Enquete-Kommission Internet und digitale Gesellschaft

Deutscher Bundestag

Projektgruppe Datenschutz, Persönlichkeitsrechte

Bestandsaufnahme bestehender Datenschutzregelungen (Stand: 15. März 2011)

15. März 2011

1. Bestandsaufnahme bestehender Datenschutzregelungen (Stand: 7. März 2011)

1.1 Völkerrechtliche Rechtsquellen

1.1.1 Allgemeine völkerrechtliche Abkommen zum Schutze 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 „Konvention zum Schutze der Menschenrechte und Grundfreiheiten“ (Europäische Menschenrechtskonvention - EMRK) vom 4. November 1950 [Fußnote: BGBl. II 1952, S. 686.] „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. [Fußnote: Meyer-Ladewig, EMRK, Handkommentar, 2. Auflage 2006, Art. 8 EMRK, Rn. 11.] Als Korrespondenz gelten auch die Individualkommunikation mittels E-Mail, Telefon und Internet-Telefonie. [Fußnote: Kühling, Seidel, Sivridis, Datenschutzrecht, 2008, S. 37.] 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. [Fußnote: Meyer-Ladewig, EMRK, Handkommentar, 2. Auflage 2006, Art. 8 EMRK, Rn. 2.] 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 Pakts über bürgerliche und politische Rechte“ (Bürgerrechts-Paktgesetz – IPBürgRG) vom 19. Dezember 1966 [Fußnote: BGBl. II 1973, S. 1533.], 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 Menschrechtsabkommen 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. [Fußnote: Hofmann/Boldt, IPBürgRG, Kommentar, Erl. zu Art. 17 IPBürgRG.] Art. 16 des „Übereinkommens der Vereinten Nationen über die Rechte des Kindes“ vom 20. November 1989 [Fußnote: BGBl. II 1992, S. 122.] („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.

Allerdings enthält gerade die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) zu Art. 8 EMRK zahlreiche Hinweise auf Schutzbereich des Datenschutzes und

Eingriffsvoraussetzungen. In dem jüngeren „Übereinkommen über die Rechte von Menschen mit Behinderungen“ der Vereinten Nationen vom 13. Dezember 2006 (Behindertenrechtskonvention – BRK) [Fußnote: BGBl. II 2008, S. 1419.] 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“ (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) vom 23. September 1980 [Fußnote: Vgl. Bundesanzeiger Nr. 251 vom 14. November 1981.], 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. [Fußnote: Kühling/Seidel/Sivridis, Datenschutzrecht, 2008, S. 36.] In den Leitlinien wird zwischen „sensitiven“ und „trivialen“ Angaben [Fußnote: Simitis, Kommentar zum BDSG, 6. Auflage 2006, Einleitung, Rn. 186.] , 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. [Fußnote: Simitis, Kommentar zum BDSG, 6. Auflage 2006, Einleitung, Rn. 198.] Die Leitlinien gelten als „Indiz für die internationale Verbreitung bestimmter Datenschutzgrundsätze“ [Fußnote: Ennulat, Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und –einrichtungen, 2008, S. 72.], die jedoch weder völkerrechtliche Verbindlichkeit noch einen hohen Schutzstandard aufweisen. Dessen ungeachtet sollen sie jedoch auch dazu beigetragen haben, „den Datenschutz als Gegen-stand internationaler Regulierung zu etablieren.“ [Fußnote: Kühling/Seidel/Sivridis, Datenschutzrecht, 2008, S. 36.]

Das „Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten“ des Europarates vom 28. Januar 1981 [Fußnote: BGBl. II 1985, S. 538.] („Europäische Datenschutzkonvention“) begründet hingegen rechtliche Verpflichtungen der Unterzeichnerstaaten, einen bestimmten Katalog von Datenschutzgrundsätzen einzuhalten und in nationales Recht umzusetzen. [Fußnote: Nach Nr. 39 der Denkschrift 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.] 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 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 [Fußnote: BGBl. II 2002, S. 1882.] 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 „Übereinkommen über Computerkriminalität“ (Cybercrime Convention) des Europarates vom 23. November 2001 [Fußnote: BGBl. II 2008, S. 1242, für Deutschland in Kraft mit Wirkung vom 1. Juli 2009.] 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. [Fußnote: Denkschrift (I. Allgemeines), BT-Drs. 16/7218, S. 40.]

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. [Fußnote: Guidelines on the Use of Computerized Personal Data Flow, Resolution der Generalversammlung vom 14. Dezember 1990.] 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 das Primärrecht 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. [Fußnote: Zerdick, in: Lenz/Borchardt (Hrsg.), EU-Verträge, 5. Auflage 2010, Art. 16 AEUV, Rn. 7.] Art. 16 AEUV [Datenschutz] lautet:

„(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 perso-

> nenbezogener 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 [Fußnote: Kotzur, in: Geiger/Khan/Kotzur, EUV/AEUV, 5. Auflage 2010, Art. 16 AEUV, Rn. 2; Kingreen, in: Calliess/Ruffert (Hrsg.), Das Verfassungsrecht der EU, 3. Auflage 2007, Art. 286 EGV, Rn. 29; Hatje, in: Schwarze (Hrsg.), EU-Kommentar, 2. Auflage 2009, Art. 286 EGV, Rn. 6.], 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. [Fußnote: 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.]

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. [Fußnote: Geiger, in: Geiger/Khan/Kotzur, EUV/AEUV, 5. Auflage 2010, Art. 39 EUV, Rn. 3.]

Mit dem Vertrag von Lissabon wurde schließlich die „Charta der Grundrechte der Europäischen Union“ [Fußnote: ABl. C 83 vom 30. März 2010, S. 393, in Kraft getreten am 1. Dezember 2009.] im Dezember 2009 rechtsverbindlich. Sie steht nun auf gleicher Hierarchiestufe wie das Primärrecht. [Fußnote: S. Art. 6 Abs. 1 EUV.] 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 2 formt das unionale Grundrecht näher aus. [Fußnote: Kotzur, in: Geiger/Khan/Kotzur, EUV/AEUV, 5. Auflage 2010, Art. 16 AEUV, Rn. 2; Hatje, in: Schwarze (Hrsg.), EU-Kommentar, 2. Auflage 2009, Art. 286 EGV, Rn. 6.] Artikel 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 Grundrechtecharta verpflichtet gem. Art. 51 Abs. 1 S. 1 Grundrechtecharta zunächst die Organe und Einrichtungen der EU bei sämtlichen ihrer Aktivitäten; es gibt keinen grundrechtsfreien Raum in der EU. [Fußnote: Jarass, Charta der Grundrechte der Europäischen Union, 2010, Art. 51, Rn. 4.] 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 Grundrechtecharta verpflichtet. [Fußnote: Vgl. hierzu Rohleder, Grundrechtsschutz im europäischen Mehrebenen-System, 2009, S. 396 ff.] 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. [Fußnote: Kingreen, in: Calliess/Ruffert (Hrsg.), Das Verfassungsrecht der EU, 2007, Art. 51 GRCh, Rn. 8; Rohleder, Grundrechtsschutz im europäischen Mehrebenen-System, 2009, S. 390.] 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. [Fußnote: EuGH, Rs. C-260/89, Slg. 1991, S. I-2925, Rn. 42 ff. = EuGRZ 1991, S. 274 – ERT (Leiturteil). Hierzu Scheuing, Zur Grundrechtsbindung der EU-Mitgliedstaaten, Europarecht (EuR) 2005, S. 162 (164); Kokott/Sobotta, Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon, Europäische Grundrechtezeitschrift (EuGRZ) 2010, S. 265 (268).] Überwiegend wird in der Rechtswissenschaft davon ausgegangen, dass diese weite Auslegung des EuGH durch das Verbindlichwerden der Grundrechtecharta nicht tangiert wird. [Fußnote: Vgl. Rohleder, Grundrechtsschutz im europäischen Mehrebenen-System, 2009, S. 398; Kokott/Sobotta, Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon, EuGRZ 2010, S. 265 (268).] 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. [Fußnote: Jarass, Charta der Grundrechte der Europäischen Union, 2010, Art. 51, Rn. 10.]

1.2.2 Europäisches Sekundärrecht

Das zentrale Datenschutzinstrument auf europäischer Ebene ist die Datenschutzrichtlinie 95/46/EG [Fußnote: 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. L 281 vom 23.11.1995, S. 31).] aus dem Jahr 1995. 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 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 Datenschutzrichtlinie 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. [Fußnote: Zerdick in: Lenz/Borchardt (Hrsg.), EU-Verträge, 5. Auflage 2010, Art. 16 AEUV, Rn. 37.]

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“ [Fußnote: Art. 25 der Richtlinie.] 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 EU-Datenschutzrechts gegeben sei. [Fußnote: 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, ABl. 215 vom 25. August 2000, S. 10.] Um ein angemessenes Datenschutzniveau zu gewährleisten, haben die EU und das US-Handelsministerium im Juli 2006 eine Vereinbarung zu den Grundsätzen des sogenannten „sicheren Hafens“ (Safe Harbor) geschlossen. [Fußnote: Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000, ABl. 215 vom 25. August 2000, S. 7.] 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 sogenannten „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. [Fußnote: 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 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.]

Als bereichsspezifische Ergänzung zur Datenschutzrichtlinie regelt die E-Privacy-Richtlinie 2002/58/EG [Fußnote: 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. L 201 vom 31. Juli 2002, S. 37.] datenschutzrechtliche Aspekte im Bereich der elektronischen Kommunikation, die durch die Datenschutzrichtlinie 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 mitgliedsstaatlichen 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 [Fußnote: Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. L 337 vom 18. Dezember 2009, S. 11.] 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. [Fußnote: Jedenfalls teilweise soll dies im Rahmen der geplanten TKG-Novelle erfolgen, vgl. § 109a des Gesetzentwurfs der Bundesregierung vom 2. März 2011, http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/referentenentwurf-tkg-2011,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (abgerufen am 9.3.2011)]

In der im Jahr 2000 verabschiedeten E-Commerce Richtlinie 2000/31/EG [Fußnote: 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. L 178 vom 17. Juli 2000, S. 1.], mit der ein europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr geschaffen wurde, werden Fragen des Datenschutzes ausgeklammert [Fußnote: (14) der Erwägungsgründe, a.a.O. S. 3, sowie Artikel 1 Abs. 5 b) der Richtlinie.] und insoweit auf anderweitige Rechtsakte der Union verwiesen. In den Erwägungen der Richtlinie (Nr. 14) wird allerdings betont, dass die Grundsätze des 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 [Fußnote: 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. L 8 vom 12. Januar 2001, S. 1.] 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 [Fußnote: 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. L 105 vom 13. April 2006, S. 54.] 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. [Fußnote: Art. 1 der Richtlinie.] 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. [Fußnote: Die Europäische Kommission führt derzeit eine Evaluation der Vorratsdatenspeicherungsrichtlinie durch.]

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. [Fußnote: 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, online abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:DE:PDF (Stand: 21.9.2010).] Der eng gefasste Anwendungsbereich des Rahmenbeschlusses erstreckt sich auf solche personenbezogenen Daten, die von mit-gliedstaatlichen 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. [Fußnote: Zerdick in: Lenz/Borchardt, EU-Verträge, 5. Aufl. 2010, Art. 16, Rn. 48.] Im Gegensatz zur Datenschutzrichtlinie 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. [Fußnote: Zerdick in: Lenz/Borchardt, EU-Verträge, 5. Aufl. 2010, Art. 16, Rn. 50.]

Die Europäische Kommission hat im November 2010 ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ [Fußnote: KOM(2010) 609 endg.] vorgelegt und für 2011 einen Vorschlag für die Änderung der Datenschutzrichtlinie angekündigt.

1.3 Nationales Recht

1.3.1 Grundrechte

Das Grundgesetz kennt kein ausdrückliches Datenschutz-Grundrecht. Allerdings hat das Bundesverfassungsgericht bereits 1983 in seinem sogenannten „Volkszählungsurteil“ 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. [Fußnote: 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).] Nach der Rechtsprechung des Bundesverfassungsgerichts beinhaltet das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. [Fußnote: BVerfGE 65, 1, 43.] 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.“ [Fußnote: BVerfGE 65, 1, 43.] „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“. [Fußnote: BVerfGE 65, 1, 43.] In den Schutzbereich dieses Grundrechts fallen alle Formen der Erhebung personenbezogener Daten. Angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie geht das Bundesverfassungsgericht davon aus, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr“ gebe. [Fußnote: BVerfGE 65, 1, 45, zum Grundrecht auf informationelle Selbstbestimmung vgl. im Übrigen unter 2.1.5.]

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 [Fußnote: Di Fabio in Maunz/Dürig, Grundgesetz, 57. Auflage 2010, Art. 2 GG, Rn. 193.], sowie das 2008 durch das Bundesverfassungsgericht formulierte „Grundrecht auf Gewährleistung

der Vertraulichkeit und Integrität informationstechnischer Systeme“. [Fußnote: BVerfG, Urteil vom 27. Februar 2008, NJW 2008, 822 („Online-Durchsuchung“).] 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. [Fußnote: Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vgl. im Übrigen unter 2.1.3.]

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. [Fußnote: BVerfG, NJW 2004, 999 (1001).] 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. [Fußnote: BVerfGE 120, 274, 307.] Der Schutz erstreckt sich nicht nur auf die Inhalte der Kommunikation, sondern auch auf die Kommunikationsumstände [Fußnote: BVerfGE 113, 348, 364.], 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. [Fußnote: BVerfGE 113, 348, 365.] 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 Bundesverfassungsgerichts 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) [Fußnote: 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).] 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 Bundesverfassungsgerichts entsprechend - eine gesetzliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten zu schaffen und so den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechtes zu 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 Er-

laubnisvorbehalt“ 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. [Fußnote: Anderes gilt nach § 1 Abs. 5 S. 4 BDSG im Fall des „Transits“.]

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. [Fußnote: Gola/Schomerus, BDSG, Kommentar, 10. Auflage 2010, § 1, Rn. 14.] Beispiele für Spezialregelungen sind das Bundespolizeigesetz, das Bundeskriminalamtsgesetz, das Bundeszentralregistergesetz, die Grundbuchordnung, das Personenstandgesetz, §§ 8 ff. Handelsgesetzbuch und die Grundbuchordnung. [Fußnote: Däubler/Klebe/Wedde/Weichert, BDSG, Kommentar, 3. Auflage 2010, Einleitung, Rn. 73.] In gesonderten Vorschriften außerhalb des BDSG ist auch der Datenschutz der öffentlich-rechtlichen Religionsgemeinschaften geregelt. Im SGB X (Zweites Kapitel „Schutz der Sozialdaten, §§ 67 ff.) [Fußnote: 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).] finden sich die datenschutzrechtlichen Bestimmungen für den Sozialleistungsbereich. Sozialdaten sollen nach der Vorstellung des Gesetzgebers einem erhöhten, dem Steuergeheimnis vergleichbaren Schutz unterliegen. [Fußnote: BT-Drs. 8/4022, S. 96.] Ergänzende Bestimmungen für verschiedene Zweige der Sozialversicherung enthalten die jeweils einschlägigen Bücher des SGB.

Für das Internet von besonderer Bedeutung ist das Telemediengesetz (TMG). [Fußnote: Vom 26. Februar 2007, BGBl. I S. 179, zuletzt geändert durch Gesetz vom 14. August 2009, BGBl. I S. 2814.] Telemedien sind Waren- und Dienstleistungsangebote im Netz unter Einbeziehung redaktionell gestalteter Online-Angebote, ausgenommen jedoch der Rundfunk. [Fußnote: Hoeren, NJW 2007, 801.] 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. [Fußnote: BT-Drs. 16/3078, S. 13.] Der Datenschutz für die Teilnehmer ist im Telekommunikationsgesetz (TKG) [Fußnote: Vom 25. Juni 1996, BGBl. I S. 1120, geändert durch Gesetz vom 22. Juni 2004, BGBl. I S. 1190.], 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." [Fußnote: Robert, Beck'scher TKG-Kommentar, 3. Auflage 2006, § 91, Rn. 12.] 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. [Fußnote: Gola/Schomerus, BDSG, Kommentar, 10. Auflage 2010, § 1, Rn. 33.] Da der Datenschutz in nahezu allen Bereichen der Landesverwaltung von Bedeutung ist, weist eine Unzahl landesrechtlicher Gesetze Spezialregelungen zum Datenschutz auf, u. a. in den Landesgesetzen zum (Jugend-)Strafvollzug und zur Untersuchungshaft, in Rettungsdienstgesetzen, Brand- und Katastrophenschutzgesetzen, Schulgesetzen, usw.

Anders als im Bundesrecht finden sich auf Landesebene auch Formen untergesetzlicher Regelungen zum allgemeinen Datenschutzrecht, d. h. Rechtsverordnungen und Verwaltungsvorschriften. [Fußnote: Däubler/Klebe/Wedde/Weichert, BDSG, Kommentar, 3. Auflage 2010, Einleitung, Rn. 70.]

1.4 Rechtsprechung des Europäischen Gerichtshofs (EuGH)

Erste Entscheidungen des EuGH zur Datenschutzrichtlinie datieren aus dem Jahr 2003. [Fußnote: Roßnagel, MMR 2004, 95, 100.]

In einem am 20. Mai 2003 entschiedenen Verfahren (C-465/00) 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 Datenschutzrichtlinie, 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. [Fußnote: Dieses weite Verständnis des Anwendungsbereichs der Richtlinie trägt nach Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sehr zur „Europäisierung des Datenschutzes“ bei:
http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/Arbeit/Artikel/20050 3_OesterreichischerRundfunk.html?nn=408918]

Die Darstellung anderer Personen auf einer privaten schwedischen Website ohne deren Zustimmung war Gegenstand im Fall „Lindqvist“ vom 6. November 2003 (C-101/01). 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 Datenschutzrichtlinie 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 am 30. Mai 2006 (C-317/04) Stellung. Es erklärte die zu Grunde liegende Genehmigung des Abkommens zwischen der EU und den USA durch den Rat für nichtig. Dasselbe galt für die zum selben Sachverhalt ergangene Entscheidung der Kommission, mit der das US-amerikanische Datenschutzniveau für angemessen im Sinne des Art. 25 der Datenschutzrichtlinie 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 Datenschutzrichtlinie [Fußnote: S. a. Art. 3 Abs. 2 zweiter Spiegelstrich der Datenschutzrichtlinie.] keine geeignete Rechtsgrundlage. Mangels Rechtsgrundlage waren der Ratsbeschluss und die Kommissionsentscheidung für nichtig zu erklären. In dem Urteil des EuGH vom 10. Februar 2009 (C-301/06) über die Vorratsdatenspeicherungs-Richtlinie konzentriert sich das Gericht ebenfalls auf Fragen der Rechtsetzungskompetenz. Grundrechtliche Fragen waren nicht Gegenstand des Verfahrens. Die Vorratsdatenspeicherungs-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 („Huber", C-524/06), dass die Speicherung und Verarbeitung personenbezogener Daten namentlich genannter Personen zu statistischen Zwecken nicht dem Erforderlichkeitsgebot [Fußnote: Art. 7 Buchst. e Datenschutzrichtlinie.] 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 („Markkinapörrsi", C-73/07). 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 Datenschutzrichtlinie 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 (C-518/07) entschied der EuGH in einem Vertragsverletzungsverfahren, das die EU-Kommission gegen Deutschland angestrengt hatte. 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 Datenschutzrichtlinie. 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 vom 29. Juni 2010 im „Bavarian Lager"-Fall (C-28/08). 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 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 [Fußnote: Verordnung des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den öffentlichen Zugang zu Dokumenten des Parlaments, des Rates und der Kommission (ABl. 2001 L 8, S. 43).] 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 (Urteil vom 9. November 2010, C-92/09, C-93/09).

1.5 Rechtsprechung des Bundesverfassungsgerichts

Neben den unter 3.1 erwähnten grundlegenden Entscheidungen, dem „Volkszählungsurteil“ sowie dem Urteil zur „Online-Durchsuchung“, hat sich das Bundesverfassungsgericht in einer Reihe weiterer Entscheidungen mit Fragen der informationellen Selbstbestimmung und verwandter Grundrechte befasst. Die Rechtsprechung des Bundesverfassungsgericht enthält im Bereich des Datenschutzes vielfach sehr konkrete und detaillierte Vorgaben für das gesetzgeberische Handeln. [Fußnote: Gurlit, NJW 2010, 1035; Wolff NVwZ 2010, 751.] Aus der umfangreichen Rechtsprechung des Gerichts zum Datenschutz sei beispielhaft auf folgende Entscheidungen hingewiesen:

Gegenstand des Urteils vom 14. Juli 1999 [Fußnote: „Telekommunikationsüberwachung“, BVerfGE 100, 313 ff.] 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 [Fußnote: Verbrechensbekämpfungsgesetz vom 28. Oktober 1994, BGBl. I S. 3186.]. Mit Beschluss vom 5. Juli 1995 [Fußnote: BVerfGE 93, 181.] bestimmte das Bundesverfassungsgericht 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 [Fußnote: „Genetischer Fingerabdruck“, BVerfGE 103, 21.] 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 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 [Fußnote: „GPS-Überwachung“, BVerfGE 112, 304.] äußerte sich das Bundesverfassungsgericht zu einer weiteren Vorschrift der Strafprozessordnung. Gesetzliche Grundlage für Beweiserhebungen unter Einsatz eines satellitengestützten Ortungssystem (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 [Fußnote: „Beschlagnahme von Datenträgern“, BVerfGE 113, 29.]) im Rahmen eines gegen einen der Berufsträger gerichteten Ermittlungsverfahrens qualifizierte das Bundesverfassungsgericht als erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung, dem durch strikte Beachtung des Verhältnismäßigkeitsgrundsatzes und bestimmter Verfahrensregelungen Rechnung getragen werden müsse. 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 Bundesverfassungsgericht 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 [Fußnote: „Rasterfahndung“, BVerfGE 93, 181.]. 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 [Fußnote: „Kontenabfrage“, BVerfGE 118, 68.] 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 Kreditinsti-

tuten 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.

Auch eine Geschwindigkeitsmessung auf der Grundlage einer Verwaltungsvorschrift stellt nach der Rechtsprechung des Bundesverfassungsgerichts (Beschluss vom 11. August 2009 [Fußnote: „Verkehrsüberwachung“, NJW 2009, 3293.]) 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“ [Fußnote: Vom 21. Dezember 2007, BGBl. I S. 3198.] zur Umsetzung der Richtlinie 2006/24 /EG in deutsches Recht ist Gegenstand mehrerer Entscheidungen des Bundesverfassungsgerichts. 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 [Fußnote: BVerfGE 122, 120.] im Wege der einstweiligen Anordnung Teile der Vorratsdatenspeicherung außer Kraft gesetzt hatte, entschied es mit Urteil vom 2. März 2010 [Fußnote: “Vorratsdatenspeicherung”, NJW 2010, 833.] in der Hauptsache, dass die Regelung des TKG und der StPO über die Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG nicht 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 setzte dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürften sie 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.

1.6 Rechtsprechung nationaler Verwaltungs- und Zivilgerichte

Zulässigkeit und Grenzen personenbezogener Bewertungsportale im Internet sind Gegenstand der Entscheidung des Bundesgerichtshofs vom 23. Juni 2009 [Fußnote: „Spickmich.de“, BGHZ 181, 328.]. 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. [Fußnote: Die gegen das Urteil eingelegte Verfassungsbeschwerde hat das Bundesverfassungsgericht mit Beschluss vom 16. August 2010 nicht zur Entscheidung angenommen (Az. 1 BvR 1750/09).]

Mit Urteil vom 9. Dezember 2003 [Fußnote: „Luftbildaufnahmen“, NJW 2004, 766.]hat der Bundesgerichtshof 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). [Fußnote: „Überwachungskamera“, NJW 2010, 1533.]

In der Rechtsprechung des Bundesarbeitsgerichts 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 des Bundesarbeitsgerichts vom 26. August 2008). [Fußnote: „Videoüberwachung im Betrieb“, BAGE 127, 276; 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.“] Bei Abschluss von Betriebsvereinbarungen sei gemäß § 75 Abs. 2 Satz 1 Betriebsverfassungsgesetz (BetrVG) die freie Entfaltung der Persönlichkeit der beschäftigten Arbeit-

nehmer zu schützen und hierbei auch der Grundsatz der Verhältnismäßigkeit zu wahren. Mit Beschluss vom 12. August 2008 [Fußnote: Az. 7 ABR 15/08.] 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 hat mit Urteil vom 8. März 2002 [Fußnote: „Herausgabe von Stasi-Unterlagen“, BVerwGE 116, 104.] 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. [Fußnote: 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.“.]

Werden personenbezogene Informationen durch eine sachlich unzuständige Behörde weitergegeben, stellt dies einen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung dar. Das Bundesverwaltungsgericht hat hierzu mit Urteil vom 9. März 2005 entschieden, ein Eingriff in das informationelle Selbstbestimmungsrecht sei grundsätzlich auch dann nicht gerechtfertigt, wenn die Daten zwar von einer anderen Behörde rechtmäßig hätten weitergegeben werden dürfen, im konkreten Fall aber eine sachlich unzuständige Behörde gehandelt habe. [Fußnote: „Scientology“, NJW 2005, 2330.]

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 Bundesverwaltungsgericht hat mit Urteil vom 24. März 2010 [Fußnote: „Auskunftsanspruch BND“, Az. 6 A 2/09.]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).

1.7 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 [Fußnote: So wurden 2008 von Datenschutzbehörden aus zwölf Bundesländern Bußgelder gegen 35 Vertriebsgesellschaften des Lebensmitteldiscounters Lidl verhängt (http://www.welt.de/wirtschaft/article2428529/Spitzelaffaere-kostet-Lidl-1-5-Millionen-Euro.html).].

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. [Fußnote: 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] 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.