Datenschutzrecht in der vernetzten Welt des 21. Jahrhunderts

Peter Schaar/ Dr. Jost Onstein*

I. Datenschutz im Spannungsfeld des technischen Fortschritts

Wie kaum eine andere technische Entwicklung zuvor hat das Internet, ein Grundpfeiler unserer modernen Kommunikations- und Informationsgesellschaft, die datenschutzrechtliche Diskussion der vergangenen Jahre geprägt - und dessen Instrumentarien in Frage gestellt. Schon mehren sich die Stimmen, die das klassische Konzept des Datenschutzes in der digitalen Welt des 21. Jahrhundert für nicht mehr zeitgemäß erachten, für ein Relikt aus der vordigitalen Zeit halten. Diese *Post-Privacy*-Standpunkte beruhen nicht zuletzt auf der zutreffenden Erkenntnis, dass die Einflussmöglichkeiten auf die eigenen personenbezogenen Daten in der global vernetzten Welt des Internets dramatisch geschwunden sind und eine Kontrolle der eigenen Daten durch die Nutzer immer schwieriger ist.

Schon die allein rezeptive Nutzung des Internets ist regelmäßig mit der Preisgabe persönlicher Informationen der Nutzer verbunden. Denn aus technischer Sicht ist es notwendig, die vom Nutzer beim Surfen verwendeten Komponenten und die angeforderten virtuellen Ressourcen zu identifizieren. Durch die Verknüpfung dieser technischen Daten (IP-Adressen, URLs) mit den Nutzern bzw. Anschlussinhabern und den abgerufenen Inhalten sind bereits diese Daten aussagekräftig. Praktisch jeder Mausklick hinterlässt so Datenspuren im weltweiten Netz.

Die Eingabe von Suchbegriffen in Suchmaschinen oder das elektronische Einkaufen und Bezahlen verlängert die auf den einzelnen Nutzer zurückführbaren Datenspuren. Noch umfangreicher sind die Daten, die bei Verwendung interaktiver Dienste preisgegeben werden, die das „Web 2.0“ kennzeichnen. Die Preisgabe geschieht dabei bewusst, wie etwa bei der Angabe persönlicher Vorlieben, Statusmeldungen und über Freundeslisten in sozialen Netzwerken. Im Hinblick auf die Steuerbarkeit durch den Nutzer sind jedoch gerade die Datensammlungen besonders problematisch, die im Hintergrund ohne Mitwirkung der Betroffenen stattfinden, etwa wenn durch Webanalysedienste die Surfgewohnheiten erfasst oder mittels Tracking-Mechanismen Profile gebildet und zu Zwecken adressatenbezogener Werbung ausgewertet werden.

Gerade die Web 2.0-Technologien haben zu einer enormen Steigerung des Datenaufkommens geführt, weil sie von ihrer Konzeption her auf die Interaktion der Nutzer, also den Austausch von Informationen, ausgerichtet sind. Dabei werden sowohl die bewusst eingegebenen als auch die im Hintergrund gesammelten Informationen durch die Betreiber entsprechender Plattformen zusammengeführt und kommerziell, insbesondere zu Werbezwecken, genutzt. Die verwendeten Mechanismen greifen hierbei sogar auf Nutzer zu, die selbst nicht aktiv an den Diensten teilnehmen. Denn durch die Abfrage von Kontaktdaten aus den von den registrierten Nutzern verwendeten E-Mail-Postfächern werden den Betreibern auch Angaben über Nichtmitglieder bekannt. Durch die Verwendung sogenannter Social Plug-Ins (etwa durch die Einbindung der umstrittenen „Gefällt mir“-Markierungen) auf beliebigen Webseiten finden schließlich Verknüpfungen zwischen diesen Angeboten und den Sozialen Netzwerken statt - mit der Konsequenz, dass das Nutzerverhalten noch umfassender registriert wird.

Es liegt auf der Hand, dass die fortschreitende globale Vernetzung und Digitalisierung der Daten neue Gefährdungslagen für die Privatsphäre im Allgemeinen sowie für das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis im Besondern begründen. Die Probleme beruhen auf der umfassenden Verfügbarkeit und Verknüpfbarkeit digitaler Daten, die von Wirtschaft und Staat ausgewertet werden können, zum Beispiel zu Persönlichkeits- und Verhaltensprofilen. Sie beruhen aber auch auf der fehlenden Kontrollierbarkeit der eigenen Daten in einem virtuellen Umfeld, in welcher sich Daten in Sekundenbruchteilen kopieren und übertragen lassen, auf der fehlenden Datensicherheit, die immer wieder durch erfolgreiche Hackerangriffe unter Beweis gestellt wird, und nicht zuletzt auf den Grenzen rechtlicher Datenschutznormen in einem globalen Umfeld internationaler Datenströme.

Zwar ist unzweifelhaft, dass die datenschutzrechtlichen Anforderungen auch im Internet gelten, das Internet also nicht der häufig beschworene „rechtsfreie Raum“ ist; die Eigenheiten der digitalen Welt führen allerdings zu der für den Datenschutz misslichen Situation, dass der Schutzbedarf für das Recht auf informationelle Selbstbestimmung *in Folge* der technischen Entwicklungen der Online-Welt besonders hoch ist, zugleich aber *durch* die technischen Gegebenheiten der Online-Welt die Durchsetzung der Datenschutzrechte enorm erschwert wird. Die begrenzte

* Der Autor *Schaar* ist Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, der Autor *Onstein* ist dort Referent.

Geltungskraft der klassischen, aus den 70er Jahren des 20. Jahrhunderts stammenden Konzepte des Datenschutzrechts in der digitalen Welt des 21. Jahrhunderts zeigt sich bei einer Analyse der maßgeblichen digitalen Trends:

Zum einen liegen die Gefährdungslagen für den Datenschutz in der zunehmenden *Interaktivität*, die das datenschutzrechtliche Rollenkonzept gehörig durcheinander wirbelt. Denn datenschutzrechtliche Betroffenheit und Verantwortlichkeit lassen sich nicht mehr strikt voneinander trennen, wenn der Nutzer sowohl Empfänger als auch Autor von Informationen sein kann. Dies zeigt sich insbesondere in *sozialen Netzwerken,* die beispielhaft verdeutlichen, wie stark sich die Rolle des Nutzers von einem Rezipienten fremder Inhalte in früheren Web-Generationen zu einem Produzenten eigener Inhalte im Web 2.0 gewandelt hat.

Zum anderen stellen sich schwierige datenschutzrechtliche Fragen durch die zunehmende *Entörtlichung* der Datenverarbeitung beim *Cloud Computing*, bei welchem IT-Infrastruktur und Software – und somit auch personenbezogene Daten – von lokalen Rechnern in globale und geographisch kaum zu fassende „Rechnerwolken" verlagert werden. Wenn Daten ohne Bezug zu dem Ort oder sogar Nationalstaat, in welchem sie erhoben wurden, gespeichert und gegebenenfalls in einem dritten Land verarbeitet werden, dann stellt sich nicht nur die Frage, welches Recht angesichts der kaum möglichen Bestimmbarkeit des physischen Speicherorts der Daten zur Anwendung kommt, sondern auch die Problematik des Zugriffs ausländischer staatlicher Stellen.

Ferner befinden wir uns bereits in der heutigen Zeit, in der wir uns an das Smartphone als ständigen Begleiter gewöhnt haben, auf der Schwelle zu einer allgegenwärtigen Datenverarbeitung, in welcher jedes noch so unbedeutende Datum einschließlich der jeweiligen Geokoordinaten durch „smarte" Alltagsgegenstände gespeichert und für zukünftige Verwendungen vorgehalten wird. Diese sich abzeichnende Rechnerallgegenwart, das *Ubiquitous Computing,* stellt die Zweckbindung der Datenverarbeitung und den datenschutzrechtlichen Grundsatz der Datensparsamkeit fast zwangsläufig auf den Prüfstand. Geräte, die möglichst viele Daten registrieren und speichern, um sie bei Bedarf ohne Rücksicht auf den Kontext der Erhebung wiederzugeben, führen in die *Dekontextualisierung* der Datenerhebung und -verarbeitung.

Und schließlich bewirkt die stetige Fortentwicklung der informationstechnischen Basis eine Veränderung der Softwarekonzepte, in denen „Apps", also kleine, schnell erstellte und über das Internet verteilte Anwendungsprogramme eine zentrale Rolle spielen. So einfach diese Miniprogramme herunterzuladen, zu installieren und zu bedienen sind, so intransparent ist deren Funktionsweise. Vielfach beinhalten kostenlos oder gegen geringes Entgelt erwerbbare „Apps" neben den offiziellen Funktionen verdeckte Zusatzmechanismen, mit denen der Standort des Nutzers und andere personenbezogene Daten ermittelt und über das Internet versandt werden. Auch hier stellt sich verstärkt die Frage, inwieweit die traditionellen, dem Datenschutzrecht zu Grunde liegenden Modelle und Schutzmechanismen der Realität angemessen Rechnung tragen. Daneben ergeben sich auch im Hinblick auf die IT-Sicherheit zusätzliche Risiken, deren Beherrschbarkeit außergewöhnlich anspruchsvoll erscheint.

II. Die Geltungskraft der datenschutzrechtlichen Regelungskonzepte des 20. Jahrhunderts in der Welt des 21. Jahrhunderts

1. Datenschutz in sozialen Netzwerken

Mit dem Siegeszug der Web 2.0-Anwendungen, allen voran der sozialen Netzwerke, wurde der vormals einseitige Informationsfluss im Internet um Elemente der Interaktion zwischen den Nutzern erweitert: Die Nutzer der ersten Web-Generation der 1990er Jahre waren, wenn sie nicht gerade selbst eine Webseite betrieben, in erster Linie passive Konsumenten fremder, oft von großen Wirtschaftsunternehmen erstellter Inhalte. Der Informationsfluss verlief überwiegend wie in einer Einbahnstraße, in der die Teilnehmer kaum aktiv an der Gestaltung der Inhalte mitwirkten. Das Web 2.0 änderte die Wahrnehmung und Nutzung des Internets von Grund auf. Aus einer Informationsbereitstellung von Wenigen für Viele wurde die interaktive Kommunikation Vieler mit Vielen. Ob Blogs, Wikis, soziale Netzwerke oder Media-Sharing-Plattformen: Die Interaktivität der neuen Anwendungen erlaubte den Nutzern, fremde Inhalte zu bewerten und eigene Inhalte zu erstellen und beides zu verbreiten. Aus dem passiven Konsumenten wurde ein aktiver Produzent eigener Inhalte bzw. der „Prosument", der gleichermaßen Empfänger und Sender von Informationen ist.

a) Interaktivität

Angesichts dieses neuen Rollenverständnisses verwundert es nicht, dass die datenschutzrechtliche Zuweisung von Verantwortlichkeiten, die auf einer strikten Trennung zwischen „Betroffenen" einerseits und „verantwortlichen Stellen" andererseits beruht, immer schwieriger ist. Nach der Rollenverteilung des Bundesdatenschutzgesetzes (BDSG) ist der Betroffene als Objekt der Datenverarbeitung Inhaber der personenbezogenen Daten, die Gegenstand der Erhebung, Verarbeitung oder Nutzung sind. Den Betroffenen gegenüber steht die „verantwortliche Stelle", die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies im Wege der so genannten Auftragsdatenverarbeitung vornehmen lässt (§ 3 Abs. 7 BDSG).

Wenn aber die Nutzer sozialer Medien nun selbst zu Autoren werden und dabei eigene und Daten fremder Personen ins Netz einstellen, entsteht eine Gemengelage, die Ausstrahlungswirkung auf die datenschutzrechtlichen Verantwortlichkeiten im Netz hat. Zwar erfasst das BDSG nicht den Datenumgang im ausschließlich persönlichen oder

familiären Bereich (§ 1 Abs. 3 Ziffer 3 BDSG). Verfolgt der Nutzer aber kommerzielle, politische oder auch nur karitative Zwecke, wird der Bereich der rein persönlich-familiären Tätigkeiten verlassen[1]. Gleiches gilt nach der Lindqvist-Entscheidung des EuGH[2], wenn eine Veröffentlichungsform gewählt wird, die einer unbegrenzten Zahl von Personen zugänglich ist, wie etwa die Informationsverbreitung über eine allgemein zugängliche Webseite. Auch hier wird der Bereich der rein persönlich-familiären Tätigkeiten verlassen. Der Richterspruch des EuGH hat somit, zumindest potentiell, zu einer massiven Erweiterung des Adressatenkreises der Europäischen Datenschutzrichtlinie geführt. Nutzer sozialer Netzwerke, die als Privatpersonen personenbezogene Daten Dritter in allgemein zugänglicher Weise veröffentlichen, müssen sich daher bewusst sein, als „verantwortliche Stelle" datenschutzrechtlich in der Verantwortung stehen zu können.

b) Internationalität

Aber nicht nur die Interaktivität, auch die Internationalität des Internets bereitet Probleme bei der Zuweisung datenschutzrechtlicher Verantwortlichkeiten, vor allem aber bei der Durchsetzung datenschutzrechtlicher Maßnahmen. Global agierende Unternehmen, die wie Google, Microsoft oder Facebook ihren Unternehmenssitz in den USA haben, können durch das deutsche Datenschutzrecht, insbesondere das Telemediengesetz (TMG) und das BDSG, nur dann belangt werden, wenn deutsches Recht auf diese Unternehmen überhaupt Anwendung findet. Für Unternehmen, die von einem Drittland außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums agieren, gilt deutsches Datenschutzrecht nach § 1 Abs. 5 Satz 2 BDSG aber nur, sofern personenbezogene Daten im Inland erhoben werden.

Ob es für die Anwendbarkeit deutschen Rechts ausreicht, dass der Nutzer an seinem heimischen PC personenbezogene Daten in ein Anmeldeformular auf der Website des Diensteanbieters eingibt[3], ob das Nutzen eines auf der Festplatte des Nutzers platzierten Cookies eine Datenerhebung im Inland darstellt[4] und ob es für die Anwendung europäischen Datenschutzrechts vielleicht sogar schon genügt, dass sich der Onlinedienst erkennbar auch an europäische Nutzer wendet[5] – all dies sind Fragestellungen, mit denen sich der historische Gesetzgeber nicht befasst hat und die heute Auslegungsschwierigkeiten bereiten.

2. Datenverarbeitung durch Cloud Computing

Das Cloud Computing ist nicht nur, aber eng mit der Entwicklung des Web 2.0 verbunden. Denn die rasante Zunahme von Nutzern und Diensten im Web 2.0 erforderte Strukturen, die dem steigenden Datenaufkommen Rechnung tragen. Beim Cloud Computing handelt es sich um die internetbasierte Verlagerung von IT-Infrastrukturen wie Rechenleistung und Speicherressourcen (Infrastructure-as-a-Service, IaaS), Entwicklungsplattformen (Platform-as-a-Service, PaaS) und Anwendungen (Software-as-a-Service, SaaS) in die „Rechnerwolke". Anstatt die Daten auf dem eigenen Rechner abzulegen, kann beispielsweise ein Versandhändler Kunden- und Lieferantendaten oder Daten über die Zeiterfassung der eigenen Mitarbeiter in die Cloud auslagern[6]. Dies ermöglicht dem Cloud-Anwender eine ortsungebundene und bedarfsabhängige Nutzung von IT-Ressourcen und somit eine flexible und kostengünstige Abrufbarkeit von IT-Strukturen, die von Dritten bereitgestellt werden. Technologisch handelt es sich beim Cloud Computing um die Fortsetzung der bereits seit Jahren zu beobachtenden Tendenz zur Virtualisierung und deren Erstreckung auf weltweit verteilte, vernetzte Infrastrukturen einschließlich der bereitgestellten Dienste. Während die Anfänge des Cloud Computings durch unternehmensinterne bzw. nutzerexklusive Lösungen geprägt waren (Private Cloud), haben sich mittlerweile unternehmensübergreifende Cloud-Strukturen durchgesetzt (Public Cloud).

a) Strukturelles Machtungleichgewicht beim Cloud Computing

So einfach die Idee der Rechnerwolke ist, so komplex sind die mit dem Cloud Computing verbundenen datenschutzrechtlichen Problemstellungen[7]. Zum einen geht es um die Frage, wie der Cloud-Anwender, also die Stelle, die die Cloud-Strukturen des Cloud-Anbieters in Anspruch nimmt, den Cloud-Anbieter kontrollieren und überwachen soll. Denn in aller Regel wird der Cloud-Anwender auf angemietete Ressourcen des Cloud-Anbieters zurückgreifen, ohne ihm die Aufgabe der Datenverarbeitung zu übertragen oder ihm eigenständige Handlungs- und Entscheidungsspielräume über die Daten einzuräumen. Die damit verbundene Funktion des Cloud-Anbieters als Auftragsdatenverarbeiter des Cloud-Anwenders nach § 11 BDSG hat die folgenreiche Konsequenz, dass der Cloud-Anwender datenschutzrechtlich verantwortliche Stelle im Sinne des BDSG bleibt[8]; der Cloud-Anwender hat daher für die

[1] Stellungnahme 5/2009 der Artikel-29-Datenschutzgruppe zur Nutzung sozialer Online-Netzwerke (WP 163), S. 6.

[2] EuGH C-101/01 vom 0.11.2003 (Lindqvist); Simitis/Dammann, BDSG, 7. Aufl., § 1 Rn. 151; angedeutet in der Stellungnahme 5/2009 der Artikel-29-Datenschutzgruppe (WP 163), S. 7.

[3] Mangels Erhebungswillens des Diensteanbieters verneinend S*imitis/Dammann*, BDSG, 7. Aufl., § 1 Rn. 223.

[4] *Bejahend Simitis/Dammann*, BDSG, 7. Aufl., § 1 Rn. 227 m.w.N.; Arbeitspapier der Artikel-29-Datenschutzgruppe (WP 56), S. 11f.; Stellungnahme 1/2008 der Artikel-29-Gruppe zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148), S. 12.

[5] Vgl. dazu *Simitis/Dammann*, BDSG, 7. Aufl., § 1 Rn. 220; Stellungnahme 8/2010 der Artikel-29-Datenschutzgruppe zum anwendbaren Recht (WP 179), S. 30f.

[6] *Heidrich/Wegener,* Sichere Datenwolken – Cloud Computing und Datenschutz, MMR 2010, S. 803 (805).

[7] instruktiv hierzu: *Heidrich/Wegener,* Sichere Datenwolken – Cloud Computing und Datenschutz, MMR 2010, S. 803 (805ff.); *Nägele/Jacobs*, ZUM 2010, S. 281 (289ff).

[8] Eine Auftragsdatenverarbeitung nach § 11 BDSG ist bei einer nicht-europäischen Cloud allerdings nicht möglich, da der Auftrag-

Einhaltung sämtlicher datenschutzrechtlicher Vorschriften einzustehen.

Um dies gewährleisten zu können, hat sich der Auftraggeber von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu überzeugen (§ 11 Abs. 2 Satz 4 BDSG). Zudem müssen unter anderem datenschutzrechtliche Kontrollrechte des Cloud-Anwenders (§ 11 Abs. 2 Satz 2 Ziff. 7 BDSG) und der Umfang seiner Weisungsbefugnisse gegenüber dem Cloud-Anbieter (§ 11 Abs. 2 Satz Ziff. 9 BDSG) schriftlich fixiert werden.

Ein Blick auf die tatsächliche Machtverteilung zwischen Cloud-Anwender und Cloud-Anbieter führt allerdings schnell zu dem Schluss, dass die gesetzlichen Anforderungen der Auftragsdatenverarbeitung in der Praxis kaum eingehalten werden. Wenn man sich vergegenwärtigt, dass globale Schwergewichte wie Google, IBM, Microsoft und Amazon zu den derzeit führenden Cloud-Computing-Anbietern zählen, darf man angesichts der wirtschaftlichen Überlegenheit der Cloud-Anbieter Bedenken haben, wie der Cloud-Anwender als Kunde regelmäßige Datenschutzkontrollen durchführen und seine Weisungsbefugnisse gegenüber den Cloud-Anbietern durchsetzen soll[9].

Besonders gravierend ist das Kontrolldefizit der Nutzer bei endkundenorientierten Cloud-Diensten, bei denen private Anwender und kleine Unternehmen standardisierte Lösungen in Anspruch nehmen. Für die Nutzer dieser Dienste bestehen praktisch keinerlei Einflussmöglichkeiten auf den Umgang mit personenbezogenen Daten außerhalb der von dem Anbieter angebotenen Konfigurationsmöglichkeiten. Im Hinblick darauf, dass eine Reihe dieser Dienste entgeltfrei erbracht werden, beruhen die Geschäftsmodelle der Anbieter im Wesentlichen auf der Auswertung und Vermarktung der Nutzerdaten für personalisierte Werbung.

b) Entörtlichung der Datenverarbeitung

Wenn freie Kapazitäten in der Wolke erst ad hoc zugewiesen werden, wird der Cloud-Anwender in der Regel gar nicht wissen, auf welchem Server des Cloud-Anbieters „seine" Daten (momentan oder grundsätzlich) gespeichert sind. Der Ort der physischen Speicherung der Daten kann sich zudem sehr schnell ändern, wenn der Cloud-Anbieter über mehrere Serverstandorte in unterschiedlichen Ländern verfügt[10]. Die damit verbundene *Entörtlichung* der Datenverarbeitung ist nicht nur im Rahmen der Kontrolle des Auftragnehmers problematisch, sondern wirft zugleich die Frage auf, ob in Drittstaaten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums ein angemessenes Datenschutzniveau besteht. So können in Deutschland durch den Cloud-Anwender erhobene Daten, beispielsweise Kundendaten eines Versandhandelsunternehmens, durch den Cloud-Anbieter auf weltweit verteilten Servern gespeichert sein.

In diesem Zusammenhang ist bislang nur unzureichend geklärt, ob und wie sichergestellt werden kann, dass der Zugriff ausländischer Sicherheitsbehörden auf innereuropäische Daten nur dann erfolgt, wenn die Datenweitergabe auch deutschem und europäischem Datenschutzrecht entspricht. Das gilt im Hinblick auf die Dominanz US-amerikanischer Cloud-Anbieter in besonderem Maße für den Zugriff von US-Sicherheitsbehörden auf Cloud-Daten nach dem durch den US Kongress im Zuge der Terrorangriffe erlassenen USA PATRIOT Act. Eine Zugriffsmöglichkeit der US-Sicherheitsbehörden auf Cloud-Daten amerikanischer Anbieter soll – zumindest nach amerikanischer Lesart – selbst dann bestehen, wenn diese Daten innerhalb der Europäischen Union gespeichert sind. Übersehen werden darf dabei allerdings nicht, dass auch andere Staaten ihren Sicherheitsbehörden umfangreiche Zugriffsbefugnisse einräumen, denen sich die Betreiber von Cloud-Services kaum entziehen können.

3. Ubiquitous Computing – bereits jetzt ein reales Szenario

Im Vergleich zu anderen Rechtsmaterien ist der Datenschutz eine relativ junge Disziplin, deren Ursprung in den Möglichkeiten und Gefahren automatisierter Datenverarbeitungsformen der 1960er Jahren liegt. Schon damals war Datenschutz also eine Reaktion des Gesetzgebers auf den technischen Fortschritt. Während sich die Datenverarbeitung vor 40, 50 Jahren allerdings in wenigen zentralen, gut zu kontrollierenden Rechenzentren vollzog, stieg der Schutzbedarf mit der zunehmenden Verbreitung computergestützter Datenverarbeitung durch für jedermann erschwingliche PCs ab den 1980er Jahren an. Dennoch blieben die datenschutzrechtlichen Probleme aufgrund der physischen Lokalisierbarkeit der Daten weitgehend beherrschbar. Dies änderte sich erst, als in den 1990er Jahren das Internet eine weltweite Vernetzung der Rechner ermöglichte[11].

Durch die Fortentwicklung der Chiptechnik zu immer kleineren, leistungsfähigeren und billigeren Rechnern hat der zentrale PC mittlerweile deutlich an Bedeutung verloren. An dessen Stelle ist die mobile und vernetzte Datenverarbeitung durch eine Vielzahl von Rechnern getreten, die die Nutzer kontextbezogen und im Hintergrund unter-

nehmer der Auftragsdatenverarbeitung nach der Definition in § 3 Abs. 8 Satz 2 BDSG eine Stelle im Inland, in der Europäischen Union oder innerhalb des EWR sein muss. Datenschutzrechtlich handelt es sich bei dem Datentransfer um eine Datenübermittlung i.S.d. § 3 Abs. 4 Ziffer 3 BDSG, die einer Rechtsgrundlage bedarf.

[9] Vgl. zu der Problematik auch 23. Tätigkeitsbericht des BfDI, 5.6, S. 63f.; *Heidrich/Wegener*, Sichere Datenwolken – Cloud Computing und Datenschutz, MMR 2010, S. 803 (806).

[10] *Heidrich/Wegener*, Sichere Datenwolken – Cloud Computing und Datenschutz, MMR 2010, S. 803 (806); Nägele/Jacobs, ZUM 2010, S. 281 (289f.).

[11] Vgl. zu den einzelnen Entwicklungsstufen Roßnagel, MMR 2005, S. 71ff.

stützen. Prominenteste Vertreter sind derzeit wohl die so genannten RFID-Tags (Radio Frequency Identification). Diese Funkchips, die zum Beispiel zur Warensicherung in Kaufhäusern verwendet und zunehmend auch in Kunden- und Bankkarten integriert werden, können im Umkreis von wenigen Zentimetern von stationären Kontrolleinheiten erkannt werden[12]. Aber nicht nur durch die RFID-Technik, auch durch eine Vielzahl „smarter" Alltagsgegenstände wird Datenverarbeitung allgegenwärtig. Das gilt nicht nur für die *Smartphones*, die ihre Besitzer auf Schritt und Tritt begleiten, sondern auch für Fahrzeuge, die mittlerweile derart mit Informationstechnik versehen sind, dass sie als „rollende Computer" Fahr- und Fehlverhalten ihrer Nutzer registrieren und verfügbar machen. In die Kategorie „intelligenter Gegenstände" lassen sich schließlich auch „intelligente Stromzähler", die geräte- und zeitgenau den Energieverbrauch messen und steuern, so genannte „smart meter", einordnen. Zweifellos steht die Technisierung des Alltags noch am Anfang. Der weitere Schritt von der mobilen zur allgegenwärtigen Datenverarbeitung zeichnet sich allerdings bereits ab. In der Zukunft könnte die Spannweite der Allgegenwärtigkeit der Informationstechnologie von Autoreifen, die einen kritischen Reifendruck an den Fahrer melden, über Kühlschränke, die aktuellen Einkaufsbedarf anzeigen, bis hin zu Arzneimitteln, die dem Arzneischrank den Ablauf des Verfallsdatums signalisieren, reichen[13].

Für den Datenschutz birgt diese ubiquitäre Rechner-Allgegenwart (ubiquitous computing) große Gefahren. Denn „smarte" Alltagsgegenstände, die den Nutzern das Leben erleichtern sollen, müssen schon von ihrer Zweckbestimmung her unauffällig arbeiten. Der Nutzer soll im Idealfall gar nicht merken, dass im Hintergrund eine Verarbeitung von Informationen stattfindet.

a) Intransparenz

Das Postulat der Unauffälligkeit der Datenverarbeitung ist allerdings mit dem das Datenschutzrecht prägenden Grundsatz des Verbots mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG), der jeglichen Umgang mit personenbezogenen Daten ohne Vorliegen einer Rechtsgrundlage – sei es einer Einwilligung des Betroffenen oder einer gesetzlichen Erlaubnisnorm – untersagt, kaum zu vereinbaren. Insbesondere den Erfordernissen der Einwilligung, die stets auf informierter Grundlage erfolgen muss, kann das Konzept ubiquitärer rechnergestützter Datenverarbeitung derzeit kaum gerecht werden. Eine vollständige Transparenz, zu welcher Gelegenheit welche Daten an welche Empfänger übermittelt und zu welchen Zwecken sie dort verarbeitet werden, würde die Nutzer angesichts der Vielfalt und Häufigkeit der Datenverarbeitungsvorgänge wohl überfordern[14]; in jedem Fall aber wäre die Einholung einer Einwilligung im alltäglichen Leben kaum praktikabel, weil sie von den Nutzern schnell als belästigend empfunden würde. Schon heute lässt sich beobachten, dass lange und komplizierte Einwilligungserklärungen in die Datenverarbeitung von Smartphone-Applikationen von den Nutzern erfahrungsgemäß allenfalls überflogen und in der Regel in ihrer Tragweite nicht verstanden werden. Fehlt dem Nutzer aber das Bewusstsein und der Überblick, bei welcher Gelegenheit welche personenbezogenen Daten von ihm verarbeitet werden, kann er andererseits aber auch seine datenschutzrechtlichen Ansprüche auf Auskunft, Berichtigung und Löschung nicht geltend machen.

b) Dekontextualisierung

Erhebliche Probleme bereitet auch die Umsetzung des datenschutzrechtlichen Grundsatzes der Erforderlichkeit bzw. der Datensparsamkeit sowie des Grundsatzes der Zweckbindung[15]. Der Grundsatz der Datensparsamkeit besagt, dass so wenig Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen. Dem Grundsatz der Zweckbindung entspricht es, dass die Daten nur für diejenigen Zwecke verarbeitet oder genutzt werden dürfen, für die sie erhoben wurden. Wenn nun aber „smarte" Gegenstände den Nutzer spontan und situationsbedingt unterstützen sollen, müssen die Systeme so viel verfügbare Daten wie möglich aggregieren, um diese für künftige Zwecke auf Anforderung vorhalten zu können[16]. Durch die massenhafte, nicht zweckgebundene Speicherung von Daten kommt es dann zu einer datenschutzrechtlich problematischen Vorratsdatenhaltung[17]. Damit einher geht eine *Dekontextualisierung* der Daten in der Weise, dass personenbezogene Daten, die ursprünglich zu einem bestimmten Zweck erhoben worden sind, in anderem Zusammenhang – außerhalb des Erhebungskontextes – verwendet werden können und dabei möglicherweise auch ein falsches Bild vom Nutzer zeichnen.

In der Konsequenz ermöglichen „smarte" Gegenstände, die alle Handlungen, Bewegungen und Vorlieben ihrer Nutzer registrieren, eine umfassende Katalogisierung der Person, die bis zur Bildung detaillierter Persönlichkeitsprofile reichen kann. Wer Zugriff auf die geräte- und zeitgenaue Energieverbrauchsmessung „intelligenter" Stromnetze hat, kann sehr genau abschätzen und prognostizieren, wie der Bewohner lebt. Wenn in einem zweiten Schritt die „smarte" Heizung mit dem Smartphone des Bewohners kommuniziert, um den Aufenthaltsort des Nutzers und damit den Zeitpunkt zu ermitteln, wann das Haus beim Eintreffen des Bewohners wieder warm sein soll, dann ergibt sich in der Zusammenschau eine Alltagsüberwachung, die mancher als praktisch, viele aber auch als bedrohlich empfinden werden.

---

[12] zu der datenschutzrechtlichen Problematik der RFID-Anwendungen auch der 23. Tätigkeitsbericht des BfDI, 5.9, (S. 66).

[13] Beispiele von *Mattern*, Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing; ders., Ubiquitous Computing: Schlaue Alltagsgegenstände.

[14] *Roßnagel*, MMR 2005, S. 71 (72).

[15] *Roßnagel*, MMR 2005, S. 71 (72).

[16] *Roßnagel*, MMR 2005, S. 71 (72); *Mattern*, Ubiquitous Computing: Schlaue Alltagsgegenstände.

[17] *Roßnagel*, MMR 2005, S. 71 (72).

III. Modernisierung des Datenschutzrechts

Social Networks, Cloud Computing, Apps und Ubiquitous Computing – wohin man auch schaut, in der globalen Welt des Internets stößt das derzeitige Recht – vor allem in seiner Ausformung auf nationaler Ebene – an seine Grenzen. Reformbemühungen müssen den Ursachen dieser Begrenztheit Rechnung tragen.

Erstens wird das heutige Datenschutzrecht auf ein Medium angewendet, dessen Möglichkeiten bei der Schaffung der Gesetze allenfalls ansatzweise absehbar waren. Die letzte große Novellierung des BDSG liegt mittlerweile über zehn Jahre zurück – in einem innovationsfreundlichen Umfeld wie dem Internet eine unglaublich lange Zeitspanne. Schon bei der Umsetzung der Europäischen Datenschutzrichtlinie 95/46/EG in das BDSG im Jahr 2001 war man sich darüber im Klaren, dass die Novellierung zu wenig zukunftsweisend war. Da aufgrund der abgelaufenen Umsetzungsfrist der Richtlinie allerdings Eile geboten war, wurden die Bedenken bei Seite geschoben und durch das Bundesministerium des Innern parallel zum Gesetzgebungsvorhaben ein Gutachten in Auftrag gegeben, das Ansatzpunkt für eine grundlegende Modernisierung des Datenschutzrechts sein sollte[18]. Das Gutachten fand allerdings in der Folgezeit bei den gesetzgeberischen Aktivitäten kaum Beachtung, so dass eine grundlegende Modernisierung des Datenschutzrechts überfällig ist. Ganz wesentlich wird es dabei auch darum gehen, das Datenschutzrecht internetfähig zu machen[19].

Zweitens erstreckt sich das Erfordernis eines moderneren Datenschutzrechts auch und in erster Linie auf die überstaatliche Ebene. Ein Medium, dass an keine nationalen Grenzen gebunden ist, diese sogar überwinden soll, kann durch rein nationalstaatliche Vorgaben nicht reglementiert werden. So sind datenschutzrechtliche Anordnungen oder Bußgeldbescheide deutscher Datenschutzaufsichtsbehörden nicht ohne Weiteres in den USA durchsetzbar. Nationale Bemühungen, den Datenschutz im Internet zu stärken, sei es nur bei besonders schweren Eingriffen in das Persönlichkeitsrecht[20], sei es im Sinne einer umfassenden Modernisierung, sind daher zwar notwendig, aber nicht ausreichend. Ein ganzheitlicher Ansatz muss ein verbindliches und überzeugendes internationales, wenigstens aber ein europäisches Datenschutzkonzept beinhalten. Die von der Europäischen Kommission angekündigte Revision der Europäischen Datenschutzrichtlinie[21], deren Schwerpunkt in den datenschutzrechtlichen Herausforderungen des Internets liegen soll, ist daher auch im Sinne eines ganzheitlichen europäischen Mindestdatenschutzstandards zu begrüßen. Auch die Überlegungen in den USA zur Schaffung einer „Bill of Rights“ zum Datenschutz im Internet[22] wecken Hoffnungen.

Und drittens sollte auch der wichtige Aspekt des Datenschutzes durch Technik stärker in den Vordergrund rücken. Das bisherige Datenschutzrecht ist traditionell von einem reaktiven Ansatz geprägt, welcher auf dem Verständnis beruht, dass das Datenschutzrecht der Technik folgt: Auf den technischen Fortschritt reagiert der Gesetzgeber bisweilen mit technikspezifischen punktuellen Regelungen, die genau auf die neue Technik zugeschnitten sind. Der Ansatz hat allerdings nicht nur den Nachteil einer großen zeitlichen Verzögerung des Rechtsschutzes, er leidet auch an der Unübersichtlichkeit kasuistischer Detailregelungen, die die Gesetze immer schwerer lesbar und anwendbar werden lassen.

Es ist daher effizienter, durch das Recht auf die Gestaltung der Technik einzuwirken, anstatt nachträglich die Folgen der technischen Entwicklung durch Gesetze zu regulieren. Denn was bereits technisch verhindert wird, muss später nicht mehr verboten werden[23]. Umgekehrt ist die frühzeitige Berücksichtigung von Datenschutzanforderungen bei der Technikgestaltung auch wirtschaftlich sinnvoll, weil sie nachhaltige Geschäftsmodelle ermöglicht, die ohne Nachbesserungen und unvertretbare Risiken funktionieren. Mit diesem Ansatz wird eine Vorverlagerung des Datenschutzes auf die technische Entwicklungsebene erreicht. Die technischen Datenschutzkonzepte des „Privacy by Design“ und des „Privacy by Default“ haben in dieser Idee, die sich auch in dem Gebot der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) widerspiegelt, ihren Ursprung. Während sich das Konzept des „Privacy by Design“ an die Entwickler und Hersteller von Produkten richtet, weil zuallererst sie bestimmen können, welche Daten von dem Produkt gesammelt werden, umfasst „Privacy by Default“ datenschutzfreundliche Grundeinstellungen, von denen die Nutzer selbstbestimmt abweichen können, wenn sie dies wollen.

Ein wichtiger Bestandteil eines umfassenden „Privacy by Design“-Konzepts können beispielsweise Datenschutzfolgeabschätzungen sein, also die systematische Bewertung der Auswirkungen einer konkreten Anwendung auf die Pri-

[18] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministerium des Innern, 2001.

[19] Vgl. dazu auch das im März 2010 verabschiedete Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

[20] Vgl. dazu den am 01.12.2010 angekündigten Gesetzentwurf des Bundesministerium des Innern zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht,

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile

[21] Gesamtkonzept für den Datenschutz in der Europäischen Union, Mitteilung der Kommission vom 04.11.2010, KOM(2010) 609, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf

[22] http://www.heise.de/newsticker/meldung/US-Regierung-plant-Bill-of-Rights-zum-Datenschutz-im-Internet-1209792.html

[23] *Roßnagel*, MMR 2005, S. 71 (74).

vatsphäre, wie sie die Hersteller von RFID-Anwendungen entwickelt haben[24]. In ein „Privacy by Design"-Konzept für soziale Netzwerke könnte die Überlegung einfließen, ob die Angabe des Klarnamens für die Mitgliedschaft wirklich erforderlich ist oder ob ggf. auch ein pseudonymes Profil ausreichen kann. Um „Privacy by Default" handelt es sich zum Beispiel, wenn die Profilinformationen in sozialen Netzwerken nicht standardmäßig den übrigen Mitgliedern zugänglich sind, sondern erst auf Wunsch des Nutzers öffentlich gemacht werden[25].

IV. Zusammenfassung und Ausblick

Die vernetzte digitale Welt des 21. Jahrhunderts stellt den Datenschutz vor enorme Herausforderungen. Auf die Problematik, dass der Schutzbedarf des Einzelnen in Folge der technischen Fortschritte immer höher, aufgrund der technischen Gegebenheiten der – auch grundrechtlich gebotene – Schutz zugleich aber immer schwieriger zu gewährleisten ist, hat das heutige Datenschutzrecht keine Antwort. Die Interaktivität, die Entörtlichung und die Dekontextualisierung der Datenverarbeitung macht es erforderlich, national und international neue Wege zu beschreiten. Datenschutz durch Technik kann hierbei eine entscheidende Rolle spielen, um den datenschutzrechtlichen Herausforderungen der neuen Technik Rechnung zu tragen. Wenn es gelingt, datenschutzfreundliche Standards bereits bei der Entwicklung und Bereitstellung von Produkten und Programmen einzubetten, wird Datenschutz zu einem technischen Gestaltungsanspruch, der Hersteller, Entwickler und Diensteanbieter in die Pflicht nimmt – also genau die Zielgruppe, die den Umgang mit personenbezogenen Daten im Netz auch maßgeblich steuern kann.

---

[24] http://ec.europa.eu/information_society/policy/rfid/documents/pia-de.pdf

[25] Stellungnahme 5/2009 der Artikel-29-Datenschutzgruppe (WP 163), S. 8.