entwurfs strengere Vorschläge wieder gestrichen wurden.

Die formalen Anforderungen an Einwilligungen in den §§ 4a BDSG, 13 Abs. 2 TMG sind derzeit nicht konsistent. Die BDSG-Regelungen haben bisher nicht die sich aus elektronischen Einwilligungen ergebenden Notwendigkeiten aufgegriffen. Die ungenügende Berücksichtigung des AGB-Rechts bei der Einbindung von Einwilligungen ist dagegen weniger ein Regelungs- als ein Umsetzungsproblem.

Der Entwurf der EU-DSGVO bildet weitgehend die bestehende Rechtslage ab (Art. 4 Abs. 7, 9 Abs. 2 a), geht aber teilweise darüber hinaus. Dies gilt etwa für die Frage der Beweislast für das Vorliegen einer Einwilligung (Art. 7 Abs. 1) oder die Einwilligung durch bzw. für Kinder (Art. 8). Der heftig kritisierte Regelungsvorschlag des Art. 7 Abs. 3, wonach Einwilligungen ungültig sind, „wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht“, ist entgegen der heftig formulierten Kritik keine massive Beschränkung des Instruments der Einwilligung, sondern nichts anderes als die Umsetzung der Anforderung der Freiwilligkeit, was von der deutschen Verfassungsrechtsprechung anerkannt ist (BVerfG, JZ 2007, 576).

Im Sinne eines effektiven Datenschutzes wäre in diesem Zusammenhang eine konsequente Einführung des „Privacy by Default“ revolutionär, womit insbesondere technisch das Einholen von Einwilligungen für spezifische Verarbeitungen erzwungen würde. Die konkrete Formulierung im Entwurf von Art. 23 Abs. 2 S. 3 EU-DSGVO ist insofern zu eng geraten. Der zugrundeliegende Regelungsansatz besteht darin, durch Technikgestaltung Grundrechtsverträglichkeit herzustellen. Wünschenswert wäre weiterhin zumindest bei Angeboten ohne reale Wahlmöglichkeiten für die Betroffenen ein Koppelungsverbot zwischen Erbringung von Grund- und Zusatzdiensten. Weitgehend unberücksichtigt blieb bei den bisherigen Regelungsvorschlägen, dass durch technische Gestaltungen die Informationen und die Wahlmöglichkeiten für die Betroffenen verbessert werden können. Insofern gibt es in der Praxis eine Vielzahl von gezielten Maßnahmen, mit denen heute Internetdatenverarbeiter Opt-ins zu erzwingen oder zu erschleichen bzw. Opt-outs zu verhindern versuchen.

3.8 Datenschutzkontrolle

Hinsichtlich der Praxis der Datenschutzkontrolle ist im Internetbereich eine Verbesserung des Workflow und der Kooperation der Aufsichtsbehörden nötig. Diese erfolgt derzeit intuitiv und individuell bzw. aufsichtsbehördlich unterschiedlich. Zwar gibt es eine informelle Kooperation und Koordination der regionalen und nationalen Aufsichtsbehörden in nationalen, europäischen und internationalen Datenschutzkonferenzen bzw. in der Artikel-29-Datenschutzgruppe und deren Untergruppen. Doch sind die Absprachen nicht verbindlich; das Vorgehen ist wenig strukturiert.

Der Entwurf einer EU-DSGVO sieht insofern eine grundlegende Wende vor, indem Amtshilfen (Art. 55), gemeinsame Maßnahmen (Art. 56), ein kompliziertes Kohärenzverfahren mit Handlungspflichten und strengen Fristen (Art. 58, 64 ff.), eine Kommissionsabstimmung (Art. 59) und Dringlichkeitsverfahren (Art. 60, 61) normiert werden. Allerdings ist hier Kritik angebracht: Die Interventionsmöglichkeiten der EU-Kommission würden die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen. Das vorgesehene Verfahren ist zudem äußerst aufwändig und konfliktträchtig. Es bestehen deshalb Zweifel an der Umsetzbarkeit, wenn nicht eine massive Verbesserung der Ausstattung der Aufsichtsbehörden erfolgt. Dass es insofern auch einfacher und möglicherweise ebenso verbindlich geht, legt ein Vorschlag des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit dar (Caspar, ZD 2012, 555).

Unabhängig von den normativen Vorgaben sind Verbesserungen bei der Beschwerdebearbeitung durch eine Standardisierung der Kommunikation zwischen den Beteiligten, insbesondere auch unter den Aufsichtsbehörden, möglich. Eine Absprache hinsichtlich der Sprache ist nötig: In der Praxis hat sich Englisch als gemeinsame Sprache durchgesetzt; die praktischen Kompetenzen beim Personal der Aufsichtsbehörden ist insofern zumindest teilweise noch unzureichend. Solange diese Integration nicht weiter fortgeschritten ist, sind Fortbildungsprogramme und Übersetzungshilfen unvermeidlich.

Die Sanktionspraxis bei Datenschutzverstößen bleibt derzeit noch hinter den bestehenden – eingeschränkten – rechtlichen Möglichkeiten zurück. Neben förmlichen Beanstandungen sind Untersagungsverfügungen nach § 38 Abs. 5 BDSG, Bußgeldverfahren mit einer Sanktion bis zu 300.000 Euro und in einem gewissen Maße Strafverfahren von Relevanz. In unserer Rechtskultur werden selbst gezielte Datenschutzverstöße immer noch eher als Bagatellen und Kavaliersdelikte denn als Wirtschaftskriminalität angesehen. Dies mag und muss sich künftig ändern. Förderlich sind insofern die geplanten Regelungen in der EU-DSGVO, die verstärkt gerichtliche Verfahren (Art. 73 ff.), Haftungs- und Schadenersatzregeln (Art. 77), nationale Sanktionen sowie Bußgelder in der Höhe bis zu 2 % des Jahresumsatzes eines Unternehmens (Art. 79) vorsehen.

4. Vorschläge der Fraktion der Piraten

Das ULD teilt die Einschätzung des Antrags, dass Schleswig-Holstein über eine überdurchschnittliche Datenschutzkompetenz verfügt. Es sieht hierin einen bisher nicht ausgeschöpften Wirtschaftsfaktor, der durch gesetzgeberische und durch sonstige politische Maßnahmen gestärkt werden kann. Mit der Förderung unabhängiger Datenschutzforschung und der Entwicklung und Implementierung datenschutzfreundlicher Technik können Entwicklungspotenziale für einen gehobenen Arbeitsmarkt und Investitionen genutzt werden. Schleswig-Holstein verfügt über einzigartige Kom-

petenzen im Bereich der Datenschutzauditierung und –zertifizierung, die im Rahmen der derzeit stattfindenden nationalen und europäischen Bestrebungen zum Aufbau von Infrastrukturen zur Datenschutzzertifizierung eingebracht werden können.

4.1 Verantwortlichkeit von Telekommunikationsanbietern

Rechtlich ist zu unterscheiden zwischen der zivilrechtlichen, strafrechtlichen, datenschutzrechtlichen sowie sonstigen ordnungsrechtlichen Verantwortlichkeit von Telemedien- und Telekommunikationsanbietern. Angesichts der Überschneidungen und der Abgrenzungsprobleme bei Telekommunikations- und Telemedienanbietern sollte eine Vereinheitlichung der bisher getrennten Regelungen im TKG und dem TMG (sowie des BDSG, s. o. Abschnitt 3.1) angestrebt werden. Hinsichtlich der Betreiberhaftung besteht Rechtsunsicherheit, die aber durch höchstrichterliche Rechtsprechung in Deutschland zunehmend abgebaut wird. Die Rechtsprechung orientiert sich an den bisherigen Vorgaben des TMG, die als genereller Rahmen zur Definition von Verantwortlichkeiten geeignet ist.

4.2 Schutz der Meinungs- und Informationsfreiheit im Internet

Die Umsetzung des Vorschlags, Durchleitungs- und Speicherdienste zur Entfernung oder Sperrung fremder Informationen wegen angeblicher Verletzung privater Rechte nur zu verpflichten, wenn der Anspruchsteller eine entsprechende (vorläufig) vollstreckbare Gerichtsentscheidung vorlegt, hätte eine unnötige Bürokratisierung der Inhaltskontrolle im Netz zur Folge. Die Einschaltung eines Gerichtes ist zu schwerfällig und zu kosten-, zeit- und personalaufwändig. Die aktuelle Rechtslage ist aus Gründen ungeklärter Verantwortlichkeiten und Zuständigkeiten unbefriedigend. Das bisherige abgestufte Verfahren (Kenntnisgabe eines Datenschutzverstoßes gegenüber dem Anbieter mit eigener Prüf- und Handlungspflicht, Anordnungsmöglichkeiten der Datenschutzbehörden, Möglichkeit des zivil- und strafrechtlichen Vorgehens, gerichtlicher Rechtsschutz bei entsprechenden Aktivitäten) erscheint zum Ausgleich der Grundrechte auf Persönlichkeitsschutz und auf Meinungs- und Informationsfreiheit ausreichend.

Weshalb Diensteanbieter von den Kosten der erstinstanzlichen gerichtlichen Prüfung freigehalten werden sollen, erschließt sich aus dem Antrag nicht. Bei großen Anbietern (z. B. Google, Facebook) besteht hierfür keine Notwendigkeit. Die Informationsfreiheit entbindet aber auch kleine Diensteanbieter nicht davon, von sich aus bei Kenntnisnahme von Rechtsverstößen ohne Einschaltung eines Gerichtes und auf eigene Kosten tätig zu werden. Eine Zumutbarkeitsklausel könnte dazu beitragen, einen übermäßigen Aufwand bei den Anbietern zu vermeiden.

4.3 Begrenzung der „Störerhaftung“ und Ausschluss privatpolizeilicher Überwachungspflichten

Richtig ist, dass Durchleitungs- und Speicherdiensten keine Verantwortlichkeit für Inhalte auferlegt werden kann und darf, deren Kenntnisnahme diesen nicht möglich war. Wohl aber kann diesen Diensten eine nachträgliche Überprüfungs- und im Fall eines Rechtsverstoßes eine Entfernungspflicht auferlegt werden. Hierbei handelt es sich nicht um eine privatpolizeiliche Aufgabe, sondern um die Wahrnehmung der Verantwortung für einen selbst initiierten Dienst. Über die Grenzen des Zumutbaren bedarf es einer öffentlichen Debatte.

4.4 Telemediennutzungsgeheimnis

Es wäre zu begrüßen, wenn einfachgesetzlich und verfassungsrechtlich präzisiert würde, wie Telemedienanbieter mit Nutzungsdaten umgehen dürfen und unter welchen Voraussetzungen hierauf ein staatlicher Zugriff erlaubt wird. Im Hinblick auf die Gefahren bei der Nutzung dieser Daten hat die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.03.2007 die Erweiterung des Telekommunikationsgeheimnisses zu einem Mediennutzungsgeheimnis gefordert. Die bisherige rechtliche Differenzierung zwischen Nutzungs- und Inhaltsdaten bei den gesetzlichen Eingriffsvoraussetzungen ist wegen der geringeren Eingriffstiefe von Nutzungsdaten grundsätzlich gerechtfertigt. Dem Antrag ist insofern zuzustimmen, dass die derzeit bestehenden gesetzlichen Regelungen hinsichtlich des staatlichen Zugriffs auf Nutzungsdaten teilweise zu weit gehen und zu wenig differenziert sind.

4.5 Internet-Protokolladressen

Auch hinsichtlich Internet-Protokolladressen (IP-Adressen) ist der Datenschutz zu wahren. Dass es sich bei IP-Adressen um personenbeziehbare Daten handelt und insofern das Grundrecht auf informationelle Selbstbestimmung und bei dynamischen IP-Adressen zusätzlich das Telekommunikationsgeheimnis nach Art. 10 GG anwendbar sind, ist inzwischen durch die Rechtsprechung des Bundesverfassungsgerichtes klargestellt (BVerfG NJW 2012, 1422, 1427 ff., Rz. 116, 164 ff.). Deren Einordnung als Bestands- oder als Nutzungsdaten war bisher umstritten. Wegen deren Eigenheiten und insbesondere im Hinblick auf die Ausweitung des IP-Adressbestands (IPv6) ist eine eigenständige Regelung des Schutzes sowie der Zugriffsmöglichkeiten sinnvoll. Die 82. Und die 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben am 28./29.09.2011 und am 07./08.11.2012 hierzu Entschließungen gefasst.

4.6 Internet-Nutzungsprofile

Das Verbot der Erstellung von Nutzungsprofilen ohne Einwilligung des Betroffenen mit Hilfe von Cookies besteht im europäischen Recht in Art. 5 Abs. 3 E-Privacy-Richtlinie und wurde bisher nicht im nationalen Recht umgesetzt (s. o. Abschnitt 3.4). Diese Umsetzung fordert ein Beschluss der obersten Aufsichtsbehörden für den Datenschutz (Düsseldorfer Kreis) vom 24./25.11.2010). Im Internet werden zunehmend weitere Identifikatoren zur Profilbildung genutzt. Deshalb ist es zu begrüßen, dass mit Art. 20 EU-DSGVO eine materiell-rechtliche Eingrenzung vorgenommen werden soll. Hinsichtlich der Grenzziehung, wann eine Profilbildung verfassungswidrig und damit in jedem Fall unzulässig ist und wann eine informierte Einwilligung gefordert werden muss, ist eine einfachgesetzliche Präzisierung dringend erforderlich. Hierbei ist nach den Nutzungszwecken zu differenzieren, so wie dies in § 15 Abs. 3 TMG angelegt ist.

4.7 Schutz vor Ausspionieren des Nutzers durch „Spyware“, „Web-Bugs“ usw.

In Erwägungsgrund 24 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) wird ausgeführt, dass sog. „Spyware“, „Web-Bugs“ „Hidden Identifiers“ und ähnliche Instrumente, die ohne Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, nur für rechtmäßige Zwecke und mit dem Wissen der betreffenden Nutzer gestattet sein sollen. Art. 5 Abs. 1 der Richtlinie verpflichtet die Mitgliedstaaten zur gesetzlichen Sicherstellung der Vertraulichkeit der Kommunikationsdienste. Das deutsche Recht enthält im TKG, im

TMG, im BDSG und im StGB (Strafgesetzbuch) entsprechende Normen. Diese Normen mögen als unzureichend angesehen werden. Abgesehen von der erwähnten (s. o. Abschnitt 4.6), später in die Richtlinie aufgenommenen Regelung des Art. 5 Abs. 3 sind keine Normen erkennbar, deren nationale Umsetzung europarechtlich dringend geboten wären.

4.8 Transparenz von Speicherfristen

Die Information der Nutzenden über die Dauer der Aufbewahrung ihrer Daten ist eine Maßnahme zur Verbesserung der Transparenz über die Datenverarbeitung gegenüber dem Betroffenen (s. o. Abschnitt 3.6), also zur Verbesserung der informationellen Selbstbestimmung. Neben der Speicherdauer ist für den Betroffenen ebenfalls von größter Relevanz, wer verantwortliche Stelle ist und für welche Zwecke die Speicherung erfolgt (vgl. § 13 Abs. 1 TMG). Hinsichtlich der Transparenz besteht zweifellos auch ein Regelungs-, in erheblich größerem Maße aber ein Vollzugs- bzw. Praxisdefizit (s. o. Abschnitt 3.8).

4.9 Koppelungsverbot

Ein wirksames Koppelungsverbot ist tatsächlich in der Lage, die Freiwilligkeit von Einwilligungen sicherzustellen und dem Betroffenen ein Instrument zum Umsetzen des Grundsatzes der Datensparsamkeit zu geben, indem ihm unabhängig von einem Grundnutzungsvertrag die Nutzung einzelner Anwendungen pseudonym oder anonym möglich gemacht wird (s. o. Abschnitt 3.7). Gemäß § 13 Abs. 6 TMG muss ein Diensteanbieter schon heute „die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren." Diese klare Regelung wird von vielen Diensteanbietern bisher missachtet (vgl. z.B. Presseerklärung ULD v. 17.12.2012, ULD erlässt Verfügungen gegen Facebook wegen Klarnamenpflicht). Es besteht also auch insofern eher ein Vollzugs- als ein Regelungsproblem.

4.10 Schutz vor unangemessenen Datenverarbeitungs-Einwilligungsklauseln

Einwilligungsklauseln unterliegen schon derzeit gemäß §§ 305 BGB der gerichtlichen Angemessenheitskontrolle. Klagebefugt sind insofern auch heute schon Verbraucherschutzverbände, da die AGB-Kontrolle – anders als bisher die sonstige Datenschutzkontrolle – unzweifelhaft dem Verbraucherrecht zugeordnet wird. Wegen der insofern äußerst zurückhaltenden Rechtsprechung wäre es wünschenswert, wenn gesetzlich klargestellt würde, dass Verstöße gegen Regelungen des Datenschutzes für Verbraucherinnen und Verbraucher sowie durch Verbraucherschutzklagen sanktioniert werden können, so wie dies in Art. 73 Abs. 2, 3, 76 Abs. 1 Entwurf EU-DSGVO vorgesehen ist. Die deutsche Rechtsprechung ist insofern widersprüchlich (dafür OLG Karlsruhe, NJW 2012, 3312; OLG Köln, CR 2011, 680; dagegen OLG München, MMR 2012, 317).

Für Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Thilo Weichert