Projektgruppe „Datenschutz, Persönlichkeitsrechte“

Kapitel 1

Bestandsaufnahme bestehender Datenschutzregelungen (Stand: 12. April 2011)

Bestandsaufnahme bestehender Datenschutzregelungen

1.1 Völkerrecht

1.1.1 Allgemeine völkerrechtliche Abkommen zum Schutz der Menschenrechte

Die früheren allgemeinen Menschenrechtsabkommen enthalten kein eigenes Datenschutzgrundrecht. Dennoch erstrecken die Abkommen ihren Schutzbereich auf den Datenschutz, und zwar im Rahmen des Schutzes des Privatlebens und des Schriftverkehrs.

So hat nach Art. 8 der Europäischen Menschenrechtskonvention[1] (EMRK) „jede Person (…) das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz." Der Schutz des Privatlebens umfasst auch den Schutz persönlicher Daten, insbesondere medizinischer oder sozialer Daten.[2] Als Korrespondenz gelten auch die Individualkommunikation mittels E-Mail, Telefon und Internet-Telefonie.[3] Staatliche Eingriffe sind nur auf gesetzlicher Grundlage unter den in der Vorschrift genannten Voraussetzungen zulässig, z. B. zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Die Regelung stellt nicht nur ein Abwehrrecht gegen staatliche Eingriffe dar, sie begründet auch staatliche Schutz- und Handlungspflichten, etwa zum Erlass entsprechender Regelungen.[4] Nach Art. 1 EMRK sichern die Vertragsparteien dieses völkerrechtlichen Vertrages allen ihrer Hoheitsgewalt unterstehenden Personen unter anderem die in Art. 8 EMRK bestimmten Rechte und Freiheiten zu. In Deutschland stellt Art. 8 EMRK unmittelbar geltendes Recht dar.

In ähnlicher Weise bestimmt Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte (IPBürgR)[5], dass „niemand (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden" darf. „Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen." Wie bei der EMRK ist auch bei diesem Menschenrechtsabkommen der Vereinten Nationen der Datenschutz ein Element der Privatsphäre. Die Regelung gilt sowohl hinsichtlich staatlicher Eingriffe, als auch bei Eingriffen Privater. Die Vertragsstaaten, darunter die Bundesrepublik Deutschland, sind verpflichtet, Rechtsschutz gegenüber staatlichen Eingriffen zu ermöglichen und Regelungen zum Schutz vor privaten Eingriffen zu treffen.[6] Art. 16 der so genannten Kinderrechtskonvention[7] („Schutz der Privatsphäre") deckt sich im Wortlaut mit Art. 17 IPBürgRG. Träger der gewährten Rechte ist nach Art. 16 des Kinderrechte-Übereinkommens jedoch ausdrücklich das Kind.

Da bei den vorgenannten Menschenrechtsabkommen der Datenschutz nur als Teil des Schutzes des Privatlebens anzusehen und daher sehr allgemein ausgeprägt ist, ergeben sich datenschutzspezifische Details allenfalls aus Einzelfallentscheidungen der jeweils zuständigen Instanzen.

[1] Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, BGBl. II 1952, S. 686.
[2] Meyer-Ladewig, Jens. EMRK: Handkommentar. 3. Auflage 2011, Art. 8 EMRK, Rn. 40.
[3] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 37.
[4] Meyer-Ladewig, Jens. EMRK: Handkommentar. 3. Auflage 2011, Art. 8 EMRK, Rn. 2.
[5] Internationaler Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966, BGBl. II 1973, S. 1533.
[6] Hofmann, Rainer/ Boldt, Nicki: Kommentar zu dem Internationalen Pakt über bürgerliche und poltische Rechte, in: Kölble, Josef (Hrsg.). Das Deutsche Bundesrecht - Systematische Sammlung der Gesetze und Verordnungen mit Erläuterungen. Hauptband 1949, Erl. zu Art. 17 IPbpR.
[7] Übereinkommens der Vereinten Nationen über die Rechte des Kindes vom 20. November 1989, BGBl. II 1992, S. 122.

Allerdings enthält gerade die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) zu Art. 8 EMRK zahlreiche Hinweise auf den Schutzbereich des Datenschutzes und Eingriffsvoraussetzungen. In dem jüngeren „Übereinkommen über die Rechte von Menschen mit Behinderungen“ der Vereinten Nationen (Behindertenrechtskonvention – BRK)[8] werden in Art. 22 („Achtung der Privatsphäre“), der in seinem sonstigen Wortlaut weitgehend Art. 17 IPBürgRG entspricht, Fragen der informationellen Selbstbestimmung und des Datenschutzes ausdrücklich thematisiert. So sind neben dem Schriftverkehr ausdrücklich auch „andere Arten der Kommunikation“ vor willkürlichen und rechtswidrigen Eingriffen geschützt. Außerdem erklären die Vertragsstaaten, „auf der Grundlage der Gleichberechtigung mit anderen die Vertraulichkeit von Informationen über die Person, die Gesundheit und die Rehabilitation von Menschen mit Behinderungen“ zu schützen.

1.1.2 Datenschutz in völkerrechtlichen Spezialregelungen

Die „Leitlinien der OECD für den Schutz des Persönlichkeitsrechts und den grenzüberschreitenden Verkehr personenbezogener Daten“[9], bei denen es sich nicht um einen völkerrechtlichen Vertrag, sondern um eine Empfehlung an die Mitgliedstaaten der Organisation handelt, stellen einen frühen Versuch dar, Datenschutz, freien Informationsfluss und freien Handelsverkehr in Ausgleich zu bringen. Da neben den EU-Mitgliedern u. a. auch die USA Mitglied der OECD sind, waren hierbei europäische und US-amerikanische Ansätze des Datenschutzes zu berücksichtigen.[10] In den Leitlinien wird zwischen „sensitiven“ und „trivialen“ Angaben[11] , von denen offensichtlich keine Gefahr ausgeht, unterschieden. Letztere können von der Anwendung der Leitlinien ausgeschlossen werden. Neben verschiedenen Verarbeitungsgrundsätzen für den innerstaatlichen Bereich enthalten die Leitlinien Empfehlungen zur Sicherung des freien Informationsflusses zwischen Mitgliedstaaten. So soll etwa auf unangemessen hohe Datenschutzregelungen, die den grenzüberschreitenden Datenverkehr behindern, verzichtet werden. Der Selbstregulierung wird gleicher Stellenwert wie der (nationalen) Gesetzgebung eingeräumt.[12] Die Leitlinien gelten als „Indiz für die internationale Verbreitung bestimmter Datenschutzgrundsätze“ [13], die jedoch weder völkerrechtliche Verbindlichkeit noch einen hohen Schutzstandard aufweisen. Dessen ungeachtet sollen sie jedoch auch dazu beigetragen haben, „den Datenschutz als Gegenstand internationaler Regulierung zu etablieren.“[14]

Die so genannte Europäische Datenschutzkonvention des Europarates[15] begründet hingegen rechtliche Verpflichtungen der Unterzeichnerstaaten, einen bestimmten Katalog von Datenschutzgrundsätzen einzuhalten und in nationales Recht umzusetzen.[16] Dazu gehört insbesondere die Einhaltung bestimmter Verarbeitungsgrundsätze nach Art. 5 des Übereinkommens, die zugleich einen Kanon der heute noch gültigen Grundregeln des Datenschutzes darstellen. Personenbezogene Daten, die im öffentlichen oder nicht öffentlichen Bereich automatisch verarbeitet

[8] Übereinkommen über die Rechte von Menschen mit Behinderungen vom 13. Dezember 2006, BGBl. II 2008, S. 1419.
[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data vom 23. September 1980, vgl. Bundesanzeiger Nr. 251 vom 14. November 1981.
[10] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 36.
[11] Simitis, Spiros, in: ders. (Hrsg.). Bundesdatenschutzgesetz. 6. Auflage 2006, Einleitung, Rn. 186.
[12] Simitis, Spiros, in: ders. (Hrsg.). Bundesdatenschutzgesetz. 6. Auflage 2006, Einleitung, Rn.. 198.
[13] Ennulat, Mark: Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und –einrichtungen. 2008, S. 72.
[14] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 36.
[15] Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981, BGBl. II 1985, S. 538.
[16] Nach Nr. 39 der Denkschrift zum Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten, BT-Drs. 16/7218, S. 40, können die zur Umsetzung zu ergreifenden Maßnahmen neben Gesetzen verschiedene Formen annehmen, wie Verordnungen usw. Bindende Maßnahmen können durch freiwillige Regelungen „ergänzt“ werden, die jedoch allein nicht ausreichend sind.

werden, müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft und verarbeitet werden. Die Speicherung und Verwendung ist nur gemäß festgelegter, rechtmäßiger Zwecke zulässig. Die Daten müssen im Sinne des Verhältnismäßigkeitsgrundsatzes diesen Zwecken entsprechen und dürfen nicht darüber hinaus gehen. Die sachliche Richtigkeit der Daten, gegebenenfalls durch spätere Aktualisierung, ist genauso vorgeschrieben wie die Anonymisierung der Daten nach Zweckerfüllung. Das Übereinkommen sieht weiterhin ein spezifisches Schutzniveau für besonders sensible Daten (etwa über politische Anschauungen oder Gesundheitsdaten) und bestimmte Rechte der Betroffenen vor. Nach Art. 1 des Zusatzprotokolls „betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr“ vom 8. November 2001[17] sind unabhängige Kontrollstellen einzurichten, die insbesondere die Einhaltung der in nationales Recht umgesetzten Grundsätze für den Datenschutz gewährleisten sollen. Sie nehmen ihre Aufgaben „in völliger Unabhängigkeit“ wahr. Das Zusatzprotokoll beschränkt weiterhin in Art. 2 die Datenübermittlung in Staaten, die nicht Mitglied des Übereinkommens sind. Sie ist nur dann zulässig, wenn im Empfängerstaat ein „angemessenes Schutzniveau“ gewährleistet ist. Die Weitergabe der Daten kann aber beispielsweise auch dann erlaubt werden, wenn vertragliche Garantien von der zuständigen Behörde für ausreichend befunden wurden.

Das so genannte „Cybercrime Convention“ des Europarates vom 23. November 2001[18] enthält strafrechtliche Mindeststandards bei Angriffen auf Computer- und Telekommunikationssysteme sowie ihrem Missbrauch zur Begehung von Straftaten, Vorgaben zu strafprozessualen Maßnahmen zur Durchsuchung und Beschlagnahme bei solchen Straftaten und Regelungen zur Verbesserung der internationalen Zusammenarbeit einschließlich der Rechtshilfe bei deren Verfolgung.[19]

Als datenschutzrechtliche Spezialregelung mit globalem Anwendungsbereich kann der Beschluss der Generalversammlung der Vereinten Nationen vom 14. Dezember 1990 über „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien“ gelten.[20] Die Richtlinien, die jedoch ein niedrigeres Datenschutzniveau aufweisen als die oben genannten Abkommen, haben lediglich den Charakter einer Empfehlung.

1.2 Europarecht

1.2.1 Europäisches Primärrecht

Durch das Inkrafttreten des Vertrags von Lissabon hat der Datenschutz eine Stärkung erfahren und ist nun an zwei Stellen ausdrücklich im Primärrecht verankert:

Die grundsätzliche Regelung findet sich im Vertrag über die Arbeitsweise der Europäischen Union (AEUV). Sie ist mit Art. 16 AEUV an herausgehobener Stelle im Titel II (Allgemein geltende Bestimmungen) verortet und soll so gewährleisten, dass der Datenschutz bei sämtlichen in den EU-Verträgen erfassten Bereichen und Politiken gilt.[21] Art. 16 AEUV [Datenschutz] lautet:

[17] Zusatzprotokoll zu dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 8. November 2001, BGBl. II 2002, S. 1882.
[18] Übereinkommen über Computerkriminalität des Europarates vom 23. November 2001, BGBl. II 2008, S. 1242, für die Bundesrepublik Deutschland in Kraft getreten mit Wirkung vom 1. Juli 2009.
[19] Denkschrift zu dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (I. Allgemeines), BT-Drs. 16/7218, S. 40.
[20] Guidelines on the Use of Computerized Personal Data Flow, Resolution der Generalversammlung vom 14. Dezember 1990, UN Doc. A/Res/45/95.
[21] Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Auflage 2010, Art. 16 AEUV Rn. 7.

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht. (…)“

Art. 16 AEUV enthält in Absatz 1 erstmals ein primärrechtliches Grundrecht des Datenschutzes[22], das sowohl gegenüber den EU-Organen, Einrichtungen und sonstigen Stellen gilt als auch gegenüber den Mitgliedstaaten, soweit sie im Anwendungsbereich des Unionsrechts handeln. Korrespondierend zu diesem Rechtsanspruch auf Datenschutz ist in Absatz 2 erstmals auf primärrechtlicher Ebene eine einzige und allgemeine Rechtsetzungsbefugnis der EU ausschließlich zum Schutz personenbezogener Daten normiert. So werden das Europäische Parlament und der Rat der EU im Bereich des Datenschutzes ermächtigt, Gesetzgebungsakte nach dem ordentlichen Gesetzgebungsverfahren zu beschließen.[23]

Neben Art. 16 AEUV wurde mit dem Vertrag von Lissabon mit Art. 39 des Vertrags über die Europäische Union (EUV) eine Beschlussvorschrift zum Datenschutz speziell für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik eingeführt. Art. 39 EUV „Schutz personenbezogener Daten“ lautet:

„Gemäß Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und abweichend von Absatz 2 des genannten Artikels erlässt der Rat einen Beschluss zur Festlegung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich dieses Kapitels fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.“

Art. 39 EUV knüpft an die allgemeine Vorschrift des Art. 16 AEUV an, verlangt aber für die nähere Regelung des Datenschutzes im Bereich der Gemeinsamen Außen- und Sicherheitspolitik ein anderes Verfahren der Rechtsetzung, und zwar einen Beschluss des Rates.[24]

Mit dem Vertrag von Lissabon wurde schließlich die „Charta der Grundrechte der Europäischen Union“[25] (GRC) im Dezember 2009 rechtsverbindlich. Sie steht nun auf gleicher Hierarchiestufe wie das Primärrecht.[26] Art. 8 der Charta regelt parallel zu Art. 16 AEUV den Schutz personenbezogener Daten. Art. 8 Abs. 1 der Charta stimmt wörtlich mit Art. 16 Abs. 1 AEUV überein; Absatz

[22] Kotzur, Markus, in: Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV. 5. Auflage 2010, Art. 16 AEUV Rn. 2; Kingreen, Thorsten, in: Calliess, Christian/Ruffert, Matthias (Hrsg.). EUV/EGV - Das Verfassungsrecht der Europäischen Union. 3. Auflage 2007, Art. 286 EGV Rn. 29; Hatje, Armin, in: Schwarze, Jürgen (Hrsg.). EU-Kommentar. 2. Auflage 2009, Art. 286 EGV Rn. 6.
[23] Im Zusammenhang mit Art. 16 AEUV sind weiterhin die „Erklärung Nr. 20 zu Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union“ und die „Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit“ relevant, beides veröffentlicht in Rat der Europäischen Union, Kosolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, Dok.-Nr. 6655/08, vom 15. April. 2008.
[24] Geiger, Rudolf, in: ders./Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV, 5. Auflage 2010, Art. 39 EUV, Rn. 3.
[25] ABl. EU Nr. C 83 vom 30. März 2010, S. 393, in Kraft getreten am 1. Dezember 2009.
[26] S. Art. 6 Abs. 1 EUV.

2 formt das unionale Grundrecht näher aus.[27] Art. 8 der Charta („Schutz personenbezogener Daten“) lautet:

> „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

Das Grundrecht auf Datenschutz gem. Art. 8 GRC verpflichtet gem. Art. 51 Abs. 1 S. 1 GRC zunächst die Organe und Einrichtungen der EU bei sämtlichen ihrer Aktivitäten; es gibt keinen grundrechtsfreien Raum in der EU.[28] Darüber hinaus sind auch die Mitgliedstaaten auf das unionale Grundrecht auf Datenschutz „bei der Durchführung des Rechts der Union“ gem. Art. 51 Abs. 1 S. 1 GRC verpflichtet.[29] Eine Bindung der Mitgliedstaaten an das unionale Grundrecht des Datenschutzes ist damit in jedem Fall bei der legislativen Umsetzung von Richtlinien und beim administrativen Vollzug von Verordnungen oder unmittelbar anwendbaren Richtlinien durch die Mitgliedstaaten gegeben.[30] Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) sind die Grundrechte der Union von den Mitgliedstaaten jedoch über die bloße Durchführung des Unionsrechts hinaus schon dann anzuwenden, wenn eine nationale Maßnahme in den Anwendungsbereich des Unionsrechts fällt, z. B. in den Fällen, in denen die Mitgliedstaaten Grundfreiheiten des Binnenmarkts einschränken.[31] Überwiegend wird in der Rechtswissenschaft davon ausgegangen, dass diese weite Auslegung des EuGH durch das Verbindlichwerden der GRC nicht tangiert wird.[32] Festzuhalten bleibt, dass das unionale Grundrecht auf Datenschutz nur dann nicht in den Mitgliedstaaten zum Tragen kommt, wenn sie allein im Rahmen ihrer nationalen Kompetenzen agieren.[33]

1.2.2 Europäisches Sekundärrecht

Das zentrale Datenschutzinstrument auf europäischer Ebene ist die Datenschutzrichtlinie 95/46/EG[34] aus dem Jahr 1995 (DSRL). Die Richtlinie verpflichtet die Mitgliedstaaten, für die Verarbeitung personenbezogener Daten bestimmte Mindeststandards in ihre nationale Gesetzgebung zu übernehmen. Sie zielt darauf ab, den Schutz der Privatsphäre natürlicher Personen und den grundsätzlich erwünschten freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten in Einklang zu bringen. Deshalb sieht die Richtlinie auch vor, dass der freie Verkehr

---

[27] Kotzur, Markus, in: Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV, 5. Auflage 2010, Art. 16 AEUV, Rn. 2; Hatje, Armin, in: Schwarze, Jürgen (Hrsg.). EU-Kommentar. 2. Auflage 2009, Art. 286 EGV Rn. 6.

[28] Jarass, Hans D. Charta der Grundrechte der Europäischen Union. 2010, Art. 51 Rn. 4.

[29] Vgl. hierzu Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System, 2009, S. 396 ff.

[30] Kingreen, Thorsten, in: Calliess, Christian/Ruffert, Matthias (Hrsg.). EUV/EGV - Das Verfassungsrecht der EU. 2007, Art. 51 GRCh Rn. 8; Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System. 2009, S. 390.

[31] EuGH, Urt. v. 18. Juni 1991, Rs. C-260/89, Slg. 1991, S. I-2925, Rn. 42 ff. = EuGRZ 1991, S. 274 – ERT (Leiturteil). Hierzu Scheuing, Dieter H.: Zur Grundrechtsbindung der EU-Mitgliedstaaten, EuR 2005, 162 (164); Kokott, Juliane/Sobotta, Christoph: Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon, EuGRZ 2010, 265 (268).

[32] Vgl. Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System. 2009, S. 398; Kokott, Juliane/Sobotta, Christoph: Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon, EuGRZ 2010, 265 (268).

[33] Jarass, Hans D. Charta der Grundrechte der Europäischen Union, 2010, Art. 51, Rn. 10.

[34] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 vom 23. November 1995, S. 31).

personenbezogener Daten zwischen den Mitgliedstaaten nicht unter Hinweis auf den Schutz der Grundrechte und Grundfreiheiten, insbesondere des Schutzes der Privatsphäre, beschränkt oder untersagt werden darf. Die Mitgliedstaaten können also keine Datenschutzstandards einführen, die von den in der Richtlinie festgelegten Mindeststandards abweichen, wenn dadurch der freie Verkehr der Daten innerhalb der EU eingeschränkt wird. Die DSRL ist nicht anwendbar auf die Verarbeitung personenbezogener Daten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts vor dem Vertrag von Lissabon fallen. Hierunter fallen insbesondere Tätigkeiten der EU in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (frühere 3. Säule). Eine Anpassung der Richtlinie an die mit dem Vertrag von Lissabon bewirkte Auflösung der Säulenstruktur ist bislang noch nicht erfolgt.[35]

Die in der Richtlinie vorgeschriebenen datenschutzrechtlichen Mindeststandards betreffen

- die Qualität der Daten (u. a. Verarbeitung nach Treu und Glauben, auf rechtmäßige Weise sowie für festgelegte Zwecke);
- die Zulässigkeit der Datenverarbeitung (u. a. Einwilligung der betroffenen Person oder Erforderlichkeit der Datenverarbeitung aus bestimmten in der Richtlinie festgelegten Gründen);
- erhöhte Schutzanforderungen für besonders sensible Daten, etwa über die politische Meinung oder religiöse Überzeugung;
- bestimmte Informationen, die der für die Verarbeitung Verantwortliche der betroffenen Person übermitteln muss;
- Auskunftsrechte sowie Rechte auf Berichtigung, Löschung und Sperrung von Daten;
- Widerspruchsrechte;
- die Vertraulichkeit und Sicherheit der Verarbeitung;
- Meldepflichten gegenüber einer Kontrollstelle;
- Rechtsbehelfe, Haftung und Sanktionen.

Die Richtlinie sieht weiterhin die Einrichtung von Kontrollstellen vor, die ihre Aufgaben in völliger Unabhängigkeit wahrnehmen und legt Grundsätze für die Übermittlung personenbezogener Daten an Drittländer fest. Voraussetzung hierfür ist, dass der Drittstaat ein „angemessenes Schutzniveau“[36] gewährleistet. Bei welchen Staaten dies der Fall ist, entscheidet die Kommission.

Der Verpflichtung zur Umsetzung der Richtlinie, die bis 1998 zu erfüllen war, ist Deutschland durch Änderung des Bundesdatenschutzgesetzes im Jahr 2001 nachgekommen.

Bei der Umsetzung der Vorschriften über die Datenübermittlung in Drittländer ergaben sich gegenüber den USA Probleme, die zum Abschluss der „Safe Harbor“ - Vereinbarung führten. Auf Grund unterschiedlicher datenschutzrechtlicher Ansätze verfolgen die USA in Fragen des Datenschutzes einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung beruht, während in der EU Regelungen in Form umfassender Datenschutzgesetze überwiegen. Angesichts dieser Unterschiede bestanden Unsicherheiten, ob bei der Übermittlung personenbezogener Daten in die USA ein „angemessenes Schutzniveau“ im Sinne des

[35] Zerdick, Thomas in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Auflage 2010, Art. 16 AEUV Rn. 37.
[36] Art. 25 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 vom 23.November 1995, S. 31.

EU-Datenschutzrechts gegeben sei.[37] Um ein angemessenes Datenschutzniveau zu gewährleisten, haben die EU und das US-Handelsministerium im Juli 2006 eine Vereinbarung zu den Grundsätzen des so genannten „sicheren Hafens“ (Safe Harbor) geschlossen.[38] Als „Safe Harbor Prinzipien“ wurden sieben Grundsätze für die Datenverarbeitung festgelegt (betreffend u. a. Informationspflichten und Auskunftsrechte, Möglichkeit des „opt-out“ bei der Weitergabe an Dritte oder der Nutzung für andere Zwecke, Sicherheitsvorkehrungen gegen Verlust, unbefugtem Zugriff oder Missbrauch personenbezogener Daten, Rechtsbehelfe und Sanktionen). Das Abkommen sieht vor, dass sich US-amerikanische Unternehmen öffentlich zur Einhaltung der so genannten „Safe Harbor Prinzipien“ verpflichten können. Die Zertifizierung erfolgt durch Meldung an die Federal Trade Commission (FTC). Eine Liste der beigetretenen Unternehmen wird vom FTC im Internet veröffentlicht. Die Datenübermittlung an ein zertifiziertes Unternehmen ist dann möglich, ohne dass es einer weiteren behördlichen Feststellung des angemessenen Schutzniveaus bedürfte.[39]

Als bereichsspezifische Ergänzung zur DSRL regelt die E-Privacy-Richtlinie 2002/58/EG[40] datenschutzrechtliche Aspekte im Bereich der elektronischen Kommunikation, die durch die DSRL nicht ausreichend abgedeckt wurden, etwa die Vertraulichkeit der Kommunikation, Regelungen über Verkehrsdaten, Standortdaten, Einzelgebührennachweis, Rufnummernanzeige und unerbetene Werbenachrichten. Juristische Personen werden in den Schutzbereich der Richtlinie einbezogen. Die Richtlinie dient neben der Harmonisierung der mitgliedstaatlichen Datenschutzvorschriften auch der Gewährleistung des freien Verkehrs von Daten, elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft.

Die E-Privacy Richtlinie wurde mit Richtlinie 2009/136/EG[41] geändert. Erstmalig wurde auf EU-Ebene eine Informationspflicht der Diensteanbieter bei Datensicherheitsverletzungen eingeführt, die Installation von „Cookies“ oder „Spyware“ von der Einwilligung des Internetnutzers abhängig gemacht, die Rechte Betroffener gegen unerbetene kommerzielle Nachrichten gestärkt und die Durchsetzung der Datenschutzbestimmungen durch Sanktionen verbessert. Die Umsetzung dieser Änderungen hat bis zum 25. Mai 2011 zu erfolgen.[42]

In der im Jahr 2000 verabschiedeten E-Commerce Richtlinie 2000/31/EG[43], mit der ein europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr geschaffen wurde, werden Fragen des Datenschutzes ausgeklammert[44] und insoweit auf anderweitige Rechtsakte der Union verwiesen. In den Erwägungen der Richtlinie (Nr. 14) wird allerdings betont, dass die Grundsätze des

[37] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, KOM (2000) 2441, ABl. EG Nr. L 215 vom 25. August 2000, S. 10.
[38] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000, ABl. EG Nr. L 215 vom 25. August 2000, S. 7.
[39] Nach einem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover, abrufbar unter http://www.bfdi.bund.de/cae/servlet/contentblob/1103868/publicationFile/88848/290410_SafeHarbor.pdf (zuletzt aufgerufen am: 17. März 2011) sind die datenexportierenden Unternehmen in Deutschland dennoch verpflichtet, gewisse Mindestkriterien zu prüfen, da eine „flächendeckende“ Kontrolle durch die Kontrollbehörden, ob zertifizierte Unternehmen die „Safe Harbor Prinzipien“ tatsächlich einhalten, nicht gegeben sei.
[40] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 vom 31. Juli 2002, S. 37.
[41] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. EU Nr. L 337 vom 18. Dezember 2009, S. 11.
[42] Jedenfalls teilweise soll dies im Rahmen der geplanten TKG-Novelle erfolgen, vgl. § 109a des Gesetzentwurfs der Bundesregierung vom 2. März 2011, online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/referentenentwurf-tkg-2011,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (zuletzt abgerufen am 9.3.2011).
[43] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), ABl. EG L 178 vom 17. Juli 2000, S. 1.
[44] A.a.O. (S. 3), Erwägungsgrund Nr. 14, sowie Artikel 1 Abs. 5 b) der genannten Richtlinie.

Schutzes personenbezogener Daten bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten sind, insbesondere in Bezug auf nicht angeforderte kommerzielle Kommunikation und die Verantwortlichkeit von Vermittlern.

Die Datenschutzverordnung für die EU-Organe 45/2001/EG[45] beschreibt den datenschutzrechtlichen Rechtsrahmen für das Handeln der EU-Organe. Adressat der Verordnung sind also nicht die Mitgliedstaaten, sondern alle „Organe und Einrichtungen der Gemeinschaft“. Durch die Verordnung wird weiterhin der Europäische Datenschutzbeauftragte eingesetzt, der für die unabhängige Kontrolle der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU zuständig ist.

Mit der Vorratsdatenspeicherungsrichtlinie 2006/24/EG[46] werden die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung bestimmter Daten, die von Telekommunikationsdienstleistern etwa im Rahmen von Internet und Telefonie erzeugt oder verarbeitet werden, harmonisiert. Auf diese Weise soll sichergestellt werden, dass die Daten zu Zwecken der Ermittlung und Verfolgung schwerer Straftaten verfügbar sind.[47] Die Richtlinie schreibt die vorsorgliche anlasslose Speicherung von Kommunikationsdaten vor und trifft u. a. Feststellungen zu den Kategorien der zu speichernden Daten, zu Speicherungsfristen und Fragen des Datenschutzes und der Datensicherheit. Daten, die Kommunikationsinhalte betreffen (Inhaltsdaten), sind nicht zu speichern.[48]

Im Bereich der justiziellen Zusammenarbeit in Strafsachen und bei der polizeilichen Zusammenarbeit existiert ein allgemeiner Rechtsakt mit der Annahme des Rahmenbeschlusses 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.[49] Der eng gefasste Anwendungsbereich des Rahmenbeschlusses erstreckt sich auf solche personenbezogenen Daten, die von mitgliedstaatlichen Behörden zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen erhoben bzw. verarbeitet werden. Der Rahmenbeschluss gilt nur bei einem zwischenstaatlichen Datenaustausch. Nicht anwendbar ist der Beschluss bei rein nationalen Sachverhalten.[50] Im Gegensatz zur DSRL setzt der Rahmenbeschluss 2008/977/JI zwischen den Mitgliedstaaten lediglich einen Mindeststandard fest. Die einzelnen Mitgliedstaaten sind daher nicht daran gehindert, strengere nationale Bestimmungen im Regelungsbereich des Rahmenbeschlusses zu erlassen.[51]

Die Europäische Kommission hat im November 2010 ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“[52] vorgelegt und für 2011 einen Vorschlag für die Änderung der DSRL angekündigt.

---

[45] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft zum freien Datenverkehr, ABl. EG Nr. L 8 vom 12. Januar 2001, S. 1.

[46] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentliche zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105 vom 13. April 2006, S. 54.

[47] Artikel 1 der Richtlinie, a.a.O.

[48] Die Europäische Kommission führt derzeit eine Evaluation der Vorratsdatenspeicherungsrichtlinie durch. Zu den Entscheidungen des Bundesverfassungsgerichts, die die Umsetzung der Richtlinie in deutsches Recht betreffen, vgl. auch unter 1.6.

[49] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. EU Nr. L 350 vom 30. Dezember 2008, S. 60.

[50] Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Aufl. 2010, Art. 16 Rn. 48.

[51] Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Aufl. 2010, Art. 16 Rn. 50.

[52] Mitteilung der Kommission an das Europäische Parlament, den Rat den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine digitale Agenda für Europa“, KOM (2010) 245, online abrufbar unter: http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-de.pdf (zuletzt aufgerufen am: 17. März 2010).

1.2.3 Rechtsprechung des Europäischen Gerichtshofs (EuGH)

Erste Entscheidungen des EuGH zur DSRL datieren aus dem Jahr 2003.[53] In einem 2003 entschiedenen Verfahren[54] wandten sich Mitarbeiter des Österreichischen Rundfunks gegen eine österreichische Regelung, auf Grund derer ihre Jahresbezüge mit ihren Namen dem Rechnungshof mitzuteilen waren und nachfolgend vom Rechnungshof veröffentlicht wurden. Besonders streitig war in diesem Zusammenhang, ob die DSRL, die auf die Kompetenz der Gemeinschaft zur Errichtung des Binnenmarktes gestützt wurde und durch Harmonisierung der nationalen Vorschriften den freien Datenverkehr zwischen den Mitgliedstaaten gewährleisten soll, auf diesen Sachverhalt überhaupt anwendbar war. Denn im konkreten Fall lag ein Zusammenhang mit den europarechtlichen Grundfreiheiten eher fern. Das Gericht hat die Anwendbarkeit der Richtlinie dennoch bejaht. Nach Auffassung des Gerichts kann die Anwendbarkeit der Richtlinie im Einzelfall nicht davon abhängen, ob ein Zusammenhang mit dem freien Verkehr zwischen den Mitgliedstaaten besteht.[55]

Die Darstellung anderer Personen auf einer privaten schwedischen Website ohne deren Zustimmung war Gegenstand im Fall „Lindqvist“[56]. In seinem Urteil nahm der EUGH erstmals zur Veröffentlichung personenbezogener Daten im Internet Stellung und entschied, dass die Einstellung ins Internet zwar eine Verarbeitung von Daten im Sinne der DSRL darstelle, nicht aber als Übermittlung in Drittländer und damit nicht als grenzüberschreitender Datenaustausch anzusehen sei. Das Gericht äußerte sich auch zur Frage des Ausgleichs zwischen Datenschutz und widerstreitenden Grundrechten, insbesondere der Meinungsfreiheit. Es sei Sache der nationalen Behörden und Gerichte, ein angemessenes Gleichgewicht zwischen den betroffenen Rechten und Interessen einschließlich geschützter Grundrechte herzustellen und hierbei insbesondere den Grundsatz der Verhältnismäßigkeit zu wahren. Im Übrigen sei es zulässig, dass die Mitgliedstaaten den Geltungsbereich ihrer Datenschutzgesetze über den Anwendungsbereich der Richtlinie hinaus ausdehnen, soweit dem keine Bestimmung des Gemeinschaftsrechts entgegenstehe.

Zur Übermittlung von Fluggastdaten an die USA nahm der EuGH im Mai 2006 (C-317/04) Stellung.[57] Er erklärte die zu Grunde liegende Genehmigung des Abkommens zwischen der EU und den USA durch den Rat für nichtig. Dasselbe gelte für die zum selben Sachverhalt ergangene Entscheidung der Kommission, mit der das US-amerikanische Datenschutzniveau für angemessen im Sinne des Art. 25 DSRL erklärt wurde. Wie sich aus den Begründungserwägungen ergebe, seien Sinn und Zweck der Datenübermittlung in die USA die Terrorismusbekämpfung. Gegenstand beider Rechtsakte sei daher das Strafrecht. Daher sei die DSRL[58] keine geeignete Rechtsgrundlage. Mangels Rechtsgrundlage waren der Ratsbeschluss und die Kommissionsentscheidung für nichtig zu erklären. In dem Urteil des EuGH vom Februar 2009 über die Vorratsdatenspeicherungs-Richtlinie[59] konzentriert sich das Gericht ebenfalls auf Fragen der Rechtsetzungskompetenz. Grundrechtliche Fragen waren nicht Gegenstand des Verfahrens. Die Vorratsdatenspeicherungs-

[53] Vgl. Roßnagel, Alexander: Anmerkung zu EuGH Urt. v. 6. November 2003, C-101/01, Slg. 2003, I-12971 Rn 87 – Lindqvist = MMR 2004, 95 (100).
[54] EuGH, Urteil vom 20. Mai 2003, Rs. C-465/00, Slg. I-04989 - Österreichischer Rundfunk.
[55] Dieses weite Verständnis des Anwendungsbereichs der Richtlinie trägt nach Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sehr zur „Europäisierung des Datenschutzes“ bei,
vgl.:http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/Arbeit/Artikel/200503_OesterreichischerRundfunk.html?nn=408918 (zuletzt aufgerufen am: 17. März 2011).
[56] EuGH Urteil vom 6. November 2003, C-101/01, Slg. 2003, I-12971 – Lindqvist.
[57] EuGH, Urteil vom 30. Mai 2006, verb. Rs. C‑317/04 und C‑318/04, Slg. 2006, I-4721– Europäisches Parlament gegen Rat der EU.
[58] S. a. Artikel 3 Abs. 2 zweiter Spiegelstrich der so genannten Datenschutzrichtlinie, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 vom 23. November 1995, S. 31).
[59] EuGH, Urteil vom 10. Februar 2009, Rs. C-301/06, MMR 2009, 244 ff. – Vorratsdatenspeicherung.

Richtlinie stelle keine Regelung der Strafverfolgung dar, sondern habe – anders als bei der Fluggastdatenübermittlung – den Zweck, durch Harmonisierung das Handeln der Telekommunikationsdienstleister im Binnenmarkt zu erleichtern. Die Richtlinie sei daher zu Recht auf der Grundlage der Binnenmarktkompetenz erlassen worden. Anders als von der Klage geltend gemacht, sei ein Rahmenbeschluss nach den Bestimmungen über die polizeiliche und justizielle Zusammenarbeit nicht erforderlich.

Im Hinblick auf das zentrale deutsche Ausländerregister entschied der EuGH mit Urteil vom 16. Dezember 2008[60], dass die Speicherung und Verarbeitung personenbezogener Daten namentlich genannter Personen zu statistischen Zwecken nicht dem Erforderlichkeitsgebot[61] im Sinne der europäischen Richtlinie zum Schutz personenbezogener Daten entspreche und die Nutzung der im Register enthaltenen Daten zur Bekämpfung der Kriminalität gegen das Diskriminierungsverbot verstoße, da diese Nutzung auf die Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit abstelle. Ein System zur Verarbeitung personenbezogener Daten, das der Kriminalitätsbekämpfung diene, aber nur EU-Ausländer erfasse, sei mit dem Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit unvereinbar.

Zum Verhältnis von Pressefreiheit und Datenschutz äußerte sich der EuGH in seiner Entscheidung vom 16. Dezember 2008[62]. Das Unternehmen Markkinapörrsi veröffentlicht Steuerdaten (Namen und Einkommen), die bei den finnischen Steuerbehörden öffentlich zugänglich sind. Der EuGH sah auch diese Weiterveröffentlichung bereits öffentlich zugänglicher Informationen als Datenverarbeitung im Sinne der DSRL an. Um Datenschutz und Meinungsfreiheit in Ausgleich zu bringen, seien die Mitgliedstaaten aufgerufen, Einschränkungen des Datenschutzes vorzusehen. Entsprechende Ausnahmen dürften allein zu journalistischen, künstlerischen oder literarischen Zwecken, die unter das Grundrecht der Meinungsfreiheit fallen, gemacht werden, soweit sie sich als notwendig erweisen, um das Recht der Privatsphäre mit den für die Meinungsfreiheit geltenden Vorschriften in Einklang zu bringen. In Anbetracht der hohen Bedeutung der Meinungsfreiheit müsse der Begriff des „Journalismus“ und damit zusammenhängende Begriffe weit ausgelegt werden. Andererseits müssten sich Einschränkungen des Datenschutzes aus Gründen der Meinungsfreiheit auf das absolut Notwendige beschränken.

Mit Urteil vom 9. März 2010 entschied der EuGH in einem Vertragsverletzungsverfahren, das die EU-Kommission gegen Deutschland angestrengt hatte.[63] Die organisatorische Einbindung der Datenschutzaufsicht für den nicht-öffentlichen Bereich in die Innenministerien einiger Bundesländer sowie die Aufsicht der Landesregierungen über die Datenschutzbehörden entspreche nicht den Vorgaben der DSRL. Vielmehr sei nach Art. 28 der Richtlinie erforderlich, dass diese Stellen ihre Aufgabe „in völliger Unabhängigkeit“ wahrnehmen.

Um den Widerstreit von Transparenz und Datenschutz geht es bei der Entscheidung in der Rechtssache „Bavarian Lager“ vom 29. Juni 2010.[64] Die Kommission hatte es abgelehnt, gegenüber der Gesellschaft Bavarian Lager Company die Namen der Teilnehmer eines im Rahmen eines Vertragsverletzungsverfahrens abgehaltenen vertraulichen Treffens offenzulegen. Die Kommission berief sich darauf, dass der Zugang zu Dokumenten nur unter Beachtung des Datenschutzes zulässig sei. Das Europäische Gericht hatte 2007 in erster Instanz entschieden, dass die

[60] EuGH, Urteil vom 10. Februar 2009, Rs. C-524/06, MMR 2009, 171 ff. – Huber.
[61] Artikel 7 Buchst. e DSRL, a.a.O.
[62] EuGH, Urteil vom 16. Dezember 2008, Rs. C-73/07, Slg. 2007, I-7075 - Markkinapörrsi.
[63] EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland.
[64] EuGH, Urteil vom 29. Juni 2010, Rs. C-28/08, EuZW 2010, 617 - Bavarian Lager Company.

Herausgabe der Dokumente nur dann verweigert werden könne, wenn der Schutz der Privatsphäre verletzt werde. Das sei bei einer bloßen Namensnennung auf einer Teilnehmerliste im beruflichen Kontext nicht der Fall. Auf der Grundlage der Verordnung 45/2001/EG sowie der Verordnung 1049/2001/EG[65] entschied der EuGH im Juni 2010, dass die Kommission rechtmäßig gehandelt habe. Die in dem Sitzungsprotokoll aufgeführten Teilnehmernamen seien personenbezogene Daten. Da Bavarian Lager Argumente für die Notwendigkeit der Übermittlung dieser Daten oder ein berechtigtes Interesse nicht vorgetragen habe, könne die Kommission keine Interessenabwägung vornehmen. Die Verpflichtung zur Transparenz sei daher im konkreten Falle von der Kommission hinreichend gewahrt worden.

Demgegenüber sah das Gericht bei der Internet-Veröffentlichung der Namen aller natürlichen Personen, die EU-Agrarsubventionen empfangen haben, den Grundsatz der Verhältnismäßigkeit verletzt, da hierbei nicht nach einschlägigen Kriterien wie Häufigkeit, Art und Höhe der Beihilfen unterschieden wurde. Das Interesse der Steuerzahler an Informationen über die Verwendung öffentlicher Gelder rechtfertige einen solchen Eingriff in das Recht auf Schutz der personenbezogenen Daten nach Art. 8 der Grundrechtcharta nicht.[66]

1.3 Nationales Recht

1.3.1 Grundrechte

Das Grundgesetz kennt kein ausdrückliches Datenschutz-Grundrecht. Allerdings hat das Bundesverfassungsgericht (BVerfG) bereits 1983 in seinem so genannten „Volkszählungsurteil“[67] das Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechtes (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) formuliert. Forderungen, den Datenschutz ausdrücklich als Grundrecht im Grundgesetz zu verankern, fanden bisher nicht die erforderliche Mehrheit.[68] Nach der Rechtsprechung des BVerfG beinhaltet das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[69] Die Unsicherheit, wo welche personenbezogenen Informationen gespeichert, verwendet oder weitergegeben werden, würde „nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[70] „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.[71] In den Schutzbereich dieses Grundrechts fallen alle Formen der Erhebung personenbezogener Daten. Angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie

[65] Verordnung des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den öffentlichen Zugang zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. EG Nr. L 145, S. 43).
[66] EuGH, Urteil vom 9. November 2010, Rs. C-92/09, C-93/09, EuZW 2010, 939 – Scheck GbR und Eifert gegen Land Hessen.
[67] BVerfGE 65,1.
[68] Viele Landesverfassungen enthalten hingegen ein eigenständiges Datenschutzgrundrecht, vgl. die Landesverfassungen von Berlin (Art. 33), Brandenburg (Art. 11), Bremen (Art. 12), Mecklenburg-Vorpommern (Art. 6), Nordrhein-Westfalen (Art. 4), Rheinland-Pfalz (Art. 4a), Saarland (Art. 2), Sachsen (Art. 33), Sachsen-Anhalt (Art. 6) und Thüringen (Art. 6). Vgl. im Übrigen unter 2.2.2.
[69] BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 45 - Volkszählung.
[70] BVerfGE 65, 1, 43 - Volkszählung.
[71] BVerfGE 65, 1, 43 - Volkszählung.

geht das BVerfG davon aus, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr“ gebe.[72]

Im Hinblick auf die Fragestellungen der Enquete-Kommission sind als weitere Ausprägungen des allgemeinen Persönlichkeitsrechts das Recht am eigenen Bild von Bedeutung, das u. a. den Einzelnen vor der Aufnahme, Darbietung, Verbreitung und sonstigen Verwertung seines Abbildes schützt[73], sowie das 2008 durch das BVerfG formulierte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“.[74] Nach der Rechtsprechung des Gerichts handelt es sich um ein subsidiäres Grundrecht, das hinter anderen Grundrechten, etwa dem Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG) oder der Unverletzlichkeit der Wohnung (Art. 13 GG) zurücktritt und erst dann zur Anwendung kommt, wenn vorrangige Grundrechte keinen hinreichenden Schutz vor Eingriffen in informationstechnische Systeme gewähren.[75]

Grundlegend für den Datenschutz sind weiterhin die Grundrechte nach Art. 10 GG (Brief-, Post- und Fernmeldegeheimnis, auch als „Telekommunikationsgeheimnis“ bezeichnet) und Art. 13 GG (Unverletzlichkeit der Wohnung). Das Grundrecht der Unverletzlichkeit der Wohnung schützt u. a. vor Durchsuchungen und Abhörmaßnahmen, etwa wenn hierfür in die Wohnung eingedrungen wird.[76] Durch das Fernmeldegeheimnis wird die unbeobachtete, nicht öffentliche Kommunikation unabhängig von der Übertragungsart (Kabel, Funk, analoge oder digitale Vermittlung) und unabhängig von deren Ausdrucksformen (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) geschützt, und zwar auch über das Internet, etwa als E-Mail.[77] Der Schutz erstreckt sich nicht nur auf die Inhalte der Kommunikation, sondern auch auf die Kommunikationsumstände[78], etwa die beteiligten Personen, Zeit, Ort und Häufigkeit der Kommunikation. An Art. 10 GG zu messen ist weiterhin der Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen von geschützten Kommunikationsvorgängen anschließt, sowie der Gebrauch, der von den so erlangten Kenntnissen gemacht wird.[79] Da das Telekommunikationsgeheimnis vorrangig vor der Manipulation des technischen Übertragungsvorgangs schützt, endet der Schutz des Fernmeldegeheimnisses, sobald der Übertragungsvorgang abgeschlossen ist. Bezogen auf die Telekommunikation enthält Art. 10 GG eine spezielle Garantie, die das Recht auf informationelle Selbstbestimmung verdrängt und aus der sich besondere Anforderungen für die Daten ergeben, die durch Eingriffe in das Fernmeldegeheimnis erlangt werden. Nach der Rechtsprechung des BVerfG lassen sich allerdings die Maßgaben, die für das Recht auf informationelle Selbstbestimmung gelten, weitgehend auf Eingriffe in das Fernmeldegeheimnis übertragen.

1.3.2 Einfaches Bundesrecht

Das Bundesdatenschutzgesetz (BDSG)[80] stellt das Kernstück des Datenschutzrechts auf Bundesebene dar. Es wurde 1990 als umfassende Novelle des Bundesdatenschutzgesetzes von 1977 in Reaktion auf das „Volkszählungsurteil“ verabschiedet, um – den Vorgaben des BVerfG entsprechend – eine gesetzliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten zu schaffen und so den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechtes zu

[72] BVerfGE 65, 1, 45- Volkszählung. Zum Grundrecht auf informationelle Selbstbestimmung vgl. im Übrigen unter 2.1.5.
[73] Di Fabio, Udo, in: Maunz, Theodor/Dürig, Günter. Grundgesetz. 57. Auflage 2010, Art. 2 GG Rn. 193.
[74] BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370, 595/07, BVerfGE 120, 274, 302 ff. – Onlinedurchsuchung.
[75] Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vgl. im Übrigen unter 2.1.3.
[76] BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 u. 1 BvR 1084/99, BVerfGE 109, 279 – Großer Lauschangriff.
[77] BVerfGE 120, 274, 307 – Onlinedurchsuchung.
[78] BVerfG, Urteil vom 27. Juli 2005 - 1 BvR 668/04, BVerfGE 113, 348, 364 – Vorbeugende Telekommunikationsüberwachung.
[79] BVerfGE 113, 348, 365 – Vorbeugende Telekommunikationsüberwachung.
[80] Gesetz vom 20. Dezember 1990 in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I, S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I, S. 2814).

schützen. Als Teil des allgemeinen Datenschutzrechts enthält es keine bereichsspezifischen Regelungen und gilt sowohl für Datenverarbeitung in IT-Systemen als auch auf für manuelle Verfahren.

Geschützt werden vom Gesetz „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Abs. 1 BDSG), nicht aber Angaben über juristische Personen. Wesentlicher Grundsatz des Gesetzes ist das so genannte „Verbot mit Erlaubnisvorbehalt“ nach § 4 Abs. 1 BDSG. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn ein Gesetz oder eine sonstige Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Daneben gilt der Grundsatz der Datenvermeidung und Datensparsamkeit, wonach so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen sind. Möglichkeiten der Anonymisierung und Pseudonymisierung sind weitestgehend auszuschöpfen. Das Gesetz stellt für „besondere Arten personenbezogener Daten“, etwa über die rassische oder ethnische Herkunft, politische Meinungen oder religiöse Überzeugungen, höhere Schutzanforderungen. Rechte des Betroffenen erstrecken sich auf Auskunft, Berichtigung, Löschung oder Sperrung. Der zentrale datenschutzrechtliche Grundsatz der Zweckbindung hat an verschiedenen Stellen im Gesetz Niederschlag gefunden. Das Datenschutzaudit ist Gegenstand der Regelung des § 9a BDSG.

Neben allgemeinen und gemeinsamen Bestimmungen enthält das Gesetz gesonderte Regelungen für die Datenverarbeitung öffentlicher Stellen einerseits und nicht-öffentlicher Stellen andererseits. Die Regelungen über die Datenverarbeitung öffentlicher Stellen (§§ 12 ff. BDSG) gelten für Behörden und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, bundesunmittelbare öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen sowie Organe der Rechtspflege. Für öffentliche Stellen der Länder gelten sie stets nur subsidiär gegenüber den Landesdatenschutzgesetzen. Da alle Bundesländer Landesdatenschutzgesetze erlassen haben, ergibt sich hierfür kein praktischer Anwendungsfall. Wahl, Rechtsstellung und Aufgabe des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind in §§ 22 ff. BDSG geregelt. Das Gesetz enthält weiterhin Bußgeld- und Strafvorschriften.

Der räumliche Anwendungsbereich des BDSG ist in § 1 Abs. 5 BDSG geregelt. Erhebt oder verarbeitet ein ausländisches Unternehmen mit Sitz innerhalb der EU bzw. innerhalb des EWR Daten im Inland, ist das BDSG nur dann anwendbar, wenn das Unternehmen durch eine deutsche Niederlassung tätig wird. Bei Datenerhebung und -verarbeitung im Inland durch ein Unternehmen mit Sitz außerhalb der EU bzw. außerhalb des EWR findet das BDSG hingegen Anwendung.[81]

Gegenüber spezielleren Vorschriften des Bundesrechts tritt das BDSG zurück (§ 1 Abs. 3 BDSG). Wegen zahlreicher bereichsspezifischer Regelungen in anderen Gesetzen wird das BDSG daher als Auffanggesetz des insgesamt zersplitterten Datenschutzrechts angesehen.[82] Beispiele für Spezialregelungen sind das Bundespolizeigesetz, das Bundeskriminalamtsgesetz, das Bundeszentralregistergesetz, die Grundbuchordnung, das Personenstandgesetz, §§ 8 ff. Handelsgesetzbuch und die Grundbuchordnung.[83] In gesonderten Vorschriften außerhalb des BDSG ist auch der Datenschutz der öffentlich-rechtlichen Religionsgemeinschaften geregelt. Im Sozialgesetzbuch (SGB) Band X (Zweites Kapitel „Schutz der Sozialdaten, §§ 67 ff.)[84] finden sich die datenschutzrechtli-

[81] Anderes gilt nach § 1 Abs. 5 S. 4 BDSG im Fall des „Transits“.
[82] Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 1 Rn. 14.
[83] Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo. Bundesdatenschutzgesetz - Kommentar. 3. Auflage 2010, Einleitung, Rn. 73.
[84] Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I, S. 130), zuletzt geändert durch Gesetz vom 5. August 2010 (BGBl. I, S. 1127).

chen Bestimmungen für den Sozialleistungsbereich. Sozialdaten sollen nach der Vorstellung des Gesetzgebers einem erhöhten, dem Steuergeheimnis vergleichbaren Schutz unterliegen.[85] Ergänzende Bestimmungen für verschiedene Zweige der Sozialversicherung enthalten die jeweils einschlägigen Bücher des SGB.

Für das Internet von besonderer Bedeutung ist das Telemediengesetz (TMG).[86] Telemedien sind Waren- und Dienstleistungsangebote im Netz unter Einbeziehung redaktionell gestalteter Online-Angebote, ausgenommen jedoch der Rundfunk.[87] Für diese Medien enthält das TMG Vorschriften über den Umgang mit personenbezogenen Nutzerdaten (§§ 11 ff. TMG). Auch im TMG gelten die Grundsätze der Zweckbindung, der Datenvermeidung und –sparsamkeit. Den allgemeinen Datenschutzgrundsätzen folgend ist auch im Bereich der Telemedien die Erhebung und Verarbeitung personenbezogener Daten nur mit Einwilligung des Betroffenen oder auf gesetzlicher Grundlage zulässig. Zugeschnitten auf den Bereich der Telemedien sind in § 13 TMG die Voraussetzungen für eine elektronische Einwilligung geregelt. Über Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen Diensteanbieter und Nutzer erforderlich sind (Bestandsdaten), darf der Dienstanbieter nach § 14 TMG auf Anordnung der zuständigen Stellen im Einzelfall Auskunft erteilen, etwa zum Zwecke der Strafverfolgung, zur Gefahrenabwehr, zur Terrorbekämpfung oder zur Durchsetzung der Rechte am geistigen Eigentum.

Telekommunikationsdienste sind hingegen solche Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsdienste bestehen, darunter nach Vorstellung des Gesetzgebers auch Internet-Telefonie, Internet-Access-Provider und E-Mail-Übertragung.[88] Der Datenschutz für die Teilnehmer ist im Telekommunikationsgesetz (TKG)[89], insbesondere §§ 91 ff. TKG, geregelt. Geschützt sind Angaben über persönliche und sachliche Verhältnisse, u. a. Informationen über das Kommunikationsverhalten, d.h. „wer wann mit wem von welchem Anschluss aus telefoniert hat.“[90] Das TKG enthält Regelungen u. a. über Bestands- und Verkehrsdaten, Entgeltermittlung und -abrechnung.

1.3.3 Landesrecht

Die Landesdatenschutzgesetze gelten für die Verarbeitung personenbezogener Daten durch die jeweiligen Landesbehörden und andere öffentlich-rechtliche Einrichtungen der Länder. Sie enthalten Bestimmungen über die Landesdatenschutzbeauftragten. Ganz überwiegend gilt auch für die Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen Regelungen.[91] Da der Datenschutz in nahezu allen Bereichen der Landesverwaltung von Bedeutung ist, weist eine Unzahl landesrechtlicher Gesetze Spezialregelungen zum Datenschutz auf, u. a. die Landesgesetze zum (Jugend-)Strafvollzug und zur Untersuchungshaft, die Rettungsdienstgesetze, Brand- und Katastrophenschutzgesetze, Schulgesetze.

[85] BT-Drs. 8/4022, S. 96.
[86] Telemediengesetz vom 26. Februar 2007, BGBl. I, S. 179, zuletzt geändert durch Gesetz vom 14. August 2009, BGBl. I, S. 2814.
[87] Hoeren, Thomas: Das Telemediengesetz, NJW 2007, 801.
[88] BT-Drs. 16/3078, S. 13.
[89] Telekommunikationsgesetz vom 25. Juni 1996, BGBl. I, S. 1120, geändert durch Gesetz vom 22. Juni 2004, BGBl. I, S. 1190. Zur geplanten TKG-Novelle vgl. auch Fn. 42.
[90] Robert, Anna, in: Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.). Beck’scher TKG-Kommentar. 3. Auflage 2006, § 91 Rn. 12.
[91] Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 1 Rn. 33.

Anders als im Bundesrecht finden sich auf Landesebene auch Formen untergesetzlicher Regelungen zum allgemeinen Datenschutzrecht, d. h. Rechtsverordnungen und Verwaltungsvorschriften.[92]

1.3.4 Rechtsprechung des Bundesverfassungsgerichts

Neben den unter 1.3.1 erwähnten grundlegenden Entscheidungen, dem „Volkszählungsurteil“ sowie dem Urteil zur „Online-Durchsuchung“, hat sich das BVerfG in einer Reihe weiterer Entscheidungen mit Fragen der informationellen Selbstbestimmung und verwandter Grundrechte befasst. Die Rechtsprechung des BVerfG enthält im Bereich des Datenschutzes vielfach sehr konkrete und detaillierte Vorgaben für das gesetzgeberische Handeln.[93] Aus der umfangreichen Rechtsprechung des Gerichts zum Datenschutz sei beispielhaft auf folgende Entscheidungen hingewiesen:

Gegenstand des Urteils vom 14. Juli 1999[94] waren erweiterte Befugnisse des Bundesnachrichtendienstes zur Überwachung, Aufzeichnung und Auswertung des Telekommunikationsverkehrs sowie zur Übermittlung der daraus erlangten Daten an andere Behörden. 1994 war das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) mit dem Ziel geändert worden, Informationen u. a. im Bereich des internationalen Terrorismus, des Drogenhandels und der Geldwäsche zu erlangen, um sie nachfolgend den zuständigen Behörden zur Verhinderung, Aufklärung und Verfolgung von Straftaten zur Verfügung zu stellen.[95] Mit Beschluss vom 5. Juli 1995[96] bestimmte das BVerfG im Rahmen einer einstweiligen Anordnung, dass einzelne der neugefassten Vorschriften zunächst nur eingeschränkt angewendet werden dürften. In der Hauptsache urteilte das Gericht 1999, einzelne Vorschriften verstießen gegen Art. 10 GG. Das Fernmeldegeheimnis schütze in erster Linie den Kommunikationsinhalt vor staatlicher Kenntnisnahme, daneben aber auch die Kommunikationsumstände. Der Schutz erstrecke sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen von geschützten Kommunikationsvorgängen anschließe, und den Gebrauch, der von den erlangten Kenntnissen gemacht werde. Solle der Bundesnachrichtendienst zu Eingriffen in das Fernmeldegeheimnis ermächtigt werden, sei der Gesetzgeber verpflichtet, Vorsorge gegen Gefahren zu treffen, die sich aus der Erhebung und Verwertung personenbezogener Daten ergeben. Hierzu verwies das Gericht auf die im Volkszählungsurteil entwickelten Kriterien für Eingriffe in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Diese seien auch auf die speziellere Regelung des Art. 10 GG übertragbar. Speicherung und Verwendung erlangter Daten seien grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt habe. Zweckänderungen seien nur durch Allgemeinbelange gerechtfertigt, die die grundrechtlich geschützten Interessen überwiegen. Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken sei mit diesen Vorgaben unvereinbar.

Mit Beschluss vom 14. Dezember 2000[97] stellt das Gericht fest, dass die Feststellung, Speicherung und künftige Verwendung des „genetischen Fingerabdrucks“ auf der Grundlage von § 81g StPO und § 2 DNA-Identitätsfeststellungsgesetz in das Recht auf informationelle Selbstbestimmung

[92] Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo. Bundesdatenschutzgesetz - Kommentar. 3. Auflage 2010, Einleitung, Rn. 70.
[93] Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035; Wolff, Heinrich A.: Vorratsdatenspeicherung. NVwZ 2010, 751.
[94] BVerfG, Urteil vom 14. Juli 1999 - 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, BVerfGE 100, 313 ff. – Telekommunikationsüberwachung.
[95] Verbrechensbekämpfungsgesetz vom 28. Oktober 1994, BGBl. I, S. 3186.
[96] BVerfG, Beschluss vom 5. Juli 1995 - 1 BvR 2226/94, BVerfGE 93, 181 – Rasterfahndung I.
[97] BVerfG, Beschluss vom 14. Dezember 2000 - 2 BvR 1741/99, 276, 2061/00, BVerfGE 103, 21 - Genetischer Fingerabdruck I.

eingreife, es sich aber um einen rechtlich zulässigen Grundrechtseingriff handele, da u. a. das Gebot der Normenklarheit, das Übermaßverbot und der Richtervorbehalt gewahrt seien.

Im Urteil vom 12. April 2005[98] äußerte sich das BVerfG zu einer weiteren Vorschrift der Strafprozessordnung. Gesetzliche Grundlage für Beweiserhebungen unter Einsatz eines satellitengestützten Ortungssystems (Global-Positioning-System, "GPS") und die Verwertung der Erkenntnisse war im zu Grunde liegenden Sachverhalt § 100c Abs. 1 Nr. 1 Buchst. b Strafprozessordnung (StPO) damaliger Fassung, wonach ohne Wissen des Betroffenen „besondere für Observationszwecke bestimmte technische Mittel" eingesetzt werden konnten. Die Vorschrift sei verfassungsgemäß, da sie hinreichend bestimmt sei und nicht in den unantastbaren Kernbereich privater Lebensgestaltung eingreife. Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels sei der Gesetzgeber aber aufgerufen, die technischen Entwicklungen aufmerksam zu verfolgen und notfalls korrigierend einzugreifen.

Die Durchsuchung und Beschlagnahme des gesamten elektronischen Datenbestands einer gemeinsam betriebenen Rechtsanwaltskanzlei und Steuerberatungsgesellschaft (Beschluss vom 12. April 2005[99]) – im Rahmen eines gegen einen der Berufsträger gerichteten Ermittlungsverfahrens – qualifizierte das BVerfG als erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung. Dem müsse durch strikte Beachtung des Verhältnismäßigkeitsgrundsatzes und bestimmter Verfahrensregelungen Rechnung getragen werden. Zu berücksichtigen sei u. a., dass das Vertrauensverhältnis zwischen Rechtsanwälten und Mandanten rechtlich besonders geschützt und durch die Streubreite der sichergestellten Daten eine Vielzahl gänzlich unbeteiligter Personen von der Beschlagnahme betroffen sei.

Zu den verfassungsrechtlichen Grenzen der Rasterfahndung, bei der den Polizeibehörden von anderen Stellen personenbezogene Daten übermittelt und nachfolgend einem automatisierten Abgleich nach bestimmten Merkmalen unterzogen werden, hat das BVerfG mit Beschluss vom 4. April 2006 entschieden. Eine präventive polizeiliche Rasterfahndung stelle einen Grundrechtseingriff von besonderer Intensität dar und sei daher mit dem Grundrecht auf informationelle Selbstbestimmung nur dann vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben sei[100]. Eine allgemeine Bedrohungslage, wie etwa seit dem 11. September 2001, ohne das Vorliegen weiterer Tatsachen, sei dafür nicht ausreichend.

Mit Beschluss vom 13. Juni 2007[101] erklärte das Gericht Vorschriften zum automatischen Kontenabruf teilweise für verfassungswidrig, da gegen den verfassungsrechtlichen Bestimmtheitsgrundsatz verstoßen werde. Die angegriffenen Regelungen ermächtigten einzelne Behörden zur automatisierten Abfrage von Daten, die von den Kreditinstituten vorgehalten werden müssen. Soweit das Gebot der Normenklarheit nicht eingehalten worden sei, verstoße die Regelung gegen das Recht auf informationelle Selbstbestimmung. Einen solchen Verstoß bejahte das Gericht hinsichtlich § 93 Abs. 8 Abgabenordnung (AO) damaliger Fassung, da der Kreis der zur Kontenabfrage berechtigten Behörden und die dabei verfolgten Zwecke nicht hinreichend festgelegt worden seien.

[98] BVerfG, Urteil vom 12. April 2005 - 2 BvR 581/01, BVerfGE 112, 304 - GPS-Überwachung.
[99] BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02, BVerfGE 113, 29, 46 - Beschlagnahme von Datenträgern.
[100] BVerfGE 93, 181 – Rasterfahndung I.
[101] BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03, NJW 2007, 2464 - Automatisierte Abfrage von Kontostammdaten.

Auch eine Geschwindigkeitsmessung auf der Grundlage einer Verwaltungsvorschrift stellt nach der Rechtsprechung des BVerfG (Beschluss vom 11. August 2009[102]) eine unzulässige Einschränkung des Rechts auf informationelle Selbstbestimmung dar, da eine solche Maßnahme nur auf gesetzlicher Grundlage, die dem Gebot der Normenklarheit und Verhältnismäßigkeit zu entsprechen habe, zulässig sei.

Die Einführung der Vorratsdatenspeicherung durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung“[103] zur Umsetzung der Richtlinie 2006/24/EG in deutsches Recht ist Gegenstand mehrerer Entscheidungen des BVerfG. Nach § 113a TKG waren Telekommunikationsdiensteanbieter verpflichtet, Verkehrsdaten von Telefondiensten (Festnetz, Mobilfunk, Fax, SMS, MMS), E-Mail-Diensten und Internetdiensten vorsorglich anlasslos für die Dauer von sechs Monaten zu speichern. Die zulässigen Zwecke der Datenverwendung waren in § 113b TKG, die Verwendung der Daten für die Strafverfolgung in § 100g StPO geregelt. Nachdem das Gericht mit Beschluss vom 28. Oktober 2008[104] im Wege der einstweiligen Anordnung Teile der Vorratsdatenspeicherung außer Kraft gesetzt hatte, entschied es mit Urteil vom 2. März 2010[105] in der Hauptsache, dass die Regelungen des TKG und der StPO über die Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG unvereinbar und damit nichtig seien. Die Vorratsdatenspeicherung durch private Telekommunikationsunternehmen greife in den Schutzbereich des Fernmeldegeheimnis ein, da diese als „Hilfspersonen“ für die Aufgabenerfüllung staatlicher Behörden in Anspruch genommen würden. Zwar sei eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehle aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Datensicherheit, Begrenzung der Verwendungszwecke, verfassungsrechtliche Transparenz und Rechtschutzanforderungen seien nicht hinreichend gewährleistet.
Für die Frage, zum Schutz welcher Rechtsgüter der Datenabruf als verhältnismäßig anzusehen ist, differenziert das Gericht zwischen der unmittelbaren und mittelbaren Nutzung der Daten. Der Abruf und die unmittelbare Nutzung der Daten seien nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienten. Im Bereich der Strafverfolgung setze dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürften diese Maßnahmen nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden.
Soweit die Behörden in §§ 113b Satz 1 Halbs. 2, 113 TKG zur Identifizierung von IP-Adressen berechtigt wurden, von Diensteanbietern auf der Grundlage gespeicherter Verkehrsdaten die Identität bestimmter, bereits bekannter IP-Adressen zu erfragen, sei diese nur mittelbare Nutzung der Daten auch unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung, Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die Verfolgung von Ordnungswidrigkeiten könnten solche Auskünfte hingegen nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden.

[102] BVerfG, Beschluss vom 11. August 2009 – 2 BvR 941/08, NJW 2009, 3293 - Verkehrsüberwachung.
[103] Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007, BGBl. I, S. 3198.
[104] BVerfG, Beschluss vom 28. Oktober 2008 - 1 BvR 256/08, BVerfGE 122, 120 - Vorratsdatenspeicherung/Datenermittlung.
[105] BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 - Vorratsdatenspeicherung.

1.3.5 Rechtsprechung nationaler Verwaltungs- und Zivilgerichte

Zulässigkeit und Grenzen personenbezogener Bewertungsportale im Internet sind Gegenstand der Entscheidung des Bundesgerichtshofs (BGH) vom 23. Juni 2009[106]. Der BGH lehnte einen Anspruch der klagenden Lehrerin auf Löschung oder Unterlassung der Veröffentlichung ihres Namens, des Namens der Schule, der unterrichteten Fächer sowie einer Bewertung durch die Nutzer ab. Auch Meinungsäußerungen über eine bestimmte oder bestimmbare Person oder diesbezügliche Bewertungen stellten personenbezogene Daten dar. Die Erhebung, Speicherung und Übermittlung solcher Beurteilungen richte sich daher nach dem BDSG. Im konkreten Fall sei die Erhebung und Speicherung der Bewertung trotz fehlender Einwilligung der Lehrerin gemäß § 29 BDSG zulässig. Voraussetzung hierfür ist nach § 29 BDSG, dass „kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss“ der Datenerhebung und -speicherung hat. Bei der Prüfung des „schutzwürdigen Interesses“ hat der BGH eine Abwägung zwischen der Meinungsfreiheit der Nutzer aus Art. 5 Abs. 1 GG und dem Persönlichkeitsrecht der Bewerteten vorgenommen und im Hinblick auf den konkreten Sachverhalt der Meinungsfreiheit den Vorrang eingeräumt.[107]

Mit Urteil vom 9. Dezember 2003[108] hat der BGH zivilrechtliche Ansprüche auf Unterlassung der Veröffentlichung in der Presse von Luftbildaufnahmen, die Privathäuser einer Prominenten zeigten, abgelehnt. Das Fotografieren der Außenansicht eines Grundstücks von einer allgemein zugänglichen Straße aus und die Verbreitung dieser Fotos stelle regelmäßig keine Verletzung des Persönlichkeitsrechts dar. Wenn aber jemand „unter Überwindung bestehender Hindernisse oder mit geeigneten Hilfsmitteln (Teleobjektiv, Leiter, Flugzeug)“ ein privates Anwesen ausspähe, liege grundsätzlich ein Eingriff in die Privatsphäre vor. Im konkreten Fall hat das Gericht dennoch einen Unterlassungsanspruch verneint, da bei Abwägung der betroffenen Grundrechte die Pressefreiheit aus Art. 5 Abs. 1 GG überwiege. Von der Pressefreiheit nicht gedeckt sei aber die Veröffentlichung einer Wegbeschreibung zum Grundstück. Auch die Installation von Überwachungskameras auf einem Privatgrundstück kann das Persönlichkeitsrecht eines vermeintlich überwachten Nachbars beeinträchtigen (BGH-Urteil vom 16. März 2010).[109]

Zur Frage der internationalen Zuständigkeit deutscher Gerichte gemäß § 32 Zivilprozessordnung (ZPO) für Klagen aus unerlaubten Handlungen gegen Veröffentlichungen im Internet hat sich der BGH mit Urteil vom 29. März 2011[110] geäußert. Deutsche Gerichte seien für Verletzungen des Persönlichkeitsrechts durch Veröffentlichungen im Internet dann zuständig, wenn die fraglichen Inhalte „objektiv einen deutlichen Bezug zum Inland (…) aufweisen“. Voraussetzung hierfür sei, dass eine Kollision der widerstreitenden Interessen, d. h. des Persönlichkeitsrechts einerseits und des Interesses an der Gestaltung des eigenen Internetauftritts oder an der Berichterstattung andererseits, nach den Umständen des konkreten Falls, insbesondere auf Grund des konkreten Inhalts der Veröffentlichung, im Inland tatsächlich eingetreten sei oder eintreten könne. Das hat das Gericht im konkreten Fall verneint, da es sich um die Beschreibung eines privaten Treffens in Russland – verfasst auf russisch und in kyrillischer Schrift – handelte. Aus dem deutschen Wohnsitz des Klägers und dem Standort des Servers in Deutschland ergebe sich kein hinreichend deutlicher Inlandsbezug.

[106] BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich.de.
[107] Die gegen das Urteil eingelegte Verfassungsbeschwerde hat das BVerfG mit Beschluss vom 16. August 2010 nicht zur Entscheidung angenommen (Az. 1 BvR 1750/09).
[108] BGH, Urteil vom 9. Dezember 2003 - VI ZR 404/02, NJW 2004, S. 766 – Luftbildaufnahmen.
[109] BGH, Urteil vom 16. März 2010 - VI ZR 176/09, NJW 2010, S. 1533 – Überwachungskamera.
[110] BGH, Urteil vom 29. März 2011 - VI ZR 111/10.

Mit Urteil vom 2. März 2010[111] hat der BGH die Zuständigkeit deutscher Gerichte für eine Klage gegen eine Internetveröffentlichung der „New York Times“ hingegen bejaht. Der deutliche Inlandsbezug ergab sich nach Auffassung des Gerichts aus dem Inhalt des veröffentlichten Artikels (u. a. die Wiedergabe von Berichten deutscher Strafverfolgungsbehörden über das deutsche Unternehmen des Klägers) und der Tatsache, dass die „New York Times“ als international anerkannte Zeitung auch in Deutschland wahrgenommen werde.

In der Rechtsprechung des Bundesarbeitsgerichts (BAG) sind Fragen des Datenschutzes und der Persönlichkeitsrechte u. a. in folgenden Entscheidungen aufgegriffen worden: Arbeitgeber und Betriebsrat seien grundsätzlich befugt, eine Videoüberwachung im Betrieb einzuführen. Die Zulässigkeit des damit verbundenen Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer richte sich nach dem Grundsatz der Verhältnismäßigkeit (Beschluss vom 26. August 2008).[112] Bei Abschluss von Betriebsvereinbarungen sei gemäß § 75 Abs. 2 Satz 1 Betriebsverfassungsgesetz (BetrVG) die freie Entfaltung der Persönlichkeit der beschäftigten Arbeitnehmer zu schützen und hierbei auch der Grundsatz der Verhältnismäßigkeit zu wahren. Mit Beschluss vom 12. August 2008[113] äußerte sich das Gericht zum Leserecht einzelner Mitglieder des Betriebsrates. Das Recht, die elektronisch gespeicherten Unterlagen des Betriebsrats einzusehen, umfasse auch das Leserecht auf elektronischem Weg, und zwar jederzeit, wie dies in § 34 Abs. 3 BetrVG vorgesehen sei. Dem stünden auch die Schweigepflicht der Mitglieder des Betriebsrats und datenschutzrechtliche Vorschriften nicht entgegen.

Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 8. März 2002[114] die Herausgabe von Stasi-Unterlagen mit personenbezogenen Informationen über Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger in Ausübung ihres Amtes nach der damaligen Fassung des Stasi-Unterlagen-Gesetzes für unzulässig erklärt, wenn diese systematisch vom Staatsicherheitsdienst ausgespäht wurden. Im Hinblick auf eine mögliche Änderung des Gesetzes weist das Gericht darauf hin, dass bei der Weitergabe rechtsstaatswidrig erworbener Informationen dem Persönlichkeitsrecht ein höherer Schutz zukomme, als dies bei der sonstigen Veröffentlichung von Informationen über Personen der Zeitgeschichte und Amtsträger in Ausübung ihres Amtes der Fall sei.[115]

Werden personenbezogene Informationen durch eine sachlich unzuständige Behörde weitergegeben, stellt dies einen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung dar. Das BVerwG hat hierzu mit Urteil vom 9. März 2005 entschieden, ein Eingriff in das informationelle Selbstbestimmungsrecht sei grundsätzlich auch dann nicht gerechtfertigt, wenn die Daten

[111] BGH, Urteil vom 2. März 2010 – VI ZR 23/09.
[112] BAG, Beschluss vom 26. August 2008 - 1 ABR 16/07, BAGE 127, 276 - Videoüberwachung im Betrieb. Die Regelung des § 32 BDSG „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ ist erst nach der Entscheidung am 1. September 2009 in Kraft getreten. Die Vorschrift regelt u. a.: „Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.“
[113] BAG, Beschluss vom 12. August 2009 - 7 ABR 15/08, NZA 2009, 1218.
[114] BVerwG, Urteil vom 08. März 2002 - 3 C 46/01, BVerwGE 116, 104 - Herausgabe von Stasi-Unterlagen.
[115] Der Gesetzgeber hat dem Rechnung getragen und § 32 Abs. 1 Stasi-Unterlagen-Gesetz dahingehend geändert, dass Unterlagen mit personenbezogenen Informationen ohne Einwilligung der Betroffenen nur zur Verfügung gestellt werden dürfen, „soweit durch deren Verwendung keine überwiegenden schutzwürdigen Interessen der dort genannten Personen beeinträchtigt werden. Bei der Abwägung ist insbesondere zu berücksichtigen, ob die Informationserhebung erkennbar auf einer Menschenrechtsverletzung beruht.“ , vgl. Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik in der Fassung der Bekanntmachung v. 18.2.1991 (BGBl. I, 162), geändert durch Art. 15 Abs. 64 des Gesetzes v. 5. Februar 2009 (BGBl. I, 160).

zwar von einer anderen Behörde rechtmäßig hätten weitergegeben werden dürfen, im konkreten Fall aber eine sachlich unzuständige Behörde gehandelt habe.[116]

Nach § 7 Bundesnachrichtendienstgesetz (BNDG) in Verbindung mit § 15 Abs. 1 Bundesverfassungsschutzgesetz (BVerfSchG) erteilt der Bundesnachrichtendienst dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten, soweit er ein besonderes Interesse an der Auskunft darlegt. Das BVerwG hat mit Urteil vom 24. März 2010[117] ausgeführt, dass eine Auskunftserteilung unter Berufung auf die in § 15 Abs. 2 BVerfSchG aufgeführten Geheimhaltungsgründe nur dann abgelehnt werden könne, wenn eine Abwägung im Einzelfall ergebe, dass das Auskunftsinteresse zurückstehen müsse. Dagegen erstrecke sich die Auskunftsverpflichtung von vornherein nicht auf die Herkunft der Daten (§ 15 Abs. 3 BVerfSchG).

1.3.6 Verwaltungs- und Anwendungspraxis

Da der Datenschutz in fast allen Bereichen der öffentlichen Verwaltung von Bedeutung ist und hierzu eine Fülle allgemeiner und bereichsspezifischer Regelungen sowohl auf Bundes- wie auf Landesebene existiert, lassen sich allgemeine Feststellungen zur Verwaltungs- und Anwendungspraxis nur schwer treffen, zumal der Schwerpunkt der Datenschutzaufsicht bei den Aufsichtsbehörden der Länder liegt. Insbesondere die staatliche Datenschutzkontrolle der Privatwirtschaft ist Ländersache (§ 38 Abs. 6 BDSG).

Unterschiede in der Verwaltungspraxis, etwa im Bereich von Ermessensentscheidungen, sind daher möglich, was insbesondere für deutschlandweit agierende Unternehmen von Bedeutung sein kann, da diese im Einzelfall der Aufsicht mehrerer Datenschutzbehörden unterliegen. Zwar wird nach langjähriger Praxis die Behörde tätig, in deren Zuständigkeit der Sitz des Unternehmens liegt. Bei Unternehmen mit mehreren selbstständigen Regionalgesellschaften bleibt es dennoch bei der Zuständigkeit mehrerer Aufsichtsbehörden[118].

Die obersten Landesdatenschutzbehörden für die Aufsicht im nicht-öffentlichen Bereich haben deshalb als Koordinierungsgremium den Düsseldorfer Kreis gegründet, dessen Treffen und Beschlüsse eine einheitliche Verwaltungspraxis befördern können. Beschlüsse des Düsseldorfer Kreises, die allerdings nur einstimmig getroffen werden können, betreffen unterschiedliche Bereiche der Aufsicht, im Jahr 2010 etwa die Prüfpflichten des Datenexporteurs im Rahmen des „Safe-Harbor“- Abkommens. [119] Bei einer unterschiedlichen Praxis verbleibt es, wenn eine Einigung im Düsseldorfer Kreis nicht zustande kommt. So wird etwa die Praxis von Auskunfteien, vor der Erteilung von Auskünften zur Identitätsüberprüfung die Zusendung einer Kopie des Personalausweises zu verlangen, von den Aufsichtsbehörden teilweise als unzulässig, teilweise aber auch als erforderlich angesehen. Auch bei der Videoüberwachung auf Bahnhöfen gab es unterschiedliche Bewertungen.

[116] BVerwG, Urteil vom 9. März 2005 - 6 C 3/04, NJW 2005, 2330 - Scientology..
[117] BVerwG, Urteil vom 24. März 2010 - 6 A 2/09, DVBl. 2010, 1307 - Auskunftsanspruch BND.
[118] So wurden 2008 von Datenschutzbehörden aus zwölf Bundesländern Bußgelder gegen 35 Vertriebsgesellschaften des Lebensmitteldiscounters Lidl verhängt, vgl.: http://www.welt.de/wirtschaft/article2428529/Spitzelaffaere-kostet-Lidl-1-5-Millionen-Euro.html (zuletzt aufgerufen am: 17. März 2011).
[119] Vgl. oben unter 1.3, Beschlüsse des Düsseldorfer Kreises unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/index.php (zuletzt aufgerufen am: 17. März 2011).

Enquete-Kommission Internet und digitale Gesellschaft

Deutscher Bundestag

Projektgruppe „Datenschutz, Persönlichkeitsrechte“

Kapitel 2 „Datenschutz“

2.1 Prinzipien, Ziele, Werte **(Stand: 12. April 2011)**

Inhaltsverzeichnis

Kapitel 2 Datenschutz

2.1 Prinzipien, Ziele, Werte

2.1.1 Schutzgegenstand

Datenschutz bildet den zentralen Motor des Vertrauens und der Akzeptanz moderner informationstechnischer Entwicklungen. Ziel des Datenschutzrechts ist der Erhalt und die Stärkung des Persönlichkeitsrechts unter den Bedingungen der Datenverarbeitung und -erhebung, insbesondere in Gestalt des Rechts auf informationelle Selbstbestimmung. Der Erhalt der Kontrolle über den Umgang mit Daten und Informationen, die einen selbst betreffen, ist das zwingende Äquivalent einer auf die Stärkung des Einzelnen wie auch unseres demokratischen Gemeinwesens insgesamt abzielenden gesellschaftlichen Gesamtentwicklung.

Zentraler Anknüpfungspunkt des bestehenden Datenschutzkonzepts sind die so genannten „personenbezogenen Daten“.[1] Im Mittelpunkt der Abwägungen des Datenschutzes aber stehen Informationen, nicht Daten. Es geht regelmäßig um Interessen der Grundrechtsträger, dass staatliche Stellen oder Dritte etwas nicht als Information erfahren und nutzen können, und auf der anderen Seite um deren Wissens- und Verwertungsinteressen.

Personenbezogene Daten werden definiert als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (Art. 2 lit. a DSRL, § 3 Abs. 1 BDSG). Der Begriff wird weit verstanden und umfasst praktisch jede Information, die mit einer natürlichen Person in Verbindung gebracht werden kann. Es genügt also eine „Personenbeziehbarkeit“.[2] Angaben über persönliche Verhältnisse betreffen etwa Identifikationsmerkmale, äußere Merkmale, aber auch innere Zustände (z.B. Meinungen), Angaben über sachliche Verhältnisse dagegen alle Beziehungen des Betroffenen zu Dritten und zur Umwelt (z.B. Eigentumsverhältnisse, Vertragsbeziehungen).[3]

Auch das BVerfG geht in seiner ständigen Rechtsprechung von einem weiten Verständnis aus. So hat das Gericht in seinem wegweisenden Volkszählungsurteil zu den Angaben personenbezogener Daten ausgeführt: „Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck,

[1] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 100.
[2] Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 40.
[3] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 101.

dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr.“[4]

Weiterer regulatorischer Anknüpfungspunkt ist der Umgang mit diesen Daten. Dabei werden in der DSRL und im BDSG unterschiedliche Begrifflichkeiten verwendet. Während in der DSRL die „Verarbeitung“ (im weiteren Sinne) der Daten als Oberbegriff für jeden Vorgang im Zusammenhang mit den personenbezogenen Daten zu verstehen ist (Art. 2 lit. b DSRL), unterscheidet das BDSG zwischen den einzelnen Vorgängen der Erhebung, Verarbeitung (im engeren Sinne) und (sonstigen) Nutzung der Daten (§ 4 Abs. 1 BDSG). Materiell erfasst sind vor allem die Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung und Löschung von personenbezogenen Daten. Dabei ist ein technikneutrales Verständnis zu Grunde zu legen. Erfasst sind sowohl automatische als auch nicht-automatische Verfahren.[5]

Für einen kleinen Ausschnitt der personenbezogenen Daten gilt, in Anpassung an die Vorgaben der DSRL, ein erhöhtes Schutzniveau: Hierzu gehören die so genannten sensiblen Daten wie rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit und Daten über die Gesundheit und die Sexualität (vgl. Art. 8 DSRL, § 3 Abs. 9 BDSG).

In der digitalen Welt wirft das Kriterium des Personenbezugs allerdings zunehmend Probleme auf. Durch die Möglichkeit, Daten aller Art in einem bislang nicht dagewesenen Ausmaß miteinander zu verknüpfen, kann quasi jedes Datum zu einem personenbezogenen werden.

Persönlichkeitsrechtlich problematisch erscheint zunehmend weniger der Personenbezug an sich als vielmehr die Möglichkeit, jederzeit unterschiedlichste Daten aller Art mit einzelnen Personen zu verknüpfen und in unterschiedlicher Weise auszuwerten. Geodaten, die an sich keine personenbezogenen Daten sind, jedoch schon immer personenbeziehbar waren, werden offensichtlich von vielen Menschen als problematisch im persönlichkeitsrechtlichen Sinne empfunden, wenn bestimmte technische Möglichkeiten der Verknüpfung und gezielten Recherche bestehen. Angesichts solcher Entwicklungen greift die Frage, ob Geodaten personenbezogene oder auch nur personenbeziehbare Daten sind, zu kurz.

[4] BVerfGE 65, 1, 45 - Volkszählung.
[5] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 49.

2.1.2 Grundprinzipien des Datenschutzrechts

Erlaubnisvorbehalt

Ein zentraler Grundsatz des Datenschutzrechts lässt sich in einem Satz wie folgt formulieren: Der Umgang mit personenbezogenen Daten ist verboten, es sei denn, der Betroffene willigt ein oder eine Rechtsnorm legitimiert ihn. Dieser Grundsatz ist sowohl im Gemeinschaftsrecht (Art. 7 DSRL), als auch im nationalen allgemeinen (§ 4 Abs. 1 BDSG) und bereichsspezifischen Datenschutzrecht (z. B. § 12 TMG) normiert. Demnach bestimmt sich die Zulässigkeit eines jeden einzelnen Datenverarbeitungsvorgangs danach, ob der Betroffene den Vorgang erlaubt hat oder ob er sich auf einen gesetzlichen Erlaubnistatbestand stützen lässt.[6]
Die Einwilligung ist vor allem im nicht-öffentlichen Bereich, neben den vertraglichen Legitimationen, von erheblicher Bedeutung.[7] Sie legitimiert einen Datenverarbeitungsvorgang nur dann, wenn sie wirksam erteilt wurde, wofür das Gesetz bestimmte Mindestanforderungen vorsieht (vgl. § 4a BDSG oder auch Art. 7 lit. a) DSRL). Nach nationalem Recht (§ 4a BDSG) ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, also ohne Zwang erfolgt. Dies setzt voraus, dass der Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann.

Die Einwilligung in die Datenerhebung oder –verarbeitung ist daher nur dann zulässig, wenn die betreffende Person „ohne jeden Zweifel ihre Einwilligung gegeben“[8] hat. Dies impliziert, dass die Einwilligung informiert, aktiv und freiwillig zu geschehen hat. Eine informierte Einwilligung setzt Transparenz und Kenntnis voraus. Allein durch die Nutzung einer Website kann keine aktive Einwilligung erteilt werden. Auch das Beibehalten von Einstellungen von Internetdiensten oder Browsern, die in der Voreinstellung nicht „privacy by default“ vorsehen, genügt nicht der Fiktion einer aktiven Einwilligung. Hier wird die Kenntnis der möglichen Einstellungen und ihrer Veränderungsmöglichkeiten vorausgesetzt, die jedoch weder bei jedem Nutzer gleichermaßen gegeben noch von allen Diensteanbietern gefördert wird.

An der Möglichkeit zu einer freien Entscheidung kann es jedoch fehlen, wenn die Einwilligung in einer Situation wirtschaftlicher oder sozialer Schwäche oder

[6] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 130 f.
[7] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 131.
[8] Vgl. Art. 7 lit. a) DSRL.

Unterordnung erteilt wird oder wenn der Betroffene durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wird.

Es gibt Situationen, in denen sich die Vertragspartner unterschiedlich stark gegenüberstehen. Für diese Fälle wird diskutiert, inwieweit eine freiwillige Einwilligung in die Datenerhebung vorliegt, insbesondere wenn Daten erhoben werden, die für die Erbringung der Dienstleistung selbst nicht benötigt werden. Für die Freiwilligkeit kann aber auch von Bedeutung sein, ob ein anderes Angebot in zumutbarer Weise zur Verfügung steht.

Außerdem muss der Betroffene nach § 4a BDSG auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen werden. Wenn die Situation es erfordert oder der Betroffene es verlangt, muss er auch darüber informiert werden, welche Folgen eine Verweigerung der Einwilligung nach sich zieht. Das geltende Recht lässt für das Internet die Möglichkeit einer elektronischen Einwilligung zu (§ 13 Abs. 2 TMG), die z. B. durch Ankreuzen einer Checkbox erteilt werden kann.

Nach datenschutzrechtlichen Grundsätzen ist eine Einwilligung also nur dann wirksam, wenn sie in Kenntnis der entscheidungsrelevanten Umstände erteilt wird. Der Betroffene muss auf der Grundlage der ihm vorliegenden Informationen Bedeutung und Tragweite seiner Entscheidung zur Datenfreigabe erkennen können. Im Hinblick auf die spezifischen Bedingungen im digitalen Bereich ergeben sich hier neue Herausforderungen.

Die Frage von Transparenz- und Informationspflichten stellt sich in besonderem Maße. Auch Art und Weise der Informationspraxis sind bestimmend dafür, in welchem Umfang Bürgerinnen und Bürger bei Erteilung ihrer Einwilligung einschätzen können, welche Daten zu welchem Zweck gespeichert werden sollen.

Die Einwilligung kann bislang in unterschiedlicher Form eingeholt werden („opt-in“ und „opt-out“ sowie unterschiedliche Formulierungen). Dies erfordert eine besondere Aufmerksamkeit und ein erhöhtes Textverständnis der in der Regel in juristischer Sprache formulierten Textpassagen. Eine informierte Einwilligung auf Grund dieser, der Absicherung eines Unternehmens dienenden Texte, ist auf Grund der Art des Textes und der gegebenen Informationen daher für viele Menschen nur schwer möglich. Gerade in der digitalen Welt gäbe es aber auch alternative Formen, Informationen verständlich bereitzustellen.

Einwilligungen werden unbefristet erteilt. Eine echte Transparenz und ein Überblick über die erteilten Einwilligungen ist für die Nutzer angesichts der Vielzahl der eingeforderten Einwilligungen nur schwer zu behalten. Der Betreiber des Dienstes unterscheidet sich oftmals von der datenverarbeitenden Stelle, eine Transparenz darüber, welche Dienste bzw. Unternehmen welche Daten erhalten, ist oftmals nicht vorhanden. In einer solchen Situation können die Arbeitnehmer/Bürger/Nutzer ihre Informations-, Widerrufs-, Korrektur- und Löschrechte nur unzureichend geltend machen. Eine autonome Entscheidung über die Preisgabe eigener Daten im Internet können Menschen dann fällen, wenn sie Vor- und Nachteile ihrer Einwilligung einschätzen und Handlungsalternativen erkennen können. Die Medienkompetenz des Einzelnen trägt wesentlich dazu bei, informierte Einwilligungen zu ermöglichen und zu befördern. Diese kann aber nicht in gleicher Ausprägung von allen Personen erwartet werden und kann nicht als Ersatz für bedürfnisgerechtere Anforderungen an Transparenz, Information und Einwilligung stehen.

Im öffentlichen Bereich erfolgt die Datenverarbeitung personenbezogener Daten dagegen fast ausschließlich auf der Grundlage gesetzlicher Erlaubnistatbestände, die den verfassungsrechtlichen Anforderungen genügen müssen.

Die erfolgreichen Verfassungsbeschwerden der letzten Jahre zeigen allerdings, dass die verfassungsrechtlichen Vorgaben bei der Gesetzgebung teilweise nicht eingehalten wurden.

Erforderlichkeitsgrundsatz

Der Erforderlichkeitsgrundsatz folgt aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz und ist zudem in Art. 7 lit. b) bis f) DSRL festgeschrieben. Er steht in engem Zusammenhang mit dem Grundsatz der Zweckfestlegung und der Zweckbindung. Demnach ist der Umgang mit personenbezogenen Daten auf das zum Erreichen des angestrebten Zieles erforderliche Minimum zu beschränken.[9] Es sollen nur so viele Daten erhoben, verarbeitet oder genutzt werden, wie zur Zweckerreichung unbedingt notwendig. Für den öffentlichen Bereich ist der Grundsatz in §§ 13 bis 16 BDSG (insbesondere in den Abs. 1) normiert, wobei der zulässige Zweck auf die öffentliche Aufgabenerfüllung begrenzt ist. Der Erforderlichkeitsgrundsatz gilt aber auch im

[9] BVerfGE 65, 1, 46 - Volkszählung.

nicht-öffentlichen Bereich, wo seine effektive Verwirklichung durch eine möglichst genaue Zweckbestimmung bedingt ist.[10]

Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz besagt, dass die Daten, die für einen bestimmten Zweck erhoben worden sind, auch nur zu diesem Zweck verarbeitet oder genutzt werden dürfen.[11] Der Zweck der Datenerhebung begrenzt folglich den weiteren Umgang mit den erhobenen Daten. Sie dürfen nur zu dem Zweck weiter verwendet werden, der von der Einwilligung oder der konkret legitimierenden Rechtsnorm erfasst ist. Das setzt voraus, dass das Ziel der Datenverarbeitung und/oder -nutzung bereits vor der Datenerhebung so genau wie möglich bestimmt ist. Eine Speicherung auf Vorrat für künftige, noch nicht bekannte Zwecke ist dagegen grundsätzlich unzulässig.[12]

Vor allem im nicht-öffentlichen Bereich stößt die Beibehaltung dieses Grundsatzes auf praktische Probleme. In einer vernetzten Welt ist der Datenaustausch oftmals durch Spontanität und gerade nicht durch eine vorherige Festlegung des Verarbeitungszweckes bestimmt.[13]

Transparenzgrundsatz

Die informationelle Selbstbestimmung setzt nach Auffassung des Bundesverfassungsgerichts voraus, dass Bürger wissen und grundsätzlich auch entscheiden können sollen, „wer was wann und bei welcher Gelegenheit“ über sie weiß.[14] Das setzt wiederum voraus, dass Datenerhebungs-, -verarbeitungs- und -nutzungsvorgänge transparent gestaltet werden. Zudem ist der Transparenzgrundsatz die grundlegende Voraussetzung dafür, dass Betroffene aktive Datenschutzrechte wahrnehmen können. Transparenz wird in erster Linie durch den Grundsatz der Direkterhebung verwirklicht, wonach die Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4 Abs. 2 S. 1, Abs. 3 BDSG), sodass er unmittelbar Kenntnis von dem Vorgang erlangt. Nur unter engen Voraussetzungen darf die Datenerhebung ohne Mitwirkung des Betroffenen erfolgen (§ 4 Abs. 2 S. 2 BDSG). Flankiert wird

[10] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 136.
[11] Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 48.
[12] Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 48.
[13] Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung. Verw 2007, 153 (159).
[14] BVerfGE 65, 1, 43 - Volkszählung.

das Transparenzgebot durch Auskunftsrechte und Informations-, Benachrichtigungs-, Unterrichtungs-, Hinweis- und Aufklärungspflichten der verantwortlichen Stelle.[15]

Gerade im nicht-öffentlichen Bereich wissen oftmals viele Bürgerinnen und Bürger nicht, wer eigentliche welche ihrer Daten zu welchen Zwecken speichert und verwendet.

Prinzip der Datenvermeidung und Datensparsamkeit

Der Grundsatz der Datenvermeidung und Datensparsamkeit ist – obwohl nicht durch die DSRL vorgegeben – in § 3a BDSG normiert und besagt, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen und auch die Datenverarbeitungssysteme an diesem Ziel auszurichten sind. Dabei handelt es sich um eine Konkretisierung des Erforderlichkeitsgrundsatzes auf technischer Ebene: Schon durch die entsprechende Technikgestaltung soll das Recht auf informationelle Selbstbestimmung präventiv geschützt werden.[16] Da der Grundsatz nicht sanktionsbewehrt ist, ist er – obwohl als Rechtspflicht formuliert – eher als Programmsatz zu verstehen.[17]

2.1.3 Datenschutz im Grundgesetz

Verfassungsrechtliche Verortung

Der Grundrechtekatalog des Grundgesetzes enthält im Gegensatz zur Grundrechtecharta der Europäischen Union (GRC) kein explizites Grundrecht des Datenschutzes.[18] Gleichwohl ist der Datenschutz ein Wert von Verfassungsrang und nimmt über verschiedene Grundrechte am Grundrechtsschutz teil. Namentlich finden sich datenschutzrechtliche Gehalte im Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG), im Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG) und im Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG). Als vorläufiger Höhepunkt in der Judikatur des verfassungsrechtlichen Datenschutzes wird das „IT-Grundrecht“ auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme angesehen.[19]

[15] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 136.
[16] Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 3a Rn. 1.
[17] Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 3a Rn. 2.
[18] Vgl. zur Forderung eines Grundrechtes auf Datenschutz Kloepfer, Michael/Schärdel, Florian: Grundrechte für die Informationsgesellschaft - Datenschutz und Informationszugangsfreiheit ins Grundgesetz? JZ 2009, 453 ff., sowie unter 2.2.2.
[19] Vgl. Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1036).

IT-Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Als besondere Ausprägung des allgemeinen Persönlichkeitsrechts hat das Bundesverfassungsgericht im Hinblick auf Online-Durchsuchungen das sog. IT- bzw. Computergrundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt.[20] Es „schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist.“[21] Der Schutz des Art. 10 Abs. 1 Var. 3 GG versagt, wenn der Kommunikationsvorgang beendet ist oder der Zugriff außerhalb eines laufenden Kommunikationsvorgangs des Betroffenen erfolgt, was bei der Infiltration eines Computers regelmäßig der Fall ist.[22] Art. 13 GG bietet raumbezogenen Schutz, welcher „nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren“, da der Eingriff standortunabhängig über das Internet erfolgen kann.[23] Das Recht auf informationelle Selbstbestimmung trägt „den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“[24]

Erfasst sind Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“, wie z. B. bei Personalcomputern oder Mobiltelefonen und elektronischen Terminkalendern, die

[20] BVerfGE 120, 274, 302 ff. – Onlinedurchsuchung.
[21] BVerfGE 120, 274, 302 – Onlinedurchsuchung.
[22] BVerfGE 120, 274, 307 f. – Onlinedurchsuchung.
[23] BVerfGE 120, 274, 310 – Onlinedurchsuchung.
[24] BVerfGE 120, 274, 312 f. – Onlinedurchsuchung.

über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.[25] Geschützt wird nicht nur vor einer Verletzung der Vertraulichkeit dieser Daten, sondern bereits vor dem Antasten der Integrität des Systems, da hierdurch „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen“ ist.[26]

Dabei betont das Bundesverfassungsgericht, dass „der Standort des Systems … ohne Belang und oftmals für die Behörde nicht einmal erkennbar“ sei, was „insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone“ gelte.[27] Daraus lässt sich schließen, dass der Schutz unabhängig davon zu gewährleisten ist, wo der Datenbestand gespeichert ist.

Die Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung erfolgt in erster Linie nach quantitativen Gesichtspunkten. Während das Grundrecht auf informationelle Selbstbestimmung Schutz vor Zugriff auf einzelne personenbezogene Daten gewährt, geht es beim (IT-)Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme um den Schutz einer Vielzahl von (personenbezogenen) Daten (Datenbestand), die auf einem informationstechnischen System gespeichert sind. Denn wenn lediglich Daten mit einem punktuellen Bezug zu einem bestimmten Lebensbereich abgerufen werden, unterscheidet sich der staatliche Zugriff auf informationstechnische Systeme nicht von anderen Datenerhebungen und das Recht auf informationelle Selbstbestimmung ist anzuwenden.[28] Abgrenzungskriterium sind demnach Umfang und Vielfalt der Daten und das Ausmaß der durch die Daten zu gewinnenden Rückschlüsse auf die Person des Betroffenen. Ermöglicht die Datenerhebung potentiell eine umfassende Erkenntnisgewinnung über den Betroffenen, so ist das (IT-)Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschlägig.[29]

2.1.4 Das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts

Das allgemeine Persönlichkeitsrecht wird aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet. Es enthält mehrere Elemente und dient einerseits dem Schutz eines sozialen und räumlichen Rückzugsbereichs des Einzelnen und andererseits dem

[25] BVerfGE 120, 274, 314 – Onlinedurchsuchung.
[26] BVerfGE 120, 274, 314 – Onlinedurchsuchung.
[27] BVerfGE 120, 274, 310 f. – Onlinedurchsuchung.
[28] BVerfGE 120, 274, 313 – Onlinedurchsuchung.
[29] Hinz, Christian: Onlinedurchsuchungen. JURA 2009, 141 (144).

Schutz der individuellen Freiheit, selbst über die Präsentation der eigenen Person bestimmen zu können.[30]

Zur zweiten Gruppe gehören das Recht am eigenen Bild und am eigenen Wort und das seit dem Volkszählungsurteil aus dem Jahr 1983[31] verfassungsgerichtlich anerkannte Recht auf informationelle Selbstbestimmung. „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[32]

Informationelle Selbstbestimmung und Internet

Das Internet gibt den Menschen die Chance, selbstbestimmt und selbstbewusst ihr Leben zu gestalten. Innovative Nutzungsmöglichkeiten prägen den heutigen Alltag und stellen sich oft als Bereicherung oder praktische Hilfe dar. Die Möglichkeiten zur Information, Kommunikation und Interaktion werden erweitert.

Viele dieser Chancen und Möglichkeiten gehen einher mit der Speicherung, Verarbeitung und Übermittlung zahlreicher Daten. Voraussetzung für viele Informations- und Kommunikationsdienste sind personenbezogene Daten. Diese Dienste sind aber auch missbrauchsanfällig, sei es, dass mehr Daten als erforderlich gespeichert werden, sei es, dass Nichtberechtigte Zugang zu sensiblen Daten erlangen. Der Umgang mit personenbezogenen Daten hat sich im digitalen Zeitalter erheblich verändert. Im Kontext des Internet ist die Verarbeitung von personenbezogenen Daten vielfach ein wirtschaftliches Geschäftsmodell. Insbesondere in sozialen Netzwerken, aber auch bei anderen Diensten im Internet, werden eine Vielzahl von Daten von Nutzerinnen und Nutzern selbst zur Verfügung gestellt.

Durch die zunehmende Vernetzung, die Möglichkeit der Verknüpfung von personenbezogenen Daten (Persönlichkeitsprofile) und die ständige Weiterentwicklung automatischer Datenerfassungssysteme potenziert sich die Gefahr für das allgemeine Persönlichkeitsrecht in einer „Welt der allgegenwärtigen Datenverarbeitung“[33]. Diese Gefahr besteht nicht nur im Verhältnis Bürger - Staat, sondern auch im Verhältnis Bürger - Bürger und Verbraucher - Unternehmen untereinander. Dies zeigt sich besonders deutlich bei den Diensteanbietern im Internet. Der Erfolg von Google oder sozialen Netzwerken wie Facebook und

[30] Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1037).
[31] BVerfGE 65, 1 - Volkszählung.
[32] BVerfGE 65, 1, 43 - Volkszählung.
[33] Zum diesem Begriff: Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung. Verw 2007, 153 (155 ff.).

studiVZ oder Internetprovidern ist geradezu dadurch bedingt, dass diese gigantische informationelle Infrastrukturen bereithalten.[34] Hier sind die Grundrechte zwar nicht (unmittelbar) anwendbar. Der Staat ist aber verpflichtet, „dem Einzelnen Schutz davor zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf die seine Individualität kennzeichnenden Daten nehmen“[35] (grundrechtliche Schutzpflicht). Schließlich hat die Verbreitung und Verarbeitung der eigenen personenbezogenen Daten im Internet mittlerweile die Grenzen der Nachvollziehbarkeit für den Einzelnen erreicht.

Der gegenwärtig diskutierte Datenschutz in sozialen Netzwerken wirft aber auch weitere Fragen auf. Diese betreffen insbesondere das Verhältnis der Nutzerinnen und Nutzer zu den Anbietern entsprechender Plattformen, beispielsweise wenn im Hintergrund personenbezogene Daten gesammelt und in Profilen zusammengeführt werden. Auch in diesem Fall muss der Schutz auf informationelle Selbstbestimmung erhalten bleiben. Schließlich setzt die freie Entfaltung der Persönlichkeit auch voraus, dass der Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten geschützt wird.[36] Durch diese Schutzwirkung wird der abschreckende Effekt fremden (staatlichen und in Unternehmen vorhandenen) Geheimwissens gehemmt, „der entstehen und zur Beeinträchtigung bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß.“[37] Mit anderen Worten: Wer befürchten muss, dass seine „Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[38]

Mittlerweile hat sich daher ein kontextbezogener und gesetzlich zu gewährender Schutzrahmen mit unterschiedlichen Komponenten auf verschiedenen Ebenen herausgebildet. Dies reicht von gesetzlichen Regelungen im BDSG (wie beispielsweise dem bußgeldbewährten Kopplungsverbot des § 28 Abs. 3b BDSG), über die Auferlegung entsprechender Transparenz- und Informationspflichten für Betreiber von Diensten im Internet, bis hin zu einer Förderung der Medienkompetenz

[34] Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1039).
[35] BVerfG, Urteil vom 13. Februar 2007 - 1 BvR 421/05, BVerfGE 117, 202, 229 - Vaterschaftsfeststellung.
[36] BVerfGE 65, 1, 43 - Volkszählung.
[37] BVerfGE 113, 29, 46 - Beschlagnahme von Datenträgern.
[38] BVerfGE 65, 1, 43 - Volkszählung.

der Nutzerinnen und Nutzer für einen verantwortungsvollen Umgang mit den eigenen personenbezogenen Daten.

2.1.5 Einschränkungen von Grundrechten / Kollidierende Rechtsgüter

Gerade im Bereich des Internet sind zum Teil schwierige Grundrechtskollisionen vorgezeichnet, wie z.B. die so genannte Spickmich-Entscheidung des BGH zeigt.[39] Pauschale Gegenüberstellungen etwa mit dem Eigentumsgrundrecht oder der Berufsausübungsfreiheit aber verbieten sich, da oft genug gefragt werden muss, ob bestimmte Grundrechtsausübungen zugleich den Schutz des Umgangs mit den Daten von dritten Grundrechtsträgern umfassen. Hier ist eine besonders differenzierte Darstellung zu empfehlen.

Jedermann hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Dieses „Recht auf informationelle Selbstbestimmung“, wie es das Bundesverfassungsgericht 1983 in seiner Entscheidung zur Volkszählung, also im Hinblick auf eine staatliche Maßnahme, beschrieben hat, ist einerseits - als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG – ein individuelles Abwehrrecht gegenüber staatlichen Eingriffen.

Nach der Rechtsprechung des Bundesverfassungsgerichts wirkt sich das Recht auf informationelle Selbstbestimmung aber darüberhinaus im Sinne einer Drittwirkung auch auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus und begründet staatliche Schutzpflichten. Die staatliche Gewalt ist danach verpflichtet, dem Einzelnen seine informationelle Selbstbestimmung im Verhältnis zu Dritten zu ermöglichen.[40] Gegebenenfalls müssen staatlicherseits die rechtlichen Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen kann.[41]

Nicht jede Beeinträchtigung eines grundrechtlichen Schutzbereichs führt per se zur Verfassungswidrigkeit der Maßnahme. Zum einen kann der Betroffene in die Maßnahme einwilligen und seine Daten freiwillig preisgeben, was vom Staat zu

[39] BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328; vgl. auch unter 1.3.5.
[40] BVerfG, Beschluss vom 23.Oktober 2006 – BvR 2027/02, Rn 30.
[41] BVerfG, Beschluss vom 23.Oktober 2006 – BvR 2027/02, Rn. 33.

respektieren ist.[42] Aber auch ohne Einwilligung wird der verfassungsrechtliche Datenschutz nicht grenzenlos gewährleistet, sondern kann beschränkt werden. Das Bundesverfassungsgericht hat hierzu bereits 1983 im so genannten Volkszählungsurteil dargelegt: "Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig."

Für diese Schrankenziehung hat das Bundesverfassungsgericht seit dem Volkszählungsurteil eine Reihe von Vorgaben aufgestellt, die es zu beachten gilt. Dabei gelten für die genannten Grundrechte weitgehend die gleichen Maßstäbe.[43]

Grundlegende Voraussetzung für einen zulässigen Eingriff in das Recht auf informationelle Selbstbestimmung ist das Vorhandensein einer gesetzlichen Grundlage, welche die Voraussetzungen und den Umfang der Beschränkungen klar erkennen lässt.[44] Das Erfordernis einer gesetzlichen Grundlage (Gesetzesvorbehalt) folgt bereits aus Art. 2 Abs. 1 GG, wonach das allgemeine Persönlichkeitsrecht nur innerhalb der verfassungsmäßigen Ordnung gewährleistet wird. Die gesetzliche Grundlage muss dem Gebot der Normenklarheit entsprechen, was bedeutet, dass Anlass, Zweck und Grenzen eines Eingriffs in der Ermächtigung bereichsspezifisch, präzise und für den Bürger klar erkennbar festgelegt werden müssen.[45]

Weiterhin muss der Verhältnismäßigkeitsgrundsatz beachtet werden. Das bedeutet, dass die Maßnahme einen legitimen Zweck verfolgen, zu dessen Erreichung geeignet, erforderlich und verhältnismäßig sein muss.[46] Der Zweck muss von vornherein bestimmt sein. Die ständige Rechtsprechung des Bundesverfassungsgerichts bringt deutlich zum Ausdruck, „dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist.“[47]

[42] Vgl. BVerfG, Beschluss vom 23.Oktober 2006 – BvR 2027/02, Rn. 34; Schoch, Friedrich: Das Recht auf informationelle Selbstbestimmung. JURA 2008, 352 (357).
[43] Vgl. BVerfGE, Beschluss vom 4. April 2006 - 1 BvR 518/0, BVerfGE 115, 320, 347 – Rasterfahndung II; Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1037 f.).
[44] BVerfGE 65, 1, 44 - Volkszählung.
[45] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 79 m.w.N. aus der Rechtsprechung des BVerfG.
[46] BVerfGE 115, 320, 345 ff. – Rasterfahndung II.
[47] BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08, NJW 2010, 833 (839 Rn. 213) - Vorratsdatenspeicherung.

Es besteht demnach ein "Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten". Das Grundrecht auf informationelle Selbstbestimmung wird als besondere Ausprägung des schon zuvor grundrechtlich geschützten allgemeinen Persönlichkeitsrechts angesehen. Wie dieses wird es verfassungsrechtlich aus Art. 2 Abs. 1 (so genannte allgemeine Handlungsfreiheit) in Verbindung mit Art. 1 Abs. 1 GG (Menschenwürde-Garantie) hergeleitet.

In der Verhältnismäßigkeitsprüfung findet eine Güterabwägung zwischen dem verfolgten Zweck und dem Recht auf informationelle Selbstbestimmung statt. Dabei ist von der Prämisse auszugehen, dass Grundrechte „jeweils nur soweit beschränkt werden dürfen, als es zum Schutze öffentlicher Interessen unerlässlich ist.“[48] In der Abwägung ist vor allem das Gewicht der Grundrechtsbeeinträchtigung zu beachten. Bei der Beurteilung der Schwere des Eingriffs sind z. B. die folgenden Kriterien zu berücksichtigen:

- in welche Sphäre die Maßnahme eingreift (Sozial-, Privat- oder Intimsphäre);[49] die unterschiedliche Schutzintensität der drei Sphären kann aber nicht im Sinne eines starren Schemas verstanden werden, sondern nur als erster Orientierungspunkt für die Intensität der Grundrechtsbeeinträchtigung und für die Gewichtung der diese Beeinträchtigung rechtfertigenden Gründe;
- wie viele Grundrechtsträger betroffen sind;[50]
- wie intensiv die Beeinträchtigungen sind;[51]
- welche Inhalte von dem Eingriff erfasst werden, insbesondere welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen;[52]
- ob besondere Vertraulichkeitserwartungen verletzt werden;[53]
- auf welchem Weg die Inhalte erlangt werden;[54]
- welche weiteren Folgen oder Nachteile die Datenerhebung nach sich ziehen kann, z. B.

[48] BVerfGE 65, 1, 44 - Volkszählung.
[49] In die Intimsphäre darf gar nicht eingegriffen werden, in die Privat- oder Geheimnissphäre nur unter besonders strenger Wahrung des Verhältnismäßigkeitsgrundsatzes und in die Sozialsphäre bereits nach den Kriterien, die für einen Eingriff in die allgemeine Handlungsfreiheit gelten. Vgl. Murswiek, Dietrich, in: Sachs, Michael (Hrsg.). Grundgesetz : Kommentar. 5. Auflage 2009, Art. 2 Rn. 104 m.w.N.
[50] BVerfGE 115, 320, 347 – Rasterfahndung II.
[51] BVerfGE 115, 320, 347 – Rasterfahndung II.
[52] BVerfGE 115, 320, 348 – Rasterfahndung II.
[53] BVerfGE 115, 320, 348 – Rasterfahndung II.
[54] BVerfGE 115, 320, 348 – Rasterfahndung II.

- das Risiko, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden,
- eine stigmatisierende Wirkung;[55]

- die Heimlichkeit einer staatlichen Maßnahme, welche z.B. die Möglichkeit der Inanspruchnahme von Rechtsschutz im Vergleich zur offenen Datenerhebung wesentlich erschwert;[56]
- der Verdachtsgrad;
- über welchen Zeitraum die Daten erhoben, verarbeitet und genutzt werden können;
- und die Streubreite einer Maßnahme.

Zum zuletzt genannten Punkt hat das Bundesverfassungsgericht ausgeführt: „Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – weisen grundsätzlich eine hohe Eingriffsintensität auf. (...) Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. (…) Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen (…) .“[57]

Das Bundesverfassungsgericht hat eine anlasslose Speicherung von Telekommunikationsverkehrsdaten zwar nicht schlechthin als verfassungswidrig angesehen, aber betont, dass es sich um einen besonders schweren Eingriff handele, der höchsten verfassungsrechtlichen Anforderungen bei der Ausgestaltung der Regelungen unterliegt.

[55] BVerfGE 115, 320, 351 ff. – Rasterfahndung II.
[56] Vgl. z.B. BVerfGE 120, 274, 325 – Onlinedurchsuchung; BVerfG, Beschluss vom 16. Juni 2009 - 2 BvR 902/06, BVerfGE 124, 43, 62 f. und 65 f. – Beschlagnahme von E-Mails.
[57] BVerfGE 115, 320, 354 f. – Rasterfahndung II.

Je schwerer die Grundrechtsbeeinträchtigung wiegt, desto höher muss das staatliche Schutzgut wiegen, um den Eingriff rechtfertigen zu können. In die Waagschale gelegt werden können hier z. B.:

- die Sicherheit des Staates als verfasste Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit;[58]
- die Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen Grundordnung;[59]
- die Sicherung der Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen;[60]
- die Verhütung und Verfolgung von Straftaten von erheblicher Bedeutung[61] bzw. schwerwiegender Straftaten.[62]

Eine absolute Grenze der Zulässigkeit einer Datenerhebung bildet die Schranken-Schranke des unantastbaren Kernbereichs privater Lebensgestaltung, insbesondere im Bereich der Intimsphäre. Staatliche Stellen „haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt. (…) Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen. (…) Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.“[63] Deshalb hat das Bundesverfassungsgericht als Voraussetzung für einen Zugriff auf einen Bereich, in dem solche Kernbereichsdaten (z. B. tagebuchartige Aufzeichnungen, private Film- oder Tondokumente, höchstpersönliche Telefonate oder E-Mails) zu vermuten sind, das Erfordernis besonderer gesetzlicher Vorkehrungen aufgestellt, um den Kernbereich der privaten Lebensgestaltung zu schützen.[64] So lässt sich die (beiläufige) Erfassung solcher Daten nicht immer verhindern. Jedoch sind entsprechende Maßnahmen abzubrechen,

[58] BVerfGE 120, 274, 319 und 328 – Onlinedurchsuchung.
[59] BVerfGE 115, 320, 358 – Rasterfahndung II.
[60] BVerfGE 120, 274, 328 – Onlinedurchsuchung.
[61] BVerfGE 113, 348, 385 – Vorbeugende Telekommunikationsüberwachung.
[62] BVerfG, NJW 2010, 833, 848 Rn. 279 - Vorratsdatenspeicherung.
[63] BVerfGE 120, 274, 335 – Onlinedurchsuchung.
[64] BVerfGE 120, 274, 336 ff. – Onlinedurchsuchung.

sobald erkannt wird, dass sie in den Kernbereich vordringen, oder zumindest im Nachhinein umgehend zu löschen.[65]

Aber auch unabhängig von diesem Kernbereich hat der Gesetzgeber „organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“[66] Dazu gehört auch die Sicherheit der Daten. So hat das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung vor allem die „gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit“ eingefordert.[67]

Im Falle des heimlichen Zugriffes auf die Datenverarbeitungsanlagen von Privatpersonen durch Sicherheitsbehörden (so genannte Online-Durchsuchung) bestehen besonders hohe Hürden für den Gesetzgeber, die sich vorrangig aus dem neugeschaffenen Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ableiten. Sie sind nur zulässig, wenn Gefahren für überragend wichtige Rechtsgüter bestehen, die sich in Gestalt von tatsächlichen Anhaltspunkten einer konkreten Gefahr manifestieren. Neben dem grundsätzlich geltenden Vorbehalt richterlicher Anordnung müssen u.a. auch Vorkehrungen getroffen werden, die den Kernbereich privater Lebensgestaltung schützen.

2.1.6 Anonymität und Identitätsmanagement im Internet

Schwierige rechtliche Fragen wirft das zunehmend auch und gerade wegen des Internets geforderte Recht auf Anonymität auf. Gerade angesichts der zunehmend ubiquitären alltäglich gewordenen digitalen Erfassung erscheint es als eine adäquate Antwort. Im Internet entfällt diese grundlegende Bedingung informationeller Freiheit häufig aus technischen Gründen. Der Gesetzgeber hat folgerichtig den Anbietern von Internetdiensten im Wirkungsbereich des Grundgesetzes eine Rechtspflicht zur Anonymisierung bzw. Pseudonymisierung bei der Ausgestaltung von Verfahren auferlegt (§ 3a BDSG). Für den Bereich der Telemediendienste hat er die Pflicht der Ermöglichung der anonymen bzw. pseudonymen Nutzung von Telemedien und ihrer Bezahlung festgelegt (§ 13 Abs. 6 TMG).

Technische Möglichkeiten zur Anonymisierung helfen Nutzerinnen und Nutzern des Internets, ihr Recht auf informationelle Selbstbestimmung wirksam ausüben zu

[65] BVerfGE 120, 274, 337 – Onlinedurchsuchung.
[66] BVerfGE 65, 1, 44 - Volkszählung.
[67] BVerfG, NJW 2010, 833, 840 Rn. 221 - Vorratsdatenspeicherung.

können. Sie sind daher auch weiterhin als ein Instrument des Selbstdatenschutzes zu fördern.

Die Wahrung der Anonymität gehört in der analogen Welt zu einem selbstbestimmten Leben. Diese Möglichkeit muss auch im Internet gelten. Anders als in der analogen Welt fallen hier aber personenbezogene Daten systembedingt an. Die Erhebung und Verwendung muss dennoch auf ein Mindestmaß beschränkt werden.

Mit dem Recht auf Anonymität geht auch die Möglichkeit eines selbstbestimmten Identitätsmanagement im Internet einher. Jedem Nutzer ist es selbst überlassen, wie viele und welche persönlichen Daten und Identitäten er in der digitalen Welt verwenden und preisgeben möchte. Dies schließt die Verwendung von Pseudonymen ausdrücklich ein.

Profilbildung kann Anonymität einschränken. Sie ist daher nur zulässig, wenn sie auf einer gesetzlichen Grundlage beruht (z. B. BDSG oder TMG). Der Begriff und die Konsequenzen einer Profilbildung sind allerdings noch nicht abschließend diskutiert und gesetzlich konkretisiert.

2.1.7 Sicherheit von Daten/Technischer Datenschutz

Die Entscheidungen des Bundesverfassungsgerichts zur Online-Durchsuchung[68] sowie zur Vorratsdatenspeicherung[69] unterstreichen die gewachsene Bedeutung der Datensicherheit als einem wesentlichen Element des Datenschutzes.

Datensicherheit muss die mit der zunehmenden Vernetzung und Digitalisierung gewachsene Zugänglichkeit personenbezogener Daten und die damit verbundenen Risiken einfangen. Konzeptionell konzentriert sich die Diskussion auf präventiv angelegte und flexible Datensicherheitskonzepte unter Formulierung abstrakter Schutzziele.

Beim technischen Datenschutz ist auf eine technikneutrale Ausgestaltung von gesetzlichen Regelungen zu achten. Ein geeignetes Vorgehen kann hier die Formulierung von Schutzzielen darstellen, wie es die Konferenz der

[68] BVerfGE 120, 274 - Onlinedurchsuchung.
[69] BVerfG, NJW 2010, 833 – Vorratsdatenspeicherung.

Datenschutzbeauftragten des Bundes und der Länder in ihren Eckpunkten für ein „Modernes Datenschutzrecht für das 21. Jahrhundert“[70] fordern.

Mit „privacy by design“, „privacy by default“ können bereits die Hersteller von Hard- als auch Software verpflichtet werden, Produkte zu entwickeln, die über den gesamten Lebenszyklus hinweg zentralen Datenschutzprinzipien sowie den Zielen der Datensicherheit gerecht werden, nämlich:

- Vertraulichkeit
- Integrität
- Intervenierbarkeit
- Verfügbarkeit
- Transparenz
- Möglichkeiten der Nichtverknüpfbarkeit.

Beispielsweise können mit Hilfe von Verschlüsselungstechniken, die dem Stand der Technik entsprechen, Kommunikationen als auch sensible Datenbestände abgesichert werden. Internetseiten könnten derart ausgestaltet werden, dass die Möglichkeit selbstbestimmter und informierter Entscheidung der Nutzer in Design und Technik bereits optimal eingebettet erfolgt. Im Bereich des technischen Datenschutzes bestehen erhebliche Entwicklungsspielräume für den Schutz der Bürgerinnen und Bürger.

Den Datenschutzgesetzen würden so bei neuen technischen Entwicklungen nicht immer neue spezifische Regelungen hinzugefügt, sondern es müssten lediglich konkrete Maßnahmen für die Einhaltung des Datenschutzes spezifiziert werden. Aus übergeordneten Schutzzielen wären gesetzliche Neuregelungen im Bedarfsfall idealerweise ohne neue Grundsatzdiskussionen abzuleiten.

2.1.8 Selbstdatenschutz und Medienkompetenz

Die Stärkung allein des Datenschutzbewusstseins ist von der Stärkung der Medienkompetenz, zu der auch die Datenschutzkompetenz zu zählen wäre, zu unterscheiden. Nutzer sind oft beim Umgang mit eigenen Daten nicht umsichtig genug. Einerseits erkennen sie nicht, dass personenbezogene Daten überhaupt anfallen. Andererseits erkennen sie aber auch nicht die Reichweite und die

[70] Vgl. hierzu auch Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 18 ff.

möglichen Folgen der Sammlung und Verarbeitung der angegebenen personenbezogenen Daten. Sie müssen dies aber erkennen, um bewusst mit ihren Daten umzugehen.

Daher muss den Nutzern sowohl das praktische und technische Verständnis für einen sorgfältigen Umgang mit den eigenen personenbezogenen Daten (z. B. auch deren Schutz vor unerwünschtem Zugriff oder Weitergabe) als auch die Fähigkeit, mögliche Folgen und Konsequenzen der Nutzung entsprechender Angebote zu erkennen, vermittelt werden. Dies hilft nicht nur, datenschutzrechtliche Risiken für den Einzelnen zu minimieren, sondern eröffnet zugleich auch die Chance, sein Recht auf informationelle Selbstbestimmung bewusst auszuüben. Neben anderen Voraussetzungen ermöglicht die Kenntnis der Prozesse der Datenverarbeitung einen eigenverantwortlichen Umgang mit den Daten.
Eine Stärkung des Selbstdatenschutzes kann eine Ergänzung zu, aber kein Ersatz von gesetzlichen Datenschutzregeln darstellen. Vor dem Hintergrund der Schwierigkeiten bei der Entwicklung international gültiger Datenschutzstandards gewinnt der Selbstdatenschutz auch weiter an Bedeutung.

Die Vermittlung eines praktischen und rechtlichen Verständnisses muss daher eine gesamtgesellschaftliche Aufgabe sein.

2.1.9 Die Grenzen des nationalen Datenschutzes

Die Regeln der Datenerhebung und -verarbeitung bei Dienstleistungen, die sich an Bürger der Europäischen Union wenden, bestimmen sich nach dem europäischen oder darüber hinausgehendem nationalen Recht. Die DSRL verbietet es grundsätzlich, personenbezogene Daten aus EU-Mitgliedstaaten in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Sie stellt allerdings eine Anzahl von Instrumenten zur Verfügung, die ein angemessenes Datenschutzniveau bei der Datenübermittlung in Drittstaaten sicherstellen sollen. Gegenwärtig erfolgt eine grundlegende Revision der DSRL, die auf Verbesserungen des Datenschutzes auch in diesem Bereich abzielt.

Die seit 2000 existierende „Safe Harbor“ -Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der „Safe Harbor“-Vereinbarung vorgegebenen Grundsätze verpflichten. In einem Beschluss vom April 2010 hat der Düsseldorfer Kreis die

Anforderungen an die Nachweise und auch an deutsche Unternehmen, die an Nicht-EU-Unternehmen Daten übermitteln, verstärkt.[71]

Dem Grunde nach existieren Vorschriften, die europäische Bürger und Verbraucher schützen. Durch die offenbar mangelnde Durchsetzung der Sondervereinbarung mit den USA wurden diese Rechte allerdings geschwächt. Derzeit befindet sich die EU-Kommission (DG Justice) in Verhandlungen mit den USA über ein so genanntes Allgemeines Datenschutzabkommen, das neben „Safe Harbor“ treten soll und insbesondere nach dem Inkrafttreten des Vertrags von Lissabon und der damit den EU-Institutionen zugewachsenen Mitzuständigkeit für Fragen der justiziellen und polizeilichen Zusammenarbeit auch nach außen eine Rolle spielt.

Ziel dieser Verhandlungen muss die Anwendbarkeit und Durchsetzbarkeit des europäischen Datenschutzrechts sein. Dabei wird u. a. ein Geschäftssitz in Europa als Bedingung für die Erhebung und Verarbeitung von Daten diskutiert.

Gegenwärtig gilt nach dem BDSG das Sitzlandprinzip.[72] Danach kommt dasjenige Recht zur Anwendung, das am Sitz des für die Entscheidung über die Datenverarbeitung Verantwortlichen gilt. Damit wird ein harmonisierter EWR-Rechtsraum begründet. Eine Ausnahme bilden Verarbeitungen, bei denen noch eine Niederlassung im Inland besteht, sodass nationales Datenschutzrecht zur Anwendung kommt. Eine weitere Ausnahme vom Sitzlandprinzip bilden Verarbeitungen, bei denen Verantwortliche außerhalb des EWR-Raumes befindlich sind. So gilt beispielsweise mit Blick auf US-amerikanische Unternehmen das Territorialitätsprinzip und damit grundsätzlich bundesdeutsches Recht, sodass es auf den Ort der Datenverarbeitung bzw. auf die Frage ankommt, ob sich automatisierte Mittel zur Datenerhebung räumlich gesehen in Deutschland befinden. Genau diese Verräumlichung als Anknüpfungspunkt birgt mit Blick auf reine Webinhaltsangebote Probleme. So wird die Anwendbarkeit bundesdeutschen Rechts auf bestimmte Facebook-Bestandteile etwa dann bejaht, wenn es sich um eine Datenverarbeitung handelt, bei der ein so genanntes cookie auf dem Programm der Internetnutzer

[71] „Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.“ (Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover, abrufbar unter http://www.bfdi.bund.de/cae/servlet/contentblob/1103868/publicationFile/88848/290410_SafeHarbor.pdf (zuletzt aufgerufen am: 17. März 2011). Vgl. zur „Safe Harbor“-Vereinbarung auch unter 1.2.2.

[72] § 1 Abs. 5 BDSG.

platziert wird, weil dessen privater Rechner im Inland belegen ist. Für andere Angebote ohne Verwendung dieser Technologie hingegen wird – zumindest von Teilen der Aufsichtsbehörden – von einer fehlenden Anwendbarkeit mangels Inlandsbezuges der Datenverarbeitung ausgegangen. Die „Verhandlungen“ des Hamburgischen Datenschutzbeauftragten mit Google und Facebook sind nur vor diesem Hintergrund nachvollziehbar. Handelte es sich um einen unproblematischen Fall, wären verwaltungsrechtliche Anordnungen ergangen.

Auf europäischer und weltweiter Ebene muss die Bundesrepublik Deutschland ihrer Verantwortung als führender Wirtschaftsnation gerecht werden und für einen ausgeprägten Datenschutz streiten. Die Praxis global agierender Internetunternehmen erfordert ein abgestimmtes Vorgehen über die Grenzen des Nationalstaates hinaus. Bei internationalen Ausformulierungen von Datenschutzvorgaben sollte jeweils das höchste beteiligte Datenschutzniveau Grundlage sein.

2.1.10 Datenschutz für Kinder und Jugendliche

Projektgruppe „Datenschutz, Persönlichkeitsrechte“

Kapitel 2 „Datenschutz“

2.2. Datenschutz im öffentlichen Bereich (STAND: 12.April 2011)

2.2.1 Datenschutz in öffentlichen Einrichtungen

2.2.1.1 Einführung

Das deutsche Datenschutzrecht beruht seit seinen Anfängen auf einer Unterscheidung zwischen Datenschutz im Bereich öffentlicher Einrichtungen und nicht öffentlicher Stellen, insbesondere in der Privatwirtschaft. Diese Differenzierung, die sich auch in der Struktur des BDSG niedergeschlagen hat, findet ihren Ausgangspunkt in der Konzeption des Rechts auf informationelle Selbstbestimmung als einem individuellen Abwehrrecht gegenüber staatlichen Eingriffen. In diesem Zusammenhang wird darauf hingewiesen, dass die grundrechtlichen Grenzen für staatliche Datenverarbeitung enger sind als im nichtöffentlichen Bereich. Die öffentliche Gewalt wird durch die Grundrechte verpflichtet und kann sich nicht auf eigene entgegenstehende Grundrechte berufen. Zwischen staatlichen und nichtstaatlichen Gefährdungen der informationellen Selbstbestimmung besteht daher weiterhin ein Unterschied.[1] Die DSRL kennt diese Zweiteilung jedoch nicht. Das deutsche Recht sieht derzeit zumindest teilweise eine Gleichstellung öffentlicher und privater Datenverarbeitung vor, etwa für Telemedien.[2]

Da das Grundgesetz keine zentrale Kompetenznorm für die Gesetzgebung im Bereich des Datenschutzes enthält, ergibt sich die Zuständigkeit für die Gesetzgebung als Teil der Regelungskompetenz für das jeweilige Verwaltungsverfahren aus den Sachkompetenzen der Art. 73 und 74 GG.[3] Bundesgesetze können daher den Datenschutz nur für Bereiche der Gesetzgebung des Bundes regeln. Entsprechendes gilt für Landesgesetze.

Neben der Unterscheidung datenschutzrechtlicher Bestimmungen für den privaten und öffentlichen Bereich ergibt sich also noch eine weitere Differenzierung zwischen bundes- und landesrechtlichen Normen. Dieses Nebeneinander bundes- und landesrechtlicher Vorschriften kennzeichnet besonders den öffentlichen Bereich, da im privaten Bereich im Rahmen der konkurrierenden Gesetzgebungskompetenz nach Art. 74 Nr. 11 GG („Recht der Wirtschaft“) viele Bereiche – einschließlich der jeweiligen datenschutzrechtli-

[1] Vgl. auch Di Fabio, Udo, in : Maunz/Dürig, Grundgesetz, Kommentar, 58. Ergänzungslieferung 2010, Art. 2, Rn. 190.
[2] Vgl. § 1 Abs. 1 Satz 2 TMG.
[3] Kühling, Jürgen / Seidel, Christian / Siviridis, Anastasios: Datenschutzrecht, 2008, S. 74.

chen Aspekte – durch Bundesgesetze geregelt sind, so dass für den privaten Bereich wenig Regelungsmöglichkeiten für die Länder verbleiben.[4]

Darüber hinaus sind in vielen Fallkonstellationen Fragen der Spezialität und Subsidiarität von Normen zu beantworten. So haben etwa nach § 1 Abs. 3 BDSG andere datenschutzrechtliche Vorschriften des Bundes Vorrang vor dem BDSG. Vollziehen Landesbehörden Bundesrecht, gelten auf Grund einer weiteren Subsidiaritätsregelung (§ 1 Abs. 2 Nr. 2 BDSG) statt des BDSG die Landesdatenschutzgesetze, dies jedoch nur, soweit das zu vollziehende Bundesrecht (z. B. SGB, StVG) keine datenschutzrechtlichen Bestimmungen enthält.[5] Ganz überwiegend gilt auch für die Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen Regelungen.[6]
Vielfach wird daher ein unübersehbares „Dickicht des bereichspezifischen Datenschutzes“[7] beklagt. Im Ergebnis hat dies dazu geführt, dass im Bereich öffentlicher Einrichtungen das BDSG nicht das zentrale Regelungsinstrument darstellt.[8]

Die deutliche Unterscheidung zwischen Datenschutz im öffentlichen und privaten Bereich gilt auch für die Organisation der Aufsicht und Kontrollorgane. Während Bundes- und Landesdatenschutzbeauftragte die jeweilige Kontrolle über Bundes- und Landesverwaltung ausüben, wird die Kontrolle im privaten Bereich ausschließlich auf Länderebene, teilweise durch die Landesdatenschutzbeauftragten, teilweise durch gesonderte Aufsichtsbehörden, ausgeübt. Gesonderte Kontrolleinrichtungen gibt es etwa im Bereich der Kirchen und öffentlich-rechtlicher Rundfunkanstalten.

Der Datenschutzaufsicht kommt für die Verwirklichung eines effizienten Datenschutzes eine herausragende Rolle zu. Stärkung der Aufsichtsbehörden bedeutet somit zugleich eine Verbesserung des Datenschutzes. Vor dem Hintergrund der jüngsten Rechtsprechung des EuGH[9] ist es zwingend notwendig, die völlige Unabhängigkeit der Datenschutzaufsicht zu gewährleisten. Durch die Entscheidung des EuGH könnte auch ein gesetzgeberisches Handeln auf Bundesebene erforderlich sein. Ein entsprechender Auftrag zur Prüfung ist bereits durch die fraktionsübergreifende Entschließung vom 16.12.2010 erteilt worden.[10] Die DSRL gibt vor, dass die Datenschutzaufsicht rechtlich, organisatorisch und finanziell unabhängig

[4] Kilian, Wolfgang / Weichert, Thilo, in: Kilian/Heussen (Hrsg.),Computerrechts-Handbuch, 28. Ergänzungslieferung, 2010, 1. Abschnitt, Teil 13, Punkt I., Rn. 3.
[5] Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stand April 2010, Ziff. 3.3.2.2.
[6] Gola, Peter / Schomerus, Rudolf: BDSG, Kommentar, 2010, § 1, Rn. 33.
[7] Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stand April 2010, Ziff. 4.1.2.
[8] Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stand April 2010, Ziff. 3.2.7.
[9] EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland. Vgl. hierzu auch unter 1.2.3.
[10] BT-Drs. 17/4179, S. 5.

sein muss. Hierbei unterscheidet die Richtlinie nicht zwischen öffentlichem und privatem Bereich.

2.2.1.2. Das Bundesdatenschutzgesetz (BDSG)

Das BDSG ist ein Schutzgesetz, das natürliche Personen schützen soll. Verstöße dagegen können Schadenersatzansprüche begründen. Allerdings begrenzt das BDSG die Möglichkeit einer verschuldensunabhängigen Haftung für Datenschutzverstöße auf die öffentlichen Einrichtungen (§§ 7, 8 BDSG).

Das Datenschutzgesetz ist daneben ein Eingriffsgesetz, mit dem Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gerechtfertigt werden. Die konkreten Eingriffsnormen bzw. Eingriffe müssen durch ein überwiegendes Allgemeininteresse gerechtfertigt sein. Sie müssen zudem den Grundsätzen der Verhältnismäßigkeit und der Normenklarheit genügen und Schutzvorkehrungen zum Zwecke der Datensicherheit und der Sicherheit der Betroffenenrechte vorsehen.

Nach dem BDSG gilt – wie im gesamten Datenschutzrecht - wegen des mit der Datenverarbeitung verbundenen Grundrechtseingriffs und dem Gesetzesvorbehalt das Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG). Das heißt, Datenverarbeitung ist nur dann zulässig, wenn entweder eine Rechtsvorschrift dies ausdrücklich vorsieht oder der Betroffene ausdrücklich eingewilligt hat.
Hierbei sind im Sinne der Rechtsprechung des BVerfG besonders hervorzuheben:

- die Zweckbindung für die Verwendung personenbezogener Daten,
- eine strikte Beschränkung der Datenverarbeitung und -nutzung auf das Erforderliche,
- die größtmögliche Selbstbestimmung der Betroffenen sowie
- die Transparenz der Datenverarbeitung.

Nur bei Beachtung dieser Anforderungen ist der notwendige Schutzzweck für ein modernes Datenschutzrecht gewährleistet.

Über das BDSG hinaus finden sich weitere Datenschutzregelungen mit Relevanz für den staatlichen Bereich in dem Bundespersonalvertretungsgesetz (BPersVG) sowie den jeweiligen Landespersonalvertretungsgesetzen, dem Betriebsverfassungsgesetz (BetrVG), den jeweiligen Landesvorschriften zum Datenschutz, den sozialrechtlichen Vorschriften (SGB), dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) sowie diversen EU- und UN-Richtlinien betreffend personenbezogene Daten.

Durch die engen Vorgaben zu Eingriffen in das Recht auf informationelle Selbstbestimmung wird dem Staat in Fragen des Datenschutzes eine Vorbildfunktion für nichtstaatliche Akteure zugeschrieben.

Auch wenn es im staatlichen Bereich einige Spezifika bezüglich des Beschäftigtendatenschutzes gibt, wird an dieser Stelle nicht darauf eingegangen. Vielmehr wird das Thema Beschäftigtendatenschutz übergreifend, sowohl für den privaten als auch den öffentlichen Sektor, Gegenstand des Kapitels 2.3. sein.

2.2.1.3 Staatliche Datenverarbeitung im Wandel

Die Anfänge der Datenschutzbewegung in Europa wie auch in den USA wandten sich gegen als übermächtig und bedrohlich empfundene Datenerhebungsprojekte staatlicher Stellen.

Hinter diesen Projekten stand die zunehmende Computerisierung der Verwaltung, die neue Möglichkeiten einer Zusammenführung und Auswertung von personenbezogenen Daten erst ermöglichte. Die geplante Volkszählung zu Beginn der 80er-Jahre und das daraufhin 1983 ergangene Volkszählungsurteil des BVerfG[11] etablierten dann endgültig die bis dahin noch streitigen rechtlichen Grundprinzipien des Datenschutzes.

Nachfolgend haben Gesetzgeber und Verwaltung in der Verfolgung ihrer Aufgaben weiterhin Instrumente und Verfahren vorangetrieben, die zumindest mit Blick auf den Datenschutz erhebliche Probleme aufgewiesen haben. Dies gilt in zunehmendem Maße auch für Vorhaben auf europäischer Ebene. Die Vielzahl an Entscheidungen des BVerfG zu Bundes- und Landesgesetzen (z. B. G 10-Entscheidung[12], Großer Lauschangriff[13], Online-Durchsuchung[14], Rasterfahndung[15], KFZ-Kennzeichenerfassung[16], Vorratsdatenspeicherung[17]) markiert dabei einen aktuellen Stand des Datenschutzes im öffentlichen Bereich, der auf den Widerstreit zwischen den von staatlichen Stellen in Anschlag gebrachten öffentlichen Interessen einerseits sowie dem insbesondere vom BVerfG betonten verfassungsrechtlichen Persönlichkeitsrecht andererseits hinweist.

[11] BVerfGE 65,1 - Volkszählung.
[12] Beschluss vom 20. Juni 1984 - 1 BvR 1494/78, BVerfGE 67, 157 – G 10.
[13] BVerfGE 109, 279 – Großer Lauschangriff.
[14] BVerfGE 120, 274 – Onlinedurchsuchung.
[15] BVerfGE 93, 181 – Rasterfahndung I; BVerfGE 115, 320, 345 ff. – Rasterfahndung II.
[16] BVerfG, Urteil vom 11. März 2008 - 1 BvR 2074/05 - KFZ-Kennzeichenerfassung, teilweise abgedruckt in MMR 2008, 308.
[17] BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 – Vorratsdatenspeicherung.

Die Auseinandersetzung beschränkt sich dabei nicht auf den Sicherheitsbereich, sondern findet ihre Fortsetzung auch in anderen Bereichen der öffentlichen Verwaltung, so etwa in den aktuellen Auseinandersetzungen um Grenzen zulässiger Datenerhebung bei Hartz-IV-Empfängern oder die Ausweitung staatlicher Kontodatenzugriffe.

2.2.1.4 Herausforderungen für das Datenschutzrecht in öffentlichen Einrichtungen

Die Informationsverarbeitung öffentlicher Stellen stellt besondere Herausforderungen an den Datenschutz, denn:

- viele staatliche und kommunale Aufgaben, z. B. in Steuerverwaltung, Justiz, Sicherheit, Sozialhilfe und Gesundheitswesen, erfordern naturgemäß die Erfassung und Verarbeitung personenbezogener Daten, die einen besonderen Schutzbedarf aufweisen können;
- die mit der Informationsverarbeitung einhergehenden Fachaufgaben, insbesondere in der Eingriffsverwaltung, sind gesetzlich legitimiert;
- die vollständige Durchdringung der öffentlichen Verwaltung mit IT hat zur Konsequenz, dass die öffentliche Verwaltung in ihrer Gesamtheit über ein fast lückenloses Datenprofil aller Bürger verfügt.

Datenschutz im öffentlichen Bereich muss vor diesem Hintergrund sicherstellen, dass

- die Informationsverarbeitung und die damit verbundene Einschränkung des informationellen Selbstbestimmungsrechtes in jedem Anwendungsfall rechtlich legitimiert und angemessen ist (Erforderlichkeitsgrundsatz);
- die personenbezogenen Daten nur zu dem Zweck verwendet werden, für den sie erfasst wurden (Zweckbindungsgrundsatz);
- betroffene Bürger wissen, welche öffentlichen Stellen welche Daten über sie gespeichert haben (Transparenzgrundsatz), und
- nur solche personenbezogenen Daten von Bürgern erfasst und gespeichert werden, die zur Erledigung der jeweiligen Aufgabe unbedingt erforderlich sind (Datenvermeidungs- und Datensparsamkeitsgrundsatz).

Die bereichsspezifischen Regelungen zum Datenschutz sollen nicht nur einer materiellen Verletzung dieser Grundsätze vorbeugen, sondern darüber hinaus auch vermeiden, dass die persönlichen

Grundrechte durch ein diffuses Gefühl totaler staatlicher Überwachung[18] eingeschränkt oder beeinträchtigt werden.

Gerade um diesem diffusen Gefühl totaler staatlicher Überwachung entgegenzutreten, wird diskutiert, ob und wie Auskunftsrechte für Bürgerinnen und Bürger und Auskunftspflichten staatlicher Stellen, etwa im Zusammenhang mit den Informationsfreiheitsgesetzen der Länder und des Bundes, überprüft und gegebenenfalls ausgebaut werden sollten.

Bei bisherigen Gesetzgebungsvorhaben konnten oft während des parlamentarischen Verfahrens noch Veränderungen hin zu einer Reduzierung der Menge an gesammelten personenbezogenen Daten erreicht werden, jedoch nicht ein vollständiger Verzicht auf das jeweilige Vorhaben. Gesetzliche Schutzprogramme für den Datenschutz können zudem vielfach mit der technischen Entwicklung nicht Schritt halten.
Beim Betrieb bestehender oder der Einführung neuer IT-Infrastrukturen in öffentlichen Einrichtungen ergeben sich daher eine Vielzahl datenschutzrechtlicher Fragestellungen.

Deren frühzeitige Einbeziehung in alle Projekte, u. a. bei der Entwicklung der jeweiligen Hard- und Software, ist unabdingbar. Die Umstellung bestehender Verwaltungsverfahren auf elektronische Basis birgt dabei auch Chancen für den Datenschutz. Die zukünftige Technik kann bereits frühzeitig nach den Geboten der Datensparsamkeit und -sicherheit gestaltet werden.[19]

Fragen des Datenschutzes in öffentlichen Einrichtungen werden vielfach unter den Stichworten „eGovernment und Datenschutz“ thematisiert. Als besondere Herausforderungen werden hierbei unter anderem beschrieben:[20]

- Zunahme personenbezogener Daten, d. h. die gesamte Kommunikation Einzelner mit Behörden kann erfasst und analysiert werden; im Gegensatz dazu fallen etwa bei formlosen (fern-)mündlichen Anfragen bei einer Behörde üblicherweise keinerlei Daten an;[21]
- Zunahme zentraler, bereichsübergreifender Datenbestände, etwa wenn Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer zentralen Stelle

[18] BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08, NJW 2010, 833 (Absatz-Nr. 212) - Vorratsdatenspeicherung.
[19] Bizer, Johann (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein): eGovernment: Chance für den Datenschutz, abrufbar unter: https://www.datenschutzzentrum.de/e-government/dud-200507.htm (Stand: 11.11.2010).
[20] Vgl. Der Landesbeauftragte für den Datenschutz Niedersachsen: Herausforderungen für den Datenschutz bei eGovernment, abrufbar unter: http://www.lfd.niedersachsen.de/live/live.php?navigation_id=13010&article_id=56234&_psmand=48 (Stand: 11.11.2010).
[21] Vgl. hierzu auch Yildirim, Nuriye: Datenschutz im Electronic Government, 2004, S. 64.

(etwa One-Stop-Government oder Lebenslagenkonzept) angeboten werden; beispielsweise durch den „einheitlichen Ansprechpartner“ nach der EU-Dienstleistungsrichtlinie, der als zentrale Anlaufstelle insbesondere für elektronische Behördendienste fungiert;[22]

- Fragen der Datensicherheit im Rahmen der elektronischen Kommunikation mit dem Bürger, etwa Gefährdungen des internen IT-Systems durch Systemöffnung, Notwendigkeit der Authentisierung bei Übermittlung personenbezogener Daten;
- Fragen der internen Datensicherheit;
- datenschutzrechtliche Verantwortlichkeiten bei Zusammenarbeit mehrerer Stellen, gegebenenfalls auch von Bund, Ländern und Kommunen;[23]
- Einschaltung (privater) technischer Dienstleister.

2.2.1.5 Cloud Computing in der öffentlichen Verwaltung

Cloud Computing als Möglichkeit, Speicherkapazitäten, Rechenleistung und Software bedarfsspezifisch über das Internet zu beziehen, könnte perspektivisch auch in öffentlichen Einrichtungen an Bedeutung gewinnen. Die gemeinsame Nutzung von Hard- und Software sowie Rechenkapazitäten, die auf verschiedenen Servern nachfrage- und einzelfallabhängig zur Verfügung gestellt werden, könnte auch für Behörden, Ministerien und kommunale Selbstverwaltungskörperschaften möglicherweise Sparpotentiale durch Senkung der Ausgaben für eigene Hard- und Software eröffnen.[24]

Allerdings steht diese Form der Vernetzung behördlicher IT-Infrastrukturen, also der von unterschiedlichen Trägern der öffentlichen Verwaltung eingesetzten Hard- und Software, noch am Anfang.[25] Soweit ersichtlich, gibt es in Deutschland noch keine Nutzung von Cloud-Anwendungen durch öffentliche Stellen, wohl aber entsprechende Prüfungen.[26] Dabei wird davon ausgegangen, dass sich nur Modelle einer abgeschlossenen („privaten“) Cloud in alleiniger Verantwortung der öffentlichen Verwaltung als mögliche Option erweisen könnten.[27]

[22] Vgl. hierzu auch Petersen, Christin: Einheitlicher Ansprechpartner und Datenschutz, LKV 2010, S. 344 ff.
[23] Vgl. hierzu auch Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 15.
[24] Vgl.Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 75.
[25] Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 75.
[26] Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 12., abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/ (Stand: 11.11.2010).
[27] Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78.

Daneben stehen andere Formen der Zusammenarbeit von öffentlichen Einrichtungen im IT-Bereich, etwa als „Shared Services Center“. Hierbei werden verwaltungsunterstützende Leistungen für die öffentliche Verwaltung zentral und gemeinschaftlich erbracht. Interne Dienstleistungen (etwa Personalverwaltung oder Gebäude-Management) werden also mittels gemeinsamer Nutzung von Ressourcen für mehrere Organisationseinheiten erbracht.

Die Bundesregierung strebt an, die Entwicklung und Einführung von Cloud Computing zu beschleunigen. Neben mittelständischen Unternehmen soll gerade der öffentliche Sektor frühzeitig von den Chancen profitieren. Unter anderem die Bereiche Sicherung und Schutz von Daten sind an die spezifischen Anforderungen von Cloud Computing anzupassen. Datenschutz und Datensicherheit seien eine der hierbei sich ergebenden rechtlichen Herausforderungen.[28] Hierzu hat die Bundesregierung ein „Forschungsprogramm Sichere Internet-Dienste – Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)“ aufgelegt.[29]

Datenschutzrechtlich wird die Nutzung cloud-basierter Dienste bei der Verarbeitung personenbezogener Daten zumeist als eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG eingeordnet. Verantwortlich für die Einhaltung datenschutzrechtlicher Vorschriften ist weiterhin der Auftraggeber (§ 11 Abs. 1 BDSG). Dieser ist insbesondere verpflichtet, den Gegenstand des Auftragsverhältnisses schriftlich hinsichtlich diverser Einzelaspekte genau festzulegen (etwa die nach § 9 BDSG zu treffenden technischen und organisatorischen Schutzmaßnahmen oder die Berechtigung zur Begründung von Unterauftragsverhältnissen). Diese rechtlichen Vorgaben setzen der cloud-basierten Verarbeitung personenbezogener Daten bisher enge Grenzen.[30] Im Übrigen gelten insoweit ähnliche Überlegungen wie für die datenschutzrechtliche Beurteilung von Cloud Computing durch private Unternehmen.[31]

[28] IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: . http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (Stand: 15.11.2010).

[29] IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (Stand: 15.11.2010).

[30] vgl. Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 6.1., abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/ (Stand: 11.11.2010); Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78 f. Zum Cloud Computing vgl. im Übrigen unter 2.3.3.

[31] Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78.

2.2.2 Mögliche Erweiterung des Grundgesetzes im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Der Schutz der informationellen Selbstbestimmung ist ebenso wie der Schutz der Vertraulichkeit der Kommunikation ein in vielen Landesverfassungen sowie internationalen Konventionen anerkanntes Grund- und Menschenrecht. Mit der europäischen Charta der Grundrechte wurde zudem ein Grundrecht auf Datenschutz geschaffen.[32] Das Grundgesetz enthält weder ein explizites Grundrecht auf informationelle Selbstbestimmung noch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das BVerfG hat jedoch in Rechtsfortbildung[33] diese beiden Grundrechte – das Recht auf informationelle Selbstbestimmung und das Recht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme - aus den vorhandenen Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG hergeleitet und angewendet.

Für eine ausdrückliche Aufnahme der beiden Grundrechte in die Verfassung wird vorgetragen, dass der Bedeutung der Entwicklung einer demokratischen und offenen digitalen Gesellschaft Rechnung getragen würde. Zudem hätte dies eine bessere Erkennbarkeit für den Bürger zur Folge. Mit der Aufnahme beider Grundrechte könnte auch der Verfassungsgesetzgeber die Rechtswirklichkeit an die veränderten Umstände in einer digitalen Gesellschaft anpassen, zumal das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in den kommenden Jahren noch weiter an Bedeutung gewinnen werden.

Eine entsprechende Ergänzung um das Grundrecht auf informationelle Selbstbestimmung sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme würde zudem die Übernahme des durch das BVerfG beschrittenen Weges durch den Verfassungsgesetzgeber unterstreichen.

Gleichwohl fanden entsprechende Vorschläge für eine Verfassungsänderung im Deutschen Bundestag bisher keine Mehrheit.[34] Gegen die vorgeschlagenen Formulierungen wird vorgetragen, dass das Schutzniveau gegenüber der bestehenden Rechtslage senken könnten. Außerdem müsse sichergestellt sein, dass weiterhin Raum

[32] Vgl. Art. 8 GRC.
[33] Vgl. zum Recht auf informationelle Selbstbestimmung: BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 45 - Volkszählung. Zum Recht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme siehe: BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, BVerfGE 120, 274 - Onlinedurchsuchung.
[34] Vgl. zuletzt BT-Drs. 16/9607 vom 18.06.2008 und BT-Drs. 16/13218 vom 27.05.2009

für eine künftige Auslegung des Grundgesetzes bleibe, sodass auf neue Fragen, die sich im Zusammenhang mit der technischen und gesellschaftlichen Entwicklung stellen, verfassungsrechtliche Antworten gefunden werden können.

2.2.3 Datensicherheit

Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme des öffentlichen Bereiches gegen unberechtigten Zugriff und missbräuchliche Nutzung von innen und außen geschützt sind. Die hierfür einschlägigen Schutzregelungen (z. B. Anlage zu § 9 BDSG) stammen aus einer Zeit, als Datenverarbeitung im öffentlichen Bereich durch Großrechner in abgeschotteten Rechenzentren gekennzeichnet war. Die jüngere Rechtsprechung[35] stellt in ihren Entscheidungen zunehmend auch auf die Bedeutung der informationstechnischen Sicherheit bei der Verarbeitung der personenbezogenen Daten ab.

Im Zuge des E-Government kommen längst Online-Verfahren zum Einsatz, bei denen Bürger selbst auf die IT-Systeme der Verwaltung zugreifen. Durch diese Entwicklung und die fortschreitende Vernetzung der Verwaltungssysteme untereinander wird es zunehmend schwieriger, das technisch veraltete Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden.

Weitere Gesichtspunkte und Fragen der Datensicherheit werden zu einem späteren Zeitpunkt im Schlussbericht der Enquete-Kommission im Kapitel „Zugang, Struktur und Sicherheit im Netz“ aufgegriffen.[36]

2.2.4 Datenschutzaudit und Gütesiegel zum Zwecke der Vertrauensbildung

Datenschutz in öffentlichen Einrichtungen kann durch Auditierungsverfahren gefördert und erleichtert werden. Die Verleihung von Gütesiegeln sowie die Zertifizierung und Durchführung von Audit-Verfahren können wirkungsvolle, marktsteuernde Anreize für besseren Datenschutz geben. Ähnlich wie bei der technischen Betriebssicherheit (dem TÜV) können Normen und Verfahren einen integrierten technischen Datenschutz fördern und gewährleisten. Die in den Bundesländern eingerichteten Datenschutzauditverfahren sowie das europäische Gütesiegel (EuroPriSe) können als praktische Beispiele hierfür angeführt werden.

[35] Vgl. BVerfG zur Online-Durchsuchung, BVerfGE vom 27. Februar 2008, Az. 1 BvR 370/07, abgedruckt in: NJW 2008, 822; sowie BVerfG zur Vorratsdatenspeicherung, Urteil vom 2. März 2010 - 1 BvR 256/08, BVerfGE 121, 1.

[36] Vgl. im Übrigen auch unter 2.1.7.

Dabei wird das Datenschutzkonzepts einer öffentlichen Stelle durch einen unabhängigen Gutachter förmlich geprüft und von einer anderen unabhängigen öffentlichen Stelle bestätigt.

Im Unterscheid zu einer allgemeinen Beratung erfolgt beim Datenschutzaudit ein Mehr: Die Beratung bezieht sich auf die jeweils konkret vorgelegte Frage bzw. auf den unterbreiteten Sachverhalt. Ob die gegebenen Empfehlungen umgesetzt werden, bleibt offen und auch Veränderungen maßgeblicher Umstände werden nach Abschluss der Beratung nicht berücksichtigt. Das Audit hingegen ist auf eine dauerhafte Verbesserung der Datenschutzorganisation gerichtet. In Anlehnung daran könnte eine staatlich gestützte Datenschutzstiftung als Gütesiegelgarantie wirken und der Vertrauensbildung Vorschub leisten.

Projektgruppe „Datenschutz“

2.3. Datenschutz im nicht-öffentlichen Bereich (STAND: 12. April 2011)

2.3. Datenschutz im nicht-öffentlichen Bereich

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.

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 sich auf Grund dieser meinungsbildenden Funktion 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 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 ausschließlich 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 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[1], 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 Volkszählungsurteil 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.[2] 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 Kommuni-

[1] Deutlich zuletzt BVerfG, Beschluss vom 26. Februar 2008 - 1 BvR 1602, 1606, 1626/07, BVerfGE 120, 180, 205 – Caroline von Monaco III: „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 BVerfG, Urteil vom 9. November 1999 - 1 BvR 653/96, BVerfGE 101, 361, 389 ff. – Caroline von Monaco II.

[2] Vgl. BVerfGE 65, 1, 40 f. – Volkszählung.

kationsinteressen 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 nicht 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.[3] 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.[4]

[3] Vgl. nur BVerfG, Beschluss vom 26. Juni 1990 - 1 BvR 776/84, BVerfGE 82, 236, 269 – Schubart; BVerfG, Beschluss vom 24. März 1998 - 1 BvR 131/96 , BVerfGE 97, 391, 403 - Missbrauchsbezichtigung; BVerfG, Beschluss vom 10. November 1998 - 1 BvR 1531/96, BVerfGE 99, 185, 194 - Scientology; BVerfGE, 101, 361, 380 – Caroline von Monaco II.
[4] BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich,de.

- 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.

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 entfernen. 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.

Neben dem schlichten Schalten von Werbeeinblendungen werden Kunden zum Zweck der Verkaufsförderung auch gezielt angesprochen. Dies geschieht auch über Anzeigen mit besonderen Angeboten oder Gutscheinen für Neukunden und Aktionen wie Treue-Boni oder Rabatte zur langfristigen Bindung von Bestandskunden.

Die eingesetzten Techniken ermöglichen es, sowohl Werbung, Zielseiten, aber auch Angebote und Preise in Echtzeit auf die speziellen Verhaltensweisen eines Nutzers auszurichten. Durch die Techniken des so genannten „Targeting“ ist es teilweise möglich, den Nutzer beim Besuch der Seite wiederzuerkennen, das jeweilige Verhalten zu erfassen und Webinhalte und –services dementsprechend dynamisch den Nutzerpräferenzen anzupassen. Für die Nutzer der Seite ist es dabei nicht mehr erkennbar, ob es sich um für sie bereits angepasste Webseiten und Werbeangebote oder aber Standardwebseiten handelt, die für alle Nutzer gleich sind.[5] Oftmals

[5] Zu den Geschäftsmodellen in der Online-Werbung, eine Übersicht über die eingesetzten Techniken, deren Erkennbarkeit und Beeinflussbarkeit durch die Verbraucher und dem Einsatz von Profilbildung im

werden darüberhinaus auch Kombinationen von mehreren Techniken eingesetzt.
Jenseits des Schutzes der Privatsphäre sind daher die Auswirkungen auf die Marktposition der Nutzer/Verbraucher im Internet erheblich und müssen in Transparenz- sowie Einwilligungserfordernissen berücksichtigt werden.

Die Zulässigkeit, Transparenz- und Einwilligungserfordernisse hängen wesentlich von den eingesetzten Techniken, der Sensibilität der erhobenen Daten und der Datennutzung ab. So ist von Bedeutung, ob Nutzungsdaten aggregiert erhoben sowie verarbeitet werden und eine individualisierte Auswertung nicht beabsichtigt ist. Relevant ist dabei auch, ob sie pseudonymisiert oder anonymisiert 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

Besonderen siehe „Digitale Profilbildung und Gefahren für die Verbraucher“, A. Klein, F. Leithold, C. Zell, J. Roosen, TU München, Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes e.V., November 2010

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.[6] 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

[6] Vgl. BVerfGE 65, 1 – Volkszählung.

des Profils herbeigeführt. Es besteht Einigkeit, dass solche Nutzungsprofile bei Einhaltung bestimmter Vorgaben, zulässig sind.[7] 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).[8] 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 Ano-

[7] Vgl. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) vom 26./27. November 2009: Datenschutzkonforme Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten.
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile (zuletzt aufgerufen am 23. März 2011).

[8] Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.). Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010.
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile (zuletzt aufgerufen am: 22. März 2011).

nymisierung, 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, der diese Entscheidung trifft. Damit wird die Frage der Reichweite der Reichweite bzw. der Grenze der Reichweite der Transparenzinstrumente angesprochen.

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. § 33 Abs. 1 Satz 3 BDSG). Eine namentliche Nennung der Empfänger ist jedoch nicht erforderlich, sodass 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 sie von einer verantwortlichen Stelle erhoben, verarbeitet oder genutzt werden und woher die Daten stammen, an wen die Daten weiterge-

leitet werden und zu welchem Zweck diese Daten gespeichert werden. Unter bestimmten Bedingungen kann die verantwortliche Stelle 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 so genannten „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 erteilt werden. 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

Beschreibung

Angesichts stetig steigender Datenvolumina und einer wachsenden mobilen Nutzung von Daten stellt sich dem Nutzer – sei es Privatperson oder Unternehmer – zunehmend die Frage „Wohin mit den Daten, die anfallen?“ und „Wie kann ich Datenverarbeitungsprozesse effizienter und kostengünstiger machen?“. Als Lösung wird zunehmend das so genannte Cloud Computing angeführt, übersetzt „Datenverarbeitung in der Wolke“.

Von Cloud Computing wird dann gesprochen, wenn eine oder mehrere der IT-Dienstleistungen, wie Infrastruktur (Rechenleistung, Hintergrundspeicher, etc.), Plattform oder Anwendungssoftware aufeinander abgestimmt und nach tatsächlicher Nutzung abrechenbar über ein Netz durch Dritte bereitgestellt werden.[9] Obwohl die Online-Speicherung von Daten, Online-Adressbüchern oder Online-Kalendern oder etwa die webbasierte Nutzung von E-Mail-Diensten bereits als alltägliche Cloud-Anwendungen von vielen genutzt werden, kann zum gegenwärtigen Zeitpunkt noch nicht davon ausgegangen werden, dass der Begriff und die dahinter liegende Technik des Cloud Computing geläufig sind. Es ist davon auszugehen, dass sich das Cloud Computing in den nächsten Jahren vor allem im Bereich der Geschäftsanwendungen und der Serverkapazitäten immer weiter etablieren wird.

Angebotene Dienstleistungen im Cloud Computing können u. a. bereitgestellter Speicher oder Rechenzeit sein, aber auch z. B. kom-

[9] Bundesamt für Sicherheit in der Informationstechnik. Essoh, Alexander Didier: „Cloud Computing und Sicherheit - Geht denn das?“ 19. November 2009, Folie 4. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/4GS_Tag/07_essoh_bsi.pdf?__blob=publicationFile (zuletzt aufgerufen am 23. März 2011).

plette Datenverarbeitungsverfahren. Beim Cloud Computing wird zum einen unterschieden nach der Art der angebotenen Dienstleistung in der Cloud, und zwar zwischen Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (Iaas). Zum anderen wird nach der Beschaffenheit der Cloud zwischen Privaten und Public Clouds unterschieden. Private Clouds sind vernetzte Rechner, die alle unter der rechtlichen Verantwortung einer einzigen Daten verarbeitenden Stelle stehen.[10] Als Private Clouds werden aber auch Rechnernetze von rechtlich zueinander in einem engen Verhältnis stehenden Stellen bezeichnet, z. B. Stellen der öffentlichen Verwaltung oder eines Konzerns.[11]

Eine Public Cloud ist eine öffentliche Cloud, welche von einer Vielzahl von Personen und Firmen genutzt werden kann. Die Public Cloud ist nicht auf eine bestimmte Institution, ein bestimmtes Unternehmen oder einen bestimmten Personen-/Nutzerkreis beschränkt. Wesentliches Merkmal ist, dass sie jedermann zugänglich ist und dass der Anwender nicht mitbestimmen kann, mit welchen Anwendern er sich die Nutzung einer Hardware teilt, also mit welchen anderen virtuellen Maschinen seine virtuelle Maschine auf derselben physischen Hardware läuft.[12] Dabei wird die Rechenleistung von „Dritten“ i. S. d. Datenschutzrechts (§ 3 Abs. 8, S. 2 BDSG) angeboten.[13] Zu den Anbietern solcher Public Clouds gehören IT-Unternehmen, wie z. B. Google, Amazon, IBM, SAP oder die Deutsche Telekom. Neben diesen beiden Formen existiert auch eine Mischform von Public und Private Cloud, die Hybrid Cloud, bei der eine Nutzung von eigenen und fremden Ressourcen stattfindet.

Eine der Besonderheiten des Cloud Computing liegt, je nach Angebot, in der zumeist flexiblen und grenzüberschreitenden Bereitstellung von Cloud Ressourcen durch eine Vielzahl von Beteiligten.

<u>Offene Fragen im Bereich des Datenschutzes und der Datensicherheit im Cloud Computing</u>

Die Auslagerung von Daten und Datenverarbeitung in die Cloud wirft datenschutz- und datensicherheitsrelevante Fragestellungen auf. Wenn Unternehmen ihre IT-Strukturen in eine Cloud auslagern, wird der Umfang der Datensicherheit und des Datenschutzes vom Anbieter der Cloud bestimmt.

a) Datensicherheit

[10] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (679).
[11] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).
[12] Birk, Dominik/Wegener, Christoph: Über den Wolken: Cloud Computing im Überblick. DuD 2010, 641 (642).
[13] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

Das zentrale Problem hinsichtlich der Datensicherheit besteht darin, die Integrität (Datenveränderungen können erkannt werden) und Vertraulichkeit (nur Befugte können auf Daten zugreifen) der Datenverarbeitung und die Verfügbarkeit (Daten stehen in einem angemessenen Zeitraum zur Verfügung) zu gewährleisten.[14] Wie aktuell die Datensicherheit auf Netzwerk- und Datenebene in der Cloud gewährleistet wird, welche möglichen Probleme es gibt und inwieweit sich daraus politischer Handlungsbedarf ergibt, sollte auf Grund des Sachzusammenhangs von der Projektgruppe „Zugang, Struktur und Sicherheit im Netz“ geprüft werden.

b) Datenschutz

Bei manchen Formen des Cloud Computing stellen sich besondere Herausforderungen, weil Rechtsgrundlagen wie Auftragsdatenverarbeitung oder Übermittlung das Cloud Computing nicht vollständig erfassen. Zudem werden damit typische, bereits bekannte Probleme des Outsourcings nicht nur potenziert, sondern sie gewinnen auch eine neue Qualität. Im Hinblick auf Rechenprozesse kann nicht mehr mit Bestimmtheit gesagt werden, auf welchen der oftmals weltweit verbundenen Server und damit bei welchen Beteiligten konkret welche Datenverarbeitungsprozesse vollzogen werden.

Dies führt zu rechtlichen Unsicherheiten bei der Nutzung und dem Betreiben entsprechender Angebote.

Gerade im Fall eines grenzüberschreitend angelegten Cloud Computing ergeben sich Fragen nach der Verantwortlichkeit sowie den Zugriffsmöglichkeiten Dritter. Um die Datenverarbeitung innerhalb der EU zu harmonisieren, wurde die Europäische Datenschutz-Richtlinie (DSRL) geschaffen. Da der Umstand einer grenzüberschreitenden Datenverarbeitung innerhalb des europäischen Binnenmarktes kein rechtliches Hindernis darstellen soll, dürfen gemäß Art. 1 Abs. 2 DSRL personenbeziehbare Daten im gesamten Europäischen Wirtschaftsraum (EWR) verarbeitet werden.[15] Für eine Anwendbarkeit nationalen Rechts kommt es gemäß Art. 4 Abs. 1 a, b DSRL deshalb darauf an, in welchem Mitgliedstaat die Daten verarbeitende Niederlassung ihren Sitz hat.[16] Damit auch Unternehmen, welche keine Niederlassung im Europäischen Wirtschaftsraum haben, personenbezogene Daten verarbeiten können, wurde in § 1 Abs. 5 S. 3 BDSG bestimmt, dass diese Unternehmen einen Datenschutzbeauftragten innerhalb der EU benennen, welcher dann für die Einhaltung der Richtlinien verantwortlich ist.

[14] Heidrich, Jörg/Wegener, Christoph: Sichere Datenwolken – Cloud Computing und Datenschutz. MMR 2009, 803 (804).
[15] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).
[16] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

Hinsichtlich der Verantwortlichkeit legt die DSRL in Art. 2 c fest, dass derjenige für den Datenschutz verantwortlich ist, der die Verarbeitung angeordnet hat. Dies ist grundsätzlich der Cloud-Nutzer und nicht der Anbieter.

Insgesamt sind alle Datensätze, die nicht als personenbeziehbar gelten (§ 3 Abs. 1 BDSG) zur Verarbeitung in Clouds vollkommen unproblematisch. Datenschutzrelevant ist die Form der Nutzung des Cloud Computing nach deutschem Recht nur dann, wenn personenbezogene Daten verarbeitet werden (§ 3 BDSG). Da im Rahmen der Nutzung Cloud-basierter Dienstleistungen oft personenbezogene Daten auf dem System des Cloud-Anbieters gespeichert und auch verarbeitet werden und bei grenzüberschreitenden Systemen auch auf Speichermedien, die europa- bzw. sogar weltweit verteilt sind, stellt sich die Frage nach der Behandlung dieser Verlagerung der Daten in die Cloud. Aus rechtlicher Sicht kann es sich um eine Auftragsdatenverarbeitung i. S. d. § 11 BDSG handeln. Diese erfährt datenschutzrechtlich die Grenzen ihrer Zulässigkeit zum einen dort, wo dem Verantwortlichen (dem Nutzer der Cloud) durch den Dienstleister keine Angaben über Art und Ort der Verarbeitung und den Sicherungsmaßnahmen gemacht werden. Zum anderen ist dies der Fall, wenn die datenverarbeitende Stelle außerhalb Deutschlands, eines Mitgliedstaates der EU oder des EWR liegt, in dem kein vergleichbares Datenschutzniveau existiert. In diesem Fall handelt es sich um eine Weitergabe an Dritte, wobei der Gesetzgeber unterstellt, dass bei derartigen Übermittlungskonstellationen besondere persönlichkeitsrechtliche Risiken entstehen, weil von der verantwortlichen Stelle, vom Betroffenen oder von den staatlichen Aufsichtsbehörden keine hinreichende Kontrolle der Datenverarbeitung möglich ist.[17]

Hinzu kommt, dass die in § 11 Abs. 2 BDSG geforderte „sorgfältige“ Auswahl des Auftragnehmers „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen“ in der Praxis nur schwer einzuhalten ist, da u. a. der Auftragnehmer dem Auftraggeber in der Regel nicht derart tiefgehende Einblicke in seine IT-Struktur gewährt.

Je nach verwendetem Angebot (beispielsweise Verteilung der Daten auf mehrere weltweit verteilte Server) kann die Verlagerung der Daten in die Cloud zu einer Erhöhung der Gefahr von Zugriffsmöglichkeiten durch Dritte führen. Wichtig ist daher, dass der früher selbst Datenverarbeitende die Herrschaft über die Daten bewahrt und Kenntnis und Einfluss über die ergriffenen Sicherungsmaßnahmen hat.

[17] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

Folgeproblem der Verlagerung und der Verteilung der Daten auf europa- und weltweite Server ist eine erschwerte Datenschutzkontrolle. Eine Datenschutzkontrolle durch die Aufsichtsbehörden ist auf das jeweilige Landesterritorium bzw. auf das Bundesterritorium begrenzt. Europaweit kann gegenseitig eine Amtshilfe der Aufsichtsbehörden erfolgen. Über das europäische Territorium hinaus sind koordinierte oder gemeinsame Kontrollen in Clouds mit Drittauslandsbezug praktisch nicht möglich.[18] Dies eröffnet datenschutzrechtlich verantwortlichen Stellen die Möglichkeit, sich Datenschutzkontrollen zu entziehen, in dem gezielt Clouds mit Drittlandsbezug genutzt werden. Daneben ist besonders problematisch, wenn die Datenverarbeitung in Staaten erfolgt, die nicht nur keinen ausreichenden Datenschutz gewährleisten, sondern auch bewusst und gezielt gegen Menschenrechte verstoßen und den Zugriff auf Daten in der Cloud zu politischer Überwachung und Verfolgung benutzen.[19]

Der Ort, wo die Daten gespeichert und verarbeitet werden, spielt also eine zentrale Rolle. Dies zeigt sich auch für Daten, welche für Steuerzwecke benötigt werden. Diese dürfen gem. § 146 Abs. 2 S. 1 Abgabenordnung (AO) nur im Inland gespeichert werden. Auch hier stellt sich das Problem bei länderübergreifenden Netzen und der Information, in welchem Land die Daten gelagert und verarbeitet werden. Nach § 146 Abs. 2 a AO kann die zuständige Finanzbehörde bewilligen, dass die Finanzdokumente auch außerhalb der EU oder des EWR archiviert werden.[20] Auch hier könnten die Steuerermittlungsbehörden vor Probleme gestellt werden, weil nicht ohne weiteres ein Zugriff auf die Daten erfolgen kann.

Im Ergebnis ist festzuhalten, dass es noch offene datenschutzrechtliche Fragen gibt, wenn personenbezogene Daten in die Cloud verlagert werden. Dies kann die Nutzung, aber auch die sich bietenden Möglichkeiten und Innovationen des Cloud Computing einschränken. Bisher können datenschutzrechtliche Erfordernisse nur durch besonders umfangreiche und detaillierte Vertragsvereinbarungen gewährleistet werden. Für die Ermittlung von Straftaten und Ordnungswidrigkeiten stellt die Speicherung von Daten in der Cloud dann ein Problem dar, wenn durch die Art und den Ort der Datenverarbeitung ein Zugriff für die Ermittlungsbehörden nicht möglich ist.[21] Im Inland stehen Staatsanwaltschaften und auf Anordnung auch ihren Ermittlungspersonen gemäß § 110 Abs. 3 StPO seit dem Jahr 2008 entsprechende Befugnisse auf Durchsicht von Speichermedien zu.

[18] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (684).
[19] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (684).
[20] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).
[21] Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

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. Auf Grund der einfachen Vervielfältigung digitaler Daten im Internet ist wegen 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“[22], beispielsweise auch vom „programmierten Vergessen“[23], „Verfallsdaten“ oder dem „digitalen Radiergummi“[24] 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. Auf Grund 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 zu begrenzen, ermöglichen sollen. Allerdings fehlt es bisher an einer Gesamtlösung für alle Bereiche des Internets und insbesondere für die besonders

22 Mayer-Schönberger, Viktor: Delete: The Virtue of Forgetting in the Digital Age. 2009; Jeffrey Rosen, The Web means the End of Forgetting. The New York Times vom 21. Juli 2010. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (zuletzt aufgerufen am 23. März 2011).
23 Bull, Hans Peter: Persönlichkeitsschutz im Internet : Reformeifer mit neuen Ansätzen. NVwZ 2011, 257 (260).
24 Vgl. dazu die Rede des ehemaligen Bundesinnenministers Dr. Thomas de Maizière zu den Grundlagen für eine gemeinsame Netzpolitik der Zukunft. Berlin, 22.06.2010. Thesenpapier online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/thesen_netzpolitik.pdf?__blob=publicationFile (zuletzt aufgerufen am 7. April 2011).

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.[25] Die Universität des Saarlandes stellte im vergangenen Jahr ein vergleichbares Produkt vor.[26] 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.

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.[27]

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.[28] Nachträglich möglicherweise auftretende Schwierigkeiten bei 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 Verschlüsselung von Daten, die Löschung von Daten nach erfolgter Funktionserfüllung oder technische Vorkehrungen zur Einhaltung des

25 Hickey, Hannah: This article will self-destruct: A tool to make online personal data vanish. http://uwnews.org/article.asp?articleID=50973 (zuletzt aufgerufen am 23. März 2011).
26 Universität des Saarlandes: X-pire! - Wie man dem Internet das "Vergessen" beibringt. http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/ (zuletzt aufgerufen am 23. März 2011).
27 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 04. November 2010, S. 8, KOM (2010) 609.

28Schaar, Peter : Privacy by Design. Identity in the Information Society 2010, 267-274.

Zweckbindungsgrundsatzes sein.[29] Sie unterstützen damit den Nutzer technischer Geräte und helfen ihm, sein gesetzlich gewährleistetes Recht auf informationelle Selbstbestimmung auch tatsächlich ausüben zu können. 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 so genannten „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 zentralen Leitlinie 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

Personenbezogene Daten (wie beispielsweise Adress- oder Kontaktdaten oder auch Daten zum Einkaufsverhalten) sind Gegenstand von Transaktionen. Sie werden zwischen Unternehmen verkauft, vermietet oder aber getauscht.

Neben legalem Handel mit Daten kommt es im und über das Internet zu einem illegalen Handel mit personenbezogenen Daten (national wie international). Dieser illegale Handel umfasst sowohl Daten, die unter bestimmten Voraussetzungen gehandelt werden dürften (z. B. Adress- oder Daten zum Einkaufsverhalten), als auch Daten, deren Handel in jedem Fall unzulässig ist (z. B. Passwörter zu E-Mailkonten).

Darüber hinaus wurde in der Vergangenheit aber auch eine „Grauzone“ im Bereich der Datenweitergabe und des Datenhandels fest-

29Unterrichtung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung. Technikfolgenabschätzung (TA) / Zukunftsreport – Ubiquitäres Computing vom 6. Januar 2010, BT-Drs. 17/405, S. 126.

gestellt.[30] Diese Grauzone erstreckte sich insbesondere auf die Bereiche des E-Mail- und Telefon-Marketings, die beide nicht unmittelbar unter das Bundesdatenschutzgesetz fallen, sondern vornehmlich dem Telemediengesetz (vgl. § 6 TMG), dem Telekommunikationsgesetz (vgl. § 95 TKG) und dem Gesetz gegen den unlauteren Wettbewerb (vgl. § 7 Abs. 2 Nr. 2, 3 UWG) unterliegen. Aber auch bei anderen Angeboten, die dem Bundesdatenschutzgesetz unmittelbar unterliegen, fällt eine Abgrenzung zwischen zulässiger Handlung und möglichem Verstoß gegen datenschutzrechtliche Vorschriften nicht immer leicht. Dies gilt insbesondere für die Fälle, in denen das Geschäftsmodell auch darauf abzielt, personenbezogene Daten von möglichst vielen Nutzern zu erheben und ggf. an Dritte weiterzugeben. Aber auch die in der Praxis beliebte Form der Freundschaftswerbung wirft immer wieder schwierige datenschutzrechtliche Fragen auf.

Der Bereich der Datenweitergabe und des Datenhandels im Bundesdatenschutzgesetz wurde im Jahr 2009 umfangreich novelliert. Seitdem schreibt das Bundesdatenschutzgesetz vor, dass personenbezogene Daten wie Adressen grundsätzlich nur dann an andere weitergegeben werden dürfen, wenn der Kunde hierzu vorher eingewilligt hat (so genanntes Opt-in-Verfahren). Eine Ausnahme von diesem Verfahren bildet das so genannte Listenprivileg, das das Bundesdatenschutzgesetz in § 28 Abs. 2 Nr. 1b BDSG bereits vor der letzten Novellierung der Werbewirtschaft beim Versand von (Papier-)Werbung einräumte. Das Listenprivileg erlaubt die Übermittlung oder Nutzung von Daten, sofern es sich um listenmäßig zusammengefasste personenbezogene Daten über Angehörige einer Personengruppe handelt, die sich auf Beruf, Name, Titel, akademischen Grad, Anschrift, Geburtsjahr und Angabe über die Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe (z. B. männliche Studienanfänger unter 25 Jahren in Berlin) beschränken und dabei kein überwiegendes schutzwürdiges Interesse des Betroffenen verletzt wird.

Mit der letzten Novellierung des Bundesdatenschutzgesetzes neu eingeführt wurde die Regelung, dass Betroffene über die Herkunft ihrer Adressdaten auf dem Werbemittel mit Klarnamen und in drucktechnisch deutlicher Gestaltung informiert werden müssen (vgl. § 28 Abs. 3. S. 4 BDSG). Die Verwendung von Listendaten ist demnach erlaubt, wenn dies für die Bewerbung eigener Angebote der verantwortlichen Stelle erforderlich ist.

Mit der letzten Novellierung des Bundesdatenschutzgesetzes sind zudem einige Tatbestände hinzugekommen, die die Werbung für

[30] Vgl. S. 5 des 19. Datenschutz und Informationsfreiheitsberichts der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen für die Jahre 2007 und 2008, 2009. https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/19_DIB/DIB_2009.pdf (zuletzt aufgerufen am 7. April 2011).

eigene Angebote mit zuvor erhobenen personenbezogenen Daten erleichtern. Die datenerhebende Stelle muss hierfür diese Listendaten beim Verbraucher im Rahmen des Vertragsschlusses bzw. im Rahmen einer Anfrage als Interessent erhoben haben. Ergänzend können die Listendaten auch aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben worden sein. Um Profile für eine individualisierte Werbung erstellen zu können, darf die verantwortliche Stelle für die Bewerbung eigener Angebote zu den Listendaten weitere Daten hinzufügen, wenn diese personenbezogenen Daten ebenfalls zuvor rechtmäßig erhoben wurden.

Einzelne Fallgestaltungen sehen wie folgt aus:

1. Sog. Lettershop-Verfahren

Unternehmen nutzen zur Neukundengewinnung Kundendaten, die von anderen Unternehmen für Werbezwecke vermietet werden. In diesem Fall beauftragt die verantwortliche Stelle – das Unternehmen, das Kundendaten etwa im Rahmen einer Geschäftsbeziehung erworben hat – einen Dienstleister mit der Nutzung seiner Kundendaten zur Erstellung eines Werbeschreibens. Das zu versendende Werbematerial wird dann von dem Unternehmen zur Verfügung gestellt, das die Daten zur Neukundengewinnung nutzen möchte.

Das dargestellte Verfahren ist mit den Vorgaben des Bundesdatenschutzgesetzes vereinbar, wenn das Unternehmen (verantwortliche Stelle), welches seine erworbenen Kundendaten für die Bewerbung von Produkten oder Dienstleistungen anderer Unternehmen zur Verfügung gestellt hat, für den Empfänger eindeutig erkennbar ist. Dies ist der Fall, wenn die Nennung des Unternehmens im Klartext erfolgt und der Empfänger so das Unternehmen ohne Zweifel und mit seinen Kenntnissen und Möglichkeiten identifizieren kann.

2. Übermittlung von Kundendaten (Kauf oder Tausch)

Beim Kauf oder Tausch von Kundendaten findet eine Übermittlung der Kundendaten von einem zu einem anderen Unternehmen statt. Das empfangende Unternehmen erhält die Kundendaten zur eigenen Verwendung und kann diese fortan für eigene werbliche Zwecke nutzen. Erfolgte die Übermittlung der Kundendaten ohne vorherige Einwilligung der Kunden ist der Vorgang nur dann rechtlich zulässig, wenn die gesetzlichen Informations-, Dokumentations- und Transparenzpflichten eingehalten werden.

Die gesetzliche Informationspflicht ist eingehalten, wenn der Kunde bei der Datenerhebung auf den Verwendungszweck eines Kaufs

oder Tausches der erhobenen Kundendaten hingewiesen wurde. Zu beachten ist zudem, dass ein Kauf oder Tausch nur innerhalb der Gruppe möglich ist, die dem Kunden bei der Datenerhebung genannt wurde. Der gesetzlichen Dokumentationspflicht wird entsprochen, wenn die übermittelnde Stelle für den Zeitraum von zwei Jahren den Empfänger der Kundendaten speichert. Gleichzeitig muss der Empfänger der Kundendaten den Übermittler und den zulässigen Verwendungszweck für ebenfalls mindestens zwei Jahre speichern.

Ebenso wie im o. g. Lettershop-Verfahren muss gegenüber dem Empfänger der Werbung die Quelle der Adresswerbung genannt werden. Ausfluss der gesetzlichen Transparenzpflicht ist zudem, dass gegenüber dem Empfänger der Werbung das Unternehmen zu benennen ist, welches erstmals die Kundendaten erhoben hat.

Die Übermittlung von Kundendaten zum Zwecke der Werbung ist somit letztlich, wie oben bereits dargestellt, auf die so genannten Listendaten begrenzt. Will ein Unternehmen darüber hinausgehende Daten übermitteln, muss eine Einwilligung des Betroffenen vorliegen.

3. Weitere Sonderfälle

Mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 wurden zwei weitere Sonderfälle gesetzlich für zulässig erklärt. Hierzu gehört die Nutzung und Übermittlung von Listendaten zur Bewerbung von Produkten und Dienstleistungen im gewerblichen Bereich. Allerdings erstreckt sich die gesetzliche Privilegierung auch auf Funktionsträger in Unternehmen (z. B. Abteilungsleiter Einkauf). Abgrenzungsmerkmal ist demnach, dass die Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen erfolgen muss. Zudem darf nicht die Privatadresse, sondern es muss die berufliche Anschrift des Betroffenen verwendet werden. Fallen beide Adressen zusammen, kann trotzdem von der gesetzlichen Privilegierung Gebrauch gemacht werden.

Die Ausnahmeregelung für den gewerblichen Bereich erfasst sowohl die Vermietung von Listendaten als auch den Kauf oder Tausch der Daten. Gegenüber den o. g. Regelungen besteht beim Vorliegen einer gewerblichen Ansprache keine Pflicht, die ursprüngliche Quelle der Daten zu eröffnen. Auch die dargestellten Dokumentationspflichten müssen nicht eingehalten werden. Zudem ist für das werbende Unternehmen auch ein Rückgriff auf allgemein zugängliche Quellen zulässig. Die Adressdaten können somit beispielsweise auch über das Internet unmittelbar erhoben werden.

Eine weitere Ausnahme bei der Verwendung von Listendaten gilt, wenn steuerbegünstigte Organisationen für Spenden werben wollen. Auch bei diesem Fall bedarf es keiner Pflicht zur Angabe der Quelle, bei der erstmals die Daten erhoben wurden.

2.3.7 Spannungsfeld Datenschutz und Wettbewerbsbedingungen am Beispiel sozialer Netzwerke

Eine große datenschutzrechtliche Herausforderung im Internet sind inzwischen die sozialen Netzwerke, die in jüngerer Zeit die Nutzung der Möglichkeiten des Internet zunehmend prägen. Betreiber sozialer Netzwerke haben ihren Sitz derzeit sowohl außerhalb des europäischen Wirtschaftsraums (EWR) als auch innerhalb. Es stellen sich daher zunächst die grundsätzlichen Fragen der Anwendbarkeit und Durchsetzbarkeit nationalen oder aber europäischen Datenschutzrechts.[31]

Bei sozialen Netzwerken konnte festgestellt werden, dass besonders bei Änderungen des angebotenen Dienstes unterschiedliche datenschutzrechtliche Regelungen zur Anwendung kommen. Nach europäischem Datenschutzrecht muss beispielsweise jede Änderung eines Diensteangebots, bei der personenbezogene Daten betroffen sind, vom Nutzer bestätigt werden. Das umgekehrte Verfahren (sog. Opt-out) wird in den USA angewendet. Dieses führt zu weniger Rückläufern und ermöglicht damit eine stärkere Durchsetzung des eigenen Angebotes auf dem Markt.[32]

Hinzu kommt, dass derzeit Nutzer vor der Eröffnung eines Kontos bei sozialen Netzwerken nicht in vergleichbar gut verständlicher Form über die Möglichkeiten der Datenverwendung für den Betreiber informiert werden. Zwar gibt es beispielsweise bei Facebook zahlreiche differenzierte Möglichkeiten, unter den Kontoeinstellungen oder Privatsphäre-Einstellungen den Zugriff auf Daten durch Dritte einzuschränken. Aber auf diese Möglichkeiten wird der Nutzer bei Einrichtung des Kontos nicht hingewiesen. Hier ist die datenschutzrechtliche Gefährdung höher als bei einer „Opt-out“-Lösung, bei der der Nutzer bei Kontoeröffnung über die die Möglichkeit der Einstellungen informiert wird. Eine zusätzliche und besonders brisante Dimension kommt dann noch hinzu, wenn die Datenbestände sozialer Netzwerke mit anderen Kommunikationsformen datenmäßig miteinander kombiniert werden (etwa zwi-

[31] Vgl. Darstellung in 2.1.9.

32 Vgl. Schriftliche Stellungnahme von Lars Hinrichs im Rahmen der Öffentlichen Anhörung „Auswirkungen der Digitalisierung auf unsere Gesellschaft – Bestandsaufnahme, Zukunftsaussichten“ der Enquete-Kommission „Internet und Digitale Gesellschaft“ des Deutschen Bundestages am 05.Juli 2010. A.-Drs. 17(24)004-D, online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/2010/Sitzungen/20100705/A-Drs__17_24_004-D_-_Stellungnahme_Hinrichs.pdf (zuletzt aufgerufen am 7. April 2011).

schen Facebook und Skype), ohne dass sich die Nutzer dessen auch nur bewusst wären.

2.3.8 Datenschutz als Standortfaktor

Datenschutz ist angesichts der internationalen Reichweite für viele Dienste ein wesentliches Wettbewerbselement und damit auch ein Standortfaktor einer innovativen und dynamischen Internetwirtschaft in Deutschland.

Dabei bestehen hier durchaus zwei gegensätzliche Argumentationen:

Vertreten wird die Auffassung, striktere Datenschutzregeln seien hinderlich oder jedenfalls kostentreibend, wenn es darum gehe, mit neuen Diensten Marktanteile zu gewinnen. Für Unternehmen, die im internationalen Wettbewerb stehen, könne ein niedrigeres Datenschutzniveau sowohl zu einer Vereinfachung der Produktgestaltung als auch zu einer Erleichterung bei den Kosten führen.

Auf der anderen Seite wird vertreten, ein hohes Sicherheits- und Datenschutzniveau könne durch zusätzliches Kundenvertrauen zu einem positiven Unterscheidungsmerkmal im Wettbewerb werden. Wie bereits festgestellt, besteht durchaus ein Bewusstsein für die Relevanz hoher Sicherheits- und Datenschutzstandards und damit eine Nachfrage nach entsprechend ausgestalteten Produkten. Gelingt es also, ohne relevante Einbußen der sonstigen Wettbewerbsfähigkeit, hier ein Mehr gegenüber internationalen Diensten anzubieten, kann das hohe deutsche Schutzniveau auch als Standortvorteil verstanden und positioniert werden.

Von in Deutschland tätigen Unternehmen wird der Datenschutz aber auch deswegen zunehmend als negativer Standortfaktor wahrgenommen, weil sowohl die föderale Struktur der Datenschutzaufsicht als auch die Vielzahl bereichsspezifischer Regelungen eine einheitliche Anwendung und Auslegung innerhalb Deutschlands erschweren.

So hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder festgestellt: „Eine Vielzahl von Spezialregelungen, die das Bundesdatenschutzgesetz (BDSG) ganz oder teilweise überlagern und verdrängen, haben das Recht für Anwenderinnen und Anwender wie Betroffene unübersichtlich und unverständlich gemacht.“[33]

[33]Vgl. Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 5.

2.3.9 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.

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.

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[34] 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

http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile (zuletzt aufgerufen am: 22. März 2011).

[34] BITKOM. Datenschutzkodex für Geodatendienste - Entwurf. Dezember 2010. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/rote_linie_kodex.pdf?__blob=publicationFile (zuletzt aufgerufen am 7. April 2011).

Initiativen zur Selbstregulierung zu prüfen, darunter die aktive Förderung von Verhaltenskodizes.“[35]

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.

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 so genannten „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, sodass 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 ausgestattet sind. Es erscheint daher fraglich, ob es im Datenschutz einen dem Jugendmedienschutz vergleichbaren Spielraum für die sachliche Ausfüllung von Tatbestandselementen gibt, die das Modell

[35] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 04. November 2010. KOM (2010) 609, Kapitel 2.2.5 (S.14).

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 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 DSRL) 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.[36] 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 DSRL) besteht 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.[37] 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 zu 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 Datenum-

[36] Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 7, 8.
[37] Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 8 Rn. 9.

gangs annehmen.[38] 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.[39] Darüber hinaus können sich Schadensersatzansprüche gemäß § 280 BGB wegen schuldhaft rechtswidriger bzw. missbräuchlicher Datenverarbeitung aus vorvertraglicher bzw. vertraglicher Haftung ergeben.[40]

Der Nutzen von Schadensersatzansprüchen im Datenschutzrecht ist in der Praxis dadurch beschränkt, dass es oftmals schwierig ist, einen konkreten ersatzfähigen Schaden aufzuzeigen. In vielen Fällen kann ein Schaden gar nicht beziffert werden, weil keine konkrete materielle Einbuße vorliegt. Immaterielle Schäden sind wiederum im deutschen Recht generell nur unter sehr engen Einschränkungen ersatzfähig. Schließlich kann aufgrund der technischen Zusammenhänge auch der Nachweis der Kausalität für den Schadenseintritt Schwierigkeiten bereiten.

2.3.12 Beschäftigtendatenschutz

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 Bundesdatenschutzgesetzes 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[41] soll die Rechtssicherheit für Arbeitgeber und Beschäftigte erhöht werden.

[38] Vgl. Kühling, Jürgen/Bohnen, Simon: Zur Zukunft des Datenschutzrechts. JZ 2010, 600 (609).
[39] Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 17.
[40] Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 18.
[41] Gesetzesentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes. BT-Drs. 17/4230 vom 15. Dezember 2010.

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.[42]

2.3.13 Probleme der föderalen Aufsichtsstruktur

In ähnlicher Weise wie im internationalen Bereich gibt es auch im Inland vielfältig Situationen, in denen bestehende Rechtsvorschriften unterschiedlich angewendet und ausgelegt werden. Von Vorteil ist zwar, dass der Datenschutz im nicht-öffentlichen Bereich maßgeblich durch das Bundesdatenschutzgesetz geprägt wird und damit bundeseinheitliche Vorgaben bestehen.

Durch die weitgehende Zuständigkeit der Bundesländer für die Datenschutzaufsicht kommt es allerdings häufig zu einer unterschiedlich strikten Anwendung und teils weiteren, teils engeren Auslegung vor allem von eher unbestimmten Regelungen. Manche verantwortliche Stellen sind zudem gleich mehreren Aufsichtsbehörden unterworfen, insbesondere wenn die Aufsicht teils dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, teils der Landesdatenschutzaufsicht obliegt.

Andererseits wird vorgetragen, dass der Erfolg der deutschen Datenschutzaufsicht wesentlich auf den „föderalen Wettbewerb“ und die Herausbildung von „best practices“ zurückzuführen ist. Zudem kann darauf verwiesen werden, dass erst die dezentrale Struktur eine flächendeckende Aufsicht "vor Ort" zu gewährleisten im Stande ist.

Eine Abstimmung der Aufsichtsbehörden erfolgt weitgehend informell, insbesondere in Form von Konferenzen („Konferenz der Datenschutzbeauftragten des Bundes und der Länder“ vor allem für den öffentlichen Bereich, „Düsseldorfer Kreis“ für den nicht-öffentlichen Bereich). Die Konferenzen und die daraus resultieren-

[42] Gesetzesentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes.BT-Drs. 17/4230 vom 15. Dezember 2010, S. 12

den Veröffentlichungen geben Orientierung, können aber formal keine unmittelbaren normativen Wirkungen entfalten und die bestehenden Rechtsunsicherheiten nicht gänzlich auflösen.