Projektgruppe „Datenschutz“

2.3. Datenschutz im nicht-öffentlichen Bereich (STAND: 22.3.)

Streitige Passagen sind kursiv gefasst.

2.3.1 Datennutzung als Bestandteil innovativer Dienste

Viele im Internet angebotene Dienste gehen auf Grund technischer Gegebenheiten mit einer Erhebung und Verarbeitung von Daten, in der Regel auch personenbezogener Daten, einher. Auf diese Art und Weise sind die Personalisierbarkeit und Interaktivität von Diensten im Internet realisierbar. Dienste können umso stärker an Interessen und Vorlieben ihrer Nutzer angepasst werden, je mehr Daten über das Verhalten der Nutzer verwertet werden. Auf diese Weise können die Anbieter auch möglichst passgenaue Werbung anbieten.

Strenge Datenschutzvorschriften können die Entwicklung neuer Anwendungen erschweren oder sie unbequemer in der Nutzung machen. Andererseits können strengere Vorschriften auch geeignet sein, Verbrauchervertrauen aufzubauen, das die Nutzerzahlen erhöhen kann.

Eine Missachtung der berechtigten Datenschutzerwartungen der Nutzer kann auch zu einer Gegenreaktion und Ablehnung eines Dienstes führen. Letztlich setzen Geschäftsmodelle, die auf der Verwendung von personenbezogenen Daten beruhen, immer auch eine Akzeptanz des Nutzers voraus. Hieraus kann sich ein Selbstkorrektiv in der Entwicklung von Diensten ergeben, solange sichergestellt ist, dass die Nutzer über Art und Umfang der vorgenommenen Datenverarbeitung informiert sind.

2.3.1.1 Datenschutz in der Informations- und Kommunikationsgesellschaft: Zum Spannungsverhältnis und zum Gebot der Abwägung zwischen Persönlichkeitsrechten und Kommunikationsgrundrechten

Dass das allgemeine Persönlichkeitsrecht in Konflikt geraten kann mit der Meinungsfreiheit, ist allgemein bekannt und Gegenstand des Äußerungsrechts. Die Berichterstattung durch die Medien (Presse und Rundfunk), aber auch die Wahrnehmung der Meinungsfreiheit durch den Einzelnen kann Persönlichkeitsrechte verletzen. Es handelt sich um das klassische Spannungsverhältnis zwischen Persönlichkeitsrechten und Meinungsfreiheit, und zwar unabhängig davon, ob die Meinungsfreiheit individuell vom Einzelnen oder durch Medien wahrgenommen wird.

bis Z. 260: Textvorschlag streitig.

Alternativvorschlag folgt ab Z. 266.

In der Informations- und Kommunikationsordnung des Internet gewinnt dieses Spannungsverhältnis erheblich an Bedeutung. Dies liegt vor allem daran, dass der Einzelne im Internet ohne nennenswerte Zugangsschranken an der (Massen-)Kommunikation mitwirken kann. Die starren Grenzen zwischen Medien und Rezipienten verschwimmen.

Die moderne Internetkommunikation wirft eine Vielzahl von Fragen auf, die u.a. die Zuordnung bestimmter Dienste zu den grundrechtlich geschützten Kommunikationsfreiheiten betreffen. Weil diese Zuordnungsfragen noch nicht geklärt sind, bereitet es oftmals Schwierigkeiten, die im Internet auftretenden Probleme als grundrechtliche Konflikte zwischen Persönlichkeitsgrundrechten und Kommunikationsgrundrechten wahrzunehmen. Recht einfach liegen die Dinge bei Blogs und sonstigen meinungsbildenden Portalen („Spick-mich“ etc.), die aufgrund dieser meinungsbildenden Funktion sich im Schutzbereich der Kommunikationsgrundrechte bewegen. Es handelt sich letztlich um den klassischen Konflikt zwischen Meinungsäußerungsfreiheit und dem allgemeinen Persönlichkeitsrecht des Betroffenen.

Besondere Zuordnungsprobleme ergeben sich jedoch etwa bei solchen Diensten („Informationsintermediäre“), die im Gegensatz zu klassischen Medien Informationen nicht nach meinungsbezogenen, publizistischen Gesichtspunkten zusammenstellen und veröffentlichen, sondern nach „meinungsneutralen“ formalen Kriterien Informationen zusammentragen, speichern und verbreiten. So bereitet beispielsweise die rechtliche Einordnung von Suchmaschinen erhebliche rechtliche Schwierigkeiten, auch wenn sich ihre Input-Funktion aus allgemein zugänglichen Quellen speist und die Benutzung von Suchmaschinen durch User als Ausübung der grundrechtlich geschützten Informationsfreiheit (Art. 5 Abs. 1 Satz 1 Alt. 2 GG, Art. 10 Abs. 1 Satz 2 EMRK, Art. 11 Abs. 1 Satz 2 GRC) zu qualifizieren ist. Ungeachtet dieser grundrechtlichen Zuordnungsprobleme steht in jedem Fall fest, dass solche Suchmaschinen aus der Informations- und Kommunikationsordnung des Internet nicht wegzudenken und für die Funktionsfähigkeit der modernen Informationsgesellschaft schlechthin unverzichtbar sind. Sofern solche Suchmaschinen personenbezogene Daten des Einzelnen zusammentragen, speichern und ein mehr oder weniger umfangreiches Persönlichkeits- oder Bewegungsprofil des Betroffenen auf Abruf zur Verfügung stellen, handelt es sich um einen Konflikt zwischen Kommunikationsgrundrechten und Persönlichkeitsrechten. Auch insoweit gilt es, durch Abwägung die einander widerstreitenden Güter im Sinne praktischer Konkordanz zu einem wechselseitig möglichst schonenden Ausgleich zu bringen.

Als weiteres Beispiel für die Schwierigkeiten, neue Internetdienste den klassischen Kommunikationsgrundrechten zuzuordnen, seien soziale Netzwerke genannt. Gleichwohl würde es die grundrechtliche Perspektive verengen, wenn man soziale Netzwerke ausschließ-

lich aus dem Blickwinkel des verfassungsrechtlich geschuldeten Schutzes des Grundrechts der informationellen Selbstbestimmung betrachtete.

Viele Nutzer von Sozialen Netzwerken und anderen Plattformen geben heute eine Vielzahl von Daten preis, darunter auch sensible Daten wie die religiöse oder politische Überzeugung und die sexuelle Orientierung. Die bewusste Verwendung und Offenbarung der eigenen Daten ist nicht pauschal zu kritisieren oder gar zu verurteilen. Sie ist vielmehr die Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung, also die Ausübung grundrechtlich geschützter Freiheit.

Ungeklärt ist, ob eine solche Preisgabe personenbezogener Daten darüber hinaus auch Ausdruck des Grundrechts der Meinungsfreiheit ist. In diesem Zusammenhang ist zunächst festzuhalten, dass jedenfalls die der Veröffentlichung personenbezogener Daten in entsprechenden Datenbanken sozialer Netzwerke („Profile“ ö.ä.) nachgelagerte Kommunikation zwischen „Freunden“ oder sonstigen Teilnehmern des Kommunikationsnetzwerkes auch der individuellen und öffentlichen Meinungsbildung dient und daher kommunikationsgrundrechtlich geschützt ist. Für den Schutz oder die Werthaltigkeit der Kommunikationsordnung kommt es auf den privaten bzw. nichtprivaten Charakter der Informationen prinzipiell nicht an. Auch die Offenbarung privater Informationen dient dem Kommunikationsprozess. War die Berichterstattung über Privates (insbesondere von Prominenten) in der Vergangenheit regelmäßig den Medien vorbehalten, die sich insoweit auf die grundrechtlich geschützte Presse- bzw. Rundfunkfreiheit berufen können [Fußnote: Deutlich zuletzt BVerfGE 120, 180, 205: „Der Schutzbereich der Pressefreiheit umfasst auch unterhaltende Beiträge über das Privat- oder Alltagsleben von Prominenten und ihres sozialen Umfelds, insbesondere der ihnen nahestehenden Personen.“; siehe auch BVerfGE 101, 361, 389 ff.]*, kann nunmehr der Einzelne im Internet Privates offenbaren. Diese Form der Freiheitsbetätigung beruht auf doppeltem Grundrechtsboden: Sie ist Ausdruck des Grundrechts auf informationelle Selbstbestimmung und zugleich Wahrnehmung der grundrechtlich geschützten Meinungsfreiheit. Der Schutz der Kommunikationsordnung ist umfassend und unteilbar. Er lässt sich nicht zwischen schutzbedürftigen, weniger schutzbedürftigen oder schutzlosen Informationen unterteilen. Dies gilt insbesondere unter den Bedingungen der modernen Internetkommunikation, in der – wie das Beispiel sozialer Netzwerke zeigt – die Grenze zwischen privaten und nichtprivaten Informationen zunehmend verschwimmt.*

Hieraus erhellt, dass die Veröffentlichung personenbezogener Daten in entsprechenden Datenbanken sozialer Netzwerke („Profile“ ö.ä.) als solche nicht nur Ausfluss des Grundrechts der informationellen Selbstbestimmung, sondern auch der Meinungsfreiheit ist. Zwar hat das Bundesverfassungsgericht im seinem Volkszählungs-

urteil die Verpflichtung zu Angaben im Rahmen statistischer Erhebungen nicht an der (negativen) Meinungsäußerungsfreiheit des Art. 5 Abs. 1 Satz 1 GG gemessen, weil solche Angaben nicht durch Elemente der Stellungnahme, des Dafürhaltens und des Meinens gekennzeichnet sind. [Fußnote: Vgl. BVerfGE 65, 1, 40 f.] *Anders liegen die Dinge indes bei der Veröffentlichung personenbezogener Daten in sozialen Netzwerken. Zum einen beruhen solche Daten nicht nur auf „nackten“ Tatsachen, sondern oftmals auf persönlichen Einschätzungen, denen Wertungen zugrunde liegen (zum Beispiel: Selbsteinschätzung der politischen Überzeugung in sozialen Netzwerken, „Gefällt-mir“-Button). Und zum anderen ist die Veröffentlichung von personenbezogenen Tatsachen, die für sich genommen keine „Meinungen“ sind, Voraussetzung für den Aufbau entsprechender Kommunikationsnetzwerke, in denen sich die grundrechtlich geschützte Kommunikation vollzieht. Wegen dieses engen funktionalen Zusammenhangs wird man die Veröffentlichung auch solcher Daten als Ausdruck der Meinungsäußerungsfreiheit qualifizieren können. Das gilt auch deshalb, weil die Preisgabe personenbezogener Daten im Rahmen der Kommunikation zwischen „Freunden“ oder sonstigen Teilnehmern des Kommunikationsnetzwerkes dem Schutz der Meinungsfreiheit unterfällt.*

Eine pauschale Implementierung der datenschutzrechtlichen Grundsätze überall dort, wo grundrechtlich geschützte Kommunikationsinteressen betroffen sind, würde das verfassungsrechtliche Spannungsverhältnis zwischen dem grundrechtlich gebotenen Persönlichkeitsschutz einerseits und den Kommunikationsgrundrechten andererseits verfehlen. Von Verfassungs wegen gilt es, die einander widerstreitenden Güter im Sinne praktischer Konkordanz zu einem wechselseitig möglichst schonenden Ausgleich zu bringen.

Im Folgenden seien einige Abwägungsmaßstäbe genannt:

- *Ob und in welchem Umfang der (volljährige) Einzelne personenbezogene Daten im Internet offenbart, ist prinzipiell seine Entscheidung. Der Staat hat kraft seiner ihm obliegenden Schutzpflichten allein – etwa durch Auferlegung entsprechender Transparenz- und Informationspflichten der Anbieter sozialer Netzwerke – dafür Sorge zu tragen, dass der Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann. Die grundrechtliche Schutzpflicht des Staates darf indes nicht in einen „Datenschutz vor sich selbst“ umschlagen. Nicht der Staat, sondern der Einzelne hat in Wahrnehmung seines Grundrechts auf informationelle Selbstbestimmung darüber zu entscheiden, ob und in welchem Umfang er personenbezogene Daten im Internet veröffentlicht und wem er diese öffentlich zugänglich macht (Prinzip der Eigenverantwortlichkeit). Im Rahmen der Abwägung ist dem möglicherweise ganz unterschiedlichen Schutzbedürfnis der*

verschiedenen betroffenen Personengruppen Rechnung zu tragen. Neben den individuellen Interessen des Einzelnen sind auch die Informationsinteressen der Allgemeinheit zu berücksichtigen. Alle diese Aspekte sind zu beachten, wenn der Gesetzgeber etwa vor der Entscheidung zwischen Opt-in- oder Opt-out-Regelungen steht.

- *Letztlich muss der Einzelne autonom entscheiden, ob und in welchem Umfang und zu welchem Zweck er personenbezogene Daten in sozialen Netzwerken preisgibt und auf diese Weise nicht nur von seinem Grundrecht auf informationelle Selbstbestimmung, sondern auch von seinem Grundrecht der Meinungsfreiheit Gebrauch macht. Die Entscheidung über die Preisgabe personenbezogener Daten und über die Kommunikation mit anderen in sozialen Netzwerken obliegt allein dem Einzelnen. Die besondere Problematik besteht indes darin, dass es „den“ User nicht gibt. Um nur ein Beispiel zu nennen: Während der eine weniger Wert auf die Zweckbestimmung der erhobenen Daten legt, weil sich im Zeitpunkt der Informationspreisgabe die künftigen Verwendungszwecke noch absehen lassen und weil er in der unterschiedlichen Verwendung seiner Daten gerade einen Vorteil sieht, ist für den anderen genau eine solche exakte Zweckbestimmung unverzichtbar. Hier ergeben sich in regulatorischer Hinsicht erhebliche Probleme.*

- *Für die Lösung dieses Konflikts ist insbesondere von Bedeutung, mit welcher Intensität in das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird. Eingriffe in den Kernbereich des Grundrechts bzw. in die Intimsphäre sind grundsätzlich unzulässig. Die Veröffentlichung von Daten aus dem Kernbereich privater Lebensgestaltung und Ehre oder der Intimsphäre und die Veröffentlichung aussagekräftiger Persönlichkeitsprofile durch einen Anderen sind schon zum Schutz der Menschenwürde generell unzulässig. Im Bereich der Privatsphäre wird zum Schutz des Grundrechts auf informationelle Selbstbestimmung regelmäßig eine ausdrückliche Zustimmung (Opt-In) erforderlich sein. Im äußeren Bereich der Sozialsphäre kann hingegen eine ausdrückliche Ablehnung (Opt-Out) ausreichend sein, um die Bedeutung der Kommunikationsfreiheit hinreichend zu berücksichtigen.*

- *Je mittelbarer der Personenbezug von Daten ist, desto weniger gewichtig ist das Recht auf informationelle Selbstbestimmung im Rahmen des erforderlichen Güterausgleichs. Weiter kommt es bei der Gewichtung darauf*

an, ob das Recht auf informationelle Selbstbestimmung in der Intim-, Privat- oder Sozialsphäre betroffen ist.

- *Nicht nur unter den Bedingungen der modernen Informations- und Kommunikationsordnung muss sich der Einzelne auch der Kontrolle und Kritik durch die Gesellschaft stellen. In ständiger Rechtsprechung weist das Bundesverfassungsgericht darauf hin, dass das allgemeine Persönlichkeitsrecht (im Bereich der Sozialsphäre) dem Träger keinen Anspruch darauf verleiht, nur so in der Öffentlichkeit dargestellt zu werden, wie er sich selber sieht oder gesehen werden möchte. [Fußnote: Vgl. nur BVerfGE 82, 236, 269; 97, 391, 403; 99, 185, 194; 101, 361, 380.] Die Grenzen zulässiger Berichterstattung sind erst bei schwerwiegenden Auswirkungen auf das Persönlichkeitsrecht überschritten, also dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu besorgen sind, wie es der Bundesgerichtshof kürzlich in der sogenannten Spickmich-Entscheidung nochmals klargestellt hat. [Fußnote: BGH NJW 2009, 2888, 2892.]*

- *Sofern personenbezogene Daten aus allgemein zugänglichen Quellen (Internet ö.ä.) stammen und deshalb dem besonderen Schutz des Grundrechts der Informationsfreiheit (Art. 5 Abs. 1 Satz 1 Alt. 2 GG, Art. 10 Abs. 1 Satz 2 EMRK, Art. 11 Abs. 1 Satz 2 GRC) unterfallen und nicht der Kernbereich des informationellen Selbstbestimmungsrechts bzw. die Intimsphäre betroffen sind, ist die Erhebung, Speicherung und Verwendung personenbezogener Daten zulässig, es sei denn, dass das Betroffeneninteresse offensichtlich überwiegt. Dieses Wertungsmodell könnte als Leitprinzip für die Ausgestaltung künftiger Konfliktsituationen dienen.*

Sofern der Einzelne in Kontakt oder Kommunikation mit anderen tritt (Sozialsphäre) und damit die persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt, muss er sich – im Interesse umfassender Kommunikation – Beschränkungen seines allgemeinen Persönlichkeitsrechts und seines Rechts auf informationelle Selbstbestimmung gefallen lassen. Insbesondere hat er keinen Anspruch darauf, in der Öffentlichkeit nur so dargestellt zu werden, wie er möchte.

Alternativer Textvorschlag

Alternativer Textvorschlag ebenfalls streitig.

Die Besonderheit des Schutz“gegenstandes“

Weil Information und Kommunikation Grundbedingungen u.a. der Persönlichkeitsbildung und –darstellung sind, gehen eigentumsanaloge Konzeptionen informationeller Selbstbestimmung fehl. Informationen entstehen aus Daten erst in konkreten Verwendungszusammenhängen, wobei der Konstruktion des Verwenders überragende Bedeutung zukommt. Deshalb sind Vorstellungen eines eigentumsanalogen Informationsbeherrschungsrechts von vornherein schief. Schutzkonstruktionen müssen deshalb stets mitberücksichtigen, dass sich kommunikative Selbstbestimmung in konkreten gesellschaftlichen Zusammenhängen entfaltet, die Voraussetzung für dessen Geltendmachung sind. Es geht also um ein Recht auf Schaffung und Erhalt der Bedingungen, unter denen eine freiheitliche Darstellung der Persönlichkeit möglich ist. Artikel 2 Absatz 1 GG formuliert damit eine Grundbedingung freier Kommunikationsverfassung. Es geht um die Verpflichtung des Gesetzgebers, den Kommunikationsprozess so abzusichern, dass die kommunikative Selbstbestimmung der Bürger möglich bleibt. Das Grundrecht schützt dabei vor dem Staat wie anderweitigen sozialen Institutionen gleichermaßen. Die Ebene freiwilliger Preisgabe personenbezogener Informationen durch Grundrechtsträger selbst kann bereits als Ausübung allgemeiner Handlungsfreiheit angesehen werden und betrifft ersichtlich nicht das Schutzprogramm des Rechts auf informationelle Selbstbestimmung. Mit diesem wird die kommunikative Teilhabe der Einzelnen an kommunikativen Prozessen gesichert. Deshalb müssen Verarbeitungen für Betroffene transparent sein, Gestaltungsrechte eingeräumt werden, aber auch und vor allem die Verwendungszusammenhänge beim Verarbeiter selbst und damit die Bildung der Informationen reguliert werden. Dazu braucht es objektiv-rechtliche Gehalte wie z.B. aufgabenbezogene Erhebungs- und Verarbeitungregeln.

Entgegenstehende Grundrechte der Datenverarbeiter

Einschränkungen dieser Regelungen zum Schutz informationeller Selbstbestimmung sind nur insoweit zulässig, als sie im überwiegenden Allgemeininteresse liegen (BVerfGE 65, 1 (43 f.). So kann es zu Einschränkungen der informationellen Selbstbestimmung kommen, wenn Grundrechte miteinander kollidieren. In Betracht kommt etwa für die Phase der Erhebung von Daten das Grundrecht der Informationsfreiheit nach Artikel 5 Absatz 1 Satz 1 GG sowie für die Übermittlung das Grundrecht der Meinungsfreiheit des Art. 5 Abs. 1 Satz 1 GG. Allerdings enden diese dort, wo das berechtigte Interesse oder das Recht auf informationelle Selbstbestimmung eines anderen beginnt. Insbesondere begründet die Informations-

freiheit keinen Anspruch für das Marketing, sich über das Recht auf informationelle Selbstbestimmung hinwegzusetzen (so z.B. Simitis, Kommentar zum BDSG, 5. Auflage, § 1 Rn. 91). Regelungen, die betroffenen Personen die Autonomie über die Eröffnung von Informationsquellen sichern sollen, stellen keinen Eingriff in die Informationsfreiheit dar (so z.B. Schulz, Verwaltung 1999, S. 149). Bei der Meinungsfreiheit ist zu bedenken, dass sie sich auf die individuelle Meinungsbildung und den individuellen Meinungsaustausch beschränkt, nicht alle Phasen und Verabeitungsformen umfasst und durch allgemeine Gesetze wie die Datenschutzgesetze, die sich nicht auf bestimmte Meinungen beziehen, eingeschränkt werden kann. Gesetzliche Regelungen, die den Auftrag zum Schutz der informationellen Selbstbestimmung risikobezogen umsetzen, sind deshalb auch im Geltungsbereich des Artikel 5 Absatz 1 Satz 1 GG zulässig, wenn sie die besondere Bedeutung der Informations- und Meinungsäußerungsfreiheit berücksichtigen. Artikel 5 Abs. 1 Satz 1 GG kann ist auch keine „allgemeine Kommunikationsverfassung“ zu entnehmen, die personenbezogene Daten pauschal dem Schutz des Grundgesetzes entzieht, nur weil deren Veröffentlichung einem wie auch immer gearteten „Kommunikationsprozess“ des Internet dienlich sein können.

Weiter in Betracht kommen die Unternehmerfreiheit, soweit sie als Bestandteil der Freiheit der Berufsausübung anerkannt ist. Doch an diese können regelmäßig Anforderungen gestellt werden, wenn sie vernünftigen Gründen des Allgemeinwohls entsprechen. Gesetzliche Regelungen, die die Datenverarbeitung risikoorientierten Anforderungen unterwerfen sind daher grundsätzlich mit Artikel 12 Abs. 1 GG vereinbar (vgl. nur Schulz, a.a.O., S. 148). Soweit das Grundrecht auf Eigentum gegen Regelungen zum Schutz personenbezogener Datenverarbeitung angeführt wird, gilt, dass der Schutz des Eigentums sich nur auf das Erworbene, nicht jedoch auf die Tätigkeit des Erwerbens selbst bezieht. Damit verbleiben allenfalls wenige denkbare Fallgestaltungen möglicher Kollisionen. Zum Teil wird die wirtschaftliche Betätigungsfreiheit als Unterfall der allgemeinen Handlungsfreiheit nach Artikel 2 Abs. 1 GG als eigentliche Grundlage des Grundrechtsschutzes der Datenverarbeiter angesehen. Ausgangspunkt des Gesetzgbers müsse die Freiheit aller Datenverarbeitung, nicht ihre Beschränkung sein. Diese Auffassung, die sich darauf gründet, dass ein manifestierter Geheimhaltungswille vorliege oder gesetzlich anerkannt sei, hat sich nicht durchgesetzt. Stattdessen wurde mit dem Recht auf informationelle Selbstbestimmung ein Entscheidungsvorrang der betroffenen Person über Daten, die sich auf ihre sachlichen und persönlihcen Verhältnisse beziehen, geschaffen. Die allgemeine Handlungsfreiheit steht zudem unter dem Vorbehalt der verfassungsmäßigen Ordnung und der Rechte Dritter. Sie endet regelmäßig dort, wo das informationelle Selbstbestimmungsrecht eines anderen beginnt.

Nutzerprofilierung und veröffentlichte Daten

Vor diesem Hintergrund sowie den konkreten Regelungen der Datenschutzgesetze sind deshalb die jeweils ganz unterschiedlich gelagerten Problemfälle in Kontext des Internet zu bearbeiten. Im Mittelpunkt stehen dabei immer wieder Fälle der Veröffentlichung von personenbezogenen Daten im Internet. Dabei ist jeweils sorgfältig zu differenzieren, ob etwa Datenverarbeitungen im Verhältnis von kommerziellen Anbietern (z.B. Plattformbetreiber wie etwa soziale Netzwerke; Suchmaschinen) zu betroffenen Bürgern oder etwa im Verhältnis von Bürgern untereinander gemeint sind (sog. Web 2.0) und etwa zu welchen Zwecken die Veröffentlichungen mit welchen möglichen Risiken erfolgen. So bietet etwa die sog. Spickmich-Entscheidung des BGH eine erste Klärung hinsichtlich der Verantwortlichkeit der Betreiber von Bewertungsplattformen selbst im Umgang mit den ihnen anvertrauten personenbezogenen Daten. Im Ergebnis wird das Bundesdatenschutzgesetz für anwendbar erklärt, allerdings angesichts dieser neuen Verarbeitungsform die einschlägige Gesetzesbestimmung verfassungskonform ausgelegt. Der Fall offenbart damit einen konkreten Reformbedarf der Bestimmungen des BDSG.

Hinsichtlich solcher Intermediäre wie den Suchmaschinen sowie den sozialen Netzwerken liegt die Besonderheit dieser Dienste gerade darin, dass sie einerseits für die Nutzbarkeit des Internets geradezu überragend wichtige Angebote eröffnen, die Information und Kommunikation deutlich erleichtern. Zugleich basiert ihr Erfolg allerdings auf der Verarbeitung aller erhältlichen personenbezogenen Daten, welche zu Marketingzwecken systematisch und umfassend ausgewertet und verwendet werden. Die dabei veröffentlichten personenbezogenen Informationen sind in der Dimension des Internets weltweit und oftmals dauerhaft für jeden und jede Nutzerin verfügbar. Hinsichtlich der im Hintergrund entstehenden Nutzerprofilinformationen entstehen ganz neuartige Informationszusammenhänge zu Einzelpersonen, deren Umfang weitestgehend intransparent bleibt.

Zutreffend wird mit Blick auf Dienste des Mitmach-Web wie den sozialen Netzwerken, Blogs etc. konstatiert, dass heute Einzelne nahezu problemlos durch Webveröffentlichungen selbst Massenkommunikation betreiben können. Wenn diese Beiträge eine meinungsbildende Funktion haben, ergeben sich auch hier Grundrechtskollisionen, die besondere Probleme hinsichtlich der Anwendbarkeit und der Durchsetzbarkeit der Datenschutzrechte der Bürger untereinander aufweisen. Hier wird allgemein ein erheblicher Regelungsbedarf konstatiert, der bereits auch zu konkreten Gesetzesvorschlägen geführt hat.

2.3.1.2 Geschäftsmodelle von Internet-Diensten / Online-Werbung

Das Internet besteht sowohl aus Inhalten und Diensten, die allen Nutzern kostenlos zur Verfügung stehen, als auch aus Inhalten und Diensten, die lediglich gegen Entgelt abgerufen werden können (= „Paid Content“ bzw. „Paid Services“). Dabei ist die überwiegende Zahl der Inhalte derzeit entgeltfrei abrufbar. Viele dieser unmittelbar kostenfreien Inhalte und Dienste werden kommerziell erbracht, wobei Online-Werbung nicht nur der Refinanzierung der Kosten dienen kann, sondern auch der Erzielung von Gewinnen. Aber auch nicht-kommerzielle Angebote setzen Online-Werbung ein, um zumindest einen Teil der mit der Bereitstellung verbundenen Kosten zu decken.

Online-Werbung kann damit die Bereitstellung bestimmter Angebote ermöglichen und einen Beitrag zur Vielfalt im Wettbewerb leisten. Auch im Online-Bereich ist es beispielsweise über Bannerwerbung möglich, Werbung ohne die Erhebung von Nutzerdaten zu schalten.

Gegenüber anderen Werbeformen bietet die zielgerichteten Online-Werbung allerdings aufgrund der technisch angelegten individualisierten Bereitstellung von Inhalten für den Nutzer auch die Möglichkeit, auf die vermutlichen individuellen Interessen der Nutzer abgestimmte Informationen und Werbebotschaften zu liefern. Hierdurch steigt die Wahrscheinlichkeit, dass ein Werbeinhalt vom Empfänger als relevant erachtet wird. Dies erhöht wiederum die erzielbaren Gewinne je angezeigter Werbung. Damit kann sich auch die Menge der ungezielten Werbung reduzieren, die notwendig ist, um eine Finanzierung des Web-Angebots zu erreichen. Es besteht dabei aber keine Garantie, dass tatsächlich weniger Werbung eingesetzt wird.

Es gibt eine Vielzahl von Technologien und Vorgehensweisen (Algorithmen), mit deren Hilfe bei verhaltensbezogener Werbung („Behavourial Advertising“) eine Vorhersage über das vermutliche Interesse des Werbeadressaten getroffen wird. Die Methoden nutzen in sehr verschiedener Weise und in sehr unterschiedlichem Umfang und Intensität Daten aus der aktuellen bzw. vorangegangenen Internetnutzung des Werbeempfängers.

Allerdings muss verhaltensbezogene Werbung nicht unbedingt darauf beruhen, dass Informationen über das Surfverhalten der Nutzer dauerhaft gespeichert werden. Sie kann auch über eine anonymisierte Zuordnung zu Interessenkategorien realisiert werden, die auf einer bestimmten Art der Verwendung der Cookie-Technik basiert. Diese Cookies kann der Nutzer gegebenenfalls manuell wieder ent-

fernen. Allerdings gibt es keine Möglichkeit auszuschließen, dass Webseiten, die Cookies auf dem Rechner des Nutzers ablegen, bei diesem Nutzer auch Daten erheben.

In allen Fällen, in denen nutzungsbezogene Daten verarbeitet werden, muss es allerdings eine zentrale Voraussetzung sein, dass der Nutzer Informationen über die vorgenommene Verwendung erhält und ihm eine Wahlmöglichkeit zusteht, mit der er den Einsatz solcher individualisierender Werbetechniken beeinflussen kann.

Absatz streitig.

Inwieweit eine vorab zu erteilende Einwilligung erforderlich ist, hängt wesentlich von der Art der Daten, der Datenerhebung und –nutzung und der Schwere des damit verbundenen Eingriffs in das informationelle Selbstbestimmungsrecht ab. So ist zu unterscheiden, ob Nutzungsdaten nur aggregiert verarbeitet und dabei pseudonymisiert bzw. anonymisiert werden oder aber bezogen oder zumindest beziehbar auf eine spezifische Person sind und auch zu diesem Zwecke eingesetzt werden.

Ebenso ist es relevant, ob die Datenverarbeitung durch den Anbieter der Webseite selbst erfolgt oder ob die Daten durch an dem Leistungsverhältnis gar nicht beteiligte Dritte erhoben und verwendet werden. Während die Datenverarbeitung im ersten Fall auf Basis der vom Webseitenanbieter bereitgestellten Datenschutzerklärung transparent gemacht werden kann und der Nutzer die Möglichkeit erhält, gegenüber einem klar identifizierbaren Ansprechpartner von seinem Wahlrecht hinsichtlich der Datenerhebung und –verwendung Gebrauch zu machen, ist im letzteren Fall die geforderte Transparenz für den Nutzer oft nicht mehr gegeben, und es fehlt ihm häufig die Möglichkeit, Einfluss auf die Datenerhebung und –verwendung zu nehmen.

Die Kontrolle des Nutzers wird auch davon beeinflusst, ob die Daten – etwa in Form von Cookies – auf seinem Gerät und damit in seinem Herrschaftsbereich gespeichert werden, so dass er beispielsweise über Browser-Einstellungen einwirken kann, oder ob gesammelte Daten zentral und damit seinem Zugriff entzogen gespeichert werden.

Schließlich können besondere Umstände einen besonders schwerwiegenden Eingriff darstellen und deshalb auch unzulässig sein. Dies ist etwa der Fall, wenn für die zielgerichtete Ansprache (Targeting) auch sensible Daten verwendet werden, wie etwa Informationen über Gesundheit oder sexuelle Orientierung. Problematisch ist auch, wenn Daten aus besonders geschützten Bereichen wie etwa der Individualkommunikation gewonnen werden, etwa durch die Analyse von E-Mail-Inhalten. Besondere Fragen wirft auch die übergreifende Nachverfolgung („Tracking“) des Surfverhaltens einzelner Nutzer über eine Vielzahl von Webangeboten hinweg auf, da hier nicht nur Informationen bezüglich der Nutzung

eines bestimmten Angebots gewonnen, sondern ein umfassendes Bewegungsprofil der Nutzer im Netz gewonnen werden.

2.3.1.3 Bildung von Persönlichkeitsprofilen / Tracking über die Grenzen einzelner Webseiten hinweg

Personenbezogene Daten können in unterschiedlicher Intensität Aussagen über Personen und deren soziale Beziehungen enthalten. Je nach Umfang und Qualität der Daten lassen sich Daten durch Zusammenführung aus unterschiedlichen sozialen Zusammenhängen zu Persönlichkeitsbildern verdichten. Dem entspricht, beispielsweise übertragen auf das Internet, die Zusammenführung von Daten über das Nutzungsverhalten von unterschiedlichen Webangeboten. Entsprechende Geschäftsmodelle reichen von der Zusammenführung von Nutzungsdaten innerhalb des Webangebotes eines einzelnen Anbieters bis hin zu komplexen webseitenübergreifenden Kooperationen unterschiedlicher Anbieter, oftmals unter Einschaltung von Dienstleistern (z. B. doubleclick; Facebook-Like-Button). Aufgegriffen wurde der Begriff u.a. vom Bundesverfassungsgericht im Volkszählungsurteil. Das Gericht betont das Verbot von Profilbildungen, die geeignet sind, die Persönlichkeit von Menschen vollständig oder nur teilweise abzubilden. Befürchtet wird, dass die in öffentlicher Hand und zu ganz unterschiedlichen Zwecken gesammelten Datenbestände zusammengeführt werden und ein nahezu lückenloses Bild der Bürger zum Zweck der Herrschaftsausübung schaffen könnten. Als Risiko im Kontext der Privatwirtschaft gilt der Missbrauch entsprechend reichhaltiger Profile und die oftmals intransparent bleibende Beeinflussung der wirtschaftlichen Entscheidungen der Verbraucher durch gezielte Werbung. In Folge der technischen Entwicklung spielen Fragen der Profilbildung nicht nur im öffentlichen Bereich (z.B. Rasterfahndungen), sondern auch im nicht-öffentlichen Bereich eine große Rolle. Dabei ist zwischen ganz unterschiedlichen Arten von Profilen und deren Nutzung zu unterscheiden.

Im Internet sind für bestimmte Nutzergruppen angepasste oder sogar besonders detaillierte und personalisierte Angebote möglich und gängig. Seit Jahren werden Auswertungstools verwendet, mit denen das Nutzerverhalten auf einer Website statistisch erfasst und analysiert werden kann. Die dabei untersuchten Daten werden häufig nur aggregiert und/oder pseudonymisiert ausgewertet. Ob es sich dabei um anonyme und damit nicht mehr dem Anwendungsbereich der Datenschutzgesetze unterfallende Profildaten handelt, ist jedoch umstritten. In einigen Fällen wird allerdings durch die Einbeziehung von personenbezogenen Webangeboten (soziale

Netzwerke; Mailangebote) insgesamt eine Personenbeziehbarkeit des Profils herbeigeführt. Es besteht Einigkeit, dass solche Nutzungsprofile bei Einhaltung bestimmter Vorgaben, zulässig sind. [Fußnote: Vgl. Beschluss des Düsseldorfer Kreises vom 26. November 2009: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile] Anhand dieser Nutzungsprofile können Websites z.B. nutzerfreundlicher gestaltet werden. Durch eine entsprechende Optimierung der Website können Effizienzgewinne bei der Bewerbung und dem Verkauf von Produkten erreicht werden.

Auch andere Methoden der Profilbildung wie etwa das sog. Scoring, d.h. die Bewertung von Personen anhand der Zuordnung von statistischen Erfahrungswerten sind in der Wirtschaft üblich. Der Gesetzgeber hat darauf reagiert und Grenzen wie das Verbot automatisierter Einzelbewertung sowie zusätzliche Transparenzanforderungen geschaffen. Die Ergebnisse der Profilbildung beim Scoring basieren zumeist auf statistischen Annahmen, die ohne weiteres auf Individuen angewandt werden. Entscheidungen zu Personen, die auf Grundlage solcher Profile getroffen werden, basieren damit nicht mehr auf individuellen Gegebenheiten, obwohl es im Einzelfall stets ganz anders sein kann als im statistischen Mittel. Dementsprechend können Diskriminierungen bis hin zur Ausgrenzung ganzer Gruppen eintreten. Diese Nichtberücksichtigung individueller Verhältnisse berührt Grundrechte des Persönlichkeitsschutzes wie auch die Menschenwürde .

Weitergehende Analysen z.B. auf der Grundlage aller zu einer Person verfügbaren Informationen (z.B. webseitenübergreifend wie durch den Facebook-Like-Button) sind denkbar. Durch die Möglichkeit allgegenwärtiger Datenverarbeitung (ubiquitious computing) und Vernetzung potenzieren sich die Möglichkeiten als auch das Risikopotenzial von Profilbildung im Internet. Dementsprechend wird auch und gerade im Kontext des Internets die eingehende Regulierung des zulässigen Einsatzes der Profilbildung gefordert (so zuletzt die Konferenz der Datenschutzbeauftragten in ihrem Eckpunktepapier zur Modernisierung des Datenschutzes). Diskutiert werden in diesem Zusammenhang eine gesetzliche Definition der Profilbildung und die Schaffung von gesetzlichen Grundlagen, die dem besonderen Gefährdungspotential von Profilbildungen Rechnung tragen. Für die Beurteilung des Gefährdungspotentials kommt es maßgeblich darauf an, welche Art von Daten, in welcher Form und zu welchem Zweck und in welchem Umfang erfasst und ausgewertet werden können. Gefordert wird auch eine Anonymisierung, soweit dies möglich ist. Zusätzliche Transparenzanforderungen wie die Anforderung der Erläuterung von Profilbildungsverfahren sollen Verbrauchern helfen, die Folgen

der Nutzung von entsprechenden Angeboten einschätzen zu können.

2.3.2 Ausgestaltung und Reichweite von Transparenzinstrumenten (Informationspflichten, Auskunftsrechte)

Transparenz und damit Informationen sind Kernelemente für informierte Entscheidungen und Aktivitäten der Aufsichtsbehörden, Wettbewerber bzw. anderer Unternehmen und Verbraucher. Eine wesentliche Voraussetzung für die auch praktische Durchsetzung des Datenschutzes – damit der Realisierung des Rechts auf informationelle Selbstbestimmung – ist die Kenntnis über sowohl das Recht bzw. die eigenen Rechte als auch über die tatsächlich durchgeführte Datenerhebung und –verarbeitung.

Transparenz für die Nutzer setzt voraus, dass sich der Nutzer seinem Bedarf entsprechend und frühzeitig über Art und Umfang der Datenerfassung und –verarbeitung informieren kann. Dabei ist es angesichts oft komplexer technischer Zusammenhänge besonders wichtig, für die Verständlichkeit der vermittelten Informationen zu sorgen.

Wie wichtig Transparenz für den Nutzer ist, zeigt das Beispiel der Einführung neuer Technologien und Dienste: Hier steht, wie z.B. bei Apps, am Anfang das positive Nutzungserlebnis und die Freude über den Mehrwert der Innovation. Ohne vorherige Information kämen erst nach und nach Erfahrungen dazu, die aufhorchen lassen und die Frage nach dem Datenschutz und möglichen Missbrauchsszenarien laut werden lassen. Die berechtigte Sorge wird dabei aus dem Umstand genährt, dass Dinge im Hintergrund passieren, die unbekannt und vermeintlich nicht beeinflussbar bzw. kontrollierbar sind.

Hier ist der Ansatz für die Transparenz und deren Instrumente. Der Nutzer soll in die Lage versetzt werden zu verstehen, was mit den Daten passiert und ob er das so und in diesem Umfang will.

Letztlich muss der Nutzer aber derjenige bleiben dürfen, der diese Entscheidung trifft. Und hier sind wir an dem Punkt der Reichweite bzw. an der Grenze der Reichweite der Transparenzinstrumente.

Ziel sollte also die verständliche, neutrale Information über die tatsächlichen technischen Vorgänge im Vordergrund stehen. Dem Nutzer muss klar werden, wer persönliche Daten verarbeitet, wie, in welchem Umfang und zu welchen Zwecken dies geschieht und wer sein Ansprechpartner für Fragen und – besonders wichtig – die Ausübung seiner Selbstbestimmung über die Datenverarbeitung ist.

Das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) sehen jeweils bereits eine Reihe von Transparenzinstrumenten vor. Diese Regelungen sind somit eine gesetzliche Konkretisierung des Rechts auf informationelle Selbstbestimmung.

Informationspflichten von Diensteanbietern

Diensteanbieter haben grundsätzlich die Pflicht, die Nutzer über Art, Umfang und Zweck von Erhebung und Verwendung personenbezogener Daten zu unterrichten (§ 13 TMG, § 33 BDSG). Die Informationspflichten sollen sicherstellen, dass die Adressaten Kenntnis erhalten über die Datenverarbeitung. Es muss über die Identität der verantwortlichen Stelle informiert werden, damit bekannt ist, wer die Daten erhebt und als Adressat eines Auskunftsanspruchs zur Verfügung steht. Über sämtliche Zweckbestimmungen der Verarbeitung und Nutzung der Daten muss informiert werden, die oftmals über die der Vertragsdurchführung notwendigen Daten hinausgehen. Der oder die Empfänger der Daten müssen zumindest als Kategorie bekannt sein (vgl. § …). Eine namentliche Nennung der Empfänger ist jedoch nicht erforderlich, so dass eine lückenlose Verfolgung des Weges der Daten nicht ohne weitere Informationen bzw. Auskunftsersuchen möglich ist. Dieses Wissen ist für eine Person jedoch notwendig, um die Auskunftsrechte bei allen Stellen, die Daten über diese Person haben, geltend machen zu können.

Die Unterrichtung muss in einer allgemein verständlichen Form geschehen. Damit soll gewährleistet werden, dass die Bürger eine informierte Entscheidung zur Preisgabe ihrer persönlichen Daten treffen und ggf. eine Einwilligung verweigern können. In der Regel sind diese Informationen in den allgemeinen Geschäftsbedingungen (AGB) und Nutzungsbedingungen der Diensteanbieter enthalten. Da es sich zumeist um umfangreiche und aufgrund gesetzlicher Vorgaben rechtssicher zu formulierende Texte handelt, sind sie für viele Menschen oftmals nicht in Gänze nachvollziehbar und nur schwer zu verstehen.

Auskunftsrechte des Betroffenen

Neben der Informationspflicht der Diensteanbieter bei Erhebung, Speicherung und Verwendung von personenbezogenen Daten sind in § 34 BDSG umfassende Auskunftsrechte für Betroffene festgeschrieben. Diese berechtigen Betroffene dazu, jederzeit und bedingungsfrei zu erfahren, welche personenbezogenen Daten über ihn von einer verantwortlichen Stelle erhoben, verarbeitet oder genutzt werden und woher die Daten stammen, an wen die Daten weitergeleitet werden und zu welchem Zweck diese Daten gespeichert werden. Unter bestimmten Bedingungen kann die verantwortliche Stel-

le die Auskunft allerdings verweigern, etwa zur Wahrung von Geschäftsgeheimnissen (vgl. § 34 BDSG). Wenngleich diese Auskunftsrechte ein starkes Instrument zur Wahrung der informationellen Selbstbestimmung für Betroffene sind, erscheint die praktische Nutzung in einer Umgebung, in der immer mehr Anwendungen im Alltag personenbezogene Daten nutzen, zunehmend weniger handhabbar

In letzter Zeit ist deshalb die Idee des sogenannten „Datenbriefs“ im Gespräch. Unternehmen, Behörden oder sonstige Institutionen könnten gesetzlich verpflichtet werden, Bürgerinnen und Bürger regelmäßig darüber zu informieren und zu erläutern, welche Daten zu welchem Zweck über sie gespeichert werden. Dies käme einem Paradigmenwechsel gleich: Das derzeitige Auskunftsrecht würde durch eine Informationspflicht ergänzt. Der Betroffene müsste also nicht mehr selbst aktiv werden, um zu erfahren, welche Daten wo über ihn gespeichert sind, sondern würde automatisch darüber benachrichtigt.

Für den Datenbrief wird angeführt, dass viele Betroffene derzeit oft gar nicht wissen würden, wo überall Daten über sie gespeichert werden. Sie könnten daher gar nicht von ihrem gesetzlich eingeräumten Auskunftsrecht Gebrauch machen. Dieser Anspruch würde daher häufig ins Leere laufen. Mit dem Datenbrief würde zudem das Verantwortungsbewusstsein der für die Datenverarbeitung verantwortlichen Stellen gestärkt. Sie würden unter Umständen genauer prüfen, ob und wie lange personenbezogene Daten tatsächlich gespeichert werden müssten.

Gegen den Datenbrief wird angeführt, dass er zunächst bei vielen datenverarbeitenden Stellen zu einer zentralen Zusammenführung der Daten führen könnte. An diese Konzentration von Daten müssten dann nicht nur höhere Sicherheitsanforderungen gestellt werden, sondern dies könnte auch wegen einer damit verbundenen Möglichkeit der verstärkten Profilbildung zu einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung führen. Auch die praktische Umsetzung des Datenbriefs wird als zu bürokratisch und kostenintensiv für die betroffenen Unternehmen kritisiert.

Informationspflichten bei „Datenpannen“

Die „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten“ (§ 42a BDSG) verpflichtet verantwortliche Stellen im nicht-öffentlichen Bereich, die Betroffenen sowie die zuständigen Aufsichtsbehörden umgehend zu informieren, wenn gespeicherte sensible personenbezogene Daten unrechtmäßig an Dritte gelangen. Diese Regelung wurde jedoch erst im Jahr 2009 in das BDSG aufgenommen. Ursache hierfür waren vorhergegangene unerlaubte und

missbräuchliche Erhebungen und Verarbeitungen von personenbezogenen Daten in der Wirtschaft.

Ziel aller Informationspflichten ist es, Transparenz über die Speicherung und Verarbeitung von Daten herzustellen. Diese Transparenz ist Voraussetzung dafür, die informationelle Selbstbestimmung tatsächlich ausüben zu können. Ohne ausreichende Transparenz kann keine informierte Einwilligung existieren. Wenn Betroffene in die Lage versetzt werden sollen, bereits nach dem BDSG bestehende Auskunfts-, Lösch-, Widerspruchs- und Berichtigungsrechte auch tatsächlich geltend machen zu können, ist die Kenntnis notwendig, wer welche Daten zu welchem Zweck gespeichert hat.

2.3.3 Cloud Computing

Text wird von der Projektgruppe noch bearbeitet.

2.3.4 „Verfallsdaten“ im Internet, regelmäßig erneuerbare Zustimmungspflicht

Im Kontext des Internets bereitet die Rückgängigmachung einer einmal gewollten Datennutzung oder auch Datenveröffentlichung bei geänderter Einschätzung besondere Schwierigkeiten.

Schwierig stellt sich die Lage bei veröffentlichten Daten dar. Aufgrund der einfachen Vervielfältigung digitaler Daten im Internet ist auf Grund der technischen Gegebenheiten davon auszugehen, dass einmal veröffentlichte Daten nicht mehr „zurückzuholen“ sind. Selbst wenn es gelingt, die weitere Verwendung bzw. Veröffentlichung an einer bestimmten Stelle zu unterbinden, ist bei Daten anzunehmen, dass sie an anderer Stelle bereits dupliziert wurden.

Seit einigen Jahren wird mit zunehmender Bedeutung des Internets auch die Diskussion über ein „Recht auf Vergessen an den eigenen Daten“ geführt. Allerdings sind die hierfür in der Diskussion verwendeten Begrifflichkeiten noch sehr unterschiedlich. So wird neben dem „Recht auf Vergessen“ [Fußnote: Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age; Jeffrey Rosen, The Web means the End of Forgetting, 21.07.2010, The New York Times], beispielsweise auch vom „programmierten Vergessen“ [Bull, NVwZ 2011, 257 (260)], Verfallsdaten oder dem „digitalen Radiergummi“ [BM Dr. Thomas de Maizière MdB, Rede zu den Grundlagen für eine gemeinsame Netzpolitik der Zukunft, Berlin, 22.06.2010] gesprochen. Die unterschiedlich verwendeten Terminologien haben teilweise nicht nur unterschiedliche Argumentationsansätze, sondern auch eine sehr unterschiedliche Reichweite. Auch wenn sie daher nicht vollständig als Synonym für das Recht auf Vergessen verwendet werden sollten, haben sie einen gemeinsamen Kerngedanken. Demnach soll der Nutzer des Internets mit Hilfe einer oder mehrerer technischen Lösungen,

selbst darüber bestimmen können, wie lange seine personenbezogenen Daten im Internet gespeichert bleiben sollen bzw. nach welcher Zeit, der „menschliche Vorgang“ des Vergessens beginnen soll. Er kann im Idealfall bereits mit dem Einstellen der personenbezogenen Daten festlegen, dass eine (vollständige) Löschung der Daten an einem zuvor bestimmten Datum in der Zukunft erfolgen soll. Aufgrund der nahezu unbegrenzten Speicher- und Vervielfältigungsmöglichkeiten des Internets stellt dies die bisherigen technischen Gegebenheiten vor besondere Anforderungen.

Bereits jetzt existieren einzelne webbasierte Anwendungen, die dem Nutzer die Abrufbarkeit der Daten zeitlich begrenzen ermöglichen sollen. Allerdings fehlt es bisher an einer Gesamtlösung für alle Bereiche des Internets und insbesondere für die besonders datenintensiven sozialen Netzwerke. Erste technische Ansätze hierfür wurden bereits vor zwei Jahren in den USA entwickelt. Die University of Washington programmierte eine entsprechende Technik für den Verfall der eigenen personenbezogenen Daten, die auch auf soziale Netzwerke angewendet werden kann. [http://uwnews.org/article.asp?articleID=50973] Die Universität des Saarlandes stellte im vergangenen Jahr ein vergleichbares Produkt vor. [Fußnote: http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/] Beide Techniken stehen jedoch noch am Anfang der Entwicklung und verhindern keineswegs die Möglichkeit der Vervielfältigung von eingestellten personenbezogenen Daten (insbesondere Bildern). Ein Recht auf Vergessen kann somit aus technischer Sicht zum jetzigen Zeitpunkt nicht durchgesetzt oder gewährleistet werden.

Ergänzender Textvorschlag, streitig

Allerdings ist die Technik einem permanenten Wandel unterworfen. Im Rahmen der Technologie-Förderung durch das Bundeswirtschaftsministerium könnten beispielsweise gezielt Projekte gefördert werden, welche auf die Entwicklung von Datenschutz-Techniken abzielen. Da die Erhebung und Speicherung privater Daten für viele Unternehmen mittlerweile einen festen Bestandteil ihres Geschäftsmodells darstellt, hat die private Wirtschaft verständlicherweise bislang kaum ein Interesse an der Entwicklung derartiger Techniken gehabt. So man ein „Recht auf Vergessen“ für politisch sinnvoll und wünschenswert hält, hätte die Politik jedoch die Möglichkeit, entsprechende Anreize zu setzen.

Bereits heute gibt es Techniken, die in eine ähnliche Richtung weisen. Etwa ist eine zeitlich begrenzte Ver- und Entschlüsselung von Daten möglich, wenn diese nicht bei dem jeweiligen Anbieter, sondern bei spezialisierten Trust Centren abgelegt werden. Daten, die von Nutzern freiwillig zur Verfügung gestellt werden, können also jeweils beim Abruf entschlüsselt werden – so lange, bis eine dafür festgelegte Befristung abläuft. Entscheidend für die technische

Funktionalität sind dabei sogenannte sticky policies, die festlegen, welche Metadaten zusammen mit den Nutzdaten gespeichert und übertragen werden.

Jenseits der Technik sind zudem gesetzgeberische Initiativen denkbar. So könnten Anbieter dazu verpflichtet werden, freiwillige Einwilligungen der Nutzer grundsätzlich nur befristet einzuholen. Das würde bedeuten, dass Letztere nach Ablauf einer gewissen Frist ihr Einverständnis mit der Datenerhebung durch den Anbieter aktiv erneuern müssten. Insofern Daten ohnehin nur zu klar definierten Zwecken erhoben werden dürfen, stünde eine solche Regelung im Einklang mit der Grundintention des ohnehin schon geltenden Rechts. Ein Zweck, für den Daten unbefristet lange gespeichert werden müssten, ist schlichtweg nicht denkbar.

Die politische und rechtliche Diskussion um ein Recht auf Vergessen hat in den letzten Monaten weiter an Fahrt gewonnen.

Satz entspricht dem nachfolgenden Satz, aber andere Überleitung.

Ungehindert dessen, hat die politische und rechtliche Diskussion um ein Recht auf Vergessen in den letzten Monaten weiter an Fahrt gewonnen. Auch die EU-Kommission hat das Recht auf Vergessen als prüfungswerten Punkt für eine Überarbeitung der Datenschutzrichtlinie 95/46/EG mit in die bevorstehende Konsultation aufgenommen. [Fußnote: Mitteilung der EU-Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 04.11.2010, S. 8]

2.3.5 „Privacy by design“ („privacy by design“ / „privacy by default“)

„Privacy by design“ beschreibt den Ansatz, bereits bei der Konzeption und Ausgestaltung von Technologien den Datenschutz mit einzubeziehen. [Fußnote: Peter Schaar (2010): Privacy by Design; in: Identity in the Information Society (2), 2010, S. 267-274] Nachträglich möglicherweise auftretene Schwierigkeiten mit der Einhaltung der gesetzlichen Vorgaben der Datenschutzgesetze können so bereits im Vorfeld vermieden und verhindert werden. Eine Korrektur solcher Schwierigkeiten im Nachhinein ist oft nur sehr mühsam und mit viel Aufwand zu bewältigen.
In einer Zeit, in der zunehmend auch technische Geräte des Alltags beginnen, personenbezogene Daten zu erfassen und über das Internet zu kommunizieren, werden die Herausforderungen an die Sicherung des Rechts auf informationelle Selbstbestimmung und den Vollzug des geltenden Datenschutzrechts wachsen.
Die konsequente und frühzeitige Umsetzung von „privacy by design“ stellt auch eine Möglichkeit zur Problemlösung im Bereich der Einwilligung nach § 4 BDSG dar. Elemente von „privacy by design“ können beispielsweise eine grundsätzliche Verschlüsse-

lung von Daten, die Löschung von Daten nach erfolgter Funktionserfüllung oder technische Vorkehrungen zur Einhaltung des Zweckbindungsgrundsatzes sein. [Fußnote: Technikfolgenabschätzung (TA) / Zukunftsreport – Ubiquitäres Computing (2010); Deutscher Bundestag Drucksache 17/405, S. 126] Sie unterstützen damit den Nutzer technischer Geräte und helfen ihm, auch weiterhin den gesetzlich gewährleisteten Schutz seines Rechts auf informationelle Selbstbestimmung zu erhalten. Gleichzeitig konkretisieren sie auf diese Weise das Gebot der Datensparsamkeit und Datenvermeidung.

In Ergänzung zu „privacy by design“ stellt das Prinzip des „privacy by default“ eine wichtige Option zur Gestaltung von elektronischen Diensten und Anwendungen wie etwa sozialen Netzwerken oder so genannten „location based services“ dar. Nach diesem Prinzip gestaltete Dienste sehen ab dem ersten Moment der Nutzung die jeweils höchstmöglichen nutzbaren Datenschutzeinstellungen vor. Nutzerinnen und Nutzer können dann mittels eines sog. „opt-out“ die Einstellungen des Datenschutzniveaus nach ihren Vorstellungen anpassen. Eine konsequente Anwendung des Prinzips „privacy by default“ erscheint gerade angesichts der Vielfalt der einzelnen technischen Einstellungen vieler webbasierter Angebote und der oftmals nicht leicht erkennbaren Konsequenzen sinnvoll. „privacy by design“ und „privacy by default“ orientieren sich an den Vorgaben der Datenvermeidung und Datensparsamkeit (§ 3e BDSG) und damit an einer zentralenLeitlinie des Datenschutzrechts. Sie sind als immanente Grundprinzipien geeignet, den gegenwärtigen und zukünftigen Herausforderungen für einen Datenschutz wirksam und effektiv zu begegnen.

2.3.6 Datenweitergabe und –handel

Text wird von der Projektgruppe noch bearbeitet.

2.3.7 Spannungsfeld Datenschutz und (internationale) Geschäftsmodelle (Beispiel Facebook und VZ)

Text wird von der Projektgruppe noch bearbeitet.

2.3.8 Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft

Staatliche Aufsicht ist unverzichtbar, gleichzeitig muss man aber anerkennen, dass sie systembedingt auch an Grenzen stößt. Selbst bei großer Sachnähe und einer hinreichenden personellen Ausstattung werden sich Behörden schwer tun, alle sich ständig wandelnden Phänomene im Internet in ihrer technischen Komplexität und Dynamik wirksam zu erfassen und eine hinreichende Aufsicht zu

gewährleisten. Schließlich ergibt sich angesichts der Vielzahl der im Netz angebotenen Dienste unweigerlich ein Ressourcenproblem, das eine effektive, hinreichend enge Kontrolle der tatsächlichen Praxis bei den verantwortlichen Stellen erschwert.

Absatz streitig

Diese potentiellen Defizite staatlicher Aufsicht könnten durch eine Einbindung der Unternehmen in die Festsetzung und Durchsetzung von Datenschutzstandards ausgeglichen werden.

Darüber hinaus können Selbstverpflichtungen der Internetwirtschaft in Zukunft auch im Datenschutz eine wichtige Ergänzung zu gesetzlichen Vorgaben darstellen. Gerade in einem sich schnell wandelnden Technikumfeld, aus dem sich ständig neue Geschäftsmodelle entwickeln, kann mit diesem Instrument flexibel auf Veränderungen reagiert und auf spezielle Bedürfnisse in einzelnen Anwendungsfällen eingegangen werden. Während mit der Gesetzgebung abstrakt-generelle Wertungen und Vorgaben von einer gewissen Nachhaltigkeit geschaffen werden müssen, kann mit Selbstverpflichtungen kurzfristiger und detaillierter eingegriffen werden, um auf Entwicklungen in einzelnen Geschäftsfeldern zu reagieren.

Absatz streitig

Dabei sind verschiedene formale und inhaltliche Ausgestaltungen denkbar, die von einseitigen Verpflichtungserklärungen der Verantwortlichen bis zu einer gesetzlich eingebundenen regulierten Selbstregulierung gehen. Bereits im geltenden BDSG stellt § 38a einen rechtlichen Anknüpfungspunkt dar, über den Selbstverpflichtungen in den gesetzlichen Rahmen integriert werden können. Bislang wurde dieses Instrument kaum genutzt. Jüngste Beispiele wie z.B. der Datenschutz-Kodex für Geodatendienste könnten jedoch der Anfang einer deutlich intensiveren Nutzung dieses Regulierungsinstruments sein. Diese Entwicklung ist zu beobachten und gegebenenfalls durch entsprechende Ergänzung des Rechtsrahmens zu fördern. Auch die EU-Kommission hat in ihrer Mitteilung angekündigt, „Möglichkeiten zur verstärkten Förderung von Initiativen zur Selbstregulierung zu prüfen, darunter die aktive Förderung von Verhaltenskodizes.“ [Fußnote: Mitteilung der EU-Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4.11.2010, Kapitel 2.2.5 (S.14)]

Absatz streitig

So wird zurzeit auf europäischer Ebene auch die Einführung von Selbstregulierungsmechanismen für angemessene Formen der Datenerhebung und –verwendung im Zusammenhang mit Online-Werbung erörtert. Dies könnte ein wichtiger Schritt sein, um auch in diesem Bereich zu mehr Transparenz und Selbstbestimmungsmöglichkeiten für die Nutzer zu kommen. Denn klare Kennzeichnungen von verpflichtungskonformen Angeboten bieten dem Nutzer eine zusätzliche Transparenz und eine einfache Orientierungsmöglichkeit.

Alternativer Textvorschlag

Alternativer Textvorschlag zu Z. 936 - 938 und 950 – 975, streitig

Die staatliche Aufsicht über die Einhaltung datenschutzrechtlicher Bestimmung stößt im Zuge neuer technischer Entwicklungen immer mehr an Grenzen. Dies kann als Folge einer mangelnden personellen Ausstattung der zuständigen Behörden betrachtet werden, ist jedoch sicher auch der Schwierigkeit geschuldet, in einer zunehmend vernetzten Welt eine effektive Kontrolle auszuüben. Je mehr Daten erhoben, gespeichert und kopiert werden, desto schwerer ist ihre Verbreitung nachzuvollziehen. Folglich sind die Behörden bei der Durchsetzung des Datenschutzrechts stets auch auf die Mitarbeit der privaten Unternehmen angewiesen.

In letzter Zeit wird daraus oft der Schluss gezogen, die Defizite staatlicher Aufsicht könnten durch eine stärkere Einbindung der Unternehmen in die Festsetzung und Durchsetzung von Datenschutzstandards ausgeglichen werden. Selbstverpflichtungen der Internetwirtschaft werden immer häufiger als Alternative zu möglicherweise rigiden gesetzlichen Vorgaben dargestellt. In Eigeninitiative könne die Wirtschaft kurzfristiger und flexibler auf neue Herausforderungen reagieren. Regulierte Selbstregulierung heißt dabei das Schlagwort.

Derartige Bestrebungen begegnen allerdings auch skeptischen Einwänden. Denn Selbstregulierung kann nur dann eine Alternative zu gesetzlicher Normierung darstellen, wenn klar definiert ist, in welchen Grenzen sie sich bewegt, wie sie konkret umgesetzt wird, wer für die Umsetzung der Selbstverpflichtung in den Unternehmen verantwortlich ist, welche Sanktionen im Falle einer Nicht-Umsetzung drohen und unter welchen Umständen der Gesetzgeber sich vorbehält, einen zunächst der Selbstregulierung überlassenen Bereich nachträglich doch noch gesetzlich zu regulieren. Absichtserklärungen und Willensbekundungen privater Unternehmen stellen keine Alternative zu gesetzgeberischem Handeln dar, wenn ihre Nichtumsetzung mit keinerlei Sanktionen behaftet ist. Eine effektive Selbstregulierung zu etablieren, setzt also voraus, dass Kontroll- und Evaluationsmechanismen entwickelt werden, dass kurz- und langfristige Ziele klar ausformuliert sind und dass Sanktionen für den Fall eines Scheiterns der Selbstregulierung vorgesehen sind. Anders gesagt: Regulierte Selbstregulierung darf nicht als Rückzug des Gesetzgebers zugunsten einer Selbstdiziplinierung der privaten Wirtschaft verstanden werden, sondern kann stets nur eine Ergänzung innerhalb des vom Datenschutzrecht vorgegebenen Rahmen darstellen. Ob zum Beispiel der freiwillige Datenschutz-Kodex für Geodatendienste diesem Anspruch gerecht wird oder zukünftig gesetzgeberisch ergänzt werden sollte, braucht an dieser Stelle nicht erörtert zu werden. Auch Skeptiker werden jedoch einräumen, dass Initiativen zur Selbstregulierung, wie sie etwa von der EU-Kommission befürwortet werden (vergl. Mitteilung der EU-Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4.11.2010, Kapitel 2.2.5), stets zu begrüßen sind,

wenn sie tatsächlich zu mehr Transparenz und Selbstbestimmungsmöglichkeiten für die Nutzer beitragen.

2.3.9 Schadensersatzansprüche im Datenschutzrecht

Bei der Verletzung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG tritt selten ein materieller, sondern ein immaterieller Schaden ein. Dem Betroffenen steht nach § 7 BDSG (in Umsetzung von Art. 23 der Richtlinie 95/46/EG) gegenüber der verantwortlichen (nicht-öffentlichen und öffentlichen) Stelle ein Schadensersatzanspruch zu, sofern personenbezogene Daten unzulässig oder unrichtig erhoben, verarbeitet oder genutzt wurden und ein Schaden entstanden ist. Die fehlerhafte Datenverarbeitung muss ursächlich für den Schaden geworden und i. S. v. § 276 BGB schuldhaft, d. h. durch vorsätzlichen oder fahrlässigen Umgang erfolgt sein. [Fußnote: Gola/Schomerus, Kommentar zum BDSG, 10. Aufl., 2010, § 7 Rn. 7, 8.] Dabei wird zunächst schuldhaftes Handeln durch die verantwortliche Stelle unterstellt, die nach § 7 S. 2 BDSG jedoch den Entlastungsbeweis führen kann und damit die Möglichkeit zur Exkulpation hat. Der zugefügte Schaden muss eine materielle Beeinträchtigung des Betroffenen zur Folge haben, d. h. ein sogenannter Vermögensschaden muss vorliegen, der konkret beziffert werden muss.

Nach § 8 Abs. 1 BDSG (ebenfalls in Umsetzung von Art. 23 der Richtlinie 95/46/EG) besteht für den Betroffenen bei automatisierter Datenverarbeitung durch öffentliche Stellen für den Betroffenen ein Schadensersatzanspruch bei unzulässiger oder unrichtiger Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten. Diese verschuldensunabhängige Gefährdungshaftung soll die „typische Automationsgefährdung“ abdecken, also Schäden, die durch automatisierte Verfahren eingetreten sind. [Fußnote: Gola/Schomerus, a.a.O., § 8 Rn. 9.] Es besteht keine Exkulpationsmöglichkeit für die datenverarbeitende Stelle. Ersetzt werden nicht nur materielle, sondern auch immaterielle Schäden, sofern eine schwere Verletzung des Persönlichkeitsrechts geltend gemacht werden kann.

Das Verhältnis der gesetzlichen Ansprüche von §§ 7, 8 BDSG mit dem deliktischen Schadensersatzanspruch nach § 823 BGB ist bisher jedoch noch umstritten. Hierzu werden verschiedene Auffassungen vertreten, die jedoch im Ergebnis mehrheitlich auch einen Ersatz von immateriellen Schäden bei einer schwerwiegenden Verletzung aufgrund eines unzulässigen oder unrichtigen Datenumgangs annehmen. [Fußnote: Vgl. Kühling/Bohnen JZ 2010, 600 [609]] Hierzu gibt es jedoch noch keine Rechtsprechung.

Bei öffentlichen Stellen kann sich eine über §§ 7, 8 BDSG hinausgehende Haftung im Rahmen hoheitlicher Tätigkeit nach Art. 34 GG i. V. m. § 839 BGB oder im fiskalischen Bereich aufgrund vertraglicher oder deliktischer Haftung nach §§ 31, 89 bzw. 831 BGB ergeben. [Fußnote: Gola/Schomerus, a.a.O., § 7 Rn. 17.] Darüber hinaus können sich Schadensersatzansprüche gem. § 280 BGB wegen schuldhaft rechtswidriger bzw. missbräuchlicher Datenverarbeitung aus vorvertraglicher bzw. vertraglicher Haftung ergeben. [Fußnote: Gola/Schomerus, a.a.O., § 7 Rn. 18.]

Die zunehmende Datenverarbeitung durch öffentliche und nicht-öffentliche Stellen birgt ein Risiko für die Betroffenen. Nicht nur, dass kaum noch erkennbar ist, wer welche Daten wie verarbeitet. Auch die Durchsetzung von Schadensersatzansprüchen kann die Betroffenen vor erhebliche Herausforderungen stellen. Dies gilt insbesondere für den Fall, dass schwierige und aufwändige Beweiserhebungen für den Nachweis des Verschuldens und den entstandenen Schaden erforderlich werden. Gleiches gilt auch für den Nachweis der Höhe des eingetretenen Schadens.

Absatz streitig.

2.3.10 Transfermöglichkeit der regulierten Selbstregulierung auf den Bereich des Datenschutzes

Insbesondere im Jugendmedienschutz hat sich neben staatlicher Regulierung und reiner Selbstregulierung eine Form der sog. „regulierten Selbstregulierung“ bzw. Co-Regulierung entwickelt. Sie ist dadurch gekennzeichnet, dass die staatliche Hand einen gesetzlichen Rahmen schafft, innerhalb dessen die Selbstkontrolle der Wirtschaft in eigener Verantwortung die Ausgestaltung und Anwendung von Verhaltensgrundsätzen organisieren kann. Sie unterliegt dabei aber wiederum einer übergeordneten Erfolgskontrolle durch die staatliche Hand, die im Falle von Fehlentwicklungen bzw. Verstößen gegen den vorgegebenen Rahmen ihrerseits durchgreifen kann. Der Erfolg dieses Modells im Jugendmedienschutz hängt wesentlich damit zusammen, dass es in diesem Bereich einen Beurteilungsspielraum bei der Bewertung der der Kontrolle unterliegenden Medieninhalte gibt. Für die Einschätzung der potentiellen Entwicklungsbeeinträchtigung und der damit verbundenen Altersklassifizierung existieren keine gesetzlichen Vorgaben, so dass diese rein tatsächliche Beurteilung am besten von möglichst sachnahen Personen durchgeführt werden sollte.
Einen solchen Beurteilungsspielraum kennt das viel stärker von Rechts- als von Tatsachenfragen geprägte Datenschutzrecht allerdings nicht. Hier bestehen bereits aus verfassungsrechtlichen Gründen durchgehende gesetzliche Regelungen, deren Auslegung zwar im Einzelfall schwierig und auch streitig sein kann, die aber trotzdem mit einem vollumfänglichen Geltungsanspruch ausgestat-

tet sind. Es erscheint daher fraglich, ob es im Datenschutz einen dem Jugendmedienschutz vergleichbaren Spielraum für die sachliche Ausfüllung von Tatbestandselementen gibt, die das Modell einer „regulierten Selbstregulierung“ tragen könnten. Es liegt näher, dass sich in diesem Bereich angesichts des voll umfänglichen Geltungsanspruchs staatlicher Regulierung nur ein Nebeneinander, aber eben kein ineinander verwobenes Miteinander von staatlicher Regulierung einerseits und Selbstregulierung der Wirtschaft andererseits entwickeln kann.

2.3.11 Beschäftigtendatenschutz

Zu 2.3.11 liegen zwei alternative Textvorschläge vor.

Erster Textvorschlag

Aktuell werden Beschäftigtendaten im Rahmen der allgemeinen Normen, wie BDSG, TKG oder im (kollektiven) Arbeitsrecht, wie im BetrVG geregelt. Im Bundesbeamtengesetz wird der Umgang mit der Personalakte im Beamtenverhältnis geregelt. Andere spezialgesetzliche Normen hinsichtlich des Datenschutzes für private oder öffentliche Arbeitgeber existieren nicht. Die oft darüber hinaus gehenden Sachverhalte zum Schutz der Beschäftigtendaten hat der Gesetzgeber der Rechtsprechung in Form einer Vielzahl von Einzelentscheidungen des Bundesarbeits- und des Bundesverfassungsgerichts überlassen.

Datenschutzskandale in der Vergangenheit bei verschiedenen deutschen Großunternehmen haben gezeigt, dass eine Diskrepanz zwischen dem Recht des Beschäftigten auf informationelle Selbstbestimmung und dem Recht des Arbeitgebers auf Schutz des Eigentums in dem besonders zu betrachtenden Arbeitsverhältnis besteht und es hier einer Regelung durch den Gesetzgeber bedarf.

Im Bereich der Beschäftigtendaten gilt es deshalb das Persönlichkeitsrecht des Beschäftigten einerseits zu schützen, dem Arbeitgeber aber auch Möglichkeiten zu geben, sein Rechte wahrzunehmen. Der Gesetzgeber hat bereits erkannt, dass es hier gesetzlicher Regeln bedarf.

Dies gilt insbesondere in einer Welt des digitalen Wandels und Wachsens von immer neuen, komplexeren Datenverarbeitungen, Anwendungen und Internet, die in den Arbeitsalltag hineinwirken. Hier muss der Schutz von Beschäftigtendaten einen bedeutenderen Stellenwert bekommen. Auch das Privatleben unterliegt in den vergangenen Jahren einem rasanten technischen Wandel, der anhält und stetig komplexer wird. Die Benutzung von Internet, E-Mail Systemen, sozialen Netzwerken, Mobiltelefonen, Online-Banking, Kreditkarten oder Bonuskartensystemen im Privatleben haben Einfluss auf das Berufsleben, weil im Netz persönliche Daten dokumentiert und Arbeitgebern zugänglich gemacht werden. Es fallen persönli-

che Daten an, die oft nur unzureichend gegen unrechtmäßige Nutzung und Weitergabe an Dritte gesichert sind.

Im Arbeitsverhältnis werden Chipkarten eingesetzt, die den Zugang der Beschäftigten aufzeichnen, bei der Verwendung von RFID (radio frequency identification) können Tätigkeitsprofile erstellt werden und Handys ermöglichen über GPS (global positioning system) jederzeit die Feststellung, wo sich Beschäftigte befinden. Durch vielfältige Spuren im Netz steigen die Möglichkeiten, Leistungsüberprüfungen von Beschäftigten durchzuführen. Hinzu kommt außerdem, dass unter den Stichwort Terrorbekämpfung von staatlichen Stellen über den Arbeitgeber im Rahmen sogenannter Sicherheitsüberprüfungen Daten, etwa über religiöse Präferenzen oder ethnische Herkunft weitergegeben werden, obwohl diese Daten dem Persönlichkeitsschutz unterliegen. Außerdem entstehen durch Verfahren wie ELENA (elektronischer Entgeltnachweis) oder die geplante Gesundheitskarte riesige Datenmengen, deren Verwendung zwar gesetzlich geregelt wurde, die aber Anlass für Kritik geben. Diese Auffassung wird auch von Seiten der Landesbeauftragten für den Datenschutz geteilt. Unter staatlicher Verantwortung und Verfügungsmacht werden eine riesige Datenmenge (und das noch bis 2014) auf Vorrat gesammelt, was einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.

Darüber hinaus bedienen sich Arbeitgeber immer neuerer Techniken (wie z. B. Videoüberwachung, GPS-/Ortungs-Systeme oder Fingerabdruck- oder Iriserkennungssysteme) sowohl im Unternehmensalltag, als auch zum Schutze ihrer Betriebs-/Geschäftsgeheimnisse oder ihres Eigentums.

All diese Vorgänge bergen erhebliche Gefahren und machen deutlich, dass die persönlichen Daten von Beschäftigten außerordentlich missbrauchsanfällig sind. Die Rechte der Beschäftigten bei der Verarbeitung ihrer personenbezogenen und personenbeziehbaren Daten müssen deshalb einem besonderen Schutz unterliegen. Gerade im Arbeitsverhältnis, das davon geprägt ist, dass eine Abhängigkeit der Beschäftigten zum Arbeitgeber besteht, müssen klare gesetzliche Regelungen Datenmissbrauch verhindern. Das Beschäftigungsverhältnis ist keine gleichrangige Beziehung und gerade deshalb besonders anfällig für Generaleinwilligungen zur Datenerhebung, -verarbeitung und –nutzung.

Vor diesem Hintergrund gibt es keine Alternative zu einem wirksamen, eigenständigen Beschäftigtendatenschutzgesetz. Nur so kann sichergestellt werden, dass dem Persönlichkeitsrecht der Beschäftigten Rechnung getragen wird. Datenschutz muss dabei den Schutz personenbezogener und personenbeziehbarer Daten von Beschäftigten vor Missbrauch bedeuten. Die Grundsätze des Daten-

schutzes, wie Datensparsamkeit, Transparenz, Datensicherheit und die Unmittelbarkeit der Datenerhebung müssen sich im Beschäftigtendatenschutz wiederfinden und dem besonderen Verhältnis zwischen Arbeitnehmer und Arbeitgeber Rechnung tragen. Daher bedürfen sie einer besonders genauen an den Rechtssprechungsgrundsätzen orientierten Ausgestaltung.

Eine eigenständige gesetzliche Regelung ist notwendig, um klare und möglichst verständliche Regelungen zu schaffen. Der Schutz vor unzulässiger Datenerhebung, - verarbeitung und –nutzung kann nur in Form übersichtlicher Regelungen verbessert werden.

Als Grundansatz eines Beschäftigtendatenschutzes müssen die Persönlichkeitsrechte und das Recht auf informationelle Selbstbestimmung gewählt werden, die nach der Rechtsprechung des Bundesverfassungsgerichts den Status von Grundrechten haben. Eingriffe in diese Grundrechte dürfen durch die gesetzliche Regelung nur ausnahmsweise erlaubt werden. Dabei dürfen die Persönlichkeitsrechte der Beschäftigten auch nicht in Abwägung zu unternehmerischen Interessen gestellt werden.

Allein mit Hilfe eines eigenständigen, dem Wandel der Technik angepassten und bereits im Ansatz an Grundrechte anknüpfenden Datenschutzrecht für Beschäftigte können Datenskandale der Vergangenheit verhindert werden. Die Vorfälle bei Lidl und anderen Discountern, die eine Überwachung der Beschäftigten mittels Videokameras bis in die Umkleideräume praktizierten, die Telefonbespitzelung bei der Deutsche Telekom AG oder die Weitergabe von Kundendaten bei der Deutschen Bahn AG haben gezeigt, dass die Hemmschwelle, Persönlichkeitsrechte zu verletzten, sehr niedrig ist. Einer der Gründe dafür sind fehlende oder zu geringe Sanktionsmechanismen, die solche Vorgehensweisen als nicht „verwerflich“ erscheinen lassen. Zudem wird die Rechtsdurchsetzung von Einzelnen dadurch erschwert, dass das aktuell gültige Beschäftigtendatenschutzrecht keinen kollektiven Schutz in Form einer Verbandsklage enthält. Mit Hilfe dieser Mechanismen erhält die digitale Gesellschaft einen effektiven und schutzorientierten Datenschutz, der modernen, demokratischen Werten entspricht, die für eine Gesellschaft im 21. Jahrhundert unverzichtbar sind.

<u>*Alternativtext:*</u>

alternativer Textvorschlag zu 2.3.11

Seit Jahrzehnten wird die Schaffung umfassender gesetzlicher Regelungen für den Arbeitnehmerdatenschutz diskutiert. Die christlich-liberale Koalition hat sich daher bereits im Koalitionsvertrag vom 26. Oktober 2009 für eine Erweiterung des Bundesdaten-

schutzgesetzes ausgesprochen. Denn gegenwärtig existieren nur wenige spezifische gesetzliche Vorschriften zum Schutz der personenbezogenen Daten von Beschäftigten. Für zahlreiche Fragen der Praxis zum Beschäftigtendatenschutz bestehen keine speziellen gesetzlichen Regelungen. Teilweise ergibt sich der rechtliche Rahmen für den Beschäftigtendatenschutz aus verschiedenen allgemeinen Gesetzen wie dem Bundesdatenschutzgesetz und dem Betriebsverfassungsgesetz. Daneben existiert eine Vielzahl an gerichtlichen Einzelfallentscheidungen, anhand derer wichtige Grundsätze für den Beschäftigtendatenschutz entwickelt worden sind. Jedoch sind insbesondere die gerichtlichen Entscheidungen für die betroffenen Beschäftigten teilweise nur schwer zu erschließen.

Durch die Erweiterung des Bundesdatenschutzgesetzes [Fußnote: BT-Drs. 17/4230 vom 15.12.2010] soll die Rechtssicherheit für Arbeitgeber und Beschäftigte erhöht werden. So sollen einerseits die Beschäftigten vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten geschützt werden, andererseits soll das Informationsinteresse des Arbeitgebers beachtet werden. Beides dient dazu, ein vertrauensvolles Arbeitsklima zwischen Arbeitgebern und Beschäftigten am Arbeitsplatz zu unterstützen.

Es sollen für Zwecke des Beschäftigungsverhältnisses nur solche Daten verarbeitet werden dürfen, die für dieses Verhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Beschäftigungsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante Gesundheitszustände beziehen, sollen (zukünftig) ausgeschlossen sein. Mit den Neuregelungen sollen Mitarbeiter an ihrem Arbeitsplatz zudem wirksam vor Bespitzelungen geschützt und gleichzeitig den Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand gegeben werden. [Fußnote: *BT-Drs. 17/4230 vom 15.12.2010, S. 12]*

2.3.12 Datenschutz als Standortfaktor

Text wird von der Projektgruppe noch bearbeitet.

2.3.13 Problem der Rechtszersplitterung innerhalb Deutschlands durch föderale Aufsichtsstruktur

Text wird von der Projektgruppe noch bearbeitet.