Wolfgang Kilian

Strukturwandel der Privatheit

In seinem großen Gutachten zum Datenschutz, das im Jahre 1972 die Grundlage für die deutsche und europäische Datenschutzgesetzgebung gelegt hat, schrieb mein Freund und langjähriger Fachkollege Wilhelm Steinmüller: „Die Privatsphäre hat ausgedient“[1]. Er wollte damit nicht die Schutzwürdigkeit der Privatsphäre bestreiten, sondern vielmehr die Tauglichkeit des gewohnheitsrechtlich in § 823 BGB verankerten Allgemeinen Persönlichkeitsrechts und der damit verbundenen „Sphärentheorie“[2] als Rechtsgrundlage gegen Missbräuche bei der elektronischen Verarbeitung personenbezogener Daten in Frage stellen. Der Persönlichkeitswert hänge von Ort, Zeit und den Trägern ab[3]. Als EDV-angemessenen neuen Ansatz empfahl er, die Verarbeitung personenbezogener Individualinformationen als Ausdruck der Selbstbestimmung und der allgemeinen Handlungsfreiheit zum Gegenstand eines Datenschutzrechts zu machen. Für diesen Ansatz lag die Bezeichnung „informationelle Selbstbestimmung“ in der Luft. Die Bezeichnung ist von Steinmüller, Podlech und Lutterbeck entwickelt worden[4] und taucht bereits in dem Gutachten auf[5] auf, lange bevor das Bundesverfassungsgericht die Formulierung im Volkszählungsurteil[6] ohne weitere Belege aufgriff und dafür weltweit berühmt wurde.

Mark Zuckerberg, der Gründer von Facebook, hat im Jahre 2010 festgestellt: „Privacy is no longer a social norm“[7]. Nach seiner Meinung möchten die Menschen heute mehr Informationen untereinander frei austauschen. Mit diesem empirischen Befund zeigt er sich verständlicherweise sehr zufrieden. Zur Schutzwürdigkeit solcher Informationen und des Informationsaustauschs nimmt er keine Stellung.

In den Meinungen könnte ein Strukturwandel der Privatheit und der Möglichkeit von Rechtsschutz bei elektronischer Kommunikation impliziert sein. Auch wenn der deutsche „Persönlichkeitsschutz“ nicht mit dem US-amerikanischen Konzept der „Privacy“ identisch sind, betreffen sie doch überlappende Gegenstände. Im Kern geht es um die Frage, ob und in wieweit Informationen über eine Person auch dann frei zirkulieren sollen, wenn sie nicht für die Öffentlichkeit bestimmt sind, sondern aus ethischen, moralischen, sexuellen, religiösen, medizinischen, politischen oder sonstigen Gründen von der Person selbst als einem vernunftbegabten Subjekt beansprucht werden.

Aus philosophischer, historischer und linguistischer Sicht hat Trendelenburg[8] exegetisch nachgewiesen, dass „Person“ das Besondere eines Menschen umfasst, die tiefere Bezeichnung des Menschlichen (Leibniz[9]), und dass die Person Zweck an sich selbst ist und nicht bloß ein zu gebrauchendes Mittel (Kant[10]). Trendelenburg begründet die moralische Idee der Persönlichkeit letztlich psychologisch als „Vermögen des Menschen, sich in den verschiedenen Zuständen seines Daseins der Identität selbst bewusst zu werden“[11].

In der deutschen juristischen Tradition des 19. Jahrhunderts – von Kohler[12] über Gierke[13] bis Dernburg[14] – lag es, Persönlichkeitsrechte (Individualrechte) auf Respektierung einer Geheimsphäre zu postulieren. Das Bürgerliche Gesetzbuch verzichtete aber auf die Einführung einer ausdrücklichen Schutzvorschrift und entsprechend erkannte das Reichsgericht[15] Persönlichkeitsrechte im Rahmen von § 823 Abs.1 BGB nicht als „sonstige Rechte“ an. Erst der Bundesgerichtshof[16] und bis heute das Bundesverfassungsgericht[17] gehen vom Bestand nicht präzise definierter Schutzsphären um eine Person („Sphärentheorie“) aus, die seit dem Jahr 1947 in einem gewohnheitsrechtlich anerkannten „Allgemeinen Persönlichkeitsrecht“[18] als „sonstigem Recht“ verankert gesehen werden.

1. Empirischer Befund zur Privatheit personenbezogener Daten

Es lässt sich nicht leugnen, dass praktisch alle Informationen, die sich auf eine bestimmte Person beziehen, heute elektronisch für staatliche oder private Zwecke umfassend gesammelt und ausgewertet werden. Zwar gilt im deutschen und europäischen Datenschutzrecht der Grundsatz, dass die Verarbeitung personenbezogener Daten nur zulässig ist, wenn dafür eine Rechtsvorschrift besteht oder die Einwilligung der betroffenen Person vorliegt[19]. Beide Voraussetzungen wirken sich jedoch kaum als effektive Schranke für die Art, den Umfang oder den Zweck der Verarbeitung personenbezogener Daten aus.

Im *öffentlichen Bereich* bestehen eine unüberschaubare Zahl von Ermächtigungsgrundlagen. Sie sind teils sehr präzise gefasst (Sozialgesetzgebung, Steuerverwaltung), teils sehr vage formuliert (geheimdienstliche Tätigkeit). Einschränkungen der Verarbeitung personenbezogener Daten müssen oft gerichtlich erkämpft werden. Die Gerichte begründen das dann regelmäßig mit dem Recht auf informationelle Selbstbestimmung (Interpretation von Art. 2 Abs. 1 i. V. m. Art 1 Abs. 1 GG) oder mit der Rechtswidrigkeit der zu Grunde gelegten Zweck-Mittel-Relation[20].

Die Voraussetzung der Einwilligung der betroffenen Person in die Verarbeitung personenbezogener Daten hat bei Vorliegen anerkannter öffentlicher Zwecke keine Funktion mehr. Insoweit wird die Person zwangsweise „entprivatisiert". Über die Legitimität der Entprivatisierung wird allerdings in einem Rechtsstaat öffentlich diskutiert und parlamentarisch entschieden, so dass sich Legalität und Legitimität dann offenbar decken. Die Existenz und das Schutzniveau der Privatheit hängen somit von politischen und kulturellen Einflüssen sowie von Rechtstraditionen ab. Angaben über die

Besteuerung einer Person etwa sind in Finnland frei zugänglich, in Deutschland nicht.

Die Verarbeitung personenbezogener Daten im *nichtöffentlichen Bereich* wurde ursprünglich nicht als Gefahr für die Privatsphäre wahrgenommen[21]. Das hat sich mit der weiteren Entwicklung der Informations- und Kommunikationstechnologie dramatisch geändert, denn leistungsfähige Computer und globale Netzwerke ermöglichen eine nach Menge, Inhalt, Zweck, Ort und Zeit unbegrenzte Verarbeitung personenbezogener Daten. Die personalisierte Medizin (Gendiagnostik; Onkogenomik) erfasst immer tiefere biologische Schichten eines Individuums und produziert sehr sensible Daten.

Parallel zur technologischen Entwicklung haben sich die moralischen und sittlichen Auffassungen in der Gesellschaft nachhaltig verändert. Vieles, was früher undenkbar oder verboten war, gilt heute als Ausdruck liberaler Gesinnung: „Reality"-Shows im Fernsehen; Versenden von Nacktfotos der eigenen Person über soziale Netzwerke; detaillierte Berichte über Erkrankungen. Das „Outen" einer Person als „homoerotisch" findet nur noch dann überhaupt besondere öffentliche Aufmerksamkeit, wenn es sich um Fußballnationalspieler handelt. Informationen, die früher zur „Intimsphäre" zählten, werden heute von ihren Trägern bewusst öffentlich zugänglich gemacht.

Manche personenbezogene Daten sind heute in vielen Marktsituationen allerdings auch unentbehrlich geworden. Ein Arbeitsvertrag könnte beispielsweise nicht erfüllt werden, wenn der Arbeitgeber nicht Angaben über den Familienstand, die Zahl der Kinder, das Vorliegen einer Schwerbehinderung oder weitere ungefähr 70 personenbezogene Daten eines Arbeitnehmers erfragen, speichern und für Abrechnungs-, Verwaltungs- und Planungszwecke verwenden dürfte.

Schon länger haben aber auch spezielle Dienstleistungsunternehmen sehr erfolgreich Geschäftsmodelle entwickelt, deren Gegenstand die systematische elektronische Sammlung und Verarbeitung personenbezogener Daten zum Zweck der Weitergabe gegen Bezahlung bildet. Digitalisierte Adressen, persönliche Fotos, biometrische Daten, individuelle Präferenzen, Kommunikationsdaten, individuelle Bewertungen, fast alles, was früher als „privat" und unveräußerlich galt, wird heute vermarktet. Der Marktwert von Facebook, der fast ausschließlich auf dem Verkauf solcher personenbezogenen Daten beruht, wird auf über 100 Millarden US-Dollar geschätzt[22].

Anreize für die Erlangung personenbezogener Daten bieten solche Dienstleistungsunternehmen dadurch an, dass sie die Nutzung der technischen Infrastruktur für die Kommunikation und die damit verbundenen Netzwerkeffekte kostenlos zur Verfügung stellen. Auf diese Weise sind die elektronischen Märkte entstanden, auf denen personenbezogene Daten angeboten und nachgefragt werden, beispielsweise für Marketingzwecke. Daten, die detaillierte Aufschlüsse über Motivationen, Präferenzen, Beziehungen, Gesundheit oder sonstige Faktoren des Selbstwerts einer Person geben, sind dadurch zu wertvollen marktfähigen Gütern geworden. Die Person wird entschlüsselt, virtualisiert, enttabuisiert, lokalisiert, vernetzt, entrechtlicht und langfristig dokumentiert, also letztlich als Mittel für zahlreiche Zwecke „entpersonalisiert".

Nach einer Untersuchung aus dem Jahr 2012 beträgt schon der Wert einer Adresse, die von deutschen Einwohnermeldeämtern an die Privatwirtschaft weitergegeben wird, fünf Euro. Ganz andere Umsätze werden im Bereich des sogenannten „big data"-Geschäfts erzielt: Die US-amerikanischen Unternehmen Allot Ltd./Mediaswift bieten einen Marktplatz für Daten aus sozialen Netzwerken an, der auf dem Filtern von Computerkennungen (URL) und der persönlichen Kommunikation zwischen Netzwerkteilnehmern (P2P catching) im Hinblick auf Twitter, Facebook, YouTube und anderen

sozialen Netzwerken beruht. Täglich werden auf diesem Marktplatz 230 Millionen Datensätze verkauft[23]. Das US-Unternehmen Grip Ltd., ein Großhändler für personenbezogene Daten, bietet für 30.000 US-Dollar monatlich die Übergabe aller Tweets an, die auf Schlüsselwörter in Weblinks zurückgeführt werden können[24]. Das kanadische Unternehmen Sysomos Inc. bietet personenbezogene Daten an, die durch Echtzeit-Analysen darüber gewonnen werden, was die Leute über bestimmte Produkte wie Coca-Cola, Reebok, Toyota, Nokia oder McDonalds denken[25].

Der Charakter dieser Daten als Informationen über private Verhältnisse oder Ansichten einer Person führt nicht zu Einschränkungen in der Verwertbarkeit. Im Gegenteil, je spezifischer und individueller diese Daten sind, um so höher ist ihr Marktwert. Insoweit sind personenbezogene Daten zu einem ökonomischen Gut geworden. Der Einsatz dieser Ressource hängt davon ab, wer an diesen kommerziell verwertbaren personenbezogenen Daten Rechte geltend machen kann.

Nicht nur in Steinmüllers Beiträgen, sondern auch in Orwells „1984“ steht die Verwendung personenbezogener Informationen für staatliche Zwecke ganz im Blickfeld. Insoweit ist es berechtigt, die verfassungsmäßig garantierten Freiheitsrechte einer Person (Art.2 Abs.1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 MRK, Art. 8 EU-Charta) als Maßstab zur Begrenzung der Verarbeitung personenbezogener Daten durch öffentliche Stellen heranzuziehen. Für die private Vermarktung personenbezogener Daten gelten diese Freiheitsrechte aber grundsätzlich nicht[26]. Hier geht es um den vertraglichen Austausch von Gütern und Leistungen auf elektronischen Märkten. Die „Person“, auf die sich die Daten beziehen, ist – wenn auch oft unbewusst – Marktbeteiligter.

2. Ökonomische Analyse

Würde das System der Privatheit bestimmter Informationen noch funktionieren, dann wäre die Erlangung von Informationen aus diesem System schwierig und mit erheblichen Kosten verbunden. Die Mitglieder eines Systems, beispielsweise einer Familie, könnten personenbezogene Informationen der Familienmitglieder geheim halten und nur für sich selbst nutzen. Sie wären bis zu einem gewissen Grad in der Lage, außenstehende Personen von der Kenntnisnahme auszuschließen. In einer solchen Situation stellen personenbezogene Daten kein öffentliches Gut dar, denn öffentliche Güter zeichnen sich dadurch aus, dass sie nicht exklusiv sind, also von jedem genutzt werden können, und dass hinsichtlich der Nutzung keine Rivalität besteht, die personenbezogenen Informationen also gleichzeitig von vielen genutzt werden könnten.

Durch das moderne Kommunikationsverhalten in der Informationsgesellschaft gelangen unzählige personenbezogene Daten in die Öffentlichkeit, die überwiegend frei zugänglich sind und prinzipiell gleichzeitig von vielen genutzt werden können. Stellen solche personenbezogene Daten damit öffentliche Gütern dar? Gilt nunmehr der rechtliche Grundsatz: „Alles ist erlaubt, was nicht verboten ist“ für die Nutzung personenbezogener Daten in der Privatwirtschaft?[27]

Niemand ist bereit, für die Nutzung eines Gutes etwas zu zahlen, wenn dieses Gut auch kostenlos erlangt werden kann. Da personenbezogene Daten von Dienstleistern gegen Entgelt vermarktet werden, müssen diese Anbieter Eigentum oder eine eigentumsähnliche Position („property right“) an dem angebotenen Gut besitzen, um die für einen Markt erforderliche Knappheitssituation erzeugen zu können. „Property rights“ begrenzen die freie Nutzung der Güter und steuern damit das Ausmaß der Nutzung.

In der Tat beanspruchen Facebook und andere große Unternehmen in ihren allgemeinen Geschäftsbedingungen Ausschließlichkeitsrechte an den von ihnen gespeicherten und verarbeiteten personenbezogenen Daten. Das geschieht allerdings in wenig transparenten und versteckten Formulierungen. So heißt es bei Facebook einerseits, dass dem Teilnehmer alle Inhalte und Informationen „gehören", die er bei Facebook einstellt[28]; andererseits wird dem Teilnehmer verboten, die Inhalte oder Updates selbst zu vermarkten[29]. Vielmehr behält sich Facebook das Recht vor, alle Daten eines Teilnehmers für alle denkbaren Zwecke zu analysieren und für die Weiterverwendung zu indexieren[30]. Facebook hat mehr als 100 Petabytes an personenbezogenen Daten gespeichert[31] und bietet damit eine unerschöpfliche Fundgrube für „big data"-Auswertungen. Viele Nutzer von Facebook möchten zwar die Vorteile einer schnellen Kommunikation im Netzwerk nutzen, aber nach neuen Untersuchungen sind mehr als 85 % aller Deutschen gegen Tracking, Informationsspeicherung und Datenhandel[32].

Internetnutzer werden schon mit der Registrierung für irgendeinen Service Beteiligte im Markt für den Handel mit personenbezogenen Daten, denn die Registrierung setzt den Transfer von personenbezogenen Daten voraus. Bei der Nutzung von Suchmaschinen werden die individuellen Interessen durch spezielle Programme (Cookies) erfasst sowie an andere Webseiten weitergeleitet, dort systematisch analysiert und vermarktet. Nur wenigen Nutzern gelingt es, Cookies wirksam zu beseitigen und dennoch am Kommunikationsprozess teilzunehmen.

Man könnte argumentieren, dass die Dienstleistungsunternehmen durch ihr Geschäftsmodell, das eine Vermarktung personenbezogener Daten ihrer Kunden vorsieht, eher in der Lage wären, einen höheren Nutzen (Wohlfahrtsgewinn) zu erwirtschaften. Die Vermarktungen erfolgen jedoch zum überwiegenden Teil ohne hinreichende Kenntnis der Kunden und auf deren Kosten. Alle

Nachteile der Vermarktung, wie die fortlaufenden heimlichen Beobachtungen der Kommunikationsaktivitäten der Kunden (tracking), skalierte Bepunktungen (scoring), Profilbildungen, Analysen, Fehlbeurteilungen, Intransparenz, Durchführung der Datenverarbeitung in Drittstaaten bis hin zum Identitätsdiebstahl[33] im Internet, tragen diejenigen Personen, auf die sich die Daten beziehen. Diese Transaktionskosten werden von den Dienstleistungsunternehmen externalisiert. Es liegt an der betroffenen Person, sich dagegen zur Wehr zu setzen, was wegen der Existenz globaler Netze fast ausgeschlossen ist. Die Transaktionskosten auf Seiten der Nutzer der Kommunikationssysteme sind daher sehr hoch. Von den exorbitanten Gewinnen der Diensteanbieter, die weit höher sind als der finanzielle Aufwand für die Bereitstellung der Kommunikationsinfrastruktur, erhalten die von der Vermarktung ihrer Daten betroffenen Personen nichts, aber sie verlieren ihre Verfügungsmöglichkeit.

Demgegenüber erhöht eine Allokation des Verfügungsrechts über die vermarktbaren Persönlichkeitsmerkmale beim Träger dieser Merkmale dessen Entscheidungsfreiheit. Eine solche Person kann besser zwischen Vermarktung und Nichtvermarktung mit allen Vor- und Nachteilen wählen. Die Vorteile der Einwilligung in eine Vermarktung liegen in der kostenlosen Nutzung einer technischen Kommunikationsstruktur mit Netzwerkeffekten, die Nachteile in den nachfolgenden umfassenden Verhaltensanalysen und dem weitgehenden Verlust der Kontrollmöglichkeit über die weitere Datenverwendung. Die mit der Erlangung der Einwilligung in die Verarbeitung personenbezogener Daten verbundenen Kosten sind insgesamt erheblich geringer als die von den Dienstleistern externalisierten Kosten.

Damit spricht ökonomisch vieles für die Verankerung eines privatrechtlichen Verfügungsrechts über personenbezogene Daten bei der betroffenen Person. Es ermöglicht ihr die Wahrnehmung privatautonomer Marktentscheidungen. Ein privatrechtliche

Verfügungsrecht über personenbezogene Daten auf elektronischen Märkten bildet ein funktionales Äquivalent zum „informationellen Selbstbestimmungsrecht“ bei der Wahrnehmung von Freiheitsrechten im öffentlichen Bereich.

3. Rechtliche Analyse

Ob Facebook, Google und andere Internet-Dienstleistungsunternehmen Ausschließlichkeitsrechte an den Daten ihrer Nutzer geltend machen können, hängt nicht nur von dem Inhalt ihrer Geschäftsbedingungen ab, sondern von dem allgemeinen Rechtsrahmen, in dessen Kontext die Geschäftsbedingungen zu bewerten sind. Hierfür ist zu untersuchen, ob an personenbezogenen Daten überhaupt Ausschließlichkeitsrechte begründet werden können und, wenn ja, wem diese zustehen.

Die rechtlichen Handlungsvoraussetzungen und Handlungsformen für Marktprozesse finden sich im Vertragsrecht und im Sachenrecht. Das Datenschutzrecht enthält zwingende Rahmenbedingungen, verbietet aber einer Person nicht die Preisgabe seiner persönlichen Daten. Die informationelle Selbstbestimmung äußert sich zivilrechtlich in Privatautonomie und Vertragsfreiheit. Als vertragliche Leistung des Dienstleisters kommt die Bereitstellung der Nutzung der Netzinfrastruktur in Betracht, als Gegenleistung des Kunden die Überlassung personenbezogener Daten.

Die Vermarktung der Daten durch Dienstleistungsunternehmen setzt eine Verfügungsberechtigung an den überlassenen Daten voraus.

3.1. Eigentum an personenbezogenen Daten?

Eine anerkannte rechtliche Theorie über die *vermögensrechtliche* Zuordnung personenbezogener Daten fehlt bisher. Kann man überhaupt Eigentum oder vermögenswerte Rechte an personenbezogenen Daten beanspruchen?

Eine Schwierigkeit für die Zuordnung von Eigentum ist darin zu sehen, dass seit dem Römischen Recht „Eigentum" nur an körperlichen Dingen anerkannt ist. Die rechtliche Kategorie „Eigentum" umfasst dann alle Manifestationen wie das Recht zur Nutzung, Fruchtziehung oder den Besitz.

Personenbezogene Daten sind aber unkörperlich. Selbst für körperliche Teile einer Person, wie Gewebe oder Organe, wird die Anwendbarkeit der Eigentumskategorie traditionell verneint[34]. Die meisten theoretischen Analysen befassen sich außerdem mit personenbezogenen Daten im Verhältnis Staat/Bürger und knüpfen an Grundrechte und Freiheitsrechte, nicht aber an Vermögensrechte an. Die aus Verfassungsgarantien abgeleiteten Freiheitsrechte wie das der „informationellen Selbstbestimmung" oder der „privacy" lassen sich daher nicht mit „Eigentum" im zivilrechtlichen Sinne gleichsetzen und können daher auch nicht als Rechtsgrundlage für Markttransaktionen von personenbezogenen Daten dienen.

3.2. Eigentumsähnliche Rechte an personenbezogenen Daten?

Das Bestehen absoluter („exklusiver") Rechte an unkörperlichen Gütern ist aber nicht ausgeschlossen, denn es gibt zahlreiche unkörperliche Güter, die einen Personenbezug aufweisen und zugleich einen Marktwert haben. Zu nennen sind insbesondere patentierte

Erfindungen oder urheberrechtlich geschützte Werke. Aber auch der Name einer Person[35] oder der Name eines Unternehmens (Firma) kann einen Marktwert haben und als Marke rechtlich geschützt sein. Ob das auch für sonstige personenbezogene Daten zutrifft, ist datenschutzrechtlich und zivilrechtlich zu prüfen.

3.2.1. Datenschutzrecht und Verfügungsrechte

Soweit Datenschutzrecht eingreift, verdrängt es nach herrschender Meinung privatrechtliche Vorschriften[36].

Die datenschutzrechtlichen Vorschriften über die Rechte einer Person, auf die sich die Daten beziehen, klären für den Privatrechtsverkehr nicht ausdrücklich, ob dieser Marktteilnehmer eine vermögenswerte Position („property right") an seinen personenbezogenen Daten beanspruchen kann. Das ist nicht verwunderlich, denn das Verfügungsrecht über personenbezogene Daten wird ja bisher nicht als eine *vermögensrechtliche* Position klassifiziert[37], obwohl die personenbezogenen Daten auf elektronischen Märkten oft Vermögenswert besitzen[38]. Deshalb besteht ein erheblicher und weitreichender Streit beispielsweise darüber, ob für die Verarbeitung von marktrelevanten personenbezogenen Daten durch Dienstleister das „opt in"- oder das „opt out"- Prinzip Anwendung findet und ob das „don't track me"-Verfahren der betroffenen Person einen Vorteil verschafft oder überflüssig ist. In allen Fällen gehen die jeweiligen Vorschläge stillschweigend von unterschiedlichen Hypothesen darüber aus, wem das Verfügungsrecht über personenbezogene Daten vermögensrechtlich primär zusteht.

Auszugehen ist in unserem Kulturkreis zunächst von der philosophischen Überzeugung, dass jedes Individuum über individuelle Charakteristika, Fähigkeiten, Eigenschaften, Verhaltensweisen und Vorstellungen verfügt, die es von anderen Personen unterscheidet und über die es prinzipiell autonom disponieren können soll. In den

europäischen und deutschen Datenschutzvorschriften kommt diese Grundauffassung deutlich zum Ausdruck.

Nach den Datenschutzvorschriften muss die betroffene Person im Privatrechtsverkehr für jede Form der Verarbeitung grundsätzlich ihre Einwilligung erteilen, es sei denn, dass ein von dieser Person eingegangener Vertrag andernfalls nicht erfüllt werden kann oder zwingendes Recht die Verarbeitung personenbezogener Daten erfordert. Soweit keine zwingenden Vorschriften bestehen und eine Einwilligung privatrechtlich erforderlich ist, muss sie ohne Zwang, für den konkreten Fall, zweckgebunden und in Kenntnis der Sachlage erfolgen (Art. 2 lit. g Richtlinie 95/46/EG). Ferner hat die betroffene Person das Recht, Auskunft über die gespeicherten Daten zu verlangen und unrichtige oder unvollständige Daten löschen zu lassen (Art. 12 Richtlinie 95/46/EG). Vollautomatische personenbezogene Datenauswertungen, die erheblich beeinträchtigende oder rechtliche Folgen für den Einzelnen nach sich ziehen könnten, was beim „data mining" oder bei „big data"-Auswertungen leicht der Fall sein kann, sind unzulässig (Art. 15 Richtlinie 95/46/EG). Schließlich führt eine rechtswidrige Verarbeitung personenbezogener Daten zu Schadenersatzansprüchen aus einer modifizierten Gefährdungshaftung (Art. 23 Richtlinie 95/46/EG). Ob dabei nur ein Immaterialschaden oder ein Vermögensschaden ausgeglichen werden soll, geht aus der Datenschutzrichtlinie selbst nicht hervor[39]. Das Bundesdatenschutzgesetz umfasst jedenfalls auch Vermögensschäden (§§ 7, 8 Abs. 1 BDSG).

Fasst man dieses Bündel an datenschutzrechtlichen Teilrechten einer Person im Hinblick auf die Verfügungsmöglichkeiten über seine marktfähigen Daten zusammen, dann ergibt sich für die betroffene Person insgesamt eine Rechtsstellung, die sich bereits zu einer vermögenswerten Position verfestigt hat[40]. Auch ohne Zuerkennung zivilrechtlichen Eigentums an den Daten selbst spricht der Umfang der Verfügungsrechte der betroffenen Person über die auf

ihn beziehbaren Daten für die Anerkennung einer eigentumsähnlichen Stellung an seinen marktfähigen personenbezogenen Daten.

3.2.2. Zivilrecht und Verfügungsrechte

Es besteht kein Zweifel, dass auch Verfügungsrechte (Rechte an Rechten wie etwa Besitz, Nießbrauch, Nutzungrechte) vermögenswerte Positionen darstellen können. Es stellt sich aber die Frage, ob das Bündel an datenschutzrechtlichen Dispositionsmöglichkeiten, die einer betroffenen Person hinsichtlich seiner Daten zukommt, privatrechtlich zur Anerkennung eines *eigentumsähnlichen* Rechtes führt. Als privatrechtliche Grundlage für die Anerkennung des Verfügungsrechts an personenbezogenen Daten als vermögenswerte Position kommen in Deutschland eine Anknüpfung an das Allgemeine Persönlichkeitsrecht, die Anerkennung als eigenständiges „sonstiges Recht", das Datenschutzrecht sowie die Schaffung eines besonderen Immaterialgüterrechts in Betracht.

3.2.2.1. Allgemeines Persönlichkeitsrecht

Die verfassungsrechtliche Freiheit auf Entfaltung der Persönlichkeit muss als Grundrecht stets gegen konkurrierende Freiheitsrechte, wie Informations- oder Pressefreiheit, abgewogen werden und garantiert deshalb nur ein relatives Recht. Das zivilrechtliche „Allgemeine Persönlichkeitsrecht" ist zwar deliktsrechtlich im Sinne von § 823 Abs. 1 BGB als „absolutes" sonstiges Recht gewohnheitsrechtlich anerkannt, wird aber lediglich als „Rahmenrecht"[41] definiert und ist nicht im Interesse der Kommerzialisierung der eigenen Persönlichkeit gewährleistet[42]. Ob es ein exklusives Recht im Sinne der ökonomischen Theorie darstellt, ist deshalb fraglich. Marktfähig wird ein absolutes Recht jedenfalls grundsätzlich erst dann, wenn es auch übertragen werden kann. Als immaterielles Recht ist das Allgemeine Persönlichkeitsrecht in Deutschland nicht übertragbar. Es

ist lediglich im Hinblick auf einige Aspekte wirtschaftlich aufgrund von Verträgen nutzbar[43].

Allgemein ist anerkannt, dass ein Betroffener für die unberechtigte Veröffentlichung seiner persönlichen Bilder[44] in frei zugänglichen Medien[45] Schadenersatz fordern kann. Das ist bisher nur berühmten Leuten wie Filmstars, Prinzessinnen und Brauereibesitzern gelungen, aber noch keinem Internet-Nutzer. Auch der besondere datenschutzrechtliche Schadenersatzanspruch (§ 7 BDSG) läuft leer, weil regelmäßig kein Schaden nachgewiesen werden kann. Zudem wird das Verfügungsrecht über personenbezogene Daten nicht als Teil des wirtschaftlich verwertbaren Allgemeinen Persönlichkeitsrechts aufgefasst.

3.2.2.2 Anerkennung als eigenständiges „sonstiges Recht“

Das Bündel an Rechten, über das eine Person datenschutzrechtlich im Hinblick auf seine Daten verfügen kann, ließe sich zivilrechtlich auch als eigenständiges „sonstiges Recht“ im Sinne von § 823 Abs. 1 BGB interpretieren. Gegenüber einer Subsumtion als Bestandteil des Allgemeinen Persönlichkeitsrechts ergäben sich dadurch aber keine anderen Folgen, denn es bliebe bei einem rein deliktischen Schadenersatzanspruch. Aus Gründen der schwierigen Konkretisierung und der Beweislast ist ein deliktischer Schadenersatzanspruch kaum geeignet, das Verfügungsrecht über personenbezogene Daten wirksam durchsetzen zu helfen. Für eine effektive Durchsetzung des Verfügungsrechts über personenbezogene Daten ist statt eines bloßen deliktischen Schadenersatzanspruchs („liability rule“) eine eigentumsähnliche Rechtsstellung („property rule“) erforderlich.

3.2.2.3. Datenschutzrechtliche Teilrechte als Zuerkennung einer Eigentumsposition?

Denkbar wäre, das Bündel an Verfügungsrechten der betroffenen Person an seinen Daten, wie sie die Datenschutzgesetze als zwingendes öffentliches Recht vorsehen, zivilrechtlich bereits als Zuerkennung einer eigentumsähnlichen Rechtsposition aufzufassen. Die dem Betroffenen in den Datenschutzgesetzen eingeräumten Rechte auf Einwilligung, Auskunft, Berichtigung, Sicherung oder Löschung an marktfähigen personenbezogenen Daten stellen rechtliche Befugnisse dar, die den Bestand einer vermögenswerten Rechtsposition voraussetzen. Diese datenschutzrechtlich begründeten Teilrechte müssen bei zivilrechtlichen Vertragsabschlüssen als Rahmenbedingungen beachtet werden und engen aus der Sicht von Unternehmen ihre Vertragsgestaltung über personenbezogene Daten ein. Die Verfügungsbefugnisse können deshalb mit eigentumsähnlichen Positionen gleichgesetzt werden. Weil das europäische Datenschutzrecht nur Individuen und nicht Unternehmen schützt[46], lässt sich deshalb das auf Markttransaktionenen anwendbare Datenschutzrecht auch als modernes Verbraucherschutzrecht der Informationsgesellschaft interpretieren[47].

3.2.2.4. Neues Immaterialgüterrecht?

Personenbezogene Daten sind besondere immaterielle Güter, nämlich „Informationsgüter" oder „informationelle Güter" („biens informationnels", „informational goods")[48]. Ähnlichkeiten bestehen zur Software. Während der rechtliche Status von Software inzwischen spezialgesetzlich geregelt ist[49], fehlt eine marktrelevante juristische Klassifikation für personenbezogene Daten. Bisher wird nur der Missbrauch personenbezogener Daten datenschutzrechtlich (§§ 43, 44 BDSG), strafrechtlich (§§ 201–206 StGB) und zivilrechtlich (BDSG als Schutzgesetz i. S. von § 823 Abs. 2 BGB)[50] sanktioniert. Die Entscheidung darüber, ob und in wieweit ein Datenmissbrauch

überhaupt vorliegt, hängt aber hauptsächlich von der primären Vermögenszuordnung und den nachfolgenden privatautonomen Entscheidungen ab.

Die Nutzung von Immaterialgütern, die weder einer Person zugewiesen noch besonders vom Recht geschützt sind, führt nicht zu rechtlichen Sanktionen.

Schutzregelungen für verwandte Situationen enthält das Urheberrecht. Der Träger personenbezogener Daten tritt allerdings nur in Grenzfällen als „Schöpfer" eines „Werkes" auf, das personenbezogene Daten enthält. Das kann etwa bei der Herstellung eines künstlerisch gestalteten digitalen Eigenfoto der Fall sein. Dafür könnte das Datensubjekt als Schöpfer des digitalisierten Werkes den Urheberschutz in Anspruch nehmen. Ein genereller Schutz personenbezogener Daten in Analogie zum Urheberrecht oder zu anderen Immaterialgüterrechten kommt aber wegen des numerus clausus dieser Rechte nicht in Betracht.

Ohne Zweifel bestehen aber elektronische Märkte, auf denen die Preise für personenbezogene Daten durch Angebot und Nachfrage vertraglich vereinbart werden. Der Wert personenbezogener Daten lässt sich objektiv ermitteln. Die Vermarktung erfolgt aber bis heute nicht durch die betroffene Person, der das Datenschutzrecht zwingend bestimmte Dispositionsbefugnisse zuerkennt, sondern durch kommerzielle Diensteanbieter, die das Verfügungsrecht über personenbezogene Daten ihrer Kunden aus Überlassungsverträgen mit diesen beanspruchen.

Wie die ökonomische Analyse zeigt, führt diese Art der Verteilung von vermögenswerten Positionen zu Wohlfahrtsverlusten. Deshalb spricht auch juristisch vieles dafür, das Verfügungsrecht über die wirtschaftlich verwertbaren Bestandteile personenbezogener Daten der betroffenen Person als eigentumsähnliches immaterielles Recht

de lege ferenda[51] anzuerkennen. Dadurch erhielte die betroffene Person eine effektive Möglichkeit, die marktmäßige Nutzung personenbezogener Daten über Lizenzbedingungen zu steuern oder ganz von einer Vermarktung auszuschließen. Die betroffene Person könnte gegen eine unerlaubte Vermarktung wegen unlauteren Wettbewerbs vorgehen.[52]

Eine weitere Konsequenz einer vermögensrechtlichen Deutung des Verfügungsrechts ist, dass es sich bei der datenschutzrechtlichen „Einwilligung" um eine rechtsgeschäftliche Einwilligung im Sinne von §§ 183, 185 BGB handelt. Vermarktungen personenbezogener Daten durch Dienstleister stellen „Verfügungen" dar, die nur mit Einwilligung des Berechtigten (datenschutzrechtlich: der betroffenen Person) wirksam erfolgen können (§ 185 Abs. 1 BGB). Das schließt die Möglichkeit der betroffenen Person ein, sich gegenüber einem Dienstleister vertraglich zu verpflichten, über diese vermögenswerten Bestandteile nicht selbst zu verfügen (§ 137 S. 2 BGB). Diese Einwilligung ist widerruflich, soweit eine konkrete Vermarktung noch nicht stattgefunden hat (§ 183 S. 1 BGB).

4. Durchsetzbarkeit des Verfügungsrechts über personenbezogene Daten

Unabhängig davon, wie man das Verfügungsrecht über personenbezogene Daten rechtsdogmatisch verankert, hängt seine praktische Durchsetzbarkeit von der Marktstruktur und von dem anwendbaren Recht ab.

4.1. Marktstruktur

Die Marktstruktur für den Handel mit personenbezogenen Daten als relevantem Markt ist – insbesondere bei sozialen Netzwerken

– als enges Oligopol einzuschätzen. Wenige international tätige Unternehmen dominieren diesen globalen Markt und setzen die Marktbedingungen fest. Ökonomisch gesehen liegt deshalb ein Marktversagen vor, das den effizienten Einsatz vermögenswerter Rechte erschwert.

Ein funktionierender Markt zeichnet sich nämlich dadurch aus, dass sich die Marktteilnehmer grundsätzlich auf gleicher Verhandlungsebene begegnen. Bei Verträgen zwischen Unternehmen und Einzelpersonen wird eine strukturelle Asymmetrie in der Verhandlungsmacht angenommen, so dass zwingendes Verbraucherschutzrecht oder sonstiges Öffentliches Recht (beispielsweise Kartellrecht) eingreifen, um eine faire Verhandlungssituation herbeizuführen. Beispielsweise wäre es denkbar, über kartellrechtliche Instrumente Anreize für den Markteintritt solcher Diensteanbieter zu geben, die bereit sind, eine vergleichbare Kommunikationsinfrastruktur *gegen Bezahlung* zur Verfügung zu stellen, gleichzeitig aber auf den Handel mit personenbezogenen Daten ganz oder in transparentem Umfang zu verzichten. Auf diese Weise entstünde Wettbewerb und die betroffenen Personen hätten Wahlmöglichkeiten, ob und unter welchen Bedingungen personenbezogene Daten an die Öffentlichkeit gelangen sollen.

Ein effektives Kartellrecht gibt es jedoch nur in Europa und in sehr abgeschwächter Form in den Vereinigten Staaten von Amerika[53]. Andererseits ist in Europa[54] und Amerika das politische und historische Bewusstsein für die Implikationen und Verwendungsmöglichkeiten personenbezogener Daten am höchsten (und nach Snowden hier wie dort im Steigen begriffen).

4.2 Anwendbares Recht

Aus rechtlicher Sicht führt die Globalisierung der Märkte zu erheblichen Schwierigkeiten in der Anwendung des zwingenden europäischen Datenschutzrechts. Das betrifft insbesondere die Durchsetzung der grundsätzlich erforderlichen Einwilligung der betroffenen Person als Voraussetzung für die Verarbeitung seiner personenbezogenen Daten im nichtöffentlichen Bereich.

Das zeigt der Versuch des Wiener Jurastudenten Max Schrems, der von Facebook Auskunft über die zu seiner Person gespeicherten Daten haben wollte. Nach mehreren vergeblichen Anläufen konnte er sein datenschutzrechtlich garantiertes Recht auf Auskunft nur deshalb durchsetzen, weil die Facebook Inc./Menlo Park/Kalifornien/USA aus steuerrechtlichen Gründen in Dublin eine Tochtergesellschaft Facebook Ireland Ltd. unterhält, die irischem und damit europäischem Recht unterliegt. Die unvollständige Auskunft von Facebook an Schrems umfasste 1226 Seiten (Fotos nicht eingeschlossen). Das hat im Internet eine gewaltige Diskussion über die Rechte und Pflichten der Marktbeteiligten und über die Durchsetzbarkeit von Rechten ausgelöst.[55]

Die Anerkennung eines Verfügungsrechts über personenbezogene Daten als vermögenswerte Position im Privatrechtsverkehr und die damit verbundene Klassifikation der datenschutzrechtlichen „Einwilligung“ als Voraussetzung für einen Vertragsschluss führt nicht zwangsläufig zu einer Kommerzialisierung personenbezogener Daten. Dies zeigt das Beispiel der GNU Public Licence für urheberrechtlich geschützte Open Source Software[56]. Die Hauptvorteile der Anerkennung und des Schutzes von Verfügungsrechten liegen vielmehr in der Zuordnung der primären Dispositionsbefugnis. Dies hat Auswirkungen auf den Inhalt der Allgemeinen Geschäftsbedingungen von Dienstleistungsunternehmen und auf die Geschäftstätigkeit.

Interessant ist die Beobachtung, dass die US-amerikanischen sozialen Netzwerke inzwischen ihre Geschäftsbedingungen für Nutzer mit Wohnsitz in Deutschland zu modifizieren beginnen[57].

Soweit eine betroffene Person die Option einer vermögensrechtlichen Verwertung seiner Daten wählt, dürfte die praktische individuelle Rechtsdurchsetzung allerdings schwierig sein. Bei Klassifikation des Marktteilnehmers als „Verbraucher" würde eine besondere gerichtliche Zuständigkeit dort bestehen, wo die betroffene Person den Mittelpunkt ihrer Interessen hat (Wohnsitz, gewöhnlicher Aufenthalt, Arbeitsplatz)[58].

Ähnlich wie für die Durchsetzung von Urheberrechten könnten spezielle Wahrnehmungsgesellschaften gegründet und damit beauftragt werden, datenschutzrechtliche Verfügungsrechte begrenzt oder umfassend nach den individuellen Präferenzen der Wahrnehmungsberechtigten zu verwalten. Wahrnehmungsgesellschaften wären auch eher in der Lage, den globalen Markt zu beobachten und die Rechte international geltend zu machen.

5. Reformvorhaben

In der Europäischen Union und in den Vereinigten Staaten von Amerika gibt es im Zusammenhang mit der Förderung elektronischer Märkte Initiativen für eine Reform des Datenschutzrechts.

In der Europäischen Union wird eine Datenschutzverordnung diskutiert, die mehr Vertrauen in den Online-Handel bringen und dem Individuum mehr Kontrolle seiner Daten ermöglichen soll[59]. Der Verordnungsentwurf sieht beispielsweise ein Recht der betroffenen Person vor, verlangen zu können, dass seine personenbezogenen Daten „vergessen" (physikalisch gelöscht) werden[60]. Außerdem soll ein Recht auf „Portabilität" der Daten[61] einer Monopolisierung der

Vermarktung entgegenwirken. Ferner werden individuell abgestufte technische Sicherungsmaßnahmen empfohlen („privacy by design"). Letztere setzen freilich die klare rechtliche Zuordnung der Verfügungsrechte voraus[62].

Auch im Hinblick auf diese ergänzenden Datenschutzregelungen im privatwirtschaftlichen Bereich bietet ein ökonomisch begründbares und rechtlich sinnvolles eigentumsähnliches Verfügungsrecht des Betroffenen die theoretische Grundlage. Darüber hinaus behalten die allgemeinen Prinzipien des Datenschutzrechts wie Transparenz, Proportionalität, Zweckbindung, faire Verarbeitung, wie sie in der Datenschutzkonvention Nr. 108 des Europarats[63], in der allgemeinen EG-Datenschutzrichtlinie 95/46[64], den UN-Richtlinien von 1990[65], den OECD-Richtlinien[66] und in den asiatisch-pazifischen Datenschutz-Rahmenrichtlinien[67] enthalten sind, als zwingendes öffentliches Recht ihre Bedeutung auch im privatwirtschaftlichen Bereich.

Eine weitere Konsequenz der Zuerkennung einer eigentumsähnlichen Rechtsposition an die betroffene Person sollte nicht unterschätzt werden: Solange aufgrund des Marktversagens keine faire Chance für eine freie Vereinbarung über den Austausch ihrer vermarktbaren personenbezogenen Daten bestehen, müssen die Betroffenen als „Verbraucher" angesehen werden. Ein hohes Verbraucherschutzniveau (Art. 114 Abs. 3; 12 und 169 AEUV) korrespondiert dann mit einem hohen Datenschutzniveau. Auch die geplante EU-Datenschutzgrundverordnung lässt sich leicht als Verbraucherschutzrecht im Bereich des Datenschutzes interpretieren.

Selbst der Entwurf der Grundverordnung enthält trotz seiner 91 Artikel aber keine Vorschläge darüber, welche Rahmenbedingungen für die Wirksamkeit einer Einwilligung in die Verarbeitung personenbezogener Daten bei Vertragsabschlüssen im mobilen Internet gelten. Hier wären Hinweise auf die unterschiedlichen

Geschäftsmodelle mit Hilfe von Gütezeichen oder Prüfzeichen marktneutraler Organisationen denkbar, um Hinweise auf die Seriosität der Unternehmen im Umgang mit personenbezogenen Daten zu erlangen und einen Wettbewerb über deren Geschäftsmodelle zu erzeugen („signalling effect").

6. Zukunftsperspektiven

Ähnlich wie Habermas in seiner Habilitationsschrift über den Strukturwandel der Öffentlichkeit den „Zerfall der Öffentlichkeit" festgestellt hat[68], lässt sich fünfzig Jahre später einen Strukturwandel der Privatheit wegen des „Zerfalls der Privatheit" beobachten. „Privatheit" war früher an die Hausgemeinschaft gebunden, aber ihre schützende Funktion durch räumliche Begrenzung ist in der Informationsgesellschaft entfallen. Die interaktiven elektronischen Kommunikations- und Gebrauchsgeräte überwinden räumliche Grenzen und machen den privaten Raum öffentlich. Der moderne Mensch ist kaum noch gewillt oder individuell in der Lage, nach freiem Entschluss bestimmte Persönlichkeitsmerkmale oder Relationen von der Öffentlichkeit abzuschotten. Neben der politischen (staatlichen) Öffentlichkeit ist eine unpolitische (private) Öffentlichkeit entstanden. Diese öffentlichkeitsorientierte Privatheit ist geografisch, zeitlich und inhaltlich nahezu unbegrenzt und nur mit technischem Wissen überhaupt begrenzbar. Das zeigt sich bei vielen elektronischen Kommunikationsvorgängen wie dem „Posten" privater Fotos auf öffentlich zugänglichen elektronischen Plattformen, der Präsentation individueller sexueller Präferenzen im Fernsehen, dem Monitoring des gerätebezogenen privaten Stromverbrauchs durch Energieversorger, der Dokumentation und Analyse des individuellen Surfverhaltens durch Internetdienstleister, der geografischen Lokalisierung von Mobilfunkteilnehmern. Die geografisch und inhaltlich begrenzte nichtöffentliche Privatheit ist zur geografisch und inhaltlich unbegrenzten privaten Öffentlichkeit geworden.

Wenn „privat“ nur solche Informationen sind, „die nicht an die Öffentlichkeit gelangen sollen“[69] und der Strukturwandel der Privatheit im nichtöffentlichen Bereich nicht dem Einzelnen, sondern allein den Marktgesetzen überlassen wird, kann das Recht auf Achtung der Würde des Menschen und der Freiheit der Persönlichkeit weder direkt noch indirekt eine Leitbildfunktion erfüllen. „Die unverlierbare Würde des Menschen besteht gerade darin, daß er als selbstverantwortliche Persönlichkeit anerkannt bleibt“[70]. Die „Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“, bedarf „in besonderem Maße des Schutzes“[71]. Marktdefiziten, die freie Entscheidungen verhindern, sollte der „schützende“ Staat[72] deshalb durch rechtliche Rahmenbedingungen (Kartellrecht, Verbraucherschutzrecht, Datenschutzrecht, Immaterialgüterrecht, Internationales Privatrecht, Verfahrensrecht) entgegenwirken.

Besondere Beachtung bedarf dabei auch das Problem der Durchsetzbarkeit individueller Rechte auf globalen Märkten. Eine betroffene Person hat wenig Aussichten, ihre Verfügungsrechte individuell ausüben zu können, wenn die datenschutzrechtlich verantwortliche Stelle nicht in dem Staat ihre Niederlassung hat, in dem sich die betroffene Person befindet. Hier könnten neben verbindlichen Anknüpfungsregeln des Internationalen Privatrechts die Schaffung der Möglichkeit für organisierte Interessenwahrnehmungen und Gruppenklagen einen effektiveren Mechanismus darstellen.

Während im globalen Datenschutzrecht kaum Annäherungen für Schutzregelungen im öffentlichen Bereich zu erwarten sind, weil hier staatliche Souveranitätsrechte und unterschiedliche Auffassungen über das Ausmaß an nationaler Sicherheit eine Rolle spielen, erscheinen Annäherungen im privatwirtschaftlichen Bereich eher möglich, weil Unsicherheiten auf dem globalen Datenmarkt die Transaktionskosten der Dienstleister erhöhen.

Dem normorientierten „top-down-approach“ im Datenschutzrecht in Europa steht in den Vereinigten Staaten von Amerika und im asiatisch-pazifischen Raum ein „bottom-up-approach“ gegenüber, der auf einzelfallbezogene Selbstregulierung setzt. In den USA ist das Datenschutzniveau insgesamt so niedrig, dass es von der EU-Kommission bisher nicht als angemessen eingestuft wurde. Bemerkenswert ist aber, dass sich der jüngste Vorschlag zum US-Datenschutzrecht, die „Consumer Privacy Bill of Rights“ des Weißen Hauses aus dem Jahr 2012, ausschließlich damit befasst, wie mit personenbezogenen Daten auf Märkten umgegangen werden sollte[73]. Statt rechtlicher Regeln werden aber zwischen den Marktbeteiligten zu vereinbarende „Codes of Conduct“ ohne Vorgaben von Prinzipien und ohne gerichtliche Kontrolle vorgeschlagen.

Insgesamt würde es einen Fortschritt darstellen, wenn die Prinzipien der Datenschutzkonvention Nr. 108 des Europarats – der einzigen völkerrechtlich verbindlichen und von 46 Staaten anerkannten Konvention – von weiteren Staaten, insbesondere den Vereinigten Staaten von Amerika, anerkannt würden. Diese allgemeinen Prinzipien könnten je nach den kulturhistorischen Erfahrungen und Rechtstraditionen spezifiziert werden und ein allgemeines Datenschutzniveau sichern helfen.

Ideal wäre es, wenn für den kommerziellen Umgang mit personenbezogenen Daten auf internationaler Ebene Modellvorschriften als Vorstufe für eine künftige UN-Konvention entwickelt werden würden.[74]

Anmerkungen

1 Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider, Grundfragen des Datenschutzes, Anlage zu BT-Drs. VI/3826 vom 7.9.1972, S. 48. – Diese Meinung klingt bereits an in: Steinmüller, EDV und Recht. Einführung in die Rechtsinformatik, Berlin 1970, S. 86 und 148; sie wurde von ihm bis zuletzt vertreten: Steinmüller, Informationstechnologie und Gesellschaft, Darmstadt 1993, S. 668.
2 Hubmann, Das Persönlichkeitsrecht, 2.A. 1967, S. 268 ff.
3 Steinmüller u. a., BT-Drs. VI/3826, S. 51.
4 Bernd Lutterbeck, in: Wolfgang Büchner/Thomas Dreier, Von der Lochkarte zum globalen Netzwerk – 30 Jahre DGRI, Köln 2007, S. 16 FN 5.
5 Steinmüller u. a., BT-Drs. VI/ 3826, S. 93.
6 BVerfGE 65, 1 (43).
7 www.theguardian.com, 11.1.2010.
8 Adolf Trendelenburg, Zur Geschichte des Wortes Person, in: Kant-Studien. Philosophische Zeitschrift, hrsg. von Hans Vaihinger/Bruno Bauch, 13. Band 1908, S. 1.
9 Epistola ad Rudolph Christ. Wagnerum, De Vi activa Corporis; De Anima; De Anima Brutorum 1710 (ed. Erdmann, S. 465).
10 Kant, Metaphysik der Sitten, Gesamtausgabe 1838, Bd. IV, S. 51.
11 Adolf Trendelenburg, Zur Geschichte des Wortes Person, S. 15 f.
12 Kohler, Das Recht an Briefen, in: Archiv für bürgerliches Recht, Bd. 7, 94 (101).
13 Otto v. Gierke, Deutsches Privatrecht, Bd. 1, S. 707.
14 Heinrich Dernburg, Das bürgerliche Recht. Die Schuldverhältnisse, 2. Bd., 2. Abteilung, Halle 1901, S. 613.
15 RGZ 56, 271 (275).
16 BGHZ 13, 334 (338) – Leserbriefe.
17 BVerfGE 6, 32 (41); 80, 367 (374 f.).
18 Helmut Coing, Das Grundrecht der Menschenwürde, der strafrechtliche Schutz der Menschlichkeit und das Persönlichkeitsrecht des bürgerlichen Rechts, in: SJZ 1947, Sp. 641 (643).
19 Art. 7 (a) Datenschutzrichtlinie 95/46/EG; § 4 Abs. 1 BDSG.
20 BVerfG NJW 2010, 833 (837) – Vorratsdatenspeicherung.

21 Siehe aber bereits Wolfgang Kilian, Datenschutz in Wirtschaftsunternehmen, in: Wolfgang Kilian/Klaus Lenk/Wilhelm Steinmüller, Datenschutz, Frankfurt a.M. 1973, S.289; Andrea Hasselkuß/Klaus-Jürgen Kaminski, Persönlichkeitsrecht und Datenschutz, in: Wolfgang Kilian/Klaus Lenk/ Wilhelm Steinmüller, Datenschutz, Frankfurt 1973, S. 109.
22 www.internetworld.de (27.8.2013).
23 The Economist, 1st October 2011.
24 The Economist, 1st October 2011.
25 The Economist, 1st October 2011.
26 Die (umstrittene) Annahme einer möglichen „Drittwirkung" der Grundrechte über die Generalklauseln des Zivilrechts soll hier nicht diskutiert werden.
27 So Jochen Schneider, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip, in: Anwaltsblatt 2011, 233; Johannes Masing, Herausforderungen des Datenschutzes, in: NJW 2012, 2305 (2307).
28 „You own all of the content and information you post on Facebook" (Facebook, Terms of Services of 8th June 2012, no.2, sentence 1.
29 „You will not use your personal timeline or your own commercial gain (such as selling your status update to an advertiser)", Facebook, Statment of Rights an Resposibilities of 15th March 2012, no. 4/4.
30 „We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search)", Facebook, Statement of Rights and Resposibilities of 15th March 2012, no. 9/17.
31 Auf einer Hadoop-Plattform der Apache Software Foundation. 1 Petabyte = 1000 (hoch 5) Byte = 1 Mio. Gigabytes = 1000 Terabytes.
32 F.A.Z. vom 13.3.2013. – Interessant ist, dass die Zahl der täglichen Besuche von Teenagern bei Facebook nach der NSA-Affäre im Oktober 2013 zurückgegangen ist und seither weniger private Daten („intimate stuff") gespeichert werden, vgl. The Economist, 4th January 2014, p. 49.
33 In den U.S.A. wurden schon im Jahre 2010 rund 1300 Fälle von Identitätsdiebstahl verfolgt (The White House Paper on Consumer Privacy Protection 2012, p. 42).
34 Nils Hoppe, Bioequity - Property and the Human Body, Farnham/ Burlington 2009. – Eine Ausnahme findet sich bei John Locke, der Eigentum an der eigenen Person anerkennt (Second Treatise on Civil Government, 1690, Chapter V, Sec. 44).
35 BGH 22.11.2001, I ZR 138/99, GRUR 2002, 622 – „Shell".
36 BGHZ 91, 233 (238).
37 Ausnahmen: Richard S. Murphy, Property Rights in Personal Information: An Economic Defence of Privacy, 84 Georgetown Law Journal 2381–2418 (1996).

38 BGH NJW 2000, 2195 (2197) – Marlene Dietrich.
39 Vgl. Erwägungsgrund 55 der Datenschutzrichtlinie 95/46/EG.
40 Diese Position wird sich noch weiter verfestigen, wenn mit der geplanten EU-Datenschutzverordnung das Recht auf „Datenlöschung und Vergessen“ sowie auf „Portabilität“ der personenbezogenen Daten eingeführt werden sollte.
41 BGH NJW 2012, 2197 (2199).
42 BVerfGE 101, 361 (Caroline von Monaco II), Leitsatz 2.
43 BGHZ 143, 214 (219) – Marlene Dietrich.
44 BGHZ 143, 214 – Marlene Dietrich..
45 ECHR, Application no. 59320/00, Judgement of 24 September 2004, Caroline of Hannover v. Germany (http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853).
46 Erwägungsgrund 24 der Datenschutzrichtlinie 95/46/EG.
47 Kilian, Consumer protection in the information and telecommunications technology sector. Current state and potential developments, in: Wydanictwo Uniwersytetu Wroclawskiego, Wroclaw 2011, pp.9-31; ferner: Consumer Data Privacy in a networked world: A Framework for protecting privacy and promoting innovation in the global digital economy, The White House Washington, February 2012 (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf).
48 Vgl. Pierre Catalá, Ébauche d`une théorie juridique de l`information, Dalloz, Chronique 1984, 97 ; siehe auch BGHZ 102, 135 (140).
49 §§ 69a - 69g UrhG.
50 BGHZ 171, 180.
51 Wegen des numerus clausus der Immaterialgüterrechte müssten spezielle Vorschriften geschaffen werden.
52 Vgl. OLG Köln 19.11.2010 (6 U 73/10; Revision vor dem BGH (Az. I ZR 224/10) ist anhängig); a.A. OLG München 12.1.2012 (29 U 3926/11). - Nach Art. 39 (2)(b)(c) WTO-TRIPS Agreement können natürliche oder juristische Personen gegen die unfreiwillige Offenlegung oder Nutzung von Informationen, die deshalb einen kommerziellen Wert haben, weil sie nicht generell bekannt sind, aus Gründen des unlauteren Wettbewerbs vorgehen.
53 Google bezahlte kürzlich die Rekordsumme von 22,5 Mio. Dollar für eine Streitbeilegung mit der U.S. Federal Trade Commission. Dabei ging es um das Tracking von Cookies, um die „privat“-Einstellungsmöglichkeit im Safari-Browser von Apple auszuschalten und Zugriff auf die Kommunikationsdaten von Nutzern zu erlangen (www.ftc.gov/opa/2012/08/google.shtm).

54 See: European Commission (ed.), Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, 2011 (http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).
55 www.europe-v-facebook.org.
56 www.gnu.de.
57 https://www.facebook.com/terms/provisions/german/index/php.
58 EuGH, 25.10.2011, C-509/09 und C-161/10, eDate Advertising GmbH gegen X und Oliver Martinez, JZ 2012, 189.
59 European Commission, Proposal for a General Data Protection Regulation, COM(2012)11 final of 25 January 2012, Recital 6 („to put the individuals in control of their own data").
60 COM(2012)11 final, Art. 17 („right to be forgotten").
61 COM(2012) 11 final, Art. 18.
62 Vgl. Wolfgang Kilian, Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung?, in: Johann Bizer/Bernd Lutterbeck/Joachim Rieß (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft. Freundesgabe für Alfred Büllesbach, Stuttgart 2002, S. 151.
63 Übereinkommen zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28.1.1981 (http://conventions.coe.int/treaty/ger/treaties/html/108.htm).
64 ABlEG L 281 vom 23.11.1995, S. 31.
65 Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990 (http://www.unhcr.org/refworld/docid/3ddcafaac.html).
66 OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal data (www.oecd.org).
67 APEC Privacy Framework (http://www.apec.org/Groups/Committee-on-Trade-and-Investment/>/media/Files/Groups/ECSG/05_ecsg_privacyframework.ashx).
68 Jürgen Habermas, Strukturwandel der Öffentlichkeit, 3. A. Neuwied/Berlin 1968.
69 Wilhelm Steinmüller, EDV und Recht. Einführung in die Rechtsinformatik, Berlin 1970, S. 149.
70 BVerfGE 45, 187 (228).
71 BVerfGE 65, 1 (42).
72 BVerfGE 34, 269 (282; 292).
73 „concerned solely with how private sector entities handle personal data in commercial settings" (The White House Consumer Privacy Bill, p.5 note 1).

74 Als vorbereitende Organisation dafür würde sich am ehesten UNCITRAl anbieten. UNCITRAL hat schon früher Modellvorschriften für die elektronische Signatur und für e-commerce verabschiedet und auch die am 1.3.2013 in Kraft getretene UN Convention on the Use of Electronic Communications in International Contracts initiiert (www.uncitral.org).